Sigurnosne prijetnje na Internetu

Metode deanonimizacije cyberkriminalaca kroz primjere

Leon Sattvik Kolenc, 11. 12. 2024.

Pregled predavanja

- Operacijska Sigurnost
- Harvardski student i prijetnje bombama
- Pompompurin
- Dread Pirate Roberts
- Pharoah
- Bayrob grupa

Pitanja za ispite

- Što je operacijska sigurnost?
- Kako je Harvard uhvatio studenta koji je slao terorističke prijetnje?
- Što je korelacijski napad u kontekstu Tor mreže?
- Kako je deanonimiziran Dread Pirate Roberts?
- Kako je deanonimiziran Pharoah, owner Incognito Marketa?

Motivacija

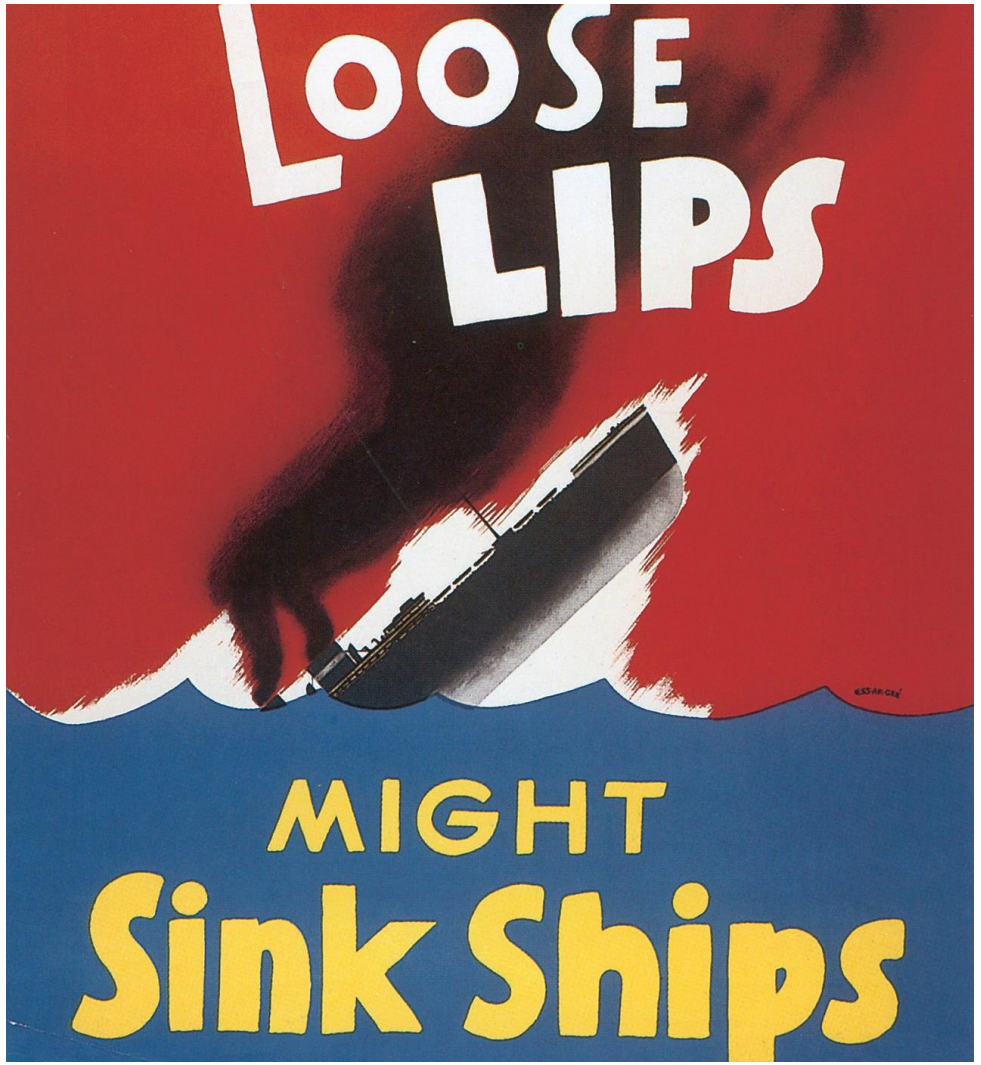
- Greške u očuvanju anonimnosti mogu biti vrlo korisne kada je u pitanju borba protiv cyberkriminala, no ako osoba čuva anonimnost iz legitimnih razloga poput novinarstva ili zviždanja može dovesti do loših posljedica
- Postoje rigorozni sustavi za očuvanje anonimnosti korisnika, no često se uspijeva pronaći način zaobilaženja tih sustava
- Dizanje svijesti o metodologiji deanonimizacije cyberkriminalaca te razmišljanje o potencijalnoj karijeri u tom konkretnom dijelu računalne sigurnosti

