VINNY TROIA

UPOLUJ CYBERPRZESTĘPCĘ

Przewodnik dla hakerów prowadzących śledztwa online

Helion

WILEY

Tytuł oryginału: Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques

Tłumaczenie: Andrzej Watrak

ISBN: 978-83-283-9205-2

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
https://helion.pl/user/opinie/upocyb
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *https://helion.pl* (księgarnia internetowa, katalog książek)

Printed in Poland.

Spis treści

Rozdział

13

Ciekawe miejsca do poszukiwań

Zgodnie z tytułem niniejszy rozdział jest poświęcony poszukiwaniu informacji w nietypowych miejscach. Przedstawia również historię hakera Cypera i wydarzenia, które doprowadziły do odkrycia jego tożsamości.

Czy jest lepszy sposób na rozpoczęcie rozdziału niż zacytowanie mojej prywatnej konwersacji na Jabberze z Cyperem? Dzieliliśmy się w niej informacjami, jak zidentyfikowaliśmy siebie nawzajem na podstawie nieprecyzyjnych wskazówek.

```
VT:      Skąd wiedziałeś, że to ja?
kickass: Lol, używasz tego samego MacBooka.
VT:      Nie sądzę, zważywszy na to, że kupiłem go 2 dni temu.
VT:      Nowiutka zabawka, i9.
kickass: Ale nie nazwa ;)
kickass: Tak czy owak odpowiedz na pytanie.
kickass: Skąd wiesz, że ja to ja?
VT:      Pomijając fakt, że twój styl zmienił się gdzieś pod koniec forum Hell/tuż
         przed BlackBoksem, kiedy w końcu otworzyliście KickAss, twój newsbot wyglądał
         jak Cypernews.
VT:      CYPERCRIME news.
VT:      Tak to było.
kickass: Lol.
kickass: Jesteś na KickAss, więc powinieneś wiedzieć, że Cyper też tam jest.
         Przy okazji, czy cię zbanowaliśmy?
VT:      Nie byłem na KickAss od dawna.
kickass: Moja rada: jeśli korzystasz z Jabbera, nie używaj tej samej nazwy użytkownika
         na wszystkich kontach. Od czasu do czasu zmieniaj też nazwę laptopa ;)
```

Cyper miał na myśli pole *hostname* w moim kliencie Jabbera. Wtedy nie wiedziałem jeszcze, że można zmienić zawartość tego pola. Jeżeli pozostawi się puste, komunikator Adium dla systemu

macOS użyje nazwy komputera. W tym przypadku Cyper wiedział, że rozmawia ze mną, ponieważ nazwa mojego komputera była wystarczająco unikatowa, aby mnie zidentyfikować. Dobra robota. To jest właśnie ten rodzaj poszlak, których będziemy szukać w tym rozdziale.

theHarvester

theHarvester to otwarte, terminalowe narzędzie śledcze, służące do wyszukiwania publicznie dostępnych adresów e-mail, subdomen, adresów IP i URL w źródłach takich, jak serwisy Baidu, Bing, Censys.io, Crt.sh, Dogpile, Google, LinkedIn, NetCraft, PGP, ThreatCrowd, Twitter i VirusTotal. Jest to prawdopodobnie jeden z najlepszych dostępnych programów rozpoznawczych, ponieważ jego możliwości wyszukiwania informacji są bardzo szerokie. Zaryzykowałbym nawet stwierdzenie, że jeśli nie dostarcza żadnych wyników, to znaczy, że nie jest właściwie używany.

Narzędzie theHarvester wykorzystuje do wyszukiwania informacji o danej domenie szereg technik, m.in.: słownikowe ataki DNS przeprowadzane metodą brutalnej siły, odwrotne odpytywanie DNS, weryfikację nazw hostów i oczywiście dorki w wyszukiwarkach internetowych.

Uwaga **Narzędzie theHarvester jest tak wszechstronne, że zastanawiałem się, w którym rozdziale je opisać. Ten wydał mi się najbardziej odpowiedni, gdyż oprogramowanie to oferuje znacznie więcej funkcji niż opisane w poprzednich rozdziałach, a jednocześnie nie chciałem pominąć żadnej opcji, która wykraczałaby poza zakres każdego z nich.**

Używam narzędzia theHarvester, kiedy potrzebuję przeszukać w szerokim zakresie publicznie dostępne informacje pod kątem nazw firm i adresów e-mail niedostępnych dla wyszukiwarek. Program jest dostępny na stronie *https://github.com/laramies/theHarvester* i ma następujące parametry:

- `-h`, `--help` — wyświetlenie tekstu pomocy i wyjście.
- `-d` *`DOMENA`*, `--domain` *`DOMENA`* — nazwa przeszukiwanej firmy lub domeny.
- `-l` *`LIMIT`*, `--limit` *`LIMIT`* — ograniczenie liczby wyników, domyślnie 500.
- `-S` *`START`*, `--start` *`START`* — rozpoczęcie poszukiwań od wyniku o podanym numerze, domyślnie 0.
- `-g`, `--google-dork` — wyszukiwanie za pomocą dorków Google'a.
- `-p` *`PORTY`*, `--port-scan` *`PORTY`* — skanowanie znalezionych hostów i sprawdzenie Takeover (21, 22, 80, 443, 80800); wartość = `True`, domyślnie `False`.
- `-s`, `--shodan` — odpytywanie znalezionych hostów za pomocą serwisu Shodan.
- `-v` *`WIRTUALNY_HOST`*, `--virtual-host` *`WIRTUALNY_HOST`* — sprawdzenie nazwy hosta za pomocą usługi DNS i wyszukanie wirtualnych hostów; wartość = `basic`, domyślnie `False`.
- `-e` *`SERWER_DNS`*, `--dns-server` *`SERWER_DNS`* — serwer DNS wykorzystywany podczas wyszukiwania.
- `-t` *`DNS_TLD`*, `--dns-tld` *`DNS_TLD`* — przeszukiwanie serwera DNS na najwyższym poziomie domeny; domyślnie `False`.

- `-n` *`WYSZUKIWANIE_DNS`*, `--dns-lookup` *`WYSZUKIWANIE_DNS`* — wyszukiwanie z wykorzystaniem DNS; wartość = `True`, domyślnie `False`.
- `-c`, `--dns-brute` — przeprowadzenie ataku DNS metodą brutalnej siły na domenę.
- `-f` *`NAZWA_PLIKU`*, `--filename` *`NAZWA_PLIKU`* — zapisanie wyników w plikach HTML-a i XML-a;
- `-b` *`ŹRÓDŁO`*, `--source` *`ŹRÓDŁO`* — źródło wyszukiwanych informacji; wartość = `baidu`, `bing`, `bingapi`, `censys`, `crtsh`, `cymon`, `dnsdumpster`, `dogpile`, `duckduckgo`, `google`, `google-certificates`, `hunter`, `intelx`, `linkedin`, `netcraft`, `securityTrails`, `threatcrowd`, `trello`, `twitter`, `vhost`, `virustotal`, `yahoo`, `all`.
- `-x` *`WYKLUCZENIE`*, `--exclude` *`WYKLUCZENIE`* — wykluczenie opcji w przypadku użycia wszystkich źródeł.

Skanowanie

Wyszukiwarki zazwyczaj blokują użytkowników masowo przeszukujących internet, dlatego narzędzie theHarvester, aby uniknąć wykrycia, wysyła zapytania w pewnych odstępach czasu. Ponadto liczbę zapytań można zmniejszyć, ograniczając liczbę wyników. Dzięki temu uzyskuje się również prostszą w analizie listę. Narzędzie zapisuje wyniki w formatach HTML-a i XML-a.

