Malware as a business model

Platform Criminality

Robert Fischer
Systems Engineer

Jason Mauchley
Account Manager
The Web of Profit

Conservative estimates in The Web of Profit 2018 research show cybercriminal revenues worldwide of at least $1.5 trillion – equal to the GDP of Russia. In fact, if cybercrime was a country it would have the 13th highest GDP in the world. This $1.5 trillion figure includes:

- $860 billion – Illicit/illegal online markets
- $500 billion – Theft of trade secrets/IP
- $160 billion – Data trading
- $1.6 billion – Crimeware-as-a-Service
- $1 billion – Ransomware

Cybersecurity Ventures predicts cybercrime damages will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015.

https://www.theslstore.com/blog/cybercrime-pays-new-study-finds-cybercriminal-revenues-hit-1-5-trillion-annually/
11 top cybersecurity statistics at-a-glance

- 90% of remote code execution attacks are associated with cryptomining.
- 92% of malware is delivered by email.
- 56% of IT decision makers say targeted phishing attacks are their top security threat.
- 77% of compromised attacks in 2017 were fileless.
- The average ransomware attack costs a company $5 million.
- It takes organizations an average of 191 days to identify data breaches.
- 69% of companies see compliance mandates driving spending.
- 88% companies spent more than $1 million on preparing for the GDPR.
- 25% of organizations have a standalone security department.
- 54% of companies experienced an industrial control system security incident.
- 61% of organizations have experienced an IoT security incident.

Estimates on the impact of cybercrime

• Cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015

• "Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm”

• Cybercrime will cost the world in excess of $6 trillion annually by 2021, making it more profitable than the global trade of all major illegal drugs combined.

https://blogs.cisco.com/financialservices/how-to-prevent-the-bank-robbery-no-one-can-see
Expected industry response

- Global spending on cybersecurity products and services will exceed $1 trillion cumulatively from 2017 to 2021

- Average of 3% of capex (capital expenditures) that’s focused on IT on security.
  - Versus Cybercriminals found to be reinvesting 20% of their revenues into further crime…

- Cybersecurity unemployment rate effectively zero
  - 6 million jobs globally by 2019
  - 3.5 million unfilled cybersecurity positions by 2021
Our Internet

Surface Web

Deep Web
- Comprises 90% of the internet
- Websites whose contents are not searchable by standard search engines
- Accessibly only by querying a search box within a particular website
- Includes dark webpages
- Examples: bank account sites, company intranets and registration-required sites

Dark Web
- Comprises 0.01% of the internet
- Not traceable by third parties
- Protected by encryption technologies
- Small part of the deep web that has been intentionally hidden and is inaccessible through standard web browsers
- Accessible via special browsers such as TOR (The Onion Router) project
- Also known as the Internet’s underground
- Examples: Silk Road – a criminal version of eBay (shutdown by FBI twice: 2013 and 2014) and untraceable financial transactions
Cybercrime platform service examples

- Zero-day Adobe exploits, up to $30,000
- Zero-day iOS exploit, $250,000
- Malware exploit kit, $200-$600 per exploit
- Blackhole exploit kit, $700 for a month’s leasing, or $1,500 for a year
- Custom spyware, $200
- SMS spoofing service, $20 per month
- Hacker for hire, around $200 for a “small” hack

IFRAME Dollars

• How much are your hosts worth?

https://unit42.paloaltonetworks.com/threat-brief-whats-driving-shift-cryptocurrency-mining-malware/
Please don’t forget IoT... Think 5G revolution (5G attack surface...)

Projections show 75.44 billion IoT devices worldwide by 2025

IoT Attacks Escalating with a 217.5% Increase in Volume

Some examples of IoT attacks

- The Mirai Botnet (aka Dyn Attack)
  - DDOS attack takes down chunks of the ‘net
  - Compromised IoT via default account/pwd via automated searches

- Hackable Cardiac Devices from St. Jude
  - Implantable cardiac devices have vulnerabilities, that exploited, could deplete the battery or administer incorrect pacing or shocks.

- Jeep hack
  - Vulnerabilities that allowed research attackers total control of SUV via vehicle’s CAN bus from Sprint cellular network

- “My friend Cayla”
  - De facto “spying device”
  - Banned by German regulators

- CrashOverRide
  - SCADA malware against electrical power grids
  - State sponsored

https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/
https://thehackernews.com/2017/06/electric-power-grid-malware.html
Straightforward IoT security

- “Devices that cannot have their software, passwords, or firmware updated should never be implemented.
- Changing the default username and password should be mandatory for the installation of any device on the Internet.
- Passwords for IoT devices should be unique per device, especially when they are connected to the Internet.
- Always patch IoT devices with the latest software and firmware updates to mitigate vulnerabilities.”

https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/
Ransomware today
150+ ransomware families
Ransomware today

• Multiple cryptovariants exist today, riding off the success of CryptoLocker

• Use of different attack vectors, such as malicious macros and exploit kits

• More sophisticated tactics, such as using anonymous networks like TOR or I2P for command and control, CAPTCHAs for limited access to payment systems, and language localization efforts

• Attacks are largely victim agnostic

• Multiple platforms targeted, including Android and OS X

• Ransomware as a Service now exists
Is the enemy of my enemy really my friend?

- MonsterCloud

- ProvenData
  - ProPublica was able to trace four payments from New York-based Proven Data Recovery to the SamSam ransomware attackers in Iran

[Diagram showing the flow of payments and bitcoin transactions]

Growth in crypto miners

- Unit42 researcher
- WildFire samples
- Does not include JavaScript type activities
What is the most commonly mined cryptocurrency?

