Open for Extortion: Upcoming Ransomware Evolutions and Revolutions

Feike Hacquebord
Senior Threat Researcher
Trend Micro Research

FIRST Symposium, Bilbao 2023
Central Research Question 1

What will happen with Ransomware Business models in

- the near future
- the far future
Central Research Question 2

What will *trigger* Ransomware Business models to change?
THIS HIDDEN SITE HAS BEEN SEIZED

Hive

The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement action taken against Hive Ransomware.

This action has been taken in coordination with the United States Attorney’s Office for the Middle District of Florida and the Computer Crime and Intellectual Property Section of the Department of Justice with substantial assistance from Europol.
Ransomware has gone down because sanctions against Russia are making life harder for attackers

NSA director of cybersecurity Rob Joyce says US sanctions on Russia are making it harder for criminals based in the country to conduct campaigns.

Source: https://www.zdnet.com/article/ransomware-has-gone-down-because-sanctions-against-russia-are-making-life-harder-for-attackers/
Crypto Winter
or Ice Age

Source: CNN
Reported Victim Losses

Cybercrime. Victim Losses (source: FBI IC3)

- Phishing/Vishing/Smishing/Pharming
- Ransomware
- Lottery/Sweepstakes/Inheritance
- Spoofing
- Advanced Fee
- Corporate Data Breach
- Credit Card Fraud
- Identity Theft
- Tech Support
- Personal Data Breach
- Confidence Fraud/Romance
- Investment
- BEC/EAC

© 2022 Trend Micro Inc.
Kill chain typical ransomware attack

- Initial Access
- Lateral Movement
- Data Exfiltration
- Ransomware
- Extortion
- Money Laundering
Ransomware payload can be replaced

Initial Access → Lateral Movement → Data Exfiltration → Extortion → Money Laundering
Extra Payload on top of ransomware
Types of Ransomware Actors

Netwalker affiliate

HolyGhost
Types of Ransomware Actors

Netwalker affiliate

HolyGhost

We have been doing ransom for 8 years and did not publish or sell data which the user paid. So for 8 years, the people who is not related on us, never heard our group name. We help poor and starving people if we earn money.
Types of Ransomware Actors

Netwalker affiliate

We have been doing ransom for 8 years and did not publish or sell data which the user paid. So for 8 years, the people who is not related on us, never heard our group name. We help poor and starving people if we earn money.

Source: CBCNews https://www.cbc.ca/newsinteractives/features/takedown-homegrown-ransomware-hacker
Types of Ransomware Actors

Netwalker affiliate

HolyGhost

We have been doing ransom for 8 years and did not publish or sell data which the user paid. So for 8 years, the people who is not related on us, never heard our group name. We help poor and starving people if we earn money.

Source: CBCNews https://www.cbc.ca/newsinteractives/features/takedown-homegrown-ransomware-hacker
Types of Ransomware Actors

- Big Game Hunters
- Nation state actors
- Traditional Cybercriminals
Triggers leading to Ransomware Evolution

- Arrests
- Sanctions
- Improved Actors’ OpSec
- Automation of ransomware attacks
- Cloud adoption
Triggers leading to Ransomware Revolution

- Cryptocurrency Regulations
- Geopolitical events
- More profitable cybercrime
Impact of Arrests

- Impact of arrests has been limited so far
- Some arrests of affiliates
- Investigations seem to take forever
- Some new arrests to be expected

- But with all the focus on ransomware: *is that all there is?*
# Evolution Trigger: Sanctions

<table>
<thead>
<tr>
<th>Date</th>
<th>Organization</th>
<th>Reason of OFAC designation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec. 29, 2016</td>
<td>Individual</td>
<td>Developer of Zeus malware</td>
</tr>
<tr>
<td>Dec. 29, 2016</td>
<td>Individual</td>
<td>Major data breaches</td>
</tr>
<tr>
<td>Nov. 28, 2018</td>
<td>Two individuals</td>
<td>SamSam ransomware</td>
</tr>
<tr>
<td>Sept. 13, 2019</td>
<td>Lazarus Group</td>
<td>WannaCry 2.0 ransomware, cryptocurrency hacks</td>
</tr>
<tr>
<td>Sept. 13, 2019</td>
<td>Bluenoroff</td>
<td>Attacks against financial institutions</td>
</tr>
<tr>
<td>Sept. 13, 2019</td>
<td>Andariel</td>
<td>ATM hacks, banking attacks</td>
</tr>
<tr>
<td>Dec. 5, 2019</td>
<td>Evil Corp</td>
<td>Development of Dridex malware</td>
</tr>
<tr>
<td>Dec. 5, 2019</td>
<td>17 individuals</td>
<td>Related to Evil Corp</td>
</tr>
<tr>
<td>Dec. 5, 2019</td>
<td>Six cooperations</td>
<td>Related to Evil Corp</td>
</tr>
<tr>
<td>Mar. 20, 2020</td>
<td>Two individuals</td>
<td>Assisted Lazarus Group with money laundering</td>
</tr>
<tr>
<td>Sept. 21, 2021</td>
<td>Suex OTC</td>
<td>Virtual currency exchange – Money laundering</td>
</tr>
<tr>
<td>Nov. 8, 2021</td>
<td>Chatex</td>
<td>Virtual currency exchange – Money laundering</td>
</tr>
<tr>
<td>Nov. 8, 2021</td>
<td>Three businesses</td>
<td>Related to Chatex</td>
</tr>
<tr>
<td>Apr. 5, 2022</td>
<td>Hydra market</td>
<td>Marketplace</td>
</tr>
<tr>
<td>May 6, 2022</td>
<td>Blender.io</td>
<td>Cryptocurrency mixer</td>
</tr>
<tr>
<td>Aug. 8, 2022</td>
<td>Tornado Cash</td>
<td>Cryptocurrency mixer</td>
</tr>
</tbody>
</table>
How 2022's Biggest Cryptocurrency Sanctions Designations Affected Crypto Crime