Skanowanie za pomocą programu theHarvester jest dość nietypowe. *Wymagane jest* podanie parametrów `-d` (domena), `-l` (limit wyników) i `-b` (źródło). Jeżeli któregoś z nich zabraknie, wynik będzie następujący:

```
root@osint > ./theHarvester.py -d apple.com
*************************************************************************
*                                                                       *
* | |_| |__   ___     /\  /\__ _ _ ____   _____  ___| |_ ___ _ __     *
* | __|  _ \ / _ \   / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__|    *
* | |_| | | |  __/  / __  / (_| | |   \ V /  __/\__ \ ||  __/ |       *
*  \__|_| |_|\___|  \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|       *
*                                                                       *
* theHarvester 3.0.6 v380                                               *
* Coded by Christian Martorella                                         *
* Edge-Security Research                                                *
* cmartorella@edge-security.com                                         *
*                                                                       *
*************************************************************************



[*] No IPs found.

[*] No emails found.

[*] No hosts found.
```

Jeżeli pojawią się komunikaty, że nie znaleziono żadnych adresów IP, e-mail ani domen, prawdopodobnie przyczyną były niepoprawnie określone parametry. Parametr `-d` wskazuje nazwę przeszukiwanej domeny lub firmy, `-l` ogranicza liczbę wysyłanych zapytań, a `-b` określa wyszukiwarkę, np.: Censys, crt.sh, Google, Bing lub Yahoo. Aby nie ograniczać się do konkretnej wyszukiwarki, *należy* użyć parametru `-b all`.

Ostrzeżenie **Użycie wysokiego limitu wyników spowoduje tymczasowe zablokowanie dostępu do Google'a lub innej wyszukiwarki. Domyślnie limit jest równy 500, co oznacza, że narzędzie theHarvester wykorzystuje 500 pierwszych wyników. Wyszukiwarka Google wyświetla na stronie 10 wyników, a więc narzędzie domyślnie szybko żąda wyświetlenia 50 kolejnych stron. To jest wystarczający sygnał dla Google'a i każdej innej wyszukiwarki, że użytkownik masowo przeszukuje internet i należy mu włączyć mechanizm Captcha lub po prostu zablokować dostęp. Aby tego uniknąć, polecam usługę proxy (np. serwis Storm Proxies), dzięki której każde zapytanie jest wysyłane z innego adresu IP.**

Teraz, gdy wiesz już, dlaczego ważne jest określanie parametrów `-d`, `-b` i `-l`, przeskanuj znajomą witrynę WhitePacket Security (*www.whitepacket.com*):

```
root@osint > ./theHarvester.py -d whitepacket.com -l 100 -b all
*************************************************************************
*                                                                       *
* | |_| |__   ___     /\  /\__ _ _ ____   _____  ___| |_ ___ _ __     *
* | __|  _ \ / _ \   / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__|    *
* | |_| | | |  __/  / __  / (_| | |   \ V /  __/\__ \ ||  __/ |       *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|       *
*                                                                       *
* theHarvester 3.0.6 v380                                               *
* Coded by Christian Martorella                                         *
* Edge-Security Research                                                *
* cmartorella@edge-security.com                                         *
*                                                                       *
*************************************************************************


[*] Target: whitepacket.com

[*] Searching Bing.
[*] Searching Censys.
       Searching IP results page 4.
[*] Searching Yahoo.
       Searching 100 results.
[*] Searching Baidu.
       Searching 100 results.
[*] Searching Google.
       Searching 100 results.

(fragment pominięty)

Users from Twitter: 3
-------------------
(fragment pominięty)


[*] IPs found: 1
-------------------
(fragment pominięty)

[*] Emails found: 2
----------------------
(fragment pominięty)

[*] Hosts found: 5
---------------------
www.whitepacket.com:104.24.118.111
(fragment pominięty)
```

Powyższe wyniki to dobry początek, zważywszy na to, że badana domena nie jest szeroko znana. Narzędzie theHarvester znalazło 5 hostów, 2 adresy e-mail i 3 konta na Twitterze. To niezły rezultat, ale zrób jeszcze jeden test na znacznie większej domenie *microsoft.com*:

```
root@osint > ./theHarvester.py -d microsoft.com -l 100 -b all
*************************************************************************
*                                                                       *
* | |_| |__   ___     /\  /\__ _ _ ____   _____  ___| |_ ___ _ __     *
* | __|  _ \ / _ \   / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__|    *
* | |_| | | |  __/  / __  / (_| | |   \ V /  __/\__ \ ||  __/ |       *
*  \__|_| |_|\___|  \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|       *
*                                                                       *
* theHarvester 3.0.6 v380                                               *
* Coded by Christian Martorella                                         *
* Edge-Security Research                                                *
* cmartorella@edge-security.com                                         *
*                                                                       *
*************************************************************************


[*] Target: microsoft.com

[*] Users found: 34
--------------------
(fragment pominięty)

Users from Twitter: 24
-------------------
(fragment pominięty)

[*] IPs found: 11
-------------------
(fragment pominięty)

[*] Emails found: 18
----------------------
(fragment pominięty)

[*] Hosts found: 2771
----------------------
(fragment pominięty)

[*] URLs found: 131
--------------------
https://trello.com/..(fragment pominięty)
```

Jak widać, tym razem wyniki robią wrażenie, tym bardziej że zostały uzyskane za pomocą jednego narzędzia: 2771 hostów, 18 adresów e-mail, 34 nazwy użytkowników, 24 konta na Twitterze i 131 adresów URL Trello powiązanych z Microsoftem.

Teraz tylko od Ciebie zależy, w którą stronę skierujesz dalsze dochodzenie. Pamiętaj o dokumentowaniu wszystkiego, co znajdziesz, abyś później mógł się do tego łatwo odnieść.

Sprawdźmy teraz, co jeszcze można wydobyć z internetu.

Serwisy wklejkowe

Hakerzy często wykorzystują serwisy wklejkowe do publikowania próbek swoich danych. W zależności od badanego obiektu na tego typu stronach można znaleźć wiele przydatnych informacji, takich jak próbki wykradzionych danych, wypowiedzi hakerów i różnego rodzaju dokumenty.

Najpopularniejsze serwisy wklejkowe to:

- *Pastebin.com*,
- *0bin.net*,
- *Doxbin.org*,
- *Justpaste.it*.

Są one szeroko wykorzystywane przez hakerów i nierzadko zawierają kluczowe dla śledztwa informacje. Problem jednak polega na tym, że wklejki naruszające warunki korzystania z serwisu lub zawierające informacje umożliwiające zidentyfikowanie osób czy prywatne dane są usuwane. Dlatego jest wiele organizacji i osób (w tym ja), które codziennie przeszukują powyższe serwisy pod kątem nowych treści. W dalszej części rozdziału opiszę, jak to zrobić w dość prosty sposób.

psbdm.ws

Jak wspomniałem, wklejki, które naruszają warunki korzystania z serwisu, np. zawierają informacje osobowe lub poufne dane, są szybko usuwane. To nie jest sprzyjająca okoliczność, zwłaszcza jeżeli wklejka zawiera wskazówki lub dowody potrzebne w dochodzeniu. Na szczęście jest serwis *psbdmp.ws*.

Przez długi czas strona *psbdmp.ws* była jedną z moich tajnych broni, ponieważ jako jedyna zawierała pełne archiwum wszystkich wklejek, począwszy od 2015 r. Co więcej, jej interfejs API jest bardzo przyjazny w użyciu i pozwala korzystać z serwisu za pomocą zewnętrznej aplikacji. Zanim napisałem program przeszukujący wszystkie serwisy wklejkowe dla mojej platformy Data Viper, interfejs API serwisu *psbdmp.ws* był kluczowym elementem mojego zestawu śledczego.

Fora internetowe

Fora internetowe są według mnie bramą do podziemnego rynku. Myślę, że wejście na nie jest jak rytuał przyjęcia do elitarnej kasty hakerów. W życiu każdego młodego hakera jest etap beztroskiej lekkomyślności. Działa bezmyślnie jak dziecko i często pozostawia po sobie ślady prowadzące do prawdziwej tożsamości.

Dlatego, moim skromnym zdaniem, prawdziwa sztuka identyfikacji zagrożeń polega na umiejętności wyszukiwania i gromadzenia informacji historycznych. Poszukiwania nie powinny się ograniczać do forów hakerskich i darkwebu (sieci TOR). Hakerzy udzielają się również na legalnych forach różnych kształtów i rozmiarów. Badając je i np. kojarząc pseudonimy z adresami e-mail, często można uzyskać kluczowe wskazówki.

