SESSION ID: SEM-M03H

Feds Fighting Ransomware: How the FBI Investigates and How You Can Help

Joel DeCapua
Supervisory Special Agent
Federal Bureau of Investigation
@jedec0x0
Here’s a Unique Idea – A Presentation About Ransomware!

What will we learn today:

• What does the FBI do to combat ransomware?
• What tools the FBI uses to investigate the cyber?
• How can the security community join the fight?
How to Stop Ransomware Actors

• Lock them up
Five Arrested for Cerber, CTB-Locker Ransomware Spread

Authorities arrest three Romanian suspects for spreading CTB-Locker malware and two for a ransomware case linked to the United States.

Romanian authorities have arrested three suspects for spreading a form of ransomware called Curve-Tor-Bitcoin Locker (CTB-Locker) throughout Europe. Two members of the same criminal group have been arrested for distributing Cerber ransomware within the United States.

An investigation into CTB-Locker began in early 2017, when authorities were alerted to Romanian nationals sending spam messages designed to look like they came from Italy, the Netherlands, and the UK. The messages infected systems and encrypted data with CTB-Locker ransomware, which targets almost all versions of Windows including XP, Vista, 7, and 8.
Zain Qaiser was sentenced in connection with ransomware scheme. (Source: U.K.'s National Crime Agency)

A 24-year-old man living in England has been sentenced to more than six years in prison for his role in a ransomware scheme that targeted millions of computers across 20 countries, the U.K.'s National Crime Agency announced Tuesday.
Microsoft Worker From FIU Gets Jail Time for Fake FBI Ransomware Attacks

Jerry Iannelli  |  August 14, 2018  |  8:00AM

Raymond Odigie Uadiaile, age 41, is great with computers. Good enough to be hired by Microsoft as a network engineer. And good enough, according to the feds, to run a virus scamming ring that froze computers via a fake warning from the Federal Bureau of Investigation, charged people a $200 "fine" to unlock their laptops, and warned users they might be sent to prison if they didn't pay up.

Instead, it's Uadiaile who's going to jail. Federal prosecutors announced
How to Stop Ransomware Actors

• Lock them up
• Take their stuff
U.S. Treasury Sanctions Bitcoin Wallets For First Time

December 05, 2018, 08:59:44 AM EDT By Safehaven

Last week, the U.S. Treasury Department of Foreign Assets Control (OFAC) targeted two bitcoin addresses, announcing that the wallets associated Iranian citizens Ali Khorashadizadeh and Mohammad Ghorbaniyan had been added to the Specially Designated Nationals sanctions list.

The sanctions, which are the first of their kind, are part of a wider move to track and restrict movements in the digital space involving money laundering and cybercrime.

Additionally, the OFAC noted that the agency would be looking into exchanges who facilitated
How to Stop Ransomware Actors

• Lock them up
• Take their stuff
• Break their things
FBI Releases Master Decryption Keys for GandCrab Ransomware

By Lawrence Abrams

July 16, 2019 06:35 AM 2

In an FBI Flash Alert, the FBI has released the master decryption keys for the Gandcrab Ransomware versions 4, 5, 5.0.4, 5.1, and 5.2. Using these keys, any individual or organization can create and release their very own GandCrab decryptor.
How to Stop Ransomware Actors

• Lock them up
• Take their stuff
• Break their things
• Call them out
SAMSAM SUBJECTS
Conspiracy to Commit Fraud and Related Activity in Connection with Computers; Conspiracy to Commit Wire Fraud; Intentional Damage to a Protected Computer; Transmitting a Demand in Relation to Damaging a Protected Computer

Mohammad Mehdi Shah Mansouri
Faramarz Shahi Savandi
Evgeniy Mikhailovich Bogachev

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

The F.B.I.’s wanted poster for America’s most wanted hacker, Evgeniy M. Bogachev, was a trove of information. F.B.I.
How to Stop Ransomware Actors

• Lock them up
• Take their stuff
• Break their things
• Call them out
• Make crime hard
Tracking Ransomware End-to-end

Danny Yuxing Huang1, Maxwell Mathias Alliopoulou2, Victor Gao Li1
Luca Invernizzi1, Kyle McFetridge3, Elle Bursztein1, Jonathan Levin1
Kirill Lechovetsko1, Alex C. Snoeren4, Damon McCoy1

1Princeton University 2New York University 3University of California, San Diego 4Google Inc 5Chainsalysis

ABSTRACT—Ransomware is a type of malware that encrypts the files of infected systems and demands a ransom payment, often in a cryptocurrency such as Bitcoin. In this paper, we create a measurement framework to study ransomware payments, victims, and operators. By combining a dataset of data sources, including ransomware binaries, seed ransom payments, victim telemetry from Tripwire, and a large database of Bitcoin addresses associated with them, we outline the timeline of this ransomware campaign and its associated third-party services. In particular, we trace the financial transactions, from the moment victims acquire bitcoins, to when ransomware operators could be paid. We also show ransomware operators cashed out using BTC-1, a now-defunct bitcoin exchange. In total we are able to identify 10,846 likely ransom payments made by 19,750 potential victims over a two-year period. While this study focuses on ransomware, our methods are potentially applicable to other cybercriminal operations that have similarly adopted Bitcoin as their currency.

I. INTRODUCTION

Ransomware is a type of malware that encrypts a victim’s documents and media, and then forces them to pay ransoms for their release. In its beginnings, ransoms were demanded via a collection of online cash-equivalent payment mechanisms, such as MoneyPak, PaySafeCard, or Ukash [1]. From the ransomware family of malware, these instruments have developed into untraceable and secure instruments for financial transactions; their development has outstripped the legal and jurisdictional limitations of major financial institutions. However, all transactions are irretrievable, and it is widely available for victims to purchase. Due to these properties, Bitcoin has also gained adoption as a payment method for other illicit activities, such as drug markets [2], online sex ads [3], and DDoS-for-hire services [4].

However, Bitcoin has a property that is undesirable to cybercriminals: all transactions are public by design. This enables researchers, through transaction clustering and tracing [5], [6], [7], to glean at the financial inner workings of myriad cybercriminal operations. Before Bitcoin, these insights had to be only pieced and infrequent, as they hinged on sporadic data leaks [8], [9], [10].

In this paper, we perform a large-scale, two-year measurement-study of ransomware payments, victims, and operators. While prior studies have estimated the success of a single ransomware campaign [6] or reverse engineered the technical inner workings of a particular ransomware family [11], this work is the first to perform an end-to-end analysis of a large portion of the ransomware ecosystem, including its revenue, affiliate schemes, and third-party support services. To do so, we combine multiple data sources, including labeled ransomware binaries, victim telemetry, and Bitcoin addresses associated with them (provided by Chainsalysis). This wealth of data allows us to follow the money trail from the moment a victim acquires bitcoins, to when the ransomware operators cash them out. In total, we establish a lower-bound estimate on ransom payments’ volume of $16 million USD, made by 19,750 potential victims over two years.

