LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Healthcare Cybercrime

07/30/2020

Report #: 202007301000

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

Image source: FBI

Slides Key:

👤	Non-Technical: managerial, strategic and high-level (general audience)
⚙	Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Terminology

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

© MARK ANDERSON, WWW.ANDERTOONS.COM
ANDERSON
"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

LEGEND:

- ALIASES
- LOCATION
- DESCRIPTION
- TTPs
- WEAPONS
- RELEVANCE TO HPH
- MAJOR OPERATIONS
- SOURCING

Cyber Criminal Groups

APT 19

Cordoso, C0d0so0, Sunshop Group, possibly DarkHydrus, possibly Deep Panda
China
Freelancers, loosely connected to the Chinese government, who target multiple industries, including pharmaceuticals.
Phishing, Watering holes
Cobalt Strike, C0d0so0, Empire, Derusbi, Beacon, PowerShell, various zero-days
Previously targeted pharmaceuticals
2017 – Phishing campaign targeting a series of law firms Forbes.com (watering hole attack)
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/ https://www.darkreading.com/attacks-breaches/chinese-hacking-group-codoso-team-uses-forbescom-as-watering-hole-/d/d-id/1319059

Cyber Criminal Groups

Corkow

Metel
Russia
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.
keystroke logging, screenshot capture, HTTP form-grabbing
Corkow/Metel,
No known historic targeting of healthcare organizations; Have targeted US non-healthcare entities.
Multiple attacks against banks in Russia and Ukraine
https://www.welivesecurity.com/2014/02/27/corkow-analysis-of-a-business-oriented-banking-trojan/ https://www.group-ib.com/resources/threat-research/corkow.html https://securelist.com/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/73638/ https://www.virusradar.com/en/Win32_Corkow.F/description https://fortune.com/2016/02/08/russian-hackers-currency-rate/

Cyber Criminal Groups

Desert Falcons

APT-C-23, Two-tailed Scorpion, Arid Viper
Gaza, but possibly geographically disbursed
Described by Kaspersky as “cybermercinaries”; 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
Social Engineering (political and current event-themed phishing
Arid Viper, DHS, DHS2015 (iRAT), custom malware (including mobile), FrozenCell, GlanceLove, GnatSpy, KASPERAGENT, MICROPSIA, Micropsia, GnatSpy, VAMP and ViperRAT.
No known historic targeting of healthcare organizations; Have targeted US non-healthcare entities.
Operation Arid Viper
https://usa.kaspersky.com/resource-center/threats/desert-falcons-malware https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064309/The-Desert-Falcons-targeted-attacks.pdf

Cyber Criminal Groups

FIN4

Wolf Spider
Romania
Attempt to manipulate stock markets via exfiltrated proprietary/confidential/insider information. Attempts to access e-mail and other non-public access.
Phishing (including spearphishing), credential harvesting, business e-mail compromise, watering holes
FIN4 Don’t often use malware
Healthcare and pharmaceutical
Unknown
https://attack.mitre.org/groups/G0085/ https://www.fireeye.com/current-threats/threat-intelligence-reports/rpt-fin4.html https://www.fireeye.com/blog/threat-research/2014/11/fin4_stealing_insid.html https://www.computerworld.com/article/2853697/fireeye-suspects-fin4-hackers-are-americans-after-insider-info-to-game-stock-market.html https://www.computerworld.com/article/2939441/sec-said-to-be-investigating-corporate-hacks-by-fin4-group.html

Cyber Criminal Groups

FIN6

Skeleton Spider
Unknown
Target payment cards and point of sale (PoS) systems.
Various forms of phishing, RDP compromise, known vulnerability compromise
Ryuk, LockerGoga, AbaddonPOS, Cobalt Strike, Golden Chickens, and Windows Credential Editor.
No known historic targeting of healthcare organizations; Have targeted US non-healthcare entities.
Unknown
https://attack.mitre.org/groups/G0037/ https://usa.visa.com/dam/VCOM/global/support-legal/documents/fin6-cybercrime-group-expands-threat-To-ecommerce-merchants.pdf https://threatpost.com/fin6-and-trickbot-combine-forces-in-anchor-attacks/154508/ https://www.zdnet.com/article/cybercrime-group-fin6-evolves-from-pos-malware-to-ransomware/ https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin6.pdf

Cyber Criminal Groups

FIN7

Possibly Carbanak/Anunak (attribution is not undisputed).
Russia
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.
Living off the land, use of snail mail.
Carbanak, Cobalt Strike, Griffon, HALFBAKED, Mimikatz, POWERSOURCE, PsExec, SQLRAT.
Unknown
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.
https://www.wired.com/story/fin7-wild-inner-workings-billion-dollar-hacking-group/ https://duo.com/decipher/fin7-attackers-roll-out-new-tools https://www.darkreading.com/analytics/fin7-cybercrime-gang-rises-again-/d/d-id/1334228 https://attack.mitre.org/groups/G0046/ https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html https://www.justice.gov/usao-wdwa/united-states-vs-fedir-oleksiyovych-hladyr-united-states-vs-dmytro-valerievich-fedorov

Cyber Criminal Groups

FIN8

Unknown
Unknown
Heavy targeting of US retail, restaurant and hospitality industries.
Spearphishing, memory scrapers, DLL injections, sandbox detection, zero-day compromises
PunchBuggy, PunchTrack, BADHATCH, credit card data collection tools, and ShellTea.
2016 – Series of spearphishing campaigns targeting retail, restaurant and hospitality victims 2019 – Series of attacks using ShellTea/PunchBuggy attempting to compromise unnamed hospitality industry target
https://attack.mitre.org/groups/G0061/ https://www.zdnet.com/article/fin8-hackers-return-after-two-years-with-attacks-against-hospitality-sector/ https://www.documentcloud.org/documents/6575126-Visa-Security-Alert-CYBERCRIME-GROUPS-TARGETING.html https://www.gigamon.com/content/dam/resource-library/english/infographic/in-atr-fin8-process.pdf https://www.fireeye.com/blog/threat-research/2017/06/obfuscation-in-the-wild.html https://threatpost.com/fin8-targets-card-data-fuel-pumps/151105/