Operacijska Sigurnost (*OpSec*)

Izraz populariziran za vrijeme Vijetnamskog rata:

„Sposobnost očuvanja znanja o manama i vrlinama od neprijatelja”

- Danas je to **kontinuirani proces i strategija očuvanja kritičkih informacija i podataka u tajnosti**
- Može se koristiti u kontekstu anonimnosti no često se radi i o poslovnim tajnama



Slučaj 1: Harvardski student i prijetnje bombama

- Harvardske studentske novine su dobile prijetnju o postavljenim bombama po zgradama sveučilišta
- Počinitelj je koristio *Guerillamail* koji u header svakog maila doda *X-Originating-IP*
- IP prepoznat kao izlazni čvor TOR mreže

To: „HarvardMail@harvard.com”<Harvard@harvard.com>

From: e6e923eh-q++@guerillamail.com

Subject: Bomba

X-Originating-IP: [198.51.233.2]

Content-Type: text/plain; charset=„utf-8”

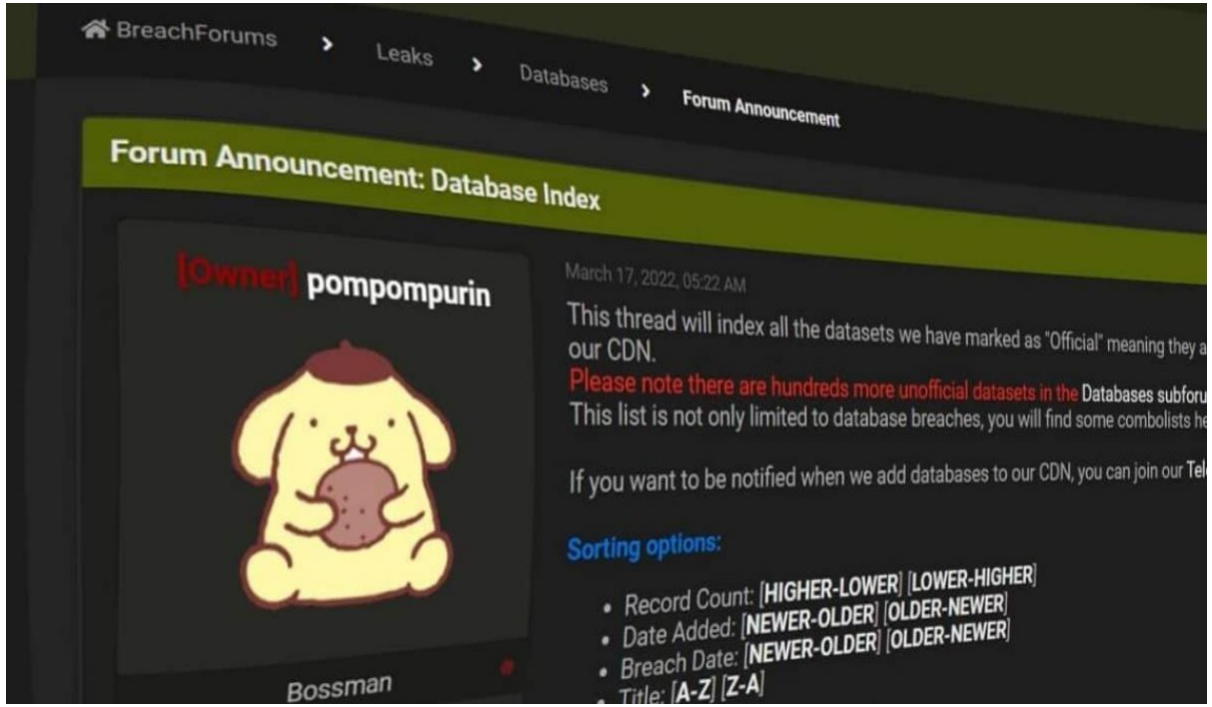
Slučaj 1: Harvardski student i prijetnje bombama (2)

- Svi ulazni i izlazni čvorovi Tor mreže su poznati
- Lako se pregleda je li itko koristio Tor na Harvardovoj mreži u tom trenutku -> Da!
- Promet povezan s Eldo Kimom, studentom koji je priznao na slanje prijetnji jer je htio izbjeći pisanje ispita

Korelacijski napad - **ISP Može analizirati prenošene podatke ovisno o vremenu i veličini i prepoznati uzorke te profilirati korisnike bez obzira na to što su podatci enkriptirani.**

Slučaj 2: Pompompurin

- Vlasnik „BreachForums”, najvećeg foruma za prodaju i razmjenu procurenih podataka
- Upravlja i posreduje novčane transakcije na forumu