In this section, we describe the timeline of the archived ransomware infection, from malware delivery to ransoms cashed out.

I. BACKGROUND

Delivery: Ransomware is distributed through a variety of vectors, including malware-infected webpage links, malicious email attachments, and social engineering. Certo and Locky were both spread via malicious email attachments [12], [13], while Kama mainly relied on pay-per-click networks populated by ad networks such as WannaCry and Net Flynn, exploiting known vulnerabilities in network services to propagate.

Execution: Once a ransomware binary executes on a host, it silently encrypts a set of files (files deemed valuable to the user, such as documents and images. When the encryption completes, the ransomware displays a ransom note on the host’s screen, informing the user that their files are held for ransom, payable in bitcoins. Payments: A ransom note usually includes a guide on how to purchase bitcoins from exchanges, online services that facilitate the conversion between bitcoins and fiat currencies. Exchanges come in different flavors: they can only operate globally (e.g., Poloniex), or regionally (e.g., Cointab, which can only trade to a U.S. citizen). Most are centralized, except for a handful of decentralized exchanges (e.g., LocalBitcoins). Ransomware notes include either random addresses, Bitcoin wallets’ addresses are expected to pay into, or a link to a payment website which displays this address. Many random addresses (e.g., Locky and Certo) generate a unique random address for each ransom note, allowing the user to confirm that the address is valid. Unlike traditional viruses, ransomware authors cannot discern information about victims; they only require the victim to seed these payments into the bitcoin system, which they do not control.

In summary, our main contributions are as follows. (1) We develop a set of methodologies that enable an end-to-end analysis of Bitcoin transactions. (2) We perform a two-year measurement study of the ecosystem, conservatively estimating that ransomware operators have collected over $16 million USD in ransoms from 19,750 potential victims. (3) We discuss possible intervention points, open challenges in ransomware research, and unique ethical issues specific to ransomware research.

I. BACKGROUND

In this section, we describe the timeline of the archived ransomware infection, from malware delivery to ransoms cashed out.

Delivery: Ransomware is distributed through a variety of vectors, including malware-infected webpage links, malicious email attachments, and social engineering. Certo and Locky were both spread via malicious email attachments [12], [13], while Kama mainly relied on pay-per-click networks populated by ad networks such as WannaCry and Net Flynn, exploiting known vulnerabilities in network services to propagate.

Execution: Once a ransomware binary executes on a host, it silently encrypts a set of files (files deemed valuable to the user, such as documents and images. When the encryption completes, the ransomware displays a ransom note on the host’s screen, informing the user that their files are held for ransom, payable in bitcoins. Payments: A ransom note usually includes a guide on how to purchase bitcoins from exchanges, online services that facilitate the conversion between bitcoins and fiat currencies. Exchanges come in different flavors: they can only operate globally (e.g., Poloniex), or regionally (e.g., Cointab, which can only trade to a U.S. citizen). Most are centralized, except for a handful of decentralized exchanges (e.g., LocalBitcoins). Ransomware notes include either random addresses, Bitcoin wallets’ addresses are expected to pay into, or a link to a payment website which displays this address. Many random addresses (e.g., Locky and Certo) generate a unique random address for each ransom note, allowing the user to confirm that the address is valid. Unlike traditional viruses, ransomware authors cannot discern information about victims; they only require the victim to seed these payments into the bitcoin system, which they do not control.

In summary, our main contributions are as follows. (1) We develop a set of methodologies that enable an end-to-end analysis of Bitcoin transactions. (2) We perform a two-year measurement study of the ecosystem, conservatively estimating that ransomware operators have collected over $16 million USD in ransoms from 19,750 potential victims. (3) We discuss possible intervention points, open challenges in ransomware research, and unique ethical issues specific to ransomware research.

I. BACKGROUND

In this section, we describe the timeline of the archived ransomware infection, from malware delivery to ransoms cashed out.

Delivery: Ransomware is distributed through a variety of vectors, including malware-infected webpage links, malicious email attachments, and social engineering. Certo and Locky were both spread via malicious email attachments [12], [13], while Kama mainly relied on pay-per-click networks populated by ad networks such as WannaCry and Net Flynn, exploiting known vulnerabilities in network services to propagate.

Execution: Once a ransomware binary executes on a host, it silently encrypts a set of files (files deemed valuable to the user, such as documents and images. When the encryption completes, the ransomware displays a ransom note on the host’s screen, informing the user that their files are held for ransom, payable in bitcoins. Payments: A ransom note usually includes a guide on how to purchase bitcoins from exchanges, online services that facilitate the conversion between bitcoins and fiat currencies. Exchanges come in different flavors: they can only operate globally (e.g., Poloniex), or regionally (e.g., Cointab, which can only trade to a U.S. citizen). Most are centralized, except for a handful of decentralized exchanges (e.g., LocalBitcoins). Ransomware notes include either random addresses, Bitcoin wallets’ addresses are expected to pay into, or a link to a payment website which displays this address. Many random addresses (e.g., Locky and Certo) generate a unique random address for each ransom note, allowing the user to confirm that the address is valid. Unlike traditional viruses, ransomware authors cannot discern information about victims; they only require the victim to seed these payments into the bitcoin system, which they do not control.

In summary, our main contributions are as follows. (1) We develop a set of methodologies that enable an end-to-end analysis of Bitcoin transactions. (2) We perform a two-year measurement study of the ecosystem, conservatively estimating that ransomware operators have collected over $16 million USD in ransoms from 19,750 potential victims. (3) We discuss possible intervention points, open challenges in ransomware research, and unique ethical issues specific to ransomware research.

I. BACKGROUND

In this section, we describe the timeline of the archived ransomware infection, from malware delivery to ransoms cashed out.

Delivery: Ransomware is distributed through a variety of vectors, including malware-infected webpage links, malicious email attachments, and social engineering. Certo and Locky were both spread via malicious email attachments [12], [13], while Kama mainly relied on pay-per-click networks populated by ad networks such as WannaCry and Net Flynn, exploiting known vulnerabilities in network services to propagate.

Execution: Once a ransomware binary executes on a host, it silently encrypts a set of files (files deemed valuable to the user, such as documents and images. When the encryption completes, the ransomware displays a ransom note on the host’s screen, informing the user that their files are held for ransom, payable in bitcoins. Payments: A ransom note usually includes a guide on how to purchase bitcoins from exchanges, online services that facilitate the conversion between bitcoins and fiat currencies. Exchanges come in different flavors: they can only operate globally (e.g., Poloniex), or regionally (e.g., Cointab, which can only trade to a U.S. citizen). Most are centralized, except for a handful of decentralized exchanges (e.g., LocalBitcoins). Ransomware notes include either random addresses, Bitcoin wallets’ addresses are expected to pay into, or a link to a payment website which displays this address. Many random addresses (e.g., Locky and Certo) generate a unique random address for each ransom note, allowing the user to confirm that the address is valid. Unlike traditional viruses, ransomware authors cannot discern information about victims; they only require the victim to seed these payments into the bitcoin system, which they do not control.
95% traced ransoms cashed out via BTC-E

Cashout list available on request
Photographer: Sakis Mitrolidis/AFP via Getty Images
Hacker gets a whopping 14 years in prison for running Scan4You service

Ruslan Bondars run a "VirusTotal-for-crooks" operation from 2009 to 2017.

