Healthcare Cybercrime

07/30/2020
Agenda

- Introduction
- Terminology
- Cyber Criminal Groups
- Cybercrime Trends
- Cybercrime, Fraud, and Money Laundering
- BEC in the Health Sector
- Ransomware in the Health Sector
- Synthetic Identity Fraud in the Health Sector
- DDoS For Hire in Darkweb

Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)
Some important terms and acronyms that we will use in this presentation:

**Advanced Persistent Threat (APT)** – Sophisticated cyberthreat actors, typically affiliated with foreign states and aligned with their goals, who are committed to their targets and often leverage significant resources towards a cyberattack.

**Tactics, Techniques and Procedures (TTPs)** – The repeatable technical steps that a threat actor regularly uses to either execute an initial compromise or carry out the latter steps of a cyberattack.

**Business E-Mail Compromise (BEC)** – The use of an email that appears to come from a known source making a legitimate request, in the furtherance of committing fraud or some related crime.

**Money mule** – A person who either wittingly or unwittingly agrees to launder money

**Attribution** – The ability to link a particular threat group with actions or attacks

**Watering hole attack** – Compromising users by poisoning a website designed to look innocuous by dropping malware on the system of anyone who visits the site

"Buzzword jargon buzzword, hyperbole buzzword buzzword, trite rhyming platitude... Yep, looks good."

Image source: Andertoons.com
Overview

Threat group review

• Obviously, all cyber criminal groups have a single motivation: money

• The following slides cover some of the more prominent publicly-known cyber criminal groups

• They either have
  • A record of targeting healthcare, or
  • They have demonstrated through their historic behavior the potential to target healthcare in the future
    • Targeting
    • Weapons
    • TTPs

• A note about the data:
  • Attribution is never 100%
  • Conflicting information has been reconciled as much as possible
  • Some information is not publicly available for some of the lesser-known criminal groups
<table>
<thead>
<tr>
<th>APT 19</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cordoso, C0d0so0, Sunshop Group, possibly DarkHydrus, possibly Deep Panda</td>
</tr>
<tr>
<td>China</td>
</tr>
<tr>
<td>Freelancers, loosely connected to the Chinese government, who target multiple industries, including pharmaceuticals.</td>
</tr>
<tr>
<td>Phishing, Watering holes</td>
</tr>
<tr>
<td>Cobalt Strike, C0d0so0, Empire, Derusbi, Beacon, PowerShell, various zero-days</td>
</tr>
<tr>
<td>Previously targeted pharmaceuticals</td>
</tr>
<tr>
<td>2017 – Phishing campaign targeting a series of law firms</td>
</tr>
<tr>
<td>Forbes.com (watering hole attack)</td>
</tr>
</tbody>
</table>

https://attack.mitre.org/groups/G0073/
https://www.fireeye.com/current-threats/apt-groups.html#apt19
https://unit42.paloaltonetworks.com/new-attacks-linked-to-c0d0s0-group/
**Corkow**

<table>
<thead>
<tr>
<th><strong>Metel</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Russia</strong></td>
<td></td>
</tr>
<tr>
<td>Banking trojan, active since at least 2011. Attacks on trading systems, banks/ATMs, credit card systems. Were able to manipulate the Ruble exchange rate to their benefit with a cyberattack.</td>
<td></td>
</tr>
<tr>
<td>keystroke logging, screenshot capture, HTTP form-grabbing</td>
<td></td>
</tr>
<tr>
<td>Corkow/Metel,</td>
<td></td>
</tr>
<tr>
<td>No known historic targeting of healthcare organizations; Have targeted US non-healthcare entities.</td>
<td></td>
</tr>
<tr>
<td>Multiple attacks against banks in Russia and Ukraine</td>
<td></td>
</tr>
<tr>
<td><a href="https://www.group-ib.com/resources/threat-research/corkow.html">https://www.group-ib.com/resources/threat-research/corkow.html</a></td>
<td></td>
</tr>
<tr>
<td><a href="https://fortune.com/2016/02/08/russian-hackers-currency-rate/">https://fortune.com/2016/02/08/russian-hackers-currency-rate/</a></td>
<td></td>
</tr>
</tbody>
</table>
# Desert Falcons