Slučaj 2: Pompompurin (2)

- Type.ai, aplikacija za AI tipkovnicu je imala masivno curenje podataka, 31 milijun zapisa
- Email, ime i prezime, broj mobitela
- Pompompurin je otišao na haveibeenpwned.com i primijetio je da se njegov email nalazi u procurenoj bazi, no ne nalazi se u procurenoj bazi koja se prodaje na forumu

Slučaj 2: Pompompurin (3)

- Komunicira s vlasnikom *RaidForumsa,* sličnim forumom za dijeljenje podataka, *Omnipotent*om o tome i navodi svoj vlastiti e-mail kao primjer
- RaidForums je bio zaposjednut od strane FBI-a te su dobili pristup bazi podataka svih razgovora

[Quoting “Omnipotent”:]

What email did you look up and how?

[Quoting “pompompurin:]

Apologies for late reply, here is another email that I found to be present on HIBP, but not inside of the file provided on the thread (I don’t want to share my actual email for obvious reasons, but this email seems to have the same case as mine):
conorfitzpatrick02@gmail.com
https://a.pomf.cat/vvxevp.png (backup: https://archive.is/uYiTq)

To search the file, I used the command “grep -i 'conorfitzpatrick' aitype.txt”

Slučaj 2: Pompompurin (4, još grešaka!)

- Osim slanja svojeg e-maila, pristupao je svojem računu na *RaidForums*u sa vlastite IP adrese koja je bila registrirana na njegovog oca.
- FBI dobija pristup zapisima od Googla za njegov gmail račun, vidi se registracija za razne VPNove i Zoom račun po imenu „Pompompurin”

64. For instance, on or about March 7, 2022, records received from Google showed that the conorfitzpatrick2002@gmail.com Google account was accessed from IP address 89.187.181.117 on or about March 7, 2022. IP address 89.187.181.117 was owned by Datacamp Limited. However, a query of this IP address on Spur.us, in turn, revealed that this IP address was actually used by the VPN provider IVPN at the time. According to records from Zoom, this IP address was used the following day, on or about March 8, 2022, to log into a Zoom account under the name of "pompompurin" with an e-mail address of pompompurin@riseup.net. The

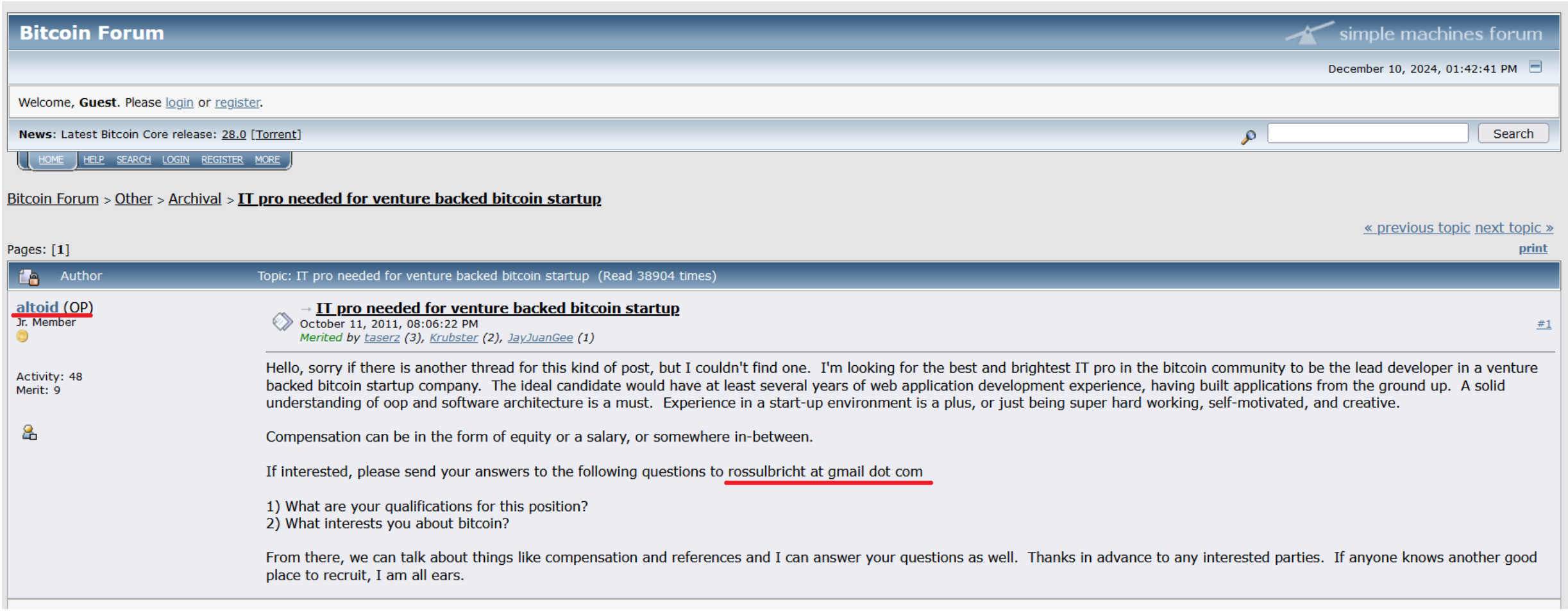
Slučaj 3: Dread Pirate Roberts i Silk Road