By Catalin Cimpanu for Zero Day | September 22, 2018 -- 08:10 GMT (01:10 PDT) | Topic: Security
Federal Authorities Close Dark Website ‘xDedic Marketplace’

An investigation run out of the federal prosecutor’s office in Tampa, Fla, resulted in the dark Web marketplace being shut down. The site sold access to identity information and hacked servers among other things.

BY GRAHAM BRINK, TAMPA BAY TIMES / JANUARY 31, 2019
Interlude:
Some New Ransomware Data
How much ransom proceeds have been paid?

$144.35 million

- Date range 10/01/2013 to 11/07/2019
- Bitcoin only
- Does not quantify loss or total cost of incident
### Which variants raised the most money?

<table>
<thead>
<tr>
<th>Variant</th>
<th>Approx. Dates of Activity</th>
<th>Amount ($ millions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ryuk</td>
<td>02/09/2018 - 10/15/2019</td>
<td>61.26</td>
</tr>
<tr>
<td>Crysis/Dharma</td>
<td>11/14/2016 - 11/07/2019</td>
<td>24.48</td>
</tr>
<tr>
<td>Bitpaymer</td>
<td>10/21/2017 - 08/09/2019</td>
<td>8.04</td>
</tr>
<tr>
<td>SamSam</td>
<td>01/14/2016 - 11/20/2018</td>
<td>6.85</td>
</tr>
<tr>
<td>Sodinokibi</td>
<td>05/18/2019 - 10/05/2019</td>
<td>6.63</td>
</tr>
<tr>
<td>IEncrypt</td>
<td>12/20/2018 - 09/27/2019</td>
<td>6.05</td>
</tr>
<tr>
<td>Phobos</td>
<td>04/16/2018 - 11/07/2019</td>
<td>5.30</td>
</tr>
<tr>
<td>Defray777</td>
<td>12/05/2018 - 09/30/2019</td>
<td>5.25</td>
</tr>
<tr>
<td>Mamba</td>
<td>08/09/2016 - 10/16/2019</td>
<td>3.10</td>
</tr>
<tr>
<td>Rapid</td>
<td>04/22/2017 - 11/05/2019</td>
<td>2.45</td>
</tr>
<tr>
<td>Aleta</td>
<td>06/04/2017 - 11/25/2017</td>
<td>.64</td>
</tr>
<tr>
<td>Mrdec</td>
<td>01/30/2019 - 10/30/2019</td>
<td>.40</td>
</tr>
<tr>
<td>GandCrab</td>
<td>06/08/2018 - 06/10/2019</td>
<td>.33</td>
</tr>
<tr>
<td>All Others</td>
<td>10/01/2013 - 11/07/2019</td>
<td>15.56</td>
</tr>
</tbody>
</table>

**Total:** 144.35
### Where did Ransomware proceeds go?

<table>
<thead>
<tr>
<th>Wallet</th>
<th>Amount ($ millions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchanges</td>
<td>63.65</td>
</tr>
<tr>
<td>Unspent Bitcoin</td>
<td>36.91</td>
</tr>
<tr>
<td>Unknown</td>
<td>22.82</td>
</tr>
<tr>
<td>Tracked to Self</td>
<td>8.35</td>
</tr>
<tr>
<td>Mixers</td>
<td>7.20</td>
</tr>
<tr>
<td>Merchant Services</td>
<td>2.21</td>
</tr>
<tr>
<td>Darknet Markets</td>
<td>.83</td>
</tr>
<tr>
<td>Gambling</td>
<td>.73</td>
</tr>
<tr>
<td>Not Tracked</td>
<td>.55</td>
</tr>
<tr>
<td>Sanctioned Wallets</td>
<td>.42</td>
</tr>
<tr>
<td>Mining Pools</td>
<td>.34</td>
</tr>
<tr>
<td>Hosted Wallets</td>
<td>.17</td>
</tr>
<tr>
<td>Fees</td>
<td>.07</td>
</tr>
<tr>
<td>Other Ransomware Scams</td>
<td>.07</td>
</tr>
<tr>
<td>Scams</td>
<td>.02</td>
</tr>
<tr>
<td>Other</td>
<td>.01</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>144.35</strong></td>
</tr>
</tbody>
</table>
## Exchanges That Received Ransomware Proceeds

<table>
<thead>
<tr>
<th>Exchange</th>
<th>Total($)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>19,000,476</td>
</tr>
<tr>
<td></td>
<td>18,856,173</td>
</tr>
<tr>
<td></td>
<td>8,384,355</td>
</tr>
<tr>
<td></td>
<td>5,279,807</td>
</tr>
<tr>
<td>BTC-e.com</td>
<td>1,324,429</td>
</tr>
<tr>
<td>All Others</td>
<td>10,809,385</td>
</tr>
</tbody>
</table>
Obligatory Slide on How to Protect Yourself from Ransomware

- RDP is still by far the primary vector
- Patch all the things – especially OSes (and quickly!)
- Do the thing with the PWs
- Monitor your network
  - You will not prevent the intrusion
  - But you can detect the lateral movement
- Have a plan (and a backup!)
The FBI’s Ransomware Investigations

- 49 Ransomware Cases
  - 26 different Field Offices
  - One “case agent” per case

Case Agents
+ Prosecutors
+ Support Personnel
= Case Team
The FBI’s Ransomware Investigations

- The “Field” Model
  - SamSam --> Newark
  - CryptoLocker --> Washington
  - Ryuk --> Anchorage/Portland
  - BitPaymer --> Detroit/Dallas
  - Crysis/Dharma --> Jackson
What are the FBI’s Challenges

- Turnkey Ransomware
Приватная партнёрская программа по криптолокеру

By UNKN, July 4, 2019 in [Software] - malware, exploits, bundles, crypts

UNKN

byte

Posted July 4, 2019

В связи с тем, что расширяем активность приглашаем адвертс по:

- Спаму;
- Дедикам и сетям;
- Дорвейному трафику и иному живому;

Работаем в приватном режиме. Количество мест ограничено.
Готовьтесь пройти собеседование и показать свои доказательства качества инсталл. Мы не тестовая площадка и "обучающимся" и "я попробую/я постараюсь" тут делать нечего. Работаем не первый год, в теме больше 5 лет.
Софт полностью работоспособен и готов к работе.