Jednym z forów, które mi w tym pomogły, jest BitcoinTalk. Nie potrafię tego wyjaśnić, ale zauważyłem, że wielu hakerów, których badałem w przeszłości, przebywało na tym forum. Dlatego nie należy ograniczać poszukiwań do jednego konkretnego typu forów lub witryn. Obszar badań powinien być jak najszerszy.

PORADA EKSPERTA: CHRIS ROBERTS

W swoim laboratorium tworzyłem własne narzędzia przeszukujące internet. Zaczynałem od przygotowania zestawu adresów URL stron, które mnie interesowały. Mogły być dowolne, np. serwisy wklejkowe. Wiadomo, jak dużo rzeczy może się tam znajdować.

Chodziło mi przede wszystkim o odpowiedź na pytanie: „Okej, które z nich naprawdę się przydadzą?". Było tam wszystko: od wczesnych materiałów po wykradzione dane.

Patrząc na to, widziałem, że można wyciągać dane z ciemniejszej strony świata. Znowu jest to ten sam rodzaj koncepcji. Jeden adres URL prowadzi do 10 lub 20 innych adresów URL. Przeprowadzasz ich szybką, wysokopoziomową analizę i decydujesz na podstawie słów, map ciepła i wielu innych kryteriów, jakie priorytety przeszukiwań im nadać.

Następnie dane trzeba zebrać i zindeksować. W ten sposób tworzy się własną wersję środowiska o bardzo, bardzo wysokim wskaźniku skuteczności. W tym przypadku korzystałem z bazy Elasticsearch. Nie używałem żadnego systemu zarządzania danymi, żeby ta cała machina działała sprawnie.

Aby zdobyć potrzebne dane, najczęściej wystarczy poczytać, co mówią inni. Załóżmy, że wchodzimy na forum, wszystko jedno jakie. Uczestnicy rozmawiają o hakowaniu, łamaniu haseł lub torrentach. Fora prowadzą do adresów URL, kolejnej witryny i następnej. Zaczynamy więc od forum X, Y, Z i sprawdzamy, czy mamy kogoś z kontem, identyfikatorem użytkownika lub czymkolwiek, co warto byłoby uzyskać. Te dane można wprowadzić bezpośrednio do bazy. Jeśli jest dobrze skonfigurowana, na pewno powie dokładnie, których kont użytkowników trzeba użyć, aby dostać wszystkie przeklęte rzeczy!

Badanie historii forum (i grupy TDO)

Jeśli śledztwo doprowadzi Cię do forów, pozyskanie danych historycznych może okazać się naprawdę trudnym zadaniem. Przetestowałem wersje demonstracyjne wielu płatnych aplikacji przeznaczonych do wykrywania zagrożeń, ale żadna nie oferowała takich danych historycznych, jakie były mi potrzebne do dalszego dochodzenia. Wielu producentów utrzymywało, że posiada obszerne dane, ale w rzeczywistości tak nie było. Dlatego ostatecznie zrobiłem to samo, co Chris Robert, tj. napisałem własną aplikację.

Moja platforma nazywa się Data Viper, a jej zbudowanie okazało się punktem zwrotnym w identyfikacji członków grupy The Dark Overlord. W rozdziałach 17. i 18. dokładniej opiszę, jak działa i dlaczego ją utworzyłem. Na razie wróćmy do głównego wątku. Dowiedz się, dlaczego przeszukiwanie forów jest takie ważne.

Kiedy badałem początki grupy TDO, wszystkie drogi prowadziły do forum Hell. Niestety, zostało ono zamknięte w 2016 r., a znalezienie posiadacza kopii wpisów okazało się najtrudniejszą częścią całego śledztwa. Na szczęście po wielu miesiącach niestrudzonych poszukiwań spotkałem kogoś, kto posiadał te dane. Prosił, aby nie podawać jego nazwiska, ale jeśli czyta tę książkę, chcę, aby wiedział, jak bardzo jestem mu wdzięczny, ponieważ dane okazały się bardziej przydatne, niż przypuszczałem.

Wszyscy członkowie grupy TDO spotkali się i zjednoczyli na forum Hell. Gdy przeczytałem ich wpisy, hierarchia grupy od razu stała się jasna. Wyglądało na to, że wszyscy wpatrywali się w niejakiego Cypera (bez „h" w środku). Poznałem jego niektóre inne przydomki, zanim dostałem się do tego forum, więc utwierdziłem się wtedy w przekonaniu, że jestem na dobrej drodze.

Cyper po tym, jak forum Hell zostało zamknięte (do czego, jak sądzę, się przyczynił), założył własne o nazwie BlackBox, gdzie udzielał się jako Ghost, oraz jeszcze jedno, KickAss, gdzie działał pod pseudonimem NSA.

Teraz opiszę, jak do tego doszedłem.

Po nitce do kłębka

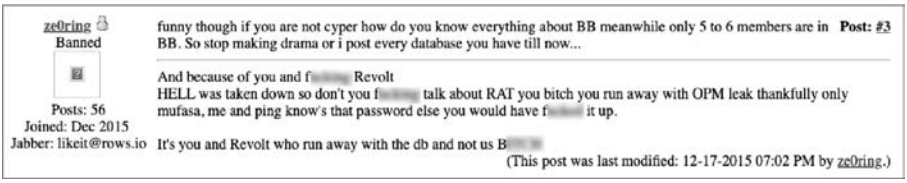
PORADA EKSPERTA: CHRIS ROBERTS

Kiedyś, gdy przygotowywałem się do włamania na stronę firmy z sektora energetycznego, rozglądałem się po okolicy, tj. przeglądałem strony powiązanych firm, jej klientów i dostawców. Na jednym z forów pewien inżynier opisał problemy, z którymi się zmagał. Umieścił wtedy odnośnik do dokumentu, który pobrałem. Był to 350-stronicowy opis całej podstacji, sieci energetycznej, architektury, włącznie z adresami IP…

Za każdym razem tak robię, prowadząc badania. Nie ma znaczenia, co produkuje firma, mogą to być nawet samoloty. To jest zresztą bardzo dobry przykład, bo ani Boeing, ani Airbus nie produkują samolotów sami, tylko wspólnie z setkami innych firm. To jest jak klocki Lego.

To, co trzeba zrobić, to znaleźć odpowiednich ludzi, tworzących elementy, którymi jesteś zainteresowany. Trzeba wyciągnąć od nich całą wiedzę i dane, tak jak ja to zrobiłem.

Tropienie hakera nie różni się od badania firmy, o czym pisze Chris. W przypadku grupy TDO trop pojawił się na 0-day (forum hakerów oparte na sieci TOR), gdzie użytkownicy ze0ring i Cyper spierali się o dane wykradzione z amerykańskiej Agencji Kadr i Zarządzania (rysunek 13.1).



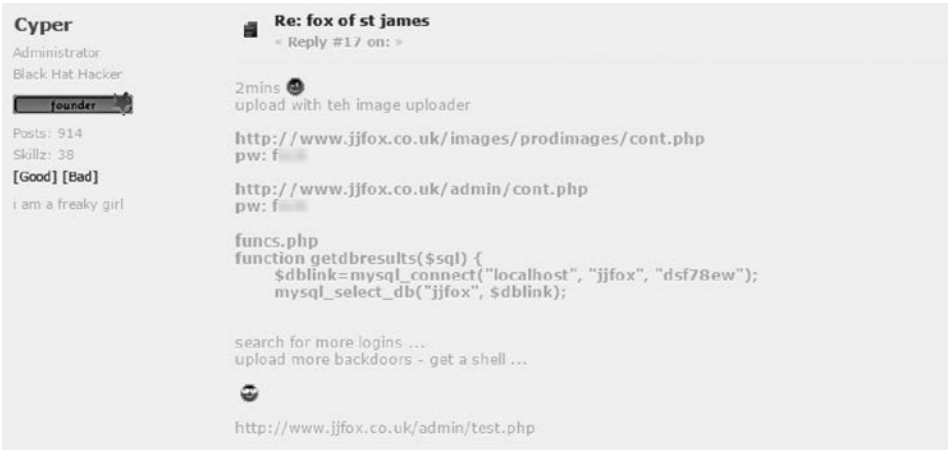
Rysunek 13.1

Sprawa była zagmatwana. W skrócie: ze0ring był wściekły, bo Cyper i Revolt uciekli z wykradzionymi danymi i spowodowali zamknięcie forum Hell (o szczegółach możesz przeczytać w moim oficjalnym raporcie na temat grupy TDO). Niezależnie od tego użytkownik Photon we wpisie pokazanym na rysunku 13.2 wyraził swoje niezadowolenie z BlackBoksa i Ghosta (dla zainteresowanych: odnośniki do serwisów Imgur i mega.nz są nadal aktywne).