<table>
<thead>
<tr>
<th>APT-C-23, Two-tailed Scorpion, Arid Viper</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaza, but possibly geographically disbursed</td>
</tr>
<tr>
<td>Described by Kaspersky as “cybermercenaries”; Have been operating since at least 2017; Develop custom malware; History of attacking targets on at least four continents with focus on Middle East/North Africa, especially Egypt</td>
</tr>
<tr>
<td>Social Engineering (political and current event-themed phishing)</td>
</tr>
<tr>
<td>Arid Viper, DHS, DHS2015 (iRAT), custom malware (including mobile), FrozenCell, GlanceLove, GnatSpy, KASPERAGENT, MICROPSIA, Micropsia, GnatSpy, VAMP and ViperRAT.</td>
</tr>
<tr>
<td>No known historic targeting of healthcare organizations; Have targeted US non-healthcare entities.</td>
</tr>
</tbody>
</table>

**Operation Arid Viper**

## FIN4

<table>
<thead>
<tr>
<th><strong>Wolf Spider</strong></th>
<th>Romania</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attempt to manipulate stock markets via exfiltrated proprietary/confidential/insider information. Attempts to access e-mail and other non-public access.</td>
<td>Phishing (including spearphishing), credential harvesting, business e-mail compromise, watering holes</td>
</tr>
<tr>
<td>FIN4 Don’t often use malware</td>
<td>Healthcare and pharmaceutical</td>
</tr>
<tr>
<td>Unknown</td>
<td></td>
</tr>
</tbody>
</table>

https://attack.mitre.org/groups/G0085/
### FIN6

<table>
<thead>
<tr>
<th>Skeleton Spider</th>
<th>Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target payment cards and point of sale (PoS) systems.</td>
<td>Various forms of phishing, RDP compromise, known vulnerability compromise</td>
</tr>
<tr>
<td>Ryuk, LockerGoga, AbaddonPOS, Cobalt Strike, Golden Chickens, and Windows Credential Editor.</td>
<td>No known historic targeting of healthcare organizations; Have targeted US non-healthcare entities.</td>
</tr>
</tbody>
</table>

**Unknown**

https://attack.mitre.org/groups/G0037/
https://www.zdnet.com/article/cybercrime-group-fin6-evolves-from-pos-malware-to-ransomware/
### FIN7

<table>
<thead>
<tr>
<th>Possibly Carbanak/Anunak (attribution is not undisputed).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Russia</td>
</tr>
<tr>
<td>Heavy targeting of many US industries, especially finance. Several “high-ranking” Ukrainian national members of the group were arrested and convicted, awaiting sentencing; group continues to operate.</td>
</tr>
<tr>
<td>Living off the land, use of snail mail.</td>
</tr>
<tr>
<td>Carbanak, Cobalt Strike, Griffon, HALFBAKED, Mimikatz, POWERSOURCE, PsExec, SQLRAT.</td>
</tr>
<tr>
<td>Unknown</td>
</tr>
<tr>
<td>2018 - Series of high-profile breaches including Red Robin, Chili’s, Arby’s, Omni Hotels and Saks Fifth Avenue. 2017 - Spearphishing campaign targeting personnel involved in Securities and Exchange Commission (SEC) filings for various organizations.</td>
</tr>
</tbody>
</table>

- [https://www.wired.com/story/fin7-wild-inner-workings-billion-dollar-hacking-group/](https://www.wired.com/story/fin7-wild-inner-workings-billion-dollar-hacking-group/)
- [https://www.darkreading.com/analytics/fin7-cybercrime-gang-rises-again-/d/d-id/1334228](https://www.darkreading.com/analytics/fin7-cybercrime-gang-rises-again-/d/d-id/1334228)
- [https://attack.mitre.org/groups/G0046/](https://attack.mitre.org/groups/G0046/)
**FIN8**