Отрывок из правил:

1. Запрещено работать по СНГ (Украина в том числе);
2. Стартовый рейт от 60% в Вашу сторону. После первых 3 выплат - 70%.

Краткое описание софта: приватный ransomware, написанный на чистом С, с использованием inline-assembler с возможностью модификации функционала "из коробки" по бизнес модели RaaS.
Софт имеет статистику, страницу оплаты и "пробные расшифровщики" на странице оплаты. Никаких школьных эмейлов. Более подробную информацию можно получить при собеседовании.
Первый контакт в ПМ.
Private Crypto Locker Affiliate Program

By UNKN, July 4, 2019 in [Software] - malware, exploits, bundles, crypts

Posted July 4, 2019

Due to the fact that we are expanding activity, we invite adverts by:

- Spam;
- Dedikam and networks;
- Doorway traffic and other living things;

We work in a private mode. Limited number of seats.
Get ready for an interview and show your evidence of the quality of the installations. We are not a test site and there are nothing for "learners" and "I will try / I will try". We have been working for several years, the topic is more than 5 years.
The software is fully operational and ready to go.

Excerpt from the rules:

1. It is forbidden to work in the CIS (including Ukraine);
2. Starting rate from 60% in your direction. After the first 3 payments - 70%.

Short description of the software: private ransomware written in pure C, using inline-assembler with the possibility of modifying functionality "out of the box" according to the RaaS business model.
The software has statistics, a payment page and "trial decoders" on the payment page. No school emails. More information can be obtained during the interview.
The first contact in the PM.
Приглашаем к сотрудничеству!
ДЛЯ ВАС РАЗРАБОТАН АВТОМАТИЗИРОВАННЫЙ КОМПЛЕКС ПО ДОБЫЧЕ И ОБРАБОТКЕ DEDICATED SERVER!
Криптотолкогер(https://prntscr.com/q2v81a) + Панель обработки + Панель сканирования + Ботнет брут!
контакты для заявок
1 jabber supp01@jabberx.biz
2 jabber supp08@xmpp.jp
3 jabber supp17@exploit.im
4 email supp37@cock.li
(для новых партнёров выдаем только билд и декриптер, после 3х оплат от вас выдаем панель и инструменты) защита от школоты и АВ контор и тд...
Что вы можете с панелью?
1) построение ботнета брут (основан на NL) http://prntscr.com/q2v3r9
2) удобная обработка дедиков (если нужны инструменты предоставляем) http://prntscr.com/q2v211 http://prntscr.com/q2v2xx http://prntscr.com/q2v3gt
3) автоматический масскан (управление с панели) http://prntscr.com/prfiwq
4) чат в торе с клиентами http://prntscr.com/q2v570
5) автодеш тестов и получение полного ключа для клиента
так же есть возможность автоматизации Z668 брут + рекогнайзер и многое другое

ГЛАВНОЕ УСЛОВИЕ ПРЕДОСТАВЛЕНИЯ ПАНЕЛИ:!!!
Работа только нашим билдом криптотолкогера!
РАБОТА ПО РБ И СНГ ЗАПРЕЩЕНА!
ЦЕНА ВОПРОСА обговаривается с каждым партнёром лично, всё зависит от кол ва времени работы с партнёром и его профита
We invite you to cooperation!
THE AUTOMATED COMPLEX FOR MINING AND PROCESSING DEDICATED SERVER IS DEVELOPED FOR YOU!
Crypto-locker (https://prnt.sc/q2v81a) + Processing Panel + Scan Panel + Botnet Brute!

contacts for applications
1 jabber supp01@jabberx.biz
2 jabber supp08@xmpp.jp
3 jabber supp17@exploit.im
4 email supp37@cock.li

(for new partners we give out only a build and a decryptor, after 3 payments we give out a panel and tools) protection against shkoloty and AV offices, etc. ...

What can you do with the panel?
1) building a brute botnet (based on NL) http://prntscr.com/q2v3r9
2) convenient handling of deda (if we need tools we provide) http://prntscr.com/q2v211 http://prntscr.com/q2v2xx http: //prntscr.com/q2v3gt
3) automatic maskcan (control from the panel) http://prntscr.com/prflwq
4) chat in the torus with clients http://prntscr.com/q2v570
5) autodesk tests and get the full key for the client
there is also the possibility of automation z668 brut + recognizer and much more

MAIN CONDITION OF PROVIDING A PANEL !!!
Work only with our crypto locker build!
WORK IN RUSSIA AND CIS IS FORBIDDEN!
QUESTION PRICE is negotiated with each partner personally, it all depends on how many times you work with the partner and his profit

Edited December 19, 2019 by ghostinweb
What are the FBI’s Challenges

- Turnkey Ransomware
- Easy to Buy Access to Victims
Rdp

- Click on check button before buy any RDP to know if it's work or not.
- There is 898 RDP Available.