JANUARY 9, 2023 | BY CHAINALYSIS TEAM

Impact of Sanctions

- Sanctions are usually used as a political tool

- Impact will be limited [anybody remembers take down of Liberty Reserve – 2013?]

- Sanctions probably only increase costs for cyber criminals somewhat
Remarks on OpSec

While RaaS actors are giving interviews to the journalists and brag about their crimes, their RaaS had been compromised for months....

-> RaaS are not immune to breaches
Tor hidden servers exposing clear web IP

- Nefilim
- HolyGhost
- AtomSilo
- Onyx
- Snatch
- RansomExx
- Ragnar
- Arvin Club
- Lorenz
- Marketo
- Xing/星 team
- Rook
RaaS with Server Status exposed

Nefilim
HolyGhost
Babuk
BigLock
Diavol
Snatch
Haron
Midas
Arvin Club
Medusa
Lorenz
Xing/星
team
Same SSH key.... for Nefilim

hxt254aygrsziejn.onion:22

78.128.x.y:22
| REvil      | - undisclosed LE agency |
| Hive      | - FBI                  |
| LockBit   | - ProDaft              |
| Conti     | - UA researcher, ProDaft, others |
| Karakurt  | - Infinitum            |
| PYSA      | - ProDaft              |
| [....]    | - [....]               |
Takedown
No arrests

‘We hacked the hackers:’ DOJ, FBI take down Hive ransomware after spending months inside gang systems

More automation

2017

Cerber already used Blockchain for C&C

Malware Coordination using the Blockchain: An Analysis of the Cerber Ransomware

Stijn Pletinckx*, Cyril Trap* and Christian Doerr
TU Delft
Cyber Security Group
2628CD Delft, The Netherlands
{S.R.G.Pletinckx@student., C.H.Trap@student., c.doerr@}

Abstract—In order for malicious software to receive configuration information or commands, malware needs to be able to locate and connect to its own. As hard-coded addresses are easy to block and thus render the malware installation inoperable, malware writers have turned to dynamically generated addresses. Domain generation algorithms (DGA) generate a list of candidate domain names, each valid for only a short amount of time, at the malware installation searches for its command & control (C&C) server. As DGAs generate a large list of potential domains – out of which one or a few is actually in use –, they leave a characteristic trace of many failed DNS lookups (NXDomain) in the network, and in result most DGAs can be efficiently detected.

In this paper we describe an entirely new principle of domain generation, actively deployed in the Cerber ransomware, which finds and coordinates with its owner based on transaction information in the bitcoin blockchain. This allows the malware author to dynamically update the location of the server in real-time, and as the malware directly goes to the right location no longer generates a sequence of NXDomain responses. We describe the concept of coordination via the blockchain, and report results on a year-long observation of the assets used in the Cerber campaign.

Index Terms—threat intelligence, blockchain, ransomware, C&C, domain-generation algorithm, campaign analysis

*Both contributed equally to this work.
Less interaction

FAQ

❓ Question: How can i decrypt my files after payment?

Answer: After payment, you can download the «Cerber Decryptor» from your personal page. We guarantee that all your files will be decrypted!

❓ Question: My files was infected more then month ago, can i still decrypt it with your software?

Answer: Yes, you can still decrypt your files after the payment!
Cloud Adoption
Impact of Cloud Adoption

• Cloud adoption will raise the bar for ransomware

BUT:

- Misconfigurations
- Theft of admin keys
- Vulnerabilities in Cloud (like no proper tenant separation)
Critical Cloud vulnerabilities

Security Advisory: Insufficient Tenant Separation in Azure Synapse Service

Source: https://orca.security/resources/blog/synapse-critical-azure-synapse-analytics-service-vulnerability/

AttachMe: critical OCI vulnerability allows unauthorized access to customer cloud storage volumes

Before it was patched, #AttachMe could have allowed attackers to access and modify any other users' OCI storage volumes without authorization, thereby violating cloud isolation. Upon disclosure, the vulnerability was fixed within hours by Oracle. No customer action was required.