<table>
<thead>
<tr>
<th>Unknown</th>
<th>Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heavy targeting of US retail, restaurant and hospitality industries.</td>
<td><strong>Spearphishing, memory scrapers, DLL injections, sandbox detection, zero-day compromises</strong></td>
</tr>
<tr>
<td></td>
<td><strong>PunchBuggy, PunchTrack, BADHATCH, credit card data collection tools, and ShellTea.</strong></td>
</tr>
<tr>
<td></td>
<td>2016 – Series of spearphishing campaigns targeting retail, restaurant and hospitality victims</td>
</tr>
<tr>
<td></td>
<td>2019 – Series of attacks using ShellTea/PunchBuggy attempting to compromise unnamed hospitality industry target</td>
</tr>
</tbody>
</table>

https://attack.mitre.org/groups/G0061/
<table>
<thead>
<tr>
<th><strong>FIN10</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Has sometimes signed extortion demands as “TeslaTeam” but possibly not the same group.</td>
</tr>
<tr>
<td>Unknown, however FireEye has stated that due to language analysis, FIN10 are likely not native-Russian speakers.</td>
</tr>
<tr>
<td>Operating since at least 2013. Focused on theft and extortion in North America, predominantly Canada but also in the United States. Historic targeting of casinos and mining industry.</td>
</tr>
<tr>
<td>RDP exploitation, Phishing; Sometimes known to destroy production systems/information (wipe critical files and force reboot) when extortion money was not paid.</td>
</tr>
<tr>
<td>Empire, SplinterRAT and other RATs, ransomware, Meterpreterd (Metasploit), destructive batch scripts.</td>
</tr>
<tr>
<td>No known historic targeting of healthcare organizations; Have targeted US non-healthcare entities.</td>
</tr>
<tr>
<td>Unknown</td>
</tr>
</tbody>
</table>

https://attack.mitre.org/groups/G0051/
Cyber Criminal Groups

Hidden Lynx

Aurora Panda, Axiom, Group 8, Moudour Trojan Campaign, Team Moudour, Team Naid.

China

Hackers for hire conducting information theft. Closely associated with APT17/Deputy Dog.

Zero days and custom exploits.

HiKit, Moudoor, Naid, GhostRAT

Have targeted US healthcare among other industries since 2012

Voho Campaign – One of the largest and most successful watering hole campaigns to date (including Bit9 breach)

https://exchange.xforce.ibmcloud.com/collection/be78e39c0cf8d529b3daed423e28904f
https://threatpost.com/large-scale-water-holing-attack-campaigns-hitting-key-targets-092512/77045/
https://www.veracode.com/moving-poisoning-ocean-poisoning-watering-hole
https://www.sentinelone.com/blog/the-curious-case-of-gh0st-malware/
### Orangeworm

<table>
<thead>
<tr>
<th>APT37, Reaper, Riccochet Chollima, Group 123, Red Eyes, Venus 121</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown</td>
</tr>
<tr>
<td>Originally discovered in 2015</td>
</tr>
<tr>
<td>Various forms of phishing, RDP compromise, known vulnerability compromise</td>
</tr>
<tr>
<td>Kwampirs</td>
</tr>
<tr>
<td>According to Symantec, 40% of Orangeworm’s targeting are healthcare organizations.</td>
</tr>
<tr>
<td>Primarily healthcare and pharmaceuticals, but also IT.</td>
</tr>
</tbody>
</table>

https://attack.mitre.org/groups/G0071/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia
https://blog.reversinglabs.com/blog/unpacking-kwampirs-rat
https://www.securityartwork.es/2019/03/13/orangeworm-group-kwampirs-analysis-update/
### Magecart

- Global consortium of at least twelve groups, unknown location(s).
- Unknown, but possibly geographically distributed
- Often target the Magento system
- Digital card skimming (formjacking), Magento compromises, advertisement banner infections, cross-site-scripting, backdoors, rogue admin account creation
- Pipka, also their web skimmer is known by Trend Micro as JS_OBFUS.C
- Have attacked healthcare targets.
- Ticketmaster, British Airways, NewEgg, Shopper Approved, Topps sports collectables, various University bookstores, Forbes magazine, MyPillow, Macy’s, Puma, The Guardian, Garmin, The American Cancer Society, Sesame Street online store