<table>
<thead>
<tr>
<th>Location</th>
<th>Hosting</th>
<th>Source</th>
<th>Ram</th>
<th>Windows</th>
<th>Access</th>
<th>Price</th>
<th>Seller</th>
<th>Check</th>
<th>Buy</th>
<th>Date Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>GB - England - London</td>
<td>Amazon Data Services UK</td>
<td>created</td>
<td>1 GB</td>
<td>Win Server 2012</td>
<td>Admin</td>
<td>3.50</td>
<td>seller15</td>
<td>Check</td>
<td>Buy</td>
<td>2019-12-13 18:58:19</td>
</tr>
<tr>
<td>US - Virginia - Ashburn</td>
<td>Amazon Technologies Inc.</td>
<td>created</td>
<td>512 MB</td>
<td>Win Server 2012</td>
<td>Admin</td>
<td>1.00</td>
<td>seller72</td>
<td>Check</td>
<td>Buy</td>
<td>2020-01-02 10:06:30</td>
</tr>
<tr>
<td>IE - Leinster - Dublin</td>
<td>Amazon Technologies Inc.</td>
<td>created</td>
<td>1 GB</td>
<td>Win Server 2012</td>
<td>Admin</td>
<td>3.00</td>
<td>seller29</td>
<td>Check</td>
<td>Buy</td>
<td>2020-01-07 15:02:32</td>
</tr>
<tr>
<td>GB - England - Purfleet</td>
<td>OVH Ltd</td>
<td>created</td>
<td>15 GB</td>
<td>Win Server 2012</td>
<td>Admin</td>
<td>10.00</td>
<td>seller64</td>
<td>Check</td>
<td>Buy</td>
<td>2019-12-22 22:47:08</td>
</tr>
<tr>
<td>IN - Karnataka - Bengaluru</td>
<td>DigitalOcean, LLC</td>
<td>created</td>
<td>16 GB</td>
<td>Win Server 2016</td>
<td>Admin</td>
<td>10.00</td>
<td>seller90</td>
<td>Check</td>
<td>Buy</td>
<td>2019-12-19 16:58</td>
</tr>
<tr>
<td>DE - Hesse - Frankfurt am Main (Innenstadt III)</td>
<td>Vultr Holdings LLC Frankfurt</td>
<td>created</td>
<td>4 GB</td>
<td>Win Server 2012</td>
<td>Admin</td>
<td>3.00</td>
<td>seller32</td>
<td>Check</td>
<td>Buy</td>
<td>2020-01-05 21:05:43</td>
</tr>
<tr>
<td>DE - North Rhine-Westphalia - Düsseldorf</td>
<td>myLoc managed IT AG</td>
<td>created</td>
<td>16 GB</td>
<td>Win Server 2019</td>
<td>Admin</td>
<td>13.00</td>
<td>seller55</td>
<td>Check</td>
<td>Buy</td>
<td>2020-01-06 12:37:02</td>
</tr>
<tr>
<td>DE - Hesse - Frankfurt am Main</td>
<td>A100 ROW GmbH</td>
<td>created</td>
<td>5 GB</td>
<td>Win Server 2012</td>
<td>Admin</td>
<td>5.00</td>
<td>seller46</td>
<td>Check</td>
<td>Buy</td>
<td>2020-01-02 21:51:46</td>
</tr>
<tr>
<td>FR - Île-de-France - Paris</td>
<td>Amazon Data Services France</td>
<td>created</td>
<td>5 GB</td>
<td>Win Server 2012</td>
<td>Admin</td>
<td>5.00</td>
<td>seller46</td>
<td>Check</td>
<td>Buy</td>
<td>2020-01-02 21:51:58</td>
</tr>
</tbody>
</table>
Скупаем дедики (RDP) под крипт
Условия:
1) Информация от 100р
2) Права админ
3) ТОП страны $25, Китай $15, бедные страны $12
4) Не криптованные, без локеров
5) Не амазон
6) Валидные
7) Оплата по факту выполнения работы
8) Оплата в Бtc
9) Оплата каждый день
10) Моментальные отчеты
11) Свой телеграм бот и площадка в торе

У нас самый удобный, ориентированный на легкость сервис 😎
Наша платформа позволяет не ждать часами когда вам ответит скупщик.
Вы в любое время суток можете отправить свой сервер и сразу же после проверки получите отчет по нему.
Заливаете свой список дедиков в нашу прогу (либо на нашем сайте, либо через телеграм бота),
после крипта оплачиваем на ваш БТС кошелек $.

Так же есть возможность в любой момент корректировать пароль и другие данные от дедика,
если обнаружилась какая-либо ошибка при проверке материала.

Ежедневно раздаем денежные бонусы самыми результативными селлерам.

Для получения регистрации на нашей платформе и ссылки на нашего настоящего телеграм бота, пишите мне на жабу или телеграм.

Связь жаб: BlackBatman64@xmpp.internatıonal
телеграм: @BlackBatman64
We buy up Dedics (RDP) for crypto

Conditions:
1) Information from 100GB
2) Admin rights
3) TOP countries $ 25, China $ 15, poor countries $ 12
4) Not crypto, without lockers
5) Not Amazon
6) Valid
7) Payment upon execution works
8) Payment in Btc
9) Payment every day
10) Instant reports
11) Your telegram bot and platform in the torus

We have the most convenient, easy-to-use service 😎

Our platform allows you not to wait for hours when the buyer answers you.
You can send your server at any time of the day and immediately after checking you will receive a report on it.
Pour your list of Dediks into our program (either on our website or via bot telegrams), after the crypt we pay $ $ to your BTC wallet.

It is also possible at any time to correct the password and other data from the Dedik, if any error was found when checking the material.

We give out cash bonuses to the most successful sellers daily.

To receive registration on our platform and links to our real telegram bot, write to me on a toad or telegram.

Communication Toad: BlackBatman64@xmpp.international
Telegram: @ BlackBatman64
What are the FBI’s Challenges

- Turnkey Ransomware
- Easy to Buy Access to Victims
- Easy to Launder Money
# RSAC

## Exchanges That Received Ransomware Proceeds

<table>
<thead>
<tr>
<th>Exchange</th>
<th>Total($)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>19,000,476</td>
</tr>
<tr>
<td></td>
<td>18,856,173</td>
</tr>
<tr>
<td></td>
<td>8,384,355</td>
</tr>
<tr>
<td></td>
<td>5,279,807</td>
</tr>
<tr>
<td>BTC-e.com</td>
<td>1,324,429</td>
</tr>
<tr>
<td>All Others</td>
<td>10,809,385</td>
</tr>
</tbody>
</table>
What are the FBI’s Challenges

- Turnkey Ransomware
- Easy to Buy Access to Victims
- Easy to Launder Money
- Easy to Stay Anonymous
anonymous.vps

Anonymous VPS - Anonymously.io
Anonymous VPS on SSD drives, KVM virtualization. Pay anonymously with just your email and Bitcoin or other Cryptocurrency. VPS is automatically activated...

Instant Anonymous VPS Windows (RDP) and Linux – Bitcoin ...
Rating: 5 - 48 reviews - Price range: Starting at $7.95
You might want to hide your identity from other people on the internet so why don't you buy a fully anonymous VPS server loaded with Windows RDP or one...

12 Best “Anonymous” Web Hosting (2020) - Web Pages ...
Mar 31, 2019 - To determine the best provider of anonymous web hosting, we took a ... The host offers anonymous shared and VPS hosting and domain ...
Domain Name: FREE (1 year) Disk Space: 10 GB SSD - 30 GB SSD
Starting Price/Mo: $2.15 Money Back Guarantee: 30 days

VPS providers allowing anonymous payment and not blocking tor ...
Jul 24, 2017 - Is there any provider that offers truly anonymous VPS, that you can pay with Bitcoin or other anonymous payment methods and that allows Tor services? A lot of ...

Anonymous VPS?: hacking Jan 28, 2019
anonymous VPS?: selfhosted Sep 5, 2017
Nice Anonymous way to Spawn instant Servers VPS with Bitcoin ... Mar 16, 2010
Best anonymous vps service and how to use it securely and ... Nov 6, 2015
More results from www.reddit.com

nicevps.net

NiceVPS.net - Uncensored Bulletproof Hosting, Bulletproof ...
The best uncensored, privacy aware, anonymous and bulletproof anti-ddos hosting in offshore locations. Pay with Bitcoin, Monero, Dash, Zcash and other...
What are the FBI’s Challenges

- Turnkey Ransomware
- Easy to Buy Access to Victims
- Easy to Launder Money
- Easy to Stay Anonymous
- Skid Training Wheels
root@kali:/usr/bin# ./msfconsole

[ ] ***rting the Metasploit Framework console...
[ ] * WARNING: No database support: No database YAML file
[ ] ***

```
=|[ metasploit v5.0.41-dev ]|
+-- ---=[ 1914 exploits - 1074 auxiliary - 330 post ]|
+-- ---=[ 556 payloads - 45 encoders - 10 nops ]|
+-- ---=[ 4 evasion ]|
```

msf5 > Can't code. Can't fuzz. Can't reverse. Will pwn 4 the lulz!!!
Initializing AutoSploit...