Rysunek 13.2

To właśnie m.in. kopie wpisów Photona na forum BlackBox potwierdziły, że Cyper i Ghost to była ta sama osoba.

W kolejnym wpisie na BlackBox (rysunek 13.3) Cyper opisał powłokę webshell, którą załadował do JJFoksa, sklepu z cygarami z Wielkiej Brytanii.



Rysunek 13.3

Kilka dni później pojawił się ten sam wpis (rysunek 13.4), ale tym razem jego autorem nie był Cyper, tylko Ghost. Te zrzuty nie były bynajmniej jedyną wskazówką, że oba pseudonimy należą do jednej osoby. Niemniej jednak przydały się.

Rysunek 13.4

Ustalenie tożsamości Cypera

Wiedziałem już, że Cyper jest tym, kto przyczynił się do zamknięcia forum Hell (pisałem o tym w rozdziale 2.). Potem, gdy ostatecznie ustaliłem, że Cyper był liderem forum BlackBox, moje zainteresowanie jego osobą gwałtownie wzrosło. Niestety BlackBox był tak ekskluzywnym forum, że znalezienie kopii jego danych okazało się niemożliwe.

Czasami jednak okruchy złota można znaleźć w najbardziej przypadkowych miejscach.

Wspomniałem wcześniej, że utworzyłem aplikację o nazwie Data Viper, zbierającą poświadczenia, zhakowane bazy danych i kopie forów. Starając się zebrać i poindeksować jak największą ilość danych historycznych, natrafiłem w sieci TOR na serwis społecznościowy o nazwie Galaxy. Jego druga wersja okazała się miejscem spotkań większości członków forum Hell, w tym Cypera i jego świty. W przedstawionej niżej gorącej konwersacji Cyper (vel CyPeRtRon) broni się przed atakami dwóch innych osób w związku z uruchomieniem swojego nowego forum, BlackBox, o adresie URL ***cyper****7cybre7u57.onion*.

Uwaga **Oto kolejna poszlaka, której nie mogłem zlekceważyć, wskazująca, że Cyper był administratorem forum BlackBox: w adresie URL znajdowało się słowo *cyper*.**

```
Arsyntex
@Unknown 8698 8698, CyPeR powinien/powinna wiedzieć, jest jednym z głupców z G***box, he,
he, Blackbox (nazwa motywu, bardzo oryginalna), i nie może się doczekać mojego Pro Forum?
Jakie Forum? To prywatna sieć i tak, śnij dalej, powiedziałem Pro, a nie Poor ;D

CyPeRtRoN
LOL, dowiedz się, jaka jest różnica między prywatną siecią a forum, głupi dzieciaku. Hell
nie jest prywatną siecią, tylko otwartym forum.
    Arsyntex 9 dni temu
    Wkrótce nowe HELL, tylko dla profesjonalistów, a nie upośledzonych lub nieświadomych
dzieci, bez doxingu, SQL-i i innego g***.

CyPeRtRoN
A dlaczego nie, skoro nazwa jest dobra dla forum… Ale obawiam się, że nie wiesz, co oznacza
słowo "Blackbox"…

CyPeRtRoN
Jesteś wkurzony, bo nie możesz grać z dużymi chłopakami i musisz z dzieciakami z okolicy…

Arsyntex
Ha, ha, znam różnicę… i napisałem "Wkrótce nowe HELL", a nie "Wkrótce to samo otwarte g***
HELL"… I nie jestem dzieciakiem ani lamerem, w przeciwieństwie do ciebie ;D
http://matrixtxri745dfw.onion/neo/uploads/150724/MATRIXtxri745dfwONION_14261OhJl_lol.png LOL

Arsyntex
Ja się wkurzam?… hahaa… Ja gram sam, a moi koledzy to bystrzy ludzie, a nie dzieci-idioci.
Po prostu lubię denerwować takie dzieciaki jak ty, jestem wielozadaniowy xD

CyPeRtRoN
Tak, to forum ma zasady. Co chcesz powiedzieć tym zrzutem? No dalej, sam tego nie wiesz…

CyPeRtRoN
Skoro jesteś taki mądry, to pewnie mówisz, że śledzisz ciasteczka, co? :D

CyPeRtRoN
Myślisz, że możesz się schować w TOR. Pomyśl jeszcze raz, dzieciaku. Nie odwiedzaj złych
serwerów. Byłeś na moim serwerze. Nie jesteś wystarczająco bystry. Mam wiele węzłów
wyjściowych. Mam nadzieję, że nie skorzystałeś z żadnego z nich. http://ow.ly/Q34fA

Arsyntex
Po pierwsze, napisałeś "grać". Powtarzam to złośliwie (dlatego w cudzysłowach). Potrafię
"grać" (LOL). Pracuję sam i mam kolegów. Czy twoje myślenie jest tak słabe, że nie
```

```
rozumiesz, czy posiadanie kolegów oznacza, że nie mogę pracować sam? A pisząc "jestem
wielozadaniowy", miałem na myśli, że mogę jednocześnie pracować i kłócić się z takimi
głupiutkimi dziewczynkami jak ty xD. Zasady forum są śmieszne… "to pewnie mówisz, że
śledzisz ciasteczka, co? :D" Co to niby jest? xD

Arsyntex
LoL, zaczynam się bać, lepiej się odłączę, hahaha.

Sugartime
Pierwsza zasada ukrywania usług: nigdy nie podawaj swojego prawdziwego IP. #telnet
cyper7cyb5re7u57.onion 25 Connected to cyper7cyb5re7u57.onion. 220 ks355296.kimsufi.com
ESMTP Exim 4.84 Fri, 24 Jul 2015 xx:xx:xx +0200 #dig ks355296.kimsufi.com 91.121.120.49
Druga zasada ukrywania usług: aby zachować anonimowość, nigdy nie używaj identyfikatora Exim
ze swoim prawdziwym IP. PORT STATE SERVICE VERSION 113/tcp open ident? #telnet 91.121.120.49
113 Connected to 91.121.120.49. 25, 25 : USERID : UNIX : fail 25,25:ERROR:NO-USER

Arsyntex
Haha xD @CyPeRtRoN http://freedomsct2bsqtn.onion/sannucjvkdoymsycrugq/cXsgtnpE.png
```

Prawdziwe złoto!

Wpisowi Sugartime'a dodatkowego kontekstu dodaje fakt, że *cyper7cybre7u57.onion* jest adresem URL byłego forum BlackBox. Jeśli ta informacja jest prawdziwa, oznacza, że adres IP BlackBoksa został ujawniony i znajdował się na serwerze OVH (nadrzędnym hoście dla *Kimsufi.com*) o adresie IP *91.121.120.49*. Co za *wspaniały* wynik! Nigdy nie lekceważ hakerów, którzy chcą się nawzajem pognębić. Gdy zaczną się kłócić, będą sobie wzajemnie dokuczać i zrobią wszystko, co w ich mocy, aby się nawzajem zniszczyć. Powyższy przykład jest tego dowodem. Znalezienie prawdziwego adresu IP witryny w sieci TOR jest prawie niemożliwe (chyba że kontroluje się węzły wyjściowe), więc fakt, że serwer został ujawniony w ten sposób, jest niezwykły. Czy to mógł być prawdziwy adres IP oryginalnego serwera BlackBoksa?