Additional links:
- [Magecart Attack: What It Is, How It Works, and How to Prevent It](https://www.techrepublic.com/article/magecart-attack-what-it-is-how-it-works-and-how-to-prevent-it/)
- [Magecart E-commerce Card Skimming Bonanza](https://threatpost.com/magecart-ecommerce-card-skimming-bonanza/147765/)
- [Magecart](https://www.ensighten.com/blog/magecart)
- [Magecart Hackers Persistent Credit Card Skimmer Groups](https://techcrunch.com/2018/11/13/magecart-hackers-persistent-credit-card-skimmer-groups/)
- [Magecart Credit Card Stealing Malware Proves Hard to Stop](https://www.nbcnews.com/tech/tech-news/what-magecart-credit-card-stealing-malware-proves-hard-stop-n948176)
- [Magecart](https://krebsonsecurity.com/tag/magecart/)
# Indrik Spider

<table>
<thead>
<tr>
<th>N/A</th>
<th>Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating since 2014. Along with Emotet, Dridex is considered one of the most prolific cybercrime banking trojans.</td>
<td>Various forms of phishing, RDP compromise, known vulnerability compromise</td>
</tr>
<tr>
<td>BitPaymer ransomware, Dridex</td>
<td>Have targeted US healthcare frequently</td>
</tr>
<tr>
<td>2017 – BitPaymer attack on UK National Health Service (NHS)</td>
<td></td>
</tr>
</tbody>
</table>

**Mummy Spider**

<table>
<thead>
<tr>
<th>TA542, ATK104, Mealybug, GOLD CRESTWOOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown, possibly Eastern Europe</td>
</tr>
<tr>
<td>Heavy collaboration with other “Spider” groups and associated malware variants (TrickBot, IcedID, Ryuk); Will often go operational for several months and then go “dark” for 3 to 12 months and emerge with Emotet with new capabilities</td>
</tr>
<tr>
<td>Botnets (Epoch 1, Epoch 2, and Epoch 3), various forms of phishing, RDP compromise, known vulnerability compromise</td>
</tr>
<tr>
<td>Emotet (Geodo)</td>
</tr>
<tr>
<td>Have targeted US healthcare frequently, along with other industries and other countries</td>
</tr>
</tbody>
</table>

2020 – Emotet using Coronavirus-themed spam campaign to infect systems
2017 – First Emotet campaign to expand targets beyond banking and finance to include healthcare, manufacturing and others

https://malpedia.caad.fkie.fraunhofer.de/actor/mummy_spider
https://www.malwarebytes.com/emotet/
https://malpedia.caad.fkie.fraunhofer.de/details/win.emotet
## Wizard Spider

<table>
<thead>
<tr>
<th>TEMP.MixMaster</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown, possibly Eastern Europe</td>
</tr>
<tr>
<td>Heavy collaboration with other “Spider” groups and associated malware variants (Emotet, IcedID, Ryuk);</td>
</tr>
<tr>
<td>Various forms of phishing, RDP compromise, known vulnerability compromise</td>
</tr>
<tr>
<td>Trickbot, Dyre, Empire</td>
</tr>
<tr>
<td>Have targeted US healthcare frequently, along with other industries and other countries</td>
</tr>
<tr>
<td>Significant overlap with Emotet activity</td>
</tr>
</tbody>
</table>

https://attack.mitre.org/groups/G0102/
https://labs.sentinelone.com/inside-a-trickbot-cobaltstrike-attack-server/
https://www.crowdstrike.com/blog/wizard-spider-lunar-spider-shared-proxy-module/
## Grim Spider