One moment please while we check the Postgresql and Apache services...

Your API key was loaded from /media/root/HDD 1TB1/Kitploit/AutoSploit/api.p

Welcome to AutoSploit. Please select an action.

1. Usage
2. Gather Hosts
3. View Hosts
4. Exploit
5. Quit

<AUTOSPLOIT>
285 modules currently loaded
0 listeners currently active
0 agents currently active

(Empire) > I'm a pen tester. I swear!
<table>
<thead>
<tr>
<th>Name</th>
<th>Disclosure Date</th>
<th>Rank</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibstat</td>
<td>2013-09-24</td>
<td>excellent</td>
<td>ibstat SPATH Privilege Escalation</td>
</tr>
<tr>
<td>AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow (AIX)</td>
<td>2009-10-07</td>
<td>great</td>
<td>AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow (AIX)</td>
</tr>
<tr>
<td>ToolTalk rpc.ttdobserverd_tt_internal_reopath Buffer Overflow (AIX)</td>
<td>2006-06-17</td>
<td>great</td>
<td>ToolTalk rpc.ttdobserverd_tt_internal_reopath Buffer Overflow (AIX)</td>
</tr>
<tr>
<td>Android ADB Debug Server Remote Payload Execution</td>
<td>2016-01-01</td>
<td>excellent</td>
<td>Android ADB Debug Server Remote Payload Execution</td>
</tr>
<tr>
<td>Samsung Galaxy KNOX Android Browser RCE</td>
<td>2014-11-12</td>
<td>excellent</td>
<td>Samsung Galaxy KNOX Android Browser RCE</td>
</tr>
<tr>
<td>Adobe Reader for Android add JavascriptInterface Exploit</td>
<td>2014-08-13</td>
<td>good</td>
<td>Adobe Reader for Android add JavascriptInterface Exploit</td>
</tr>
<tr>
<td>Android 'TwolRoot' Futex Requemer Kernel Exploit</td>
<td>2014-05-03</td>
<td>excellent</td>
<td>Android 'TwolRoot' Futex Requemer Kernel Exploit</td>
</tr>
<tr>
<td>Apple iOS MobileMail libffiff Buffer Overflow</td>
<td>2006-08-01</td>
<td>excellent</td>
<td>Apple iOS MobileMail libffiff Buffer Overflow</td>
</tr>
<tr>
<td>Apple iOS Default SSH Password Vulnerability</td>
<td>2007-08-01</td>
<td>excellent</td>
<td>Apple iOS Default SSH Password Vulnerability</td>
</tr>
<tr>
<td>Mercantec SoftCart CGI Overflow</td>
<td>2004-08-19</td>
<td>great</td>
<td>Mercantec SoftCart CGI Overflow</td>
</tr>
<tr>
<td>System V Derived /bin/login Extraneous Arguments Buffer Overflow</td>
<td>2005-06-18</td>
<td>good</td>
<td>System V Derived /bin/login Extraneous Arguments Buffer Overflow</td>
</tr>
<tr>
<td>Firefox Exec Shellcode from Privileged Javascript Shell</td>
<td>2010-11-01</td>
<td>normal</td>
<td>Firefox Exec Shellcode from Privileged Javascript Shell</td>
</tr>
<tr>
<td>ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)</td>
<td>2010-05-29</td>
<td>excellent</td>
<td>ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)</td>
</tr>
<tr>
<td>Watchguard XCS Remote Command Execution</td>
<td>2014-08-02</td>
<td>great</td>
<td>Watchguard XCS Remote Command Execution</td>
</tr>
<tr>
<td>FreeBSD 9 Address Space Manipulation Privilege Escalation</td>
<td>2013-05-09</td>
<td>excellent</td>
<td>FreeBSD 9 Address Space Manipulation Privilege Escalation</td>
</tr>
<tr>
<td>Watchguard XCS FxCorruptMail Local Privilege Escalation</td>
<td>2015-06-29</td>
<td>manual</td>
<td>Watchguard XCS FxCorruptMail Local Privilege Escalation</td>
</tr>
<tr>
<td>Samba transc0pen Overflow (&quot;BSD x86&quot;)</td>
<td>2004-04-07</td>
<td>excellent</td>
<td>Samba transc0pen Overflow (&quot;BSD x86&quot;)</td>
</tr>
<tr>
<td>XTACASD report() Buffer Overflow</td>
<td>2011-02-13</td>
<td>average</td>
<td>XTACASD report() Buffer Overflow</td>
</tr>
<tr>
<td>FreeBSD Telnet Service Encryption Key ID Buffer Overflow</td>
<td>2011-12-23</td>
<td>great</td>
<td>FreeBSD Telnet Service Encryption Key ID Buffer Overflow</td>
</tr>
<tr>
<td>HP-UX LPD Command Execution</td>
<td>2002-08-28</td>
<td>excellent</td>
<td>HP-UX LPD Command Execution</td>
</tr>
<tr>
<td>Irix LPD tagprinter Command Execution</td>
<td>2001-09-01</td>
<td>excellent</td>
<td>Irix LPD tagprinter Command Execution</td>
</tr>
<tr>
<td>eScan Web Management Console Command Injection</td>
<td>2014-04-04</td>
<td>excellent</td>
<td>eScan Web Management Console Command Injection</td>
</tr>
<tr>
<td>Adobe Flash Player ActionScript Launch Command Execution Vulnerability</td>
<td>2009-12-17</td>
<td>great</td>
<td>Adobe Flash Player ActionScript Launch Command Execution Vulnerability</td>
</tr>
<tr>
<td>ProFTPD 1.2 - 1.3.6 replaceBuffer Overflow (Linux)</td>
<td>2004-11-26</td>
<td>great</td>
<td>ProFTPD 1.2 - 1.3.6 replaceBuffer Overflow (Linux)</td>
</tr>
<tr>
<td>ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)</td>
<td>2010-11-01</td>
<td>great</td>
<td>ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)</td>
</tr>
<tr>
<td>Unreal Tournament 2004 &quot;secure&quot; Overflow (Linux)</td>
<td>2004-06-18</td>
<td>great</td>
<td>Unreal Tournament 2004 &quot;secure&quot; Overflow (Linux)</td>
</tr>
<tr>
<td>Advantech Switch Bash Environment Variable Code Injection (Shellscape)</td>
<td>2015-12-01</td>
<td>excellent</td>
<td>Advantech Switch Bash Environment Variable Code Injection (Shellscape)</td>
</tr>
<tr>
<td>Airies login-cgi Buffer Overflow</td>
<td>2013-03-01</td>
<td>normal</td>
<td>Airies login-cgi Buffer Overflow</td>
</tr>
<tr>
<td>Belkin Play N750 login-cgi Buffer Overflow</td>
<td>2013-09-17</td>
<td>normal</td>
<td>Belkin Play N750 login-cgi Buffer Overflow</td>
</tr>
<tr>
<td>Centreon SQL and Command Injection</td>
<td>2014-10-15</td>
<td>excellent</td>
<td>Centreon SQL and Command Injection</td>
</tr>
</tbody>
</table>
What are the FBI’s Challenges