Based on roughly 470,000 unique with WildFire reports and associated PCAP data Cryptocurrency targeted

- Wallet and email addresses used when connecting to mining pools
- Mining pool

This ultimately led me to collecting the following high-level information:

- 629,126 Samples
- 3,773 Emails used to connect with mining pools
- 2,995 mining pool URLs
- 2,341 Monero (XMR) wallets
- 981 Bitcoin (BTC) wallets
- 131 Electroneum (ETN) wallets
- 44 Ethereum (ETH) wallets
- 28 Litecoin (LTC) wallets

When looking at a breakdown of what cryptocurrencies are being targeted by mining malware, we see an incredible monopoly of the Monero cryptocurrency.
A little more about this Monero miner research

- By design, wallet owner’s pwd required to query balance
- By design, Monero recommends running in a ‘pool’
- Query’s against pools of the found wallets used to determine XMR mined

<table>
<thead>
<tr>
<th>Wallet</th>
<th>Mined Monero (XMR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>496ePyKuPBRWEoQigFeAlRIyKr9uXxNJ98p69ZQbwxmdZzHid5KVS524bAIyY93ASxxKPXn9XmmmcXiz29Udvss8E5SB24A</td>
<td>88,448.53</td>
</tr>
<tr>
<td>49s5ygf9Ey8x2MBQDYxigpECwm3PVEYnyaS53E3I3wTrZuZbaRcgy3rVX6QjI2ysO9HjNu5BcvFBYEchoXb8V5m9P1nuZ3Y4cV5UJh</td>
<td>79,576.81</td>
</tr>
<tr>
<td>44N9qjIowwFY7x5eX5zdyTC7U8pJwW8lX8E1le4iS5f5dpwggAYF5cB8nZRFvJZ2DAwDdDeVI5uMDY7yb3H3m4D4YH</td>
<td>56,344.09</td>
</tr>
<tr>
<td>42yjMf9GqHnKJ9XUHydTTFFFPzvugh7xExbj89Y5K4kfc77zaZ3ChyEfE8b8xXQmL6JY521cXGrKeKbu7a7Cap7pT90sJUAA</td>
<td>32,825.95</td>
</tr>
<tr>
<td>42NCdBZ7v3W01V7f4ny515XQikH9LyprE9pz5BjqL9aeqWqyKH7ahF9R9ya8gj2REyyyyBMDeMjAvPM8qV9H4q4i9y</td>
<td>26,359.34</td>
</tr>
<tr>
<td>44cw9Yn9cQgUq9vonj89am2Cv7TaU9eKU3takKAc9C8nZWC9cfYrrXg1udRt56XOj17DxThp7PYb99WcG3nTNT3XkPugk</td>
<td>23,300.37</td>
</tr>
<tr>
<td>46GHHFZ9bByK9Vvpsq9q1e1yrF8sWwWUcgExPtCpqqz9lXs9d933f6f9363eH679ThGhQsFqD1pu3vCBGP1Rq2qrg5</td>
<td>22,519.95</td>
</tr>
<tr>
<td>48c3493po9v35eE8mNqAYQdM3qpe7T9kTlTb1RabLq9JovkF4v8HDnPny2AFnDTDUCZn6Ljm7hm9W4u18m237aF5sws54U</td>
<td>21,389.34</td>
</tr>
<tr>
<td>46oCfoJFZBI7mq4A6sN9M3ynwT5KAYjV8E8U2wUx2TvWmGmLMy2c4L3mQ9PRQExVTchHwU3eKfWateELCzdJULPnP9hd</td>
<td>20,693.71</td>
</tr>
<tr>
<td>471c2w7dyMMe51cD7K5goehPp6u6W66A222W6ePHXeKhwEPy3ElPun3CQbG3JUXXMMZ47twf9zBEkwamwADLYDqPeLeYQMM</td>
<td>19,994.71</td>
</tr>
</tbody>
</table>

Total: 79,861.33 XMR
Cloud infrastructure compromised

Started at open Kubernetes console
  • Found storage pwds here
  • Spread to more hosted infrastructure
  • Was own miner instance (StratumBitcoin) rather than browser based
    • Tougher to ID

https://www.wired.com/story/cryptojacking-tesla-amazon-cloud/
Internet accessible servers

• Monero miners on Jenkins servers
  • Leveraged a known vulnerability (CVE-2017-1000353)
  • Install miner software on internet connected Jenkins servers

• Oracle WebLogic servers
  • Leveraged a known vulnerability (CVE-2017-10271)
  • Uses vuln to run powershell and download miner software
  • Eternal blue and mimikatz for lateral movement (one option)

• Apache CouchDB
  • Leveraged known vulnerabilities
    • Apache CouchDB JSON Remote Privilege Escalation Vulnerability (CVE-2017-12635)
    • Apache CouchDB _config Command Execution (CVE-2017-12636)
What can we ALL do to slow down this epidemic

- Use MFA/2-factor auth
  - Tokens, authenticator apps, even text if that is all that is supported (SIM hijacking risk exists though)

- Do not become complacent/Be Present

- Use strong password at home and the office
  - Pass phrases are great. Easier to remember and harder to crack

- Manage social media settings/Be careful what you post on social media

- Be diligent when using emails: Never click on links in email. Don’t open attachments.
  - Try the ‘ol hover trick. Usually shows you the full link so you can verify

- At UNM forward any suspicious work emails to

- Pick up the phone

- Have “The Talk” with your kids

- Learn what is out there about yourself: [https://gijn.org/2019/04/08/how-to-dox-yourself](https://gijn.org/2019/04/08/how-to-dox-yourself) and how to request info to be removed

[https://www.dhs.gov/how-do-i/protect-myself-cyber-attacks]