<table>
<thead>
<tr>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Some believe Grim Spider has ties to FIN6, but not significantly documented.</td>
</tr>
<tr>
<td>Unknown</td>
</tr>
<tr>
<td>Heavy collaboration with other “Spider” groups and associated malware variants (Emotet, IcedID, TrickBot); In operation since August 2018. They like to go “big game hunting”.</td>
</tr>
<tr>
<td>Various forms of phishing, RDP compromise, known vulnerability compromise; Often dropped by TrickBot</td>
</tr>
<tr>
<td>Ryuk ransomware</td>
</tr>
<tr>
<td>Have targeted US healthcare frequently</td>
</tr>
<tr>
<td>2019 – Used to attack many US state and local government organizations</td>
</tr>
</tbody>
</table>

https://n1ght-w0lf.github.io/malware%20analysis/ryuk-ransomware/
https://www.crowdstrike.com/blog/timelining-grim-spiders-big-game-hunting-tactics/
## Cyber Criminal Groups

### Sodinokibi

<table>
<thead>
<tr>
<th>Sodin, REvil</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown</td>
</tr>
</tbody>
</table>

Possible predecessor to Gandcrab. Operational since early 2019. Has infected thousands of clients via managed service provider compromise.

- Various forms of phishing, RDP compromise, known vulnerability compromise, zero day vulnerability exploitation, managed service provider compromise

- Sodinokibi/REvil ransomware

- Have targeted US healthcare frequently

- 2019 Oracle Weblogic compromise allowed for mass proliferation

[https://www.cybereason.com/blog/the-sodinokibi-ransomware-attack](https://www.cybereason.com/blog/the-sodinokibi-ransomware-attack)
[https://blog.malwarebytes.com/detections/ransom-sodinokibi/](https://blog.malwarebytes.com/detections/ransom-sodinokibi/)
[https://portswigger.net/daily-swig/what-is-sodinokibi-the-ransomware-behind-the-travelex-attack](https://portswigger.net/daily-swig/what-is-sodinokibi-the-ransomware-behind-the-travelex-attack)
Cybercrime Trends

2019 – Cybercriminal modify tactics, techniques and procedures

- Managed Service Provider (MSP) compromise – 13
  - Two healthcare organizations permanently closed due to ransomware attacks

- Maze exfiltrates data prior to encryption and uses it as further leverage
  - Others followed suit: AKO, CLoP, CryLock, DoppelPaymer, Nemty, Nephilim, Netwalker, ProLock, Pysa (Mespinoza), RagnarLocker, Revil (Sodinokibi), Sekhmet, Snake, Snatch

- Maze begins charging to NOT leak the stolen data
  - Maze begins selling the data for a third fee

- Per New York Times (using Emsisoft data), in 2019 there was a 41% increase in submission of files to publicly available decryptors

2020 – Continual evolution of cybercriminal tactics, techniques and procedures

- Maze shares their leak site with other operators
  - Criminal “cartel”
COVID-19 Pandemic and healthcare-related cybercrime

- 8X increase in Coronavirus related phishing from January to February, and again from February to March

"...the COVID-19 pandemic provides criminal opportunities on a scale likely to dwarf anything seen before. The speed at which criminals are devising and executing their schemes is truly breathtaking."

Michael D’Ambrosio, Head of the U.S. Secret Service Office of Investigations

Terry Wade, lead of the Federal Bureau of Investigation Criminal, Cyber, Response and Services Branch.

WashingtonPost.com, April 14, 2020
Examples of COVID-related phishing e-mails

Re:SAFETY CORONA VIRUS AWARENESS WHO

World Health Organization

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.

Click on the button below to download

Safety measures

Symptoms common symptoms include fever, cough, shortness of breath and breathing difficulties.

Regards,

Dr. Stella Chungong
Specialist wuhan-virus-advisory

Distributed via the CDC Health Alert Network
February 4, 2020
CDCHAN-00426

Dear [REDACTED]

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-ncov/newcases-cities.html)

You are immediately advised to go through the cases above to avoid potential hazards.