Source: https://www.wiz.io/blog/chaosdb-explained-azures-cosmos-db-vulnerability-walkthrough/
Expected evolutions in ransomware

- Better OpSec
- More automation
- Less interaction with victims
- Move to targeting Cloud and Linux servers
Triggers leading to Ransomware Revolution

- Cryptocurrency Regulations
- Geopolitical events
- More profitable cybercrime
Cryptocurrency Regulations

Image: Trend Micro
Crypto Winter or Ice Age

Source: CNN
Crypto Regulation

Reasons for crypto regulation

• Protect investors and consumers
• Avoid ripple effects on financial markets
• Capital flight

• Money laundering
FATF recommended Crypto regulations

Recommendation #15
- VASPs*) need to be regulated for anti-money laundering
- VASPs need to be licensed

Recommendation #16 (Crypto Travel Rule)
- Info on payer and payee for transactions to be shared among CASPs**

*) VASP: Virtual Asset Service Provider
**) CASP: Crypto Asset Service Provider
Crypto regulations – EU version

- MiCA legislation in EU
  - Stricter security rules on CASPs *)
  - CASPs need authorization to operate in EU

- Crypto Travel Rule
  - Info on payer and payee for transactions
  - no threshold for payment
Issues with regulations – worldwide

- low implementation of FATF recommendations
- different implementations between countries
  - threshold of travel rule differs
    - 0 in EU, 3000 USD in US
    - transfers to non-compliant CASPs: allowed / disallowed?
  - how about “unhosted” wallets?
- some countries are likely not to follow the FATF recommendations anytime soon
Crypto regulations: impact on ransomware

- Potentially a huge impact
- But limited for the time being
- EU regulations expected to have the biggest impact (not before 2025).
Geopolitical events

- Some RaaS might fall apart
- Some affiliates start to work for governments
- Initial access used for espionage / wiper attacks
- Usage of Ransomware as smokescreen
Geopolitical events

New “Prestige” ransomware impacts organizations in Ukraine and Poland

Microsoft Security Threat Intelligence

Initial access broker repurposing techniques in targeted attacks against Ukraine

Google TAG about Conti affiliate

SecureWorks: CN espionage smokescreen
More Profitable Cybercrime
Reported Victim Losses

Cybercrime. Victim Losses (source: FBI IC3)
Remove ransomware, extortion

- Initial Access
- Lateral Movement
- Data Exfiltration
- Ransomware
- Extortion
- Money Laundering
Kill chain BEC attack

Initial Access → Lateral Movement → Data Exfiltration → BEC → Money Laundering
Kill chain BEC attack

Ransomware and BEC in the Cyber Threat Landscape: Past vs. Present, Perception vs. Reality

Colonial Pipeline. CNA Financial. Quanta. Even the NBA. Hardly a week goes by without a ransomware story hitting the news, as organizations worldwide are targeted by an attack. But are there more dangerous threats out there?
Kill chain typical ransomware attack
Kill chain typical ransomware attack

Initial Access → Lateral Movement → Data Exfiltration → Ransomware → Extortion → Money Laundering
Kill chain typical ransomware attack

Initial Access  Lateral Movement  Data Exfiltration  Ransomware

Short and Distort

Money Laundering
Kill chain ransomware + short and distort
Caught in a bear trap: How 'short and distort' attacks are costing Australian investors billions

Australia has become a paradise for a new, aggressive form of short selling. And regulators' failure to act is costing investors billions.

Adele Ferguson
DECEMBER 7, 2020
Example: Insulet Corporation

Canon (Maze attack: Jul/Aug 2020)

- Initial drop 18%
- V-shape

Source: macrotrends.net
Nvidia (Lapsu$ attack: Feb 2022)

• Drop 4%
• V-shape

Source: macrotrends.net
Payloads that might replace ransomware

- Theft of intellectual property and other sensitive data
- Business Email Compromise
- Stocks manipulation schemes like short and distort
- Theft of cryptocurrencies at scale
Advice 1

XDR solutions will be increasingly important in the near and far future.

Near Future: Ransomware will be optimized

Far Future: Ransomware will be replaced by other profitable payloads. Emphasis on the left and middle of the kill chain is critical.
Advice 2

Advanced protection against Linux based cybercrime (server, cloud and IOT) will continue to rise in importance during the next 2 years and beyond.
Advice 3

Tracking campaigns and actors is key for understanding how future threats will look like and see the way criminal business models, and the top tier groups themselves, are evolving.
Advice 4

Collaboration between

LE
Certs
Governments
Law Makers
Private Industry
Further reading
Recommended reading
Contact details

Twitter: @FeikeHacquebord

FeikeHacquebord@infosec.exchange
Threat detection and response across multiple attack vectors by Trend Micro. Created with real data by artist Brendan Dawes.