- Najpoznatiji slučaj raskrinkavanja anonimne osobe
- DPR je bio vlasnik Silk Roada, kompletno slobodnog tržišta gdje se moglo prodati i kupiti bilo što.
- Droga, ukradeni predmeti, lažne isprave, lažne diplome...
- Promet od 1.2 milijarde dolara

Slučaj 3: Dread Pirate Roberts i Silk Road (2)

- FBI traži najranije spominjanje *Silk Road*-a na internetu
- Korisnik po imenu *Altoid* oglašava Silk Road na stranici za uzgoj psihodeličnih gljiva

Slučaj 3: Dread Pirate Roberts i Silk Road (3)



Bitcoin Forum

simple machines forum

December 10, 2024, 01:42:41 PM

Welcome, **Guest**. Please login or register.

News: Latest Bitcoin Core release: 28.0 [Torrent]

Search

HOME HELP SEARCH LOGIN REGISTER MORE

Bitcoin Forum > Other > Archival > **IT pro needed for venture backed bitcoin startup**

« previous topic next topic »

Pages: [1]

print

Author | Topic: IT pro needed for venture backed bitcoin startup (Read 38904 times)

altoid (OP)
Jr. Member

Activity: 48
Merit: 9

IT pro needed for venture backed bitcoin startup
October 11, 2011, 08:06:22 PM
Merited by taserz (3), Krubster (2), JayJuanGee (1)

#1

Hello, sorry if there is another thread for this kind of post, but I couldn't find one. I'm looking for the best and brightest IT pro in the bitcoin community to be the lead developer in a venture backed bitcoin startup company. The ideal candidate would have at least several years of web application development experience, having built applications from the ground up. A solid understanding of oop and software architecture is a must. Experience in a start-up environment is a plus, or just being super hard working, self-motivated, and creative.

Compensation can be in the form of equity or a salary, or somewhere in-between.

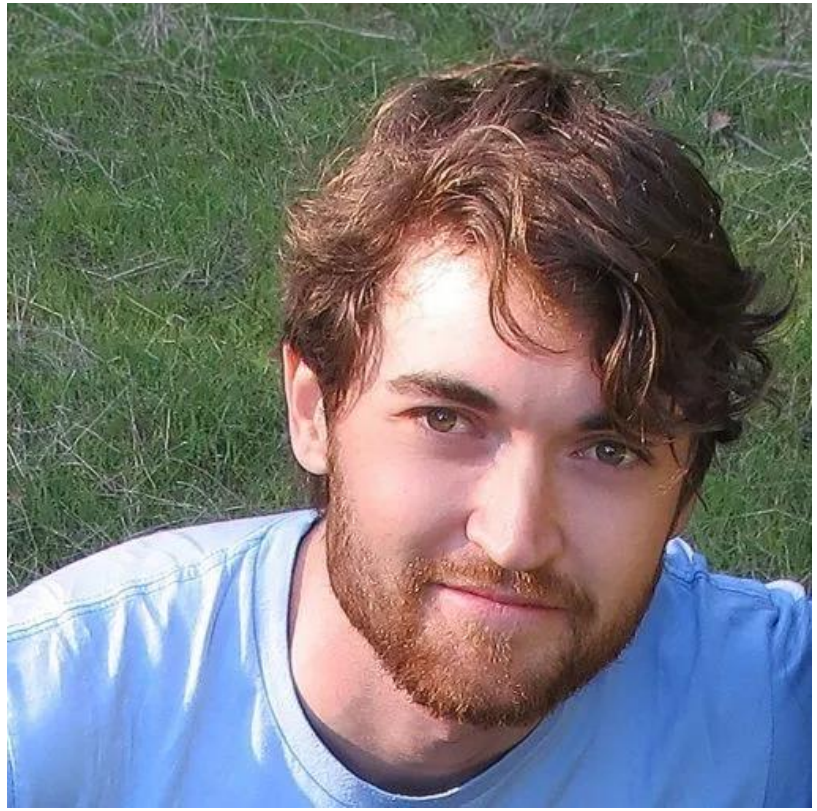
If interested, please send your answers to the following questions to rossulbricht at gmail dot com

1) What are your qualifications for this position?
2) What interests you about bitcoin?