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention
Cybercrime Trends (continued)

COVID-19 Pandemic

Fake Coronavirus tracking map drops AZORult on victim systems.
March 2020 – Owner Bleepingcomputer.com contacted ransomware operators to ask if they would continue cyberattacks during pandemic

- Clop
- Maze
- DoppelPaymer
- Nefilim
- Ryuk
- Sodinokibi/Revel
- PwndLocker
- Ako

Clop, Nefilim and DoppelPaymer claimed they don’t attack hospitals
Maze promised to cease attacks against medical organizations during the pandemic
Netwalker (incorrectly) asserted that hospitals are not targeted by ransomware

Yet…

Maze attacked a London-based medical research company
Netwalker attacked Champaign-Urbana Public Health District in Illinois
Sodinokibi attacked Genomics (American biotech company)

"As hospitals and medical organizations around the world are working non-stop to preserve the well-being of individuals stricken with the coronavirus, they have become targets for ruthless cybercriminals who are looking to make a profit at the expense of sick patients"

Secretary General Jürgen Stock of Interpol
# Cybercrime, Fraud, and Money Laundering

<table>
<thead>
<tr>
<th>BEC</th>
<th>Ransomware</th>
<th>Synthetic Identity Fraud</th>
<th>Data Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Engineering</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phishing</td>
<td>Spear Phishing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malware</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insider Threat</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drive by Exploits</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Exfiltration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extortion</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Fraud</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Healthcare &amp; Medicare Fraud</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cryptocurrencies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Money Laundering</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
BEC in the Health Sector

CYBERCRIME

- Darkweb Marketplaces
- Cybercriminal Forums

- Phishing/Spear-Phishing
- Malware
- Spoofing
- Fake Invoicing

Data

- Pharmaceuticals + Supplies
- W-2 Wage

FRAUD

- Romance Fraud/Confidence Fraud
- Lottery Scams
- Employment Scams
- Non-Payment/Non-Delivery Scams
- Elder Abuse/Scams

MONEY LAUNDERING

- Cryptocurrencies
- Gift Cards/Pre-Paid Cards
- Cash
- Money Services Businesses (MSBs)
- Bank Transfers

Images Sources: Creative Commons & FBI

(CISA, 2009) (IC3, 2019)

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

TLP: WHITE, ID# 202007301000 27
Ransomware in the Health Sector

**CYBERCRIME**
- Darkweb Marketplaces
- Cybercriminal Forums

**EXTORTION**
- Infection
  - Email
  - Compromised Website
  - Exploit Kit
- Data Exfiltration
- Files Decrypted After Ransom Paid

**MONEY LAUNDERING**
- Ransom Paid in Bitcoin
- Cybercriminals cash out ransom payment through virtual currency exchangers
- Ransoms converted to fiat currency

Image Source: Creative Commons
By leveraging synthetic identities and shell corporations, cybercriminals target healthcare organizations, insurers, and programs like Medicaid and Medicare for financial gain.
Synthetic Identity Fraud in the Health Sector

**CYBERCRIME**
- Darkweb Marketplaces
- Cybercriminal Forums
- Infection
  - Email
  - Compromised Website
  - Exploit Kit
- Data Exfiltration

**FRAUD**
- Stolen PII PHI
- Complicit medical or shell corporations
- Creation and aging of synthetic identities

**MONEY LAUNDERING**
- Cybercriminals
- Apply for and receive medical or insurance benefits

Image Source: Creative Commons

TLP: WHITE, ID# 202007301000
DDoS For Hire in Darkweb

---

**DDOS ATTACK with my Botnet: 24 hours ddos on your website target (100% SATISFACTION)**

DDOS ATTACK: I will point my botnet on your website target DURING 24 HOURS. If your target is DDOS protected by Cloudflare, Incapsula, Akami or any other kind of protection, please order my offer twice. No Guarantee of downtime as the target can mitigate the attack in some ways but I will do my best to provide the maximum downtime possible during these 24 hours. PLEASE CHECK FEEDBACK 100% SAT...