Repozytoria kodów

Repozytoria kodów, takie jak GitHub, Bitbucket i GitLab, mogą dostarczyć kluczowych wskazówek do znalezienia drogi do poznania organizacji lub osoby. Programiści umieszczają w repozytoriach swoje kody. Znajdują się w nich historie zatwierdzonych kodów, a nawet adresy e-mail osób zatwierdzających. Trzeba tylko wiedzieć, jak uzyskać te informacje.

Jeśli zastanawiasz się, na ile repozytoria mogą być przydatne, to mogę powiedzieć, że w zatwierdzonych kiedyś kodach znalazłem następujące rodzaje informacji:

- prywatne adresy e-mail,
- zakodowane na stałe hasła aplikacyjne,
- klucze AWS,
- informacje osobowe i dane użytkowników,
- hasła użytkowników,
- pełne kopie baz danych.

Jeżeli wciąż nie jesteś przekonany, poniżej zamieszczam moją konwersację ze znanym hakerem NSFW, który znalazł w repozytorium GitHub klucze AWS i włamał się do witryny pewnej dużej firmy:

```
BTC: Uzyskałem dane dyrektora technicznego czy kogoś tam.
BTC: Wszystko zhakowałem.
BTC: Dropboxa
BTC: itp.
BTC: Wszędzie było dwuetapowe uwierzytelnienie.
BTC: Ale
BTC: ten n****
BTC: to największy idiota.
BTC: Na GitHubie
BTC: nie było dwuetapowego uwierzytelnienia.
BTC: Stosowali je na najbardziej bezwartościowym g***,
BTC: ale nie na GitHubie.
BTC: Tak czy owak
BTC: znalazłem na GitHubie poświadczenia AWS,
BTC: a potem się włamałem na prywatny zasób.
BTC: Ale
BTC: nie było tam żadnych danych.
BTC: Niczego nie było w zasobniku.
BTC: Tylko RDS.
BTC: Musiałem więc czekać latami,
BTC: aż coś umieszczą
BTC: w AWS-ie.
```

SearchCode

Serwis SearchCode (*https://searchcode.com/*) umożliwia przeszukiwanie kodów zapisanych w repozytoriach GitHub, Bitbucket, Google Code, GitLab i innych. Większość hakerów koduje, więc jest bardzo prawdopodobne, że nie tylko mają konta w serwisach GitHub czy GitLab, ale także trzymają tam własne kody.

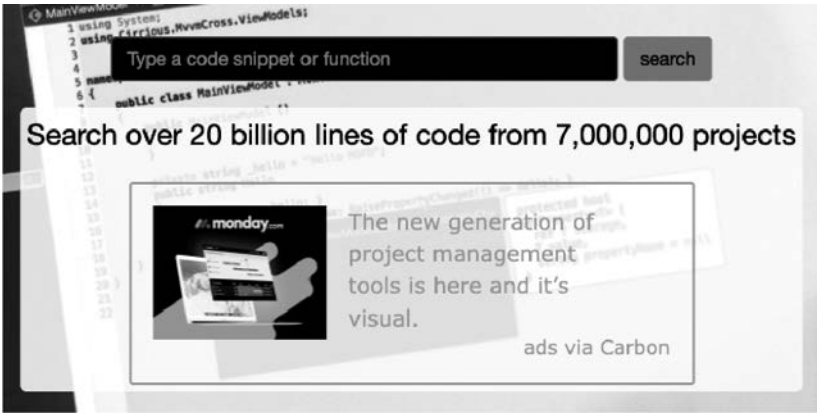
Poza tym jest jedna rzecz, o której nie można zapomnieć: *hakerzy wielokrotnie wykorzystują własne kody*. Jeśli zdobędziesz kod napisany przez badanego hakera, znajdziesz w nim błędy i ciekawe komentarze. Atrybucja na podstawie błędów ortograficznych i wielokrotnie wykorzystywanego kodu może wydawać się wątpliwa, ale stosuje się ją częściej, niż Ci się wydaje.

Uwaga **Ponadto hakerzy aplikujący do forów prawie zawsze dołączają do prośby przykładowe kody. Możliwość cofnięcia się w czasie i zebrania takich próbek może być niezwykle przydatna.**

Wracając do *SearchCode.com*: serwis może nie jest rewelacyjny, ale nie znalazłem lepszej, konkurencyjnej strony. Moim zdaniem jego największym mankamentem jest brak możliwości wyszukiwania pełnych ciągów znaków. Na przykład po wpisaniu frazy **`bardzo długi ciąg`** otrzymuje się mnóstwo nieprzydatnych wyników zawierających *którekolwiek* ze słów *bardzo*, *długi* oraz *ciąg*. Wprawdzie to lepsze niż nic, natomiast jeśli nie uzyskasz pożądanych wyników, możesz za pomocą aplikacji szybko szukać ciągów bezpośrednio w najważniejszych serwisach.

Przeszukiwanie kodu

Interfejs serwisu SearchCode jest dość oczywisty. Wystarczy w polu wyszukiwania wpisać żądaną frazę i kliknąć przycisk *Search* (rysunek 13.5).



Rysunek 13.5

W celu sprawdzenia wpisz frazę **\x48\x31\xc0\x5e\x68**, która powinna zwrócić sporo wyników. Po lewej stronie okna (rysunek 13.6) znajdują się moim zdaniem najbardziej przydatne opcje tego serwisu.

Rysunek 13.6

Wyników wyszukiwania jest zbyt dużo, aby zrobić z nich użytek, ale dzięki panelowi filtrów można je ograniczyć. Używając odpowiednich filtrów, można zaoszczędzić mnóstwo czasu, badać kody napisane w różnych językach i umieszczone w różnych repozytoriach.

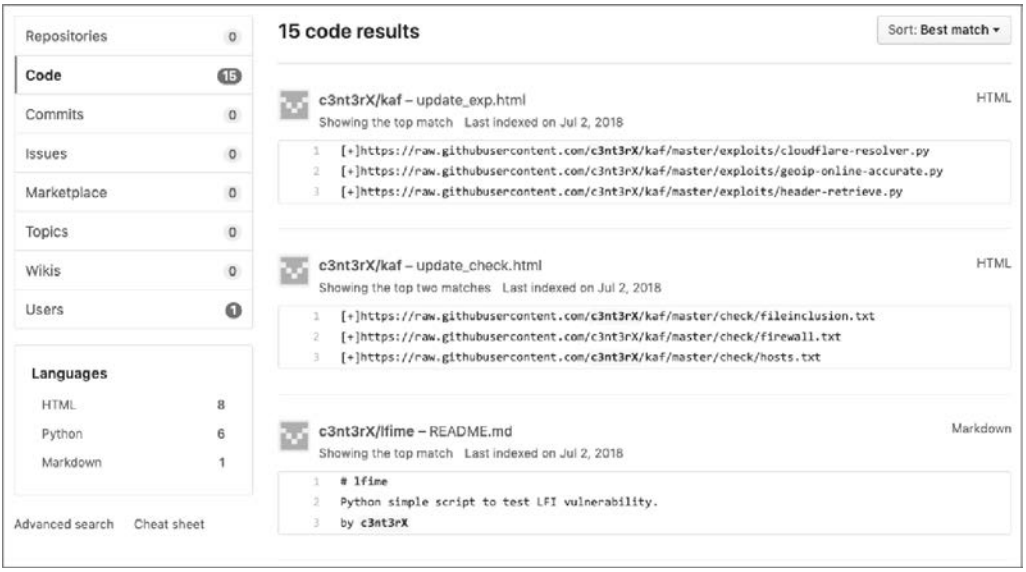
Fałszywe wyniki

Jedną z ważnych rzeczy, o których należy pamiętać, korzystając z serwisu SearchCode, jest liczba fałszywych wyników. Często pojawia się komunikat `No results found` (nie znaleziono wyników) lub, co gorsza, wyniki są niepoprawne i niezwiązane z wyszukiwaną frazą. Spróbuj np. wyszukać ciąg **`c3nt3rx`** (alias jednego z hakerów na forum KickAss). Rysunek 13.7 pokazuje, że nie znaleziono żadnych wyników.