From there, we can talk about things like compensation and references and I can answer your questions as well. Thanks in advance to any interested parties. If anyone knows another good place to recruit, I am all ears.

Slučaj 3: Dread Pirate Roberts i Silk Road (4)

- Nakon pronađenog imena, ostatak je bio jednostavan
- Pronađena je knjižnica koju je koristio za povezivanje na internet, te je organizirana sting operacija u kojoj mu je oduzet laptop na kojem je prijavljen



Slučaj 4: Pharoah

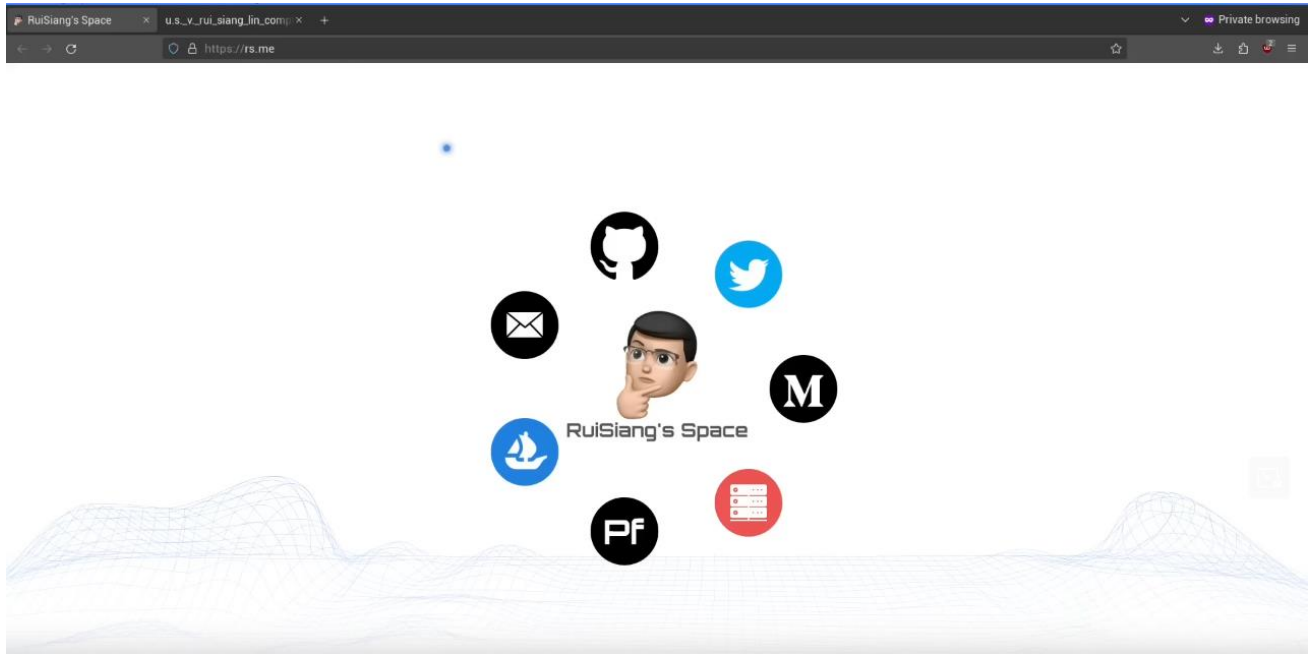
- Vlasnik *IncognitoMarket*-a, identični koncept stranici kao *Silk Road.*
- Preko 100 milijuna dolara prometa, administracija uzima 5% naknadu po transakciji
- Završio kao Exit scam, marketplace je samoinicijativno ugašen te su sva sredstva oduzeta od kupaca i prodavača

Slučaj 4: Pharoah (2)

- Odlučio je ucjenjivati bivše korisnike, prijeteći slanjem podataka marketplacea FBI-u, to mu je stvorilo mnogo neprijatelja
- Kao i kod ostalih slučajeva, FBI je vrlo tajnovit oko svojih akcija, no pretpostavlja se da su dobili anonimnu dojavu o strukturi poslužitelja te su na temelju dojave došli do sudskog naloga za rušenje i analizu poslužitelja

Slučaj 4: Pharoah (3)

- Prva greška Pharoah-a je bila registracija domene rs.me koristeći bitcoin sa IncognitoMarketa
- Preko toga je FBI dobio sudski nalog za nadziranje njegovog google računa
- FBI gasi njegove servere za prikupljanje podataka te vidi zanimljiv promet sa njegovog google računa