- Turnkey Ransomware
- Easy to Buy Access to Victims
- Easy to Launder Money
- Easy to Stay Anonymous
- Skid Training Wheels
- Jurisdictional Issues
Private Crypto Locker Affiliate Program

By UNKN, July 4, 2019 in [Software] - malware, exploits, bundles, crypts

Due to the fact that we are expanding activity, we invite adverts by:

- Spam;
- Dedikam and networks;
- Doorway traffic and other living things;

We work in a private mode. Limited number of seats. Get ready for an interview and show your evidence of the quality of the installations. We are not a test site and there are nothing for "learners" and "I will try / I will try". We have been working for several years, the topic is more than 5 years. The software is fully operational and ready to go.

Excerpt from the rules:

1. It is forbidden to work in the CIS (including Ukraine);
2. Starting rate from 60% in your direction. After the first 3 payments - 70%.

Short description of the software: private ransomware written in pure C, using inline-assembler with the possibility of modifying functionality "out of the box" according to the RaaS business model.

The software has statistics, a payment page and "trial decoders" on the payment page. No school emails. More information can be obtained during the interview. The first contact in the PM.
Excerpt from the rules:

1. It is forbidden to work in the CIS (including Ukraine);
What are the FBI’s Investigative Tools

- Grand Jury Subpoenas
- ECPA Search Warrant
- Remote Searches
- Mutual Legal Assistance Treaties
What are the FBI’s Ransomware Outcomes

- Arrests
- Release of Decryption Keys
- Seizing Virtual Currency
- Seizing Malicious Infrastructure
- Sanctioning Virtual Currency Wallets
- Public Indictments
What is the Security Community’s Role

- The FBI’s secret weapon...

You!
What is the Security Community’s Role

- Your dead end is our opportunity
  - Overseas IP Addresses?
  - Virtual Currency Wallets?
  - Suspicious Domain Names?

- Real Collaboration

- Prioritization
  - What should the FBI be targeting?
What is the Security Community’s Role

● But what’s in it for me?
  – Be a famous Internet vigilante!
Springfield - Michael Gillespie
2017 Director’s Community Leadership Award Recipient

FBI Director Recognizes Distinguished Community Leaders
In a ceremony at FBI Headquarters on April 20, 2018, Director Christopher Wray recognized the recipients of the 2017 Director’s Community Leadership Award. These leaders, selected by their area FBI field office, have demonstrated outstanding contributions to their local communities through service. The FBI is grateful for the work of each of these individuals and organizations on behalf of their communities.
THE EXTORTION ECONOMY

The Ransomware Superhero of Normal, Illinois

Thanks to Michael Gillespie, an obscure programmer at a Nerds on Call repair store, hundreds of thousands of ransomware victims have recovered their files for free.

by Renee Dudley, Oct. 28, 2019, 5 a.m. EDT
What is the Security Community’s Role

• But what’s in it for me?
  – Be a famous Internet vigilante!
  – Protect your partners and clients!
Russian Hacker Pleads Guilty For Involvement In Massive Network Intrusions At U.S. Financial Institutions, Brokerage Firms, A Major News Publication, And Other Companies

Geoffrey S. Berman, the United States Attorney for the Southern District of New York, announced today that ANDREI TYURIN, a/k/a “Andrei Tyurin,” pled guilty in Manhattan federal court to computer intrusion, wire fraud, bank fraud, and illegal online gambling offenses in connection with his involvement in a massive computer hacking campaign targeting U.S. financial institutions, brokerage firms, financial news publishers, and other American companies. These hacks included one of the largest thefts of customer data from a U.S. financial institution in history. TYURIN is charged with committing these crimes with Gery Shalon, a/k/a “Garri Shalolashvili,” a/k/a “Gabriel,” a/k/a “Gabi,” a/k/a “Phillipe Mousset,” a/k/a “Christopher Engeham”; Joshua Samuel Aaron, a/k/a “Mike Shields”; and Ziv Orenstein, a/k/a “Aviv Stein,” a/k/a “John Avery,” in furtherance of securities market manipulation, illegal online gambling, and payment processing fraud schemes perpetrated by Shalon, Aaron, Orenstein, and their co-conspirators. TYURIN pled guilty before U.S. District Judge Laura Taylor Swain.

Manhattan U.S. Attorney Geoffrey S. Berman said: “Andrei Tyurin’s extensive hacking campaign targeted major financial institutions, brokerage firms, news agencies, and other companies. Ultimately, he gathered the customer data of more than 80 million victims, one of the largest thefts of U.S. customer data from a single financial institution in history. With today’s plea, Tyurin’s global reign of computer intrusion is over and he faces significant time in a U.S. prison for his crimes.”

According to the allegations contained in the Indictments to which TYURIN pled guilty, other filings in this case, and statements made during court proceedings, including TYURIN’s guilty plea hearing:
Mr. Berman praised the investigative work of the FBI and the U.S. Secret Service, and expressed his sincere gratitude to the Chief Prosecutor’s Office of Georgia and the Ministry of Justice of Georgia for their support and assistance with the extradition proceedings. He also thanked the Securities and Exchange Commission, Homeland Security Investigations, the Financial Industry Regulatory Authority, the Office of International Affairs of the U.S. Department of Justice for its assistance with the extradition, and the Financial Services Information Sharing and Analysis Center, which significantly aided the investigation by facilitating information-sharing among the victim institutions.
What is the Security Community’s Role

• But what’s in it for me?
  – Be a famous Internet vigilante!
  – Protect your partners and clients!
  – Show your clients you know your stuff!
Two International Cybercriminal Rings Dismantled and Eight Defendants Indicted for Causing Tens of Millions of Dollars in Losses in Digital Advertising Fraud

Global Botnets Shut Down Following Arrests

A 13-count indictment was unsealed today in federal court in Brooklyn charging Aleksandr Zhukov, Boris Timokhin, Mikhail Andreev, Denis Avdeev, Dmitry Novikov, Sergey Ovysannikov, Aleksandr Isaev and Yevgeniy Timchenko with criminal violations for their involvement in perpetrating widespread digital advertising fraud. The charges include wire fraud, computer intrusion, aggravated identity theft and money laundering. Ovysannikov was arrested last month in Malaysia; Zhukov was arrested earlier this month in Bulgaria; and Timchenko was arrested earlier this month in Estonia, all pursuant to provisional arrest warrants issued at the request of the United States. They await extradition. The remaining defendants are at large.