Rysunek 13.7

Jak wspomniałem wcześniej, w przypadku braku wyników serwis SearchCode prezentuje odnośniki do różnych repozytoriów, np. GitHub, zawierających wyszukiwaną frazę. Po kliknięciu takiego odnośnika następuje przejście do repozytorium i automatyczne rozpoczęcie nowego wyszukiwania.

Jak pokazuje rysunek 13.8, w repozytorium GitHub fraza `c3nt3rx` pojawia się 15 razy. Szczęśliwym trafem użytkownik o tym pseudonimie był głównym twórcą narzędzi hakerskich KickAss Framework, utrzymywanych przez niektórych członków forum KickAss (w tym również Cypera).



Rysunek 13.8

Najważniejszy wniosek stąd płynie taki, że żadne narzędzie nie jest doskonałe i zawsze należy sprawdzać kilka źródeł. Używając narzędzi przeszukujących kilka witryn, warto również sprawdzać oryginalną stronę i mieć dzięki temu pewność, że wyniki są dokładne i spójne.

Teraz, mając do zbadania nowy trop w postaci platformy KickAss Framework, sprawdźmy, czy można się czegoś więcej dowiedzieć ze strony GitHuba.

Gitrob

Gitrob to otwarte narzędzie służące do wyszukiwania poufnych plików i informacji w publicznych repozytoriach GitHub. Jest przeznaczone zarówno dla śledczych, jak i programistów, ponieważ skanuje repozytoria pod kątem potencjalnie szkodliwych lub prywatnych informacji. Można je pobrać ze strony *https://github.com/michenriksen/gitrob*.

Narzędzie klonuje publiczne repozytoria i przegląda historie zatwierdzonych kodów. Oznacza potencjalnie niebezpieczne pliki i prezentuje wyniki w przeglądarce (można je również wyeksportować do pliku JSON) na potrzeby dalszej analizy.

Wyniki wyszukiwania frazy `c3nt3rx` za pomocą narzędzia Gitrob są następujące:

```
root@osint > gitrob -bind-address 0.0.0.0 c3nt3rx

      _ __                 __
  ___ _(_) /_____ _____   / /
 / _ `/ / __/ __/ _ \/ _ \
 \_, /_/\__/_/  \___/_.__/
/___/ by @michenriksen

gitrob v2.0.0-beta started at 2019-07-15T03:34:29Z
Loaded 91 signatures

Web interface available at http://0.0.0.0:9393
Gathering targets...

 Retrieved 7 repositories from c3nt3rX
Analyzing 7 repositories...

Findings....: 0
Files.......: 77
Commits.....: 63
Repositories: 7
Targets.....: 1
```

Ostrzeżenie **Powyższe wyniki mogą być mylące. Narzędzie Gitrob przeszukało 77 plików i 63 zatwierdzone kody, ale nie znalazło niczego ciekawego. Dlatego w przeglądarce jest widoczny komunikat o braku wyników.**

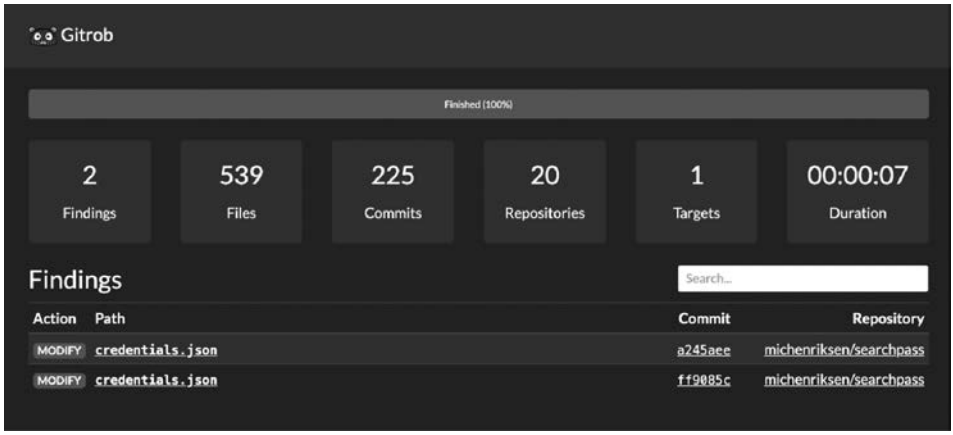
Dla odmiany, aby uzyskać lepsze wyniki, przeszukaj repozytorium michenriksen twórcy narzędzia Gitrob:

```
root@osint > gitrob -bind-address 0.0.0.0 michenriksen

      _ __                 __
  ___ _(_) /_____ _____   / /
 / _ `/ / __/ __/ _ \/ _ \
 \_, /_/\__/_/  \___/_.__/
/___/ by @michenriksen
```

```
gitrob v2.0.0-beta started at 2019-07-15T03:31:42Z
Loaded 91 signatures
Web interface available at http://0.0.0.0:9393

Gathering targets...
 Retrieved 20 repositories from michenriksen

Analyzing 20 repositories...

 MODIFY: Contains word: credential
  Path.......: credentials.json
  Repo.......: michenriksen/searchpass
  Message....: Update passwords
  Author.....: Michael Henriksen <michenriksen@neomailbox.ch>
  File URL...: https://github.com/michenriksen/searchpass/blob/a245aee..(fragment pominięty)
  Commit URL.: https://github.com/michenriksen/searchpass/commit/a245ae..(fragment
pominięty)

 MODIFY: Contains word: credential
  Path.......: credentials.json
  Repo.......: michenriksen/searchpass
  Message....: Update passwords
  Author.....: Michael Henriksen <michenriksen@neomailbox.ch>
  File URL...: https://github.com/michenriksen/searchpass/blob/ff908..(fragment pominięty)
  Commit URL.: https://github.com/michenriksen/searchpass/commit/ff9085c..(fragment
pominięty)

Findings....: 2
Files.......: 539
Commits.....: 225
Repositories: 20
Targets.....: 1

Press Ctrl+C to stop web server and exit.
```

Różnica w wynikach jest ogromna. Narzędzie prezentuje opisy znalezionych „interesujących" plików i ich lokalizacje. W tym przypadku niektóre pliki zawierają słowo `credential` (poświadczenia).

Został uruchomiony serwer WWW, więc można w przeglądarce otworzyć dokładniejszą listę znalezionych plików wraz z odnośnikami do nich (rysunek 13.9).



Rysunek 13.9

Narzędzie Gitrob wyszukuje klucze SSL, poświadczenia i wiele innych informacji. Jeśli natrafisz na repozytorium bogate w dane, ekran będzie wypełniony informacjami.

Dzienniki zatwierdzeń

Inny sposób zbierania informacji polega na zwykłym przeglądaniu dzienników zatwierdzeń kodów w repozytorium. Są w nich zapisane daty, godziny oraz informacje o osobach zatwierdzających zmiany. Ponieważ z *każdym* zatwierdzeniem jest powiązany adres e-mail, dzienniki mogą być źródłem nowych informacji, np. o aliasach lub adresach śledzonego hakera.

Zbadajmy dla przykładu repozytorium osoby *c3nt3rx* zawierające platformę KickAss Framework. O tej platformie szeroko dyskutowano na forum KickAss i prawdopodobnie była ona bezpośrednio powiązana z kilkoma kluczowymi członkami forum, w tym NSA, administratorem witryny (który w rzeczywistości jest naszym kumplem Cyperem). Platforma jest dostępna pod adresem *https://github.com/c3nt3rX/kaf*.