Slučaj 4: Pharoah (4)

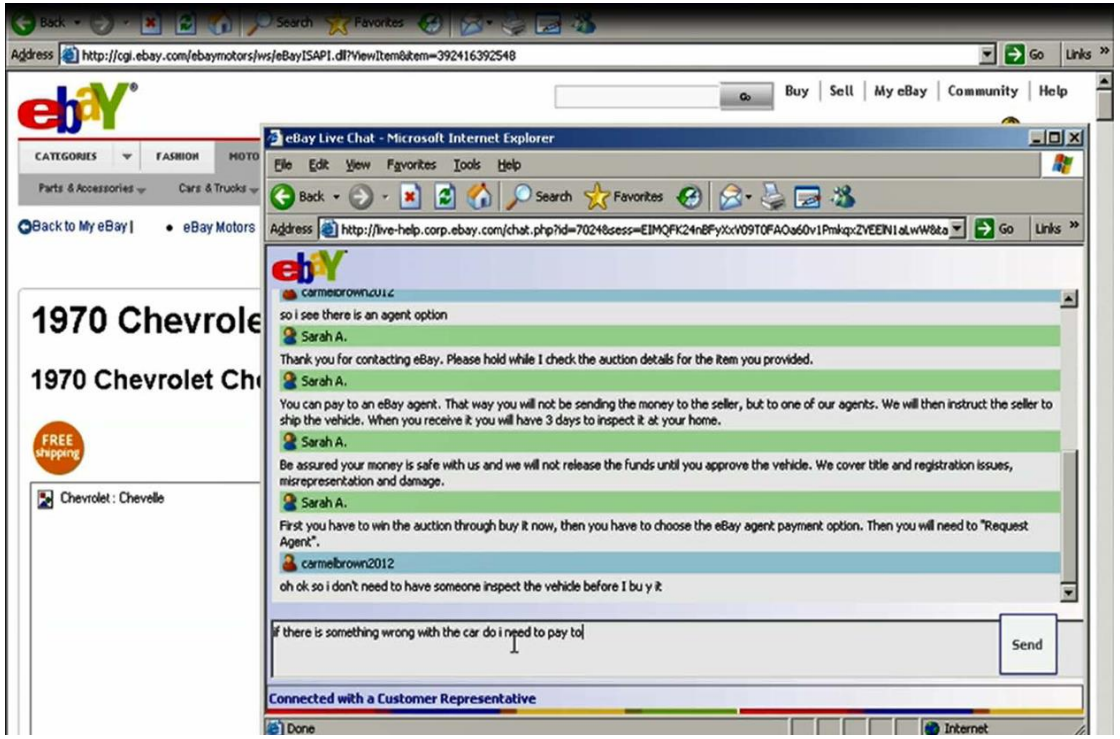
5. Troubleshooting an Offline Server

a. On or about July 19, 2022, pursuant to a judicially authorized warrant, the FBI imaged a server, which hosted Marketplace-1. To execute that search warrant, the FBI took the Marketplace-1 sever offline at approximately 23:30 UTC.

b. On or about July 20, 2022, at approximately 00:18 UTC, 00:19 UTC, 00:20 UTC, and 00:23 UTC, the user of the Lin Personal Email Account-1 searched Google for "pm2 crashed," "view pm2 daemon logs," "pm2 daemon logs," and "pm2 changelog," respectively.