Also unsealed today in federal court in Brooklyn were seizure warrants authorizing the FBI to take control of 31 internet domains, and search warrants authorizing the FBI to take information from 89 computer servers, that were all part of the infrastructure for botnets engaged in digital advertising fraud activity. The FBI, working with private sector partners, redirected the internet traffic going to the domains (an action known as “sinkholing”) in order to disrupt and dismantle these botnets.
Multiple private sector organizations also provided critical assistance in this case. The Office extends its appreciation to White Ops, Inc. and Google LLC for their assistance in the investigation and botnet takedown. The Office also extends its appreciation to Proofpoint, Inc, Fox IT B.V., Microsoft Corporation, ESET, Trend Micro Inc., Symantec Corporation, CenturyLink, Inc, F-Secure Corporation, Malwarebytes, MediaMath, the National Cyber-Forensics and Training Alliance and The Shadowserver Foundation for their assistance in the botnet takedown.
3ve (pronounced “Eve”) was a global, complex family of online fraud operations, each designed to evade detection. A cross-industry alliance led by White Ops and Google dismantled 3ve, resulting in the indictment and arrest of its perpetrators. This is the first time that consequences of this magnitude have been created for ad fraud.
How the No.1 most creative person in business this year led the FBI to its biggest ad-fraud bust ever

For helping to crack one of the most pernicious digital fraud schemes in history, White Ops CEO Tamer Hassan is the No. 1 Most Creative Person In Business in 2019.
Today at #ICCS2019, @NewYorkFBI Special Agent Evelina Aslanyan joined Dimitris Theodorakis, the White Ops Director of Detection, to discuss METHBOT & the global collaboration between law enforcement and private tech industry partners to dismantle it. 1/
What is the Security Community’s Role

But what’s in it for me?
- Be a famous Internet vigilante!
- Protect your partners and clients!
- Show your clients you know your stuff!
- Clean up your industry!
FOR IMMEDIATE RELEASE

Cyber-Criminal Residing in Latvia Convicted for Role in Operation of Counter Antivirus Service “Scan4you”

Ruslans Bondars, 37, was convicted after a five-day jury trial of one count of conspiracy to violate the Computer Fraud and Abuse Act, one count of conspiracy to commit wire fraud, and one count of computer intrusion with intent to cause damage and aiding and abetting. Sentencing is scheduled for Sept. 21.
Trend Micro Expertise Results in Conviction from Scan4You Trial

Three-year collaboration with law enforcement confirms Trend Micro’s leading role in global cybercrime fight

May 16, 2018 06:39 PM Eastern Daylight Time

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today announced details of its close cooperation with the FBI to identify, arrest and bring to trial the individuals linked to the infamous Counter Antivirus (CAV) service Scan4You. Rusians Bondars was found guilty as a result of the trial, while Jurijs Martisevs pleaded guilty in March 2018. The arrest and trial were the result of an exclusive investigative cooperation between Trend Micro researchers and the FBI.

“As a leading voice and global citizen in the fight against cybercrime, we are always proud to support law enforcement globally”

Scan4You allowed cybercriminals to check the detection of their latest malware against more than 30 modern antivirus engines, enabling them to make attacks more successful.

Trend Micro began its research back in 2012 and collaborated closely with the FBI. The service went offline following the arrest of two suspected administrators in May 2017.
Inside the Takedown of a Notorious Malware Clearinghouse

How security researchers caught the creators of counter antivirus services Scan4You.
What is the Security Community’s Role

• But what’s in it for me?
  – Be a famous Internet vigilante!
  – Protect your partners and clients!
  – Show your clients you know your stuff!
  – Clean up your industry!
  – Because...
    err, well...
  it’s the right things to do!
FOR IMMEDIATE RELEASE

Justice Department Announces Charges and Guilty Pleas in Three Computer Crime Cases Involving Significant DDoS Attacks

Defendants Responsible for Creating "Mirai" and Clickfraud Botnets, Infecting Hundreds of Thousands of IoT Devices with Malicious Software

The Justice Department announced today the guilty pleas in three cybercrime cases. In the District of Alaska, defendants pleaded guilty to creating and operating two botnets, which targeted "Internet of Things" (IoT) devices, and in the District of New Jersey, one of the defendants also pleaded guilty to launching a cyber attack on the Rutgers University computer network.


On Dec. 8, Paras Jha, 21, of Fanwood, New Jersey; Josiah White, 20, of Washington, Pennsylvania; and Dalton Norman, 21, of Metairie, Louisiana, pleaded guilty to criminal Informations in the District of Alaska charging them each with conspiracy to violate the Computer Fraud & Abuse Act in operating the Mirai Botnet. In the summer and fall of 2016, White, Jha, and Norman used a variant of Mirai to infect thousands of IoT devices with malicious software.
All three cases were investigated by the FBI’s Anchorage, Alaska and Newark, New Jersey Field Offices; and the U.S. Immigration and Customs Enforcement’s (ICE) Homeland Security Investigations (HSI) Atlanta - Greenville South Carolina Office. The Mirai Botnet and Clickfraud Botnet cases are being prosecuted by Assistant U.S. Attorney Adam Alexander of the District of Alaska and Trial Attorney C. Alden Pelker of the Computer Crime and Intellectual Property Section of the Criminal Division. The Rutgers University case is being prosecuted by Assistant U.S. Attorney Shana Chen of the District of New Jersey. Additional assistance was provided by the FBI’s New Orleans and Pittsburgh Field Offices, the U.S. Attorney’s Office for the Eastern District of Louisiana, the United Kingdom’s National Crime Agency, the French General Directorate for Internal Security, the National Cyber-Forensics & Training Alliance; Palo Alto Networks Unit 42, Google, Cloudflare, Coinbase, Flashpoint, Yahoo and Akamai. Former Department of Justice prosecutors Ethan Arenson, Harold Chun, and Yvonne Lamoureux provided invaluable support during their previous tenure at DOJ.
What is the Security Community’s Role

How can I help?

- Get in touch with your local FBI field office.
- Track down the FBI case team working what you are interested in.
  - Ransomware
  - Banking Trojans
  - Botnets
  - Cyber Underground
  - Nation-State
  - Foreign Influence
What is the Security Community’s Role

- Yeah, but how?

Joel DeCapua
Supervisory Special Agent
jedecapua@fbi.gov
@jedec0x0
Thank You!

Joel DeCapua
Supervisory Special Agent
FBI – Cyber Division
jedecapua@fbi.gov
@jedec0x0