Sold by amelia75 - 94 sold since Aug 19, 2016  
Vendor Level 2  Trust Level 4

<table>
<thead>
<tr>
<th>Product class</th>
<th>Features</th>
<th>Origin country</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Digital goods</td>
<td>Worldwide</td>
<td>Worldwide</td>
</tr>
<tr>
<td>Quantity left</td>
<td>Unlimited</td>
<td>Ships to</td>
<td>Worldwide</td>
</tr>
<tr>
<td>Ends in</td>
<td>Never</td>
<td>Payment</td>
<td>Escrow</td>
</tr>
</tbody>
</table>

Default - 1 days - USD +0.00 / item

Purchase price: USD 27.77

**Product Description**

DDOS ATTACK: I will point my botnet on your website target DURING 24 HOURS.
If your target is DDOS protected by Cloudflare, Incapsula, Akami or any other kind of protection, please order my offer twice.

No Guarantee of downtime as the target can mitigate the attack in some ways but I will do my best to provide the maximum downtime possible during these 24 hours.

PLEASE CHECK FEEDBACK 100% SATISFACTION!
# DDoS in the Health Sector

<table>
<thead>
<tr>
<th>Technique</th>
<th>Targets</th>
<th>OSI Layer</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Flood</td>
<td>Application</td>
<td>Layer 7: FTP, HTTP, POP3, &amp; SMTP</td>
<td>This technique uses simple or complex methods of harnessing IP addresses to target URLs using random referrers and user agents to flood the server.</td>
<td>2020 Threat actor seeks insiders with intent to DDoS and steal from US entities</td>
</tr>
<tr>
<td>SYN Flood</td>
<td>Infrastructure</td>
<td>Layers 3 &amp; 4: IP, ICMP, ARP, RIP, TCP, &amp; UDP</td>
<td>This technique sends requests to connect with the target server but does not complete the three-way handshake, which leaves the connected port occupied and unavailable for legitimate users.</td>
<td>2020 attack on fed. gov.</td>
</tr>
<tr>
<td>DNS Amplification</td>
<td>Bandwidth</td>
<td>Layers 3 &amp; 4: IP, ICMP, ARP, RIP, TCP, &amp; UDP</td>
<td>This technique uses open DNS servers to flood a target system with DNS response traffic via botnets, which produce large numbers of spoofed DNS queries.</td>
<td>2014 Boston Children’s Hospital attacked</td>
</tr>
</tbody>
</table>

(TREND MICRO, n.d.) (IC3, 2019)

Image Source: Creative Commons

---

**Darkweb: DDoS-as-a-Service**

**Distraction: DDoS as a misdirect for additional attacks**

**Impact: DDoS for political, hacktivism, and extortion goals**

2020 Threat actor seeks insiders with intent to DDoS and steal from US entities

2020 attack on fed. gov.

2014 Boston Children’s Hospital attacked

2014 attack against two US hospitals
References

• 6 New MSPs and/or Cloud-Based Service Providers Compromised by Ransomware, A Total of 13 for 2019, Reports Armor – Report
  • https://www.armor.com/resources/new-msps-compromised-reports-armor/

• Ransomware Attacks Grow, Crippling Cities and Businesses

• Ransomware Payments Up 33% As Maze and Sodinokibi Proliferate in Q1 2020
  • https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report

• Managed service providers a growing target for ransomware attackers
  • https://statescoop.com/ransomware-managed-service-providers-local-government/

• ‘Nobody is safe from this’: Cybercrime in health care

• Why Cyber-Criminals Are Attacking Healthcare -- And How To Stop Them
  • https://www.forbes.com/sites/kateoflahertyuk/2018/10/05/why-cyber-criminals-are-attacking-healthcare-and-how-to-stop-them/#374497737f69

• Ransomware Attacks on Healthcare Providers Rose 350% in Q4 2019

• 5 Ways to Defend Your Medical Practice Against Ransomware
  • https://healthtechmagazine.net/article/2020/05/5-ways-defend-your-medical-practice-against-ransomware

Please refer to the reference section of individual cybercriminal threat groups above for further information on each of them.
Questions

Upcoming Briefs

- Cybersecurity Maturity Models
- COVID-19 Cyber Threats Update

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.
About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

**Sector & Victim Notifications**
Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

**White Papers**
Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

**Threat Briefings & Webinar**
Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Visit us at: www.HHS.Gov/HC3
Contact

Health Sector Cybersecurity Coordination Center (HC3)
(202) 691-2110
HC3@HHS.GOV