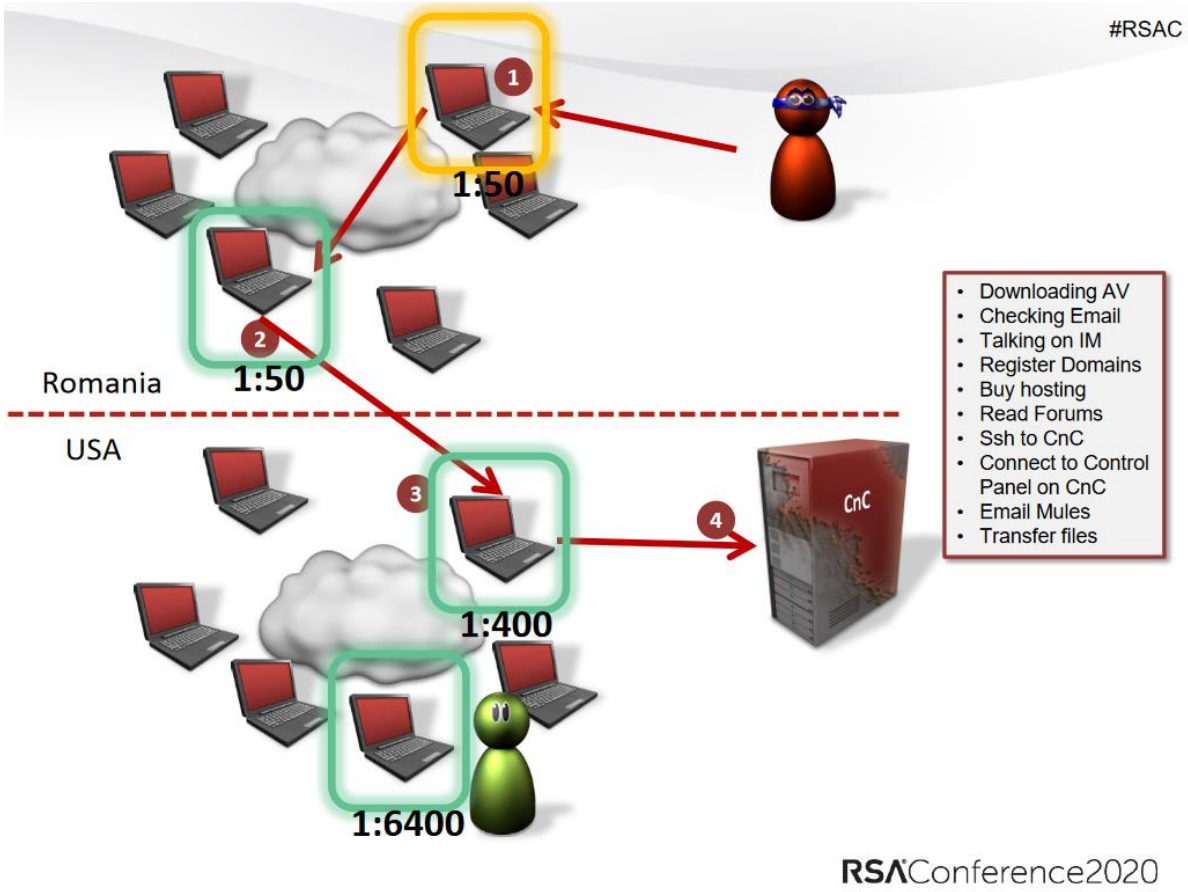
Slučaj 5: Bayrob Grupa

- Bili su najveći pošiljatelji neželjene pošte u više država u 2011
- Spam je distribuirao malware koji je imao više funkcionalnosti
- Glavni izvor prihoda su bili Ebay MITM napadi gdje bi ubrizgavali lažne aukcije i preuzimali novce od kupaca



Slučaj 5: Bayrob Grupa (2)

- Osim ubrizgavanja aukcija, malware je računalo pretvorio u čvor u P2P proxy mreži koju su koristili za komunikaciju sa C&C poslužiteljom u koju se naposljetku uključio i FBI sa svojim računalima.
- 400.000+ inficiranih računala



Slučaj 5: Bayrob Grupa (3)

- U 3 godine čekanja se napokon dogodila greška, upisane su krive vjerodajnice
- Zahtjev je poslan preko čvora koji je kontrolirao FBI i zapisan.

```
Connection 1 (TCP)

Start: 2013-05-13 14:27:05.085097 UTC
  End: 2013-05-13 14:28:36.109303 UTC

172.190.235.81:2935 -> 74.208.5.85:80 (15766 bytes)
74.208.5.85:80 -> 172.190.235.81:2935 (35935 bytes)

Referer: http://www.gmx.com/
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0;
InfoPath.2)
Host: www.gmx.com
Content-Length: 75
Connection: Keep-Alive
TextfieldEmail=raduspr&TextfieldPassword=[redacted]uttonLogin=1

Referer: http://www.gmx.com/
```

Slučaj 5: Bayrob Grupa (3)

- U 3 godine čekanja se napokon dogodila greška, upisane su krive vjerodajnice
- Zahtjev je poslan preko čvora koji je kontrolirao FBI i zapisan.

Connection 1 (TCP)

```
Start: 2013-05-13 14:27:05.085097 UTC
  End: 2013-05-13 14:28:36.109303 UTC

172.190.235.81:2935 -> 74.208.5.85:80 (15766 bytes)
74.208.5.85:80 -> 172.190.235.81:2935 (35935 bytes)

Referer: http://www.gmx.com/
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0;
InfoPath.2)
Host: www.gm
TextfieldEma l=minolta9797&TextfieldPassword=P          ttonLogin=1

Referer: http://www.gmx.com/
```

Slučaj 5: Bayrob Grupa (4)

- FBI je vrlo brzo pronašao identitet kriminalca guglanjem unesenog imena te ih je to dovelo do sudskih naloga za pretres poslužitelja i pada grupe.