Po sklonowaniu repozytorium wyświetl dziennik za pomocą polecenia `git log`:

```
root@OSINT > git log

commit 9a8d392f4265f9fafec854d06bcc86608c393b3a
Author: NSA <nightsquare@sigaint.org>
Date:   Thu Jun 16 22:11:16 2016 +0200

    Changes

commit c9282534f031f066450197f31ef985d07661daa7
Author: NSA <nightsquare@sigaint.org>
Date:   Thu Jun 16 22:09:33 2016 +0200

    some changes and new scripts

commit 20fa61ff8113dd34e2dd6a2485b9654d6e09459a
Author: NSA <nightsquare@sigaint.org>
Date:   Fri May 27 01:18:05 2016 +0200

    new banner

commit af98fc17cec67f8a3085f374161cec93e15cd177
Author: NSA <nightsquare@sigaint.org>
Date:   Wed May 25 19:01:38 2016 +0200

    new readme

commit fd594e4bbc70e184005a7a3931a02aa7d3613b5a
Author: c3nt3rX <centerx@hotmail.gr>
Date:   Sat May 21 02:53:06 2016 +0300

    Update kaf.py

commit c06b68662da1b8690963a47930d24f04e6a75028
Author: c3nt3rX <centerx@hotmail.gr>
(fragment pominięty)
commit 6fbe9999d2fb68fb0954866328ad63505f4a06a5
Author: NSA <nightsquare@sigaint.org>
Date:   Thu Jun 30 08:06:54 2016 +0200

    change donate adresse
```

Wyniki zawierają informacje o dwóch różnych użytkownikach: *NSA* i *c3nt3rx*. Każdy ma własny adres e-mail. Adres użytkownika *c3nt3rx* już znamy, natomiast bardzo ciekawy jest adres *NSA* (Cypera): *nightsquare@sigaint.org*.

Uwaga **Adres *nightsquare@sigaint.org* jest naprawdę ciekawy, ponieważ dwie pierwsze litery pseudonimu *NSA* mogą oznaczać *Night Square*. Nie wiem, czy to tylko zbieg okoliczności, czy może nazwa *NSA* ma jeszcze inne, ukryte znaczenie. Jeżeli tak, to co oznacza litera *A*? W następnym podrozdziale opiszę, jak wywnioskowałem, że Cyper mieszka w Austrii (lub sąsiednim kraju). Może alias nawiązuje do jakiegoś austriackiego rynku w nocy? Nie udało mi się tego sprawdzić. Jeżeli masz jakiś pomysł, wyślij mi wiadomość.**

Strony wiki

Nic nie sprawia mi większej satysfakcji, niż znalezienie rozstrzygającego dowodu podczas śledztwa. Uczucie jest jeszcze przyjemniejsze, jeżeli wcześniej usłyszę „co za idiota".

Przypomina mi się znów historia naszego znajomego o pseudonimie Cyper (vel CyPeRtRoN, vel Ghost, vel NSA). Jedną z jego bardziej charakterystycznych cech był sposób, w jaki opowiadał o swojej przynależności do grupy hakerskiej Hackweiser w końcu lat 90. ubiegłego wieku. Gadał o tym przy każdej okazji, co ułatwiało mi śledzenie go na różnych kontach. Gdy już wiadomo, czego szukać, lub ma się kluczowe informacje, na których można się oprzeć, wszystkie elementy zaczynają układać się w całość.

Dwudziestego czwartego lipca 2015 r. w Galaxy 2, portalu społecznościowym w sieci TOR, odbyła się następująca gorąca dyskusja użytkowników Cyper i Arsyntex:

```
24 lipca 2015

CyPeRtRoN
Przede wszystkim: nie popadaj w paranoję, nie wnerwiaj mnie, a wszystko będzie dobrze…

Arsyntex
Uważaj, bo @CyPeRtRoN to zawodowy tropiciel ciasteczek… To jeden od NSA i GCHQ xD

CyPeRtRoN
LOL, wielkie dzięki za reklamę. Nie wiesz, kim jestem. Myślisz, że puściłeś 2 exp i jesteś
gość.

CyPeRtRoN
Masz tu coś do poczytania: https://en.wikipedia.org/wiki/Hackweiser.

Arsyntex
Członkowie: R4ncid, Bighawk, [P]hoenix, Immortal, RaFa, Squirrlman, PhonE_TonE, odin,
x[beast]x, Phiz, @CyPeRtRoN i Jak-away (AKA Hackah Jak), ha, ha, ha (¬˘¬)
```

W tej dyskusji ważne są dwa szczegóły: adres URL artykułu w Wikipedii o grupie Hackweiser i reakcja Arsynteksa na udostępnienie tego adresu przez Cypera. Do tamtej pory nigdy nie uważałem Wikipedii, ani żadnej innej publicznej encyklopedii, za źródło wiarygodnych informacji wywiadowczych. Myliłem się.

Wikipedia

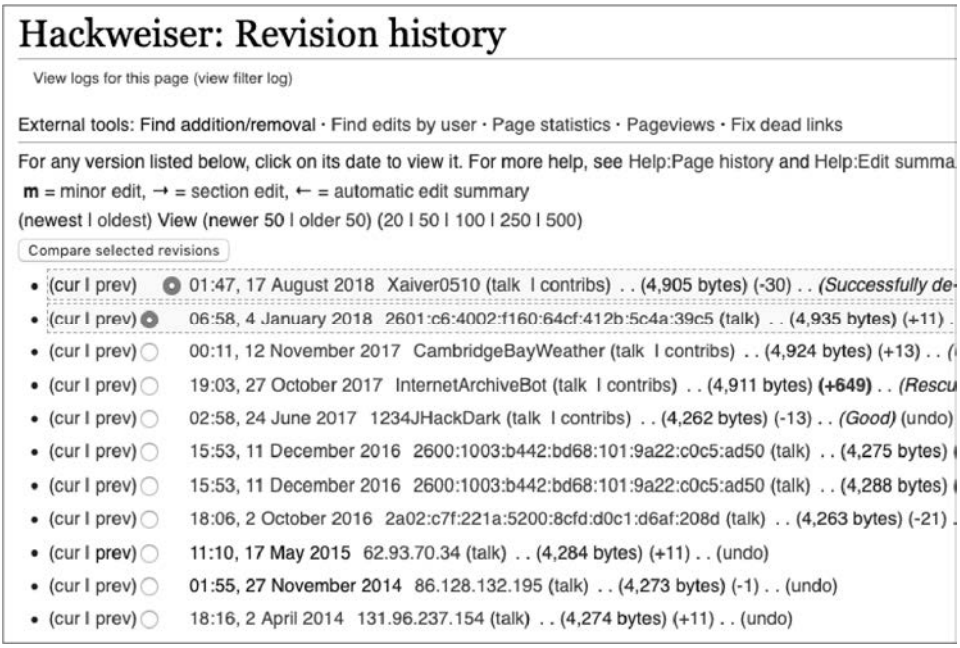
Wikipedia nie jest w pełni wiarygodnym źródłem informacji, ale ma jedną cenną cechę: posiada dokładny i publicznie dostępny rejestr zmian wprowadzanych w artykułach (żądanych i trwałych).

Obecnie w artykule poświęconym grupie Hackweiser (*https://en.wikipedia.org/wiki/Hackweiser*) wymienieni są następujący członkowie: R4ncid, Bighawk, [P]hoenix, Immortal, RaFa, Squirrlman, odin, x[beast]x, Phiz oraz Jak-away (vel Hackah Jak). Zapewne zauważyłeś, że na tej nieśmiertelnej liście nie ma najważniejszej postaci, wielkiego Cypera. Ale moment… Przed chwilą widzieliśmy wpis na forum Galaxy 2, w którym Cyper był wprost wymieniony jako członek grupy Hackweiser. Nawet sam się tym chwalił.

Pamiętaj: *młody, początkujący haker jest zawsze bardziej próżny niż ostrożny*. Aby się o tym przekonać, zajrzyj do zakładki *View History* (pokaż historię), znajdującej się przy każdym artykule (rysunek 13.10).

Rysunek 13.10

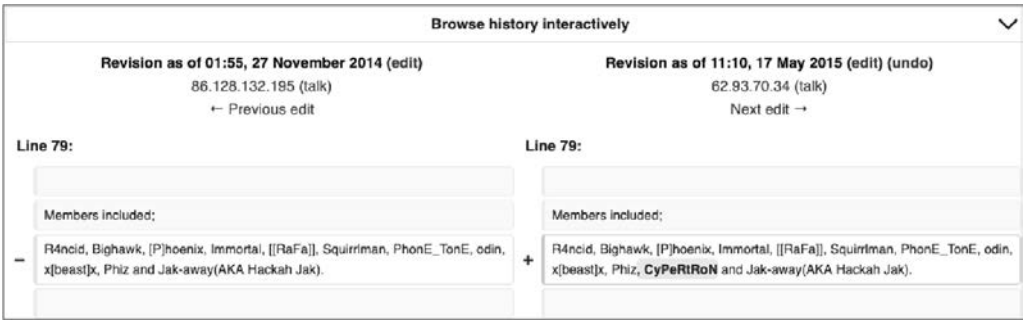
W artykule o grupie Hackweiser w tej zakładce znajduje się pełna lista wprowadzonych zmian, w tym dodanych i usuniętych treści (rysunek 13.11).



Rysunek 13.11

Wpis Cypera na forum Galaxy 2 pochodzi z czerwca 2015 r. Czy zauważyłeś na powyższym rysunku informację o zmianie wprowadzonej w maju 2015 r.? Aby przekonać się o doniosłości tej zmiany, spójrzmy na wcześniejszą, z listopada 2014 r. (bezpośredni odnośnik: *https://en.wikipedia.org/w/index.php?title=Hackweiser&oldid=635593910*). Zgodnie z artykułem z tamtego czasu grupę Hackweiser tworzyli: R4ncid, Bighawk, [P]hoenix, Immortal, RaFa, Squirrlman, PhonE_TonE, odin, x[beast]x, Phiz i Jak-away (vel Hackah Jak) — te same osoby, co w bieżącym artykule.

Wikipedia ma również bardzo przydatny przycisk *Compare Selected Revisions* (porównaj wybrane wersje). Przy opisie każdej zmiany pokazanej na rysunku 13.11 znajduje się pole opcji. Po zaznaczeniu zmiany z maja 2015 r. i kliknięciu przycisku *Compare Selected Revisions* pojawia się strona prezentująca różnice pomiędzy wybranym artykułem a bieżącym (rysunek 13.12). Możesz ją również otworzyć bezpośrednio, wpisując odnośnik *https://en.wikipedia.org/w/index.php?title=Hackweiser&diff=662753224&oldid=635593910*.



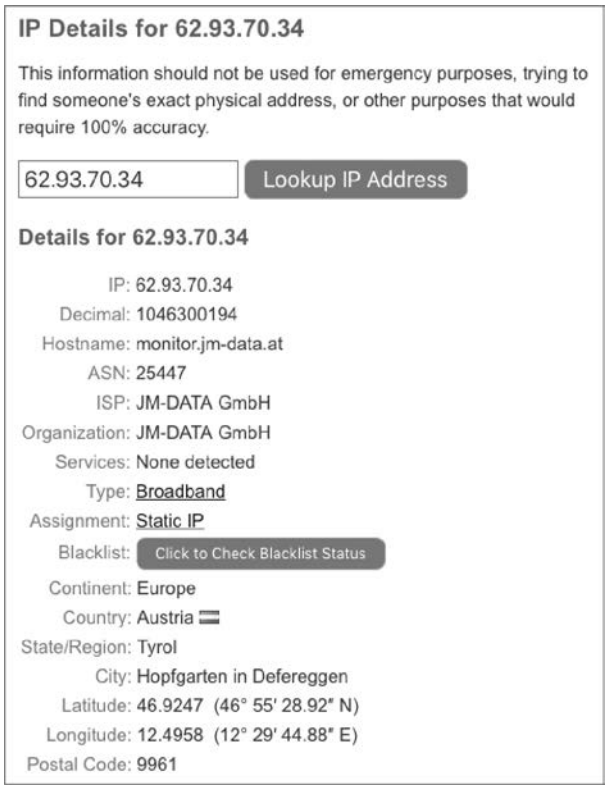
Rysunek 13.12

Jak się zapewne domyśliłeś, w maju 2015 r. artykuł zawierał jeszcze jednego członka o pseudonimie *CyPeRtRoN*. Czy nasz przyjaciel był rzeczywiście tak próżny, że celowo wpisał swoje imię do artykułu w Wikipedii? A co ważniejsze, czy ryzykował wprowadzenie tej zmiany z adresu IP innego niż VPN, żeby dodać wiarygodności swojej edycji?

Gdybyś zdążył zapomnieć: *próżność jest zawsze przed ostrożnością*. W serwisie *whatismyipaddress.com* można szybko uzyskać przybliżoną lokalizację adresu IP *62.93.70.34*, użytego do wprowadzenia zmiany w Wikipedii (rysunek 13.13).

Czy Cyper mógł być tak nieostrożny, aby dokonać edycji po prostu w swoim domu? Z prawnego punktu widzenia może nie jest to dowód, ale bardzo wiarygodny trop!

Uwaga **Więcej informacji potwierdzających, że Cyper znajdował się w Austrii lub sąsiednim kraju, znajdziesz w oficjalnym raporcie z dochodzenia w sprawie grupy The Dark Overlord.**



Rysunek 13.13

Podsumowanie

Ten rozdział był poświęcony poszukiwaniu ukrytych informacji rozrzuconych po zakamarkach internetu. Zostały opisane narzędzia theHarvester do wyszukiwania informacji na szeroką skalę oraz Gitrob do skanowania serwisu GitHub.

Przykłady przedstawione w tym rozdziale dobitnie pokazują, że w nawet najbardziej przypadkowych i niespodziewanych miejscach, takich jak fora, serwisy wklejkowe, repozytoria kodu i strony wiki, mogą znajdować się przełomowe dla dochodzenia wskazówki.

W następnym rozdziale jeszcze bardziej rozszerzymy obszar poszukiwań o publicznie dostępne bazy danych, takie jak MongoDB i Elasticsearch.

WYKRYTO CYBERATAK? CZAS NA POLOWANIE!

Korporacyjny system informatyczny musi być stale gotowy do obrony. Trzeba mieć strategię reagowania na incydenty bezpieczeństwa i zachować czujność. Cyberprzestępczość jest dziś stałym elementem środowiska biznesowego i jeśli nie chcesz narazić swojego przedsiębiorstwa na niepowetowane straty, musisz opracować solidny zestaw narzędzi umożliwiających obronę i tropienie cyberprzestępców. Mimo że w pewnych okolicznościach należy zaangażować organy ścigania, spora część dochodzenia w sprawie naruszenia bezpieczeństwa należy do organizacji.

Ta książka jest praktycznym kompendium przeznaczonym dla inżynierów bezpieczeństwa. Znajdziesz w niej opis najnowszych narzędzi, technik i zasobów. Poznasz sposoby badania źródeł niepożądanego ruchu sieciowego, wydobywania informacji z publicznie dostępnych zasobów internetowych i ścigania osób, które mogłyby wyrządzić szkodę organizacji. Dowiesz się, jak, począwszy od pojedynczego adresu IP, stopniowo zdobywać informacje potrzebne do wzmocnienia ochrony, zidentyfikowania i wytropienia hakerów. Opisana tu metodologia została zastosowana w śledztwie przeciwko członkom grupy cyberterrorystycznej. Przekonasz się, że dzięki użyciu łatwo dostępnych narzędzi można wytropić i zidentyfikować sprawców nawet wyjątkowo wyrafinowanych włamań do systemu!

W książce:

- najnowocześniejsze narzędzia do prowadzenia dochodzeń przeciw cyberprzestępcom
- techniki śledzenia niepożądanego ruchu sieciowego
- wyszukiwanie informacji wywiadowczych
- identyfikowanie potencjalnych sprawców dzięki powszechnie dostępnym informacjom
- budowa złożonych scenariuszy zaawansowanego wyszukiwania
- sztuczki i nieoczywiste techniki stosowane przez ekspertów

VINNY TROIA jest uznanym informatykiem śledczym, specjalizuje się w opracowywaniu strategii bezpieczeństwa i usuwaniu skutków jego naruszeń. Zdobył głęboką wiedzę na temat standardów bezpieczeństwa i kontroli zgodności z przepisami — doradza w tej dziedzinie podmiotom z różnych branż.

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl
KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-283-9205-2
9 788328 392052
Cena: 97,00 zł
WILEY