Cyber Criminal Groups

FIN10

Has sometimes signed extortion demands as “TeslaTeam” but possibly not the same group.
Unknown, however FireEye has stated that due to language analysis, FIN10 are likely not native-Russian speakers.
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.
RDP exploitation, Phishing; Sometimes known to destroy production systems/information (wipe critical files and force reboot) when extortion money was not paid.
Empire, SplinterRAT and other RATs, ransomware, Meterpreted (Metasploit), destructive batch scripts.
No known historic targeting of healthcare organizations; Have targeted US non-healthcare entities.
Unknown
https://www.fireeye.com/blog/threat-research/2017/06/fin10-anatomy-of-a-cyber-extortion-operation.html https://attack.mitre.org/groups/G0051/ https://blog.knowbe4.com/fin10-anatomy-of-a-ransomware-phishing-extortion-operation https://www.lloydsadd.com/news/fin10-intrusion-operations-predominately-targeting-canadian-organizations-fireeye/ https://www.darkreading.com/threat-intelligence/fin10-threat-actors-hack-and-extort-canadian-mining-casino-industries-/d/d-id/1329160

Cyber Criminal Groups

Hidden Lynx

Aurora Panda, Axiom, Group 8, Mourdour 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://www.wired.com/images_blogs/threatlevel/2013/09/hidden_lynx_final.pdf https://exchange.xforce.ibmcloud.com/collection/be78e39c0cf8d529b3daed423e28904f https://www.infosecurity-magazine.com/news/the-voho-campaign-gh0st-rat-spread-by-water-holing/ 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/

Cyber Criminal Groups

Orangeworm

APT37, Reaper, Riccochet Chollima, Group 123, Red Eyes, Venus 121
Unknown
Originally discovered in 2015
Various forms of phishing, RDP compromise, known vulnerability compromise
Kwampirs
According to Symantec, 40% of Orangeworm’s targeting are healthcare organizations.
Primarily healthcare and pharmaceuticals, but also IT.
https://attack.mitre.org/groups/G0071/ https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia http://www.documentcloud.org/documents/6821581-FLASH-CP-000111-MW-Downgraded-Version.html https://blog.reversinglabs.com/blog/unpacking-kwampirs-rat https://www.securityartwork.es/2019/03/13/orangeworm-group-kwampirs-analysis-update/ https://www.zdnet.com/article/fbi-re-sends-alert-about-supply-chain-attacks-for-the-third-time-in-three-months/

Cyber Criminal Groups

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
https://www.techrepublic.com/article/magecart-attack-what-it-is-how-it-works-and-how-to-prevent-it/ https://threatpost.com/magecart-ecommerce-card-skimming-bonanza/147765/ https://www.ensighten.com/blog/magecart https://techcrunch.com/2018/11/13/magecart-hackers-persistent-credit-card-skimmer-groups/ https://www.nbcnews.com/tech/tech-news/what-magecart-credit-card-stealing-malware-proves-hard-stop-n948176 https://krebsonsecurity.com/tag/magecart/

Cyber Criminal Groups

Indrik Spider

👤	N/A
📍	Unknown
📄	Operating since 2014. Along with Emotet, Dridex is considered one of the most prolific cybercrime banking trojans.
✖	Various forms of phishing, RDP compromise, known vulnerability compromise
🔫	BitPaymer ransomware, Dridex
❤	Have targeted US healthcare frequently
$	2017 – BitPaymer attack on UK National Health Service (NHS)
📖	https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/ https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf https://blog.trendmicro.com/trendlabs-security-intelligence/ursnif-emotet-dridex-and-bitpaymer-gangs-linked-by-a-similar-loader/ https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/ https://www.blueliv.com/downloads/documentation/reports/Network_insights_of_Dyre_and_Dridex_Trojan_bankers.pdf

Cyber Criminal Groups

Mummy Spider

TA542, ATK104, Mealybug, GOLD CRESTWOOD
Unknown, possibly Eastern Europe
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
Botnets (Epoch 1, Epoch 2, and Epoch 3), various forms of phishing, RDP compromise, known vulnerability compromise
Emotet (Geodo)
Have targeted US healthcare frequently, along with other industries and other countries
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://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-february-mummy-spider/ https://malpedia.caad.fkie.fraunhofer.de/actor/mummy_spider https://www.malwarebytes.com/emotet/ https://malpedia.caad.fkie.fraunhofer.de/details/win.emotet https://blog.trendmicro.com/trendlabs-security-intelligence/emotet-returns-starts-spreading-via-spam-botnet/ https://krebsonsecurity.com/2019/09/secret-service-investigates-breach-at-u-s-govt-it-contractor/

Cyber Criminal Groups

Wizard Spider

TEMP.MixMaster
Unknown, possibly Eastern Europe
Heavy collaboration with other “Spider” groups and associated malware variants (Emotet, IcedID, Ryuk);
Various forms of phishing, RDP compromise, known vulnerability compromise
Trickbot, Dyre, Empire
Have targeted US healthcare frequently, along with other industries and other countries
Significant overlap with Emotet activity
https://attack.mitre.org/groups/G0102/ https://www.advanced-intel.com/post/trickbot-group-