Zaključak

- Koliko se god dobar sustav za anonimnost koristi, često dolazi do de-anonimizacije zbog ljudske greške.
- Za potpunu anonimnost je potrebno potpuno odvojiti osobni život od online aktivnosti.
- Ne koristiti Google!
- Potpuno izbjeći nezakonite radnje!

Literatura

Svi linkovi su zadnji put pristupljeni 11. 12. 2024.

- OpSec:

https://www.fortinet.com/resources/cyberglossary/operational-security

https://en.wikipedia.org/wiki/Operations_security#/media/File:Loose_lips_might_sink_ships.jpg

- Harvardski student:

DEF CON 22 - Adrian Crenshaw- Dropping Docs on Darknets: How People Got Caught, https://www.youtube.com/watch?v=eQ2OZKitRwc

https://www.defcon.org/images/defcon-22/dc-22-presentations/Crenshaw/DEFCON-22-Adrian-Crenshaw-Dropping-Docs-on-Darknets-How-People-Got-Caught-UPDATED.pdf

Harvard Student Charged With Making Hoax Bomb Threat, https://www.justice.gov/usao-ma/pr/harvard-student-charged-making-hoax-bomb-threat

- Pompompurin:

UNITED STATES OF AMERICA v. CONOR BRIAN FITZPATRICK, https://www.justice.gov/usao-edva/file/1300536/dl?inline

Owner of Breach Forums Pompompurin Arrested in New York, https://hackread.com/breach-forums-owner-pompompurin-arrested-new-york/

How Hacker PomPomPurin Got Caught (Bad OPSEC), https://www.youtube.com/watch?v=1fZWHeHICws

https://www.vecteezy.com/free-videos/typing-on-mobile

Literatura

Svi linkovi su zadnji put pristupljeni 11. 12. 2024.

- Dread Pirate Roberts:

DEF CON 22 - Adrian Crenshaw- Dropping Docs on Darknets: How People Got Caught , https://www.youtube.com/watch?v=eQ2OZKitRwc

https://www.defcon.org/images/defcon-22/dc-22-presentations/Crenshaw/DEFCON-22-Adrian-Crenshaw-Dropping-Docs-on-Darknets-How-People-Got-Caught-UPDATED.pdf

UNITED STATES V. ROSS ULBRICHT, https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/US%20v.%20Ross%20Ulbricht%20Indictment.pdf

- Pharoah:

UNITED STATES OF AMERICA v. RUI-SIANG LIN, https://www.justice.gov/opa/media/1352571/dl

Worlds Dumbest Darknet Admin Gets Busted , https://www.youtube.com/watch?v=EJAs9Nb-XE8

- Bayrob Grupa:

When Cybercriminals with Good OpSec Attack , https://www.youtube.com/watch?v=zXmZnU2GdVk

https://static.rainfocus.com/rsa/presentations/USA20/2020_USA20_ht-w09_01_when-cybercriminals-with-good-opsec-attack.pdf

Dodatna literatura

- Expert perspectives on the evolution of carders, cryptomarkets and operational security https://www.researchgate.net/profile/Gert-Jan-Van-Hardeveld/publication/326547940_Expert_perspectives_on_the_evolution_of_carders_cryptomarkets_and_operational_security/links/5b54be110f7e9b240ffb0e8c/Expert-perspectives-on-the-evolution-of-carders-cryptomarkets-and-operational-security.pdf
- GEOST BOTNET. THE STORY OF THE DISCOVERY OF A NEW ANDROID BANKING TROJAN FROM AN OPSEC ERROR, https://www.virusbulletin.com/uploads/pdf/magazine/2019/VB2019-Garcia-etal.pdf
- Researchers Say They Uncovered Uzbekistan Hacking Operations Due to Spectacularly Bad OPSEC, http://nosuchorganisation.khandossos.com/articles/85.pdf
- A Study on Blue Team's OPSEC Failure, https://essay.utwente.nl/84945/1/__ad.utwente.nl_Org_BA_Bibliotheek_Documentfiles_Afstudeerverslagen__Verwerkt_caretta_crichlow_MA_eemcs.pdf
- Behavioral analysis of cybercrime: Paving the way for effective policing strategies, ☆https://www.sciencedirect.com/science/article/pii/S2949791423000349#sec0045
- Black Hat 2013 - OPSEC Failures of Spies, https://www.youtube.com/watch?v=bM0PmwOlifE
- Following APT OpSec failures , https://www.youtube.com/watch?v=NFJqD-LcpIg
- DEF CON 29 Adversary Village - Marc Smeets - Exploiting Blue Team OPSEC Failures with RedELK , https://www.youtube.com/watch?v=_7LJUjzdgiY
- Bad Opsec - How Tor Users Got Caught , https://www.youtube.com/watch?v=GR_U0G-QGA0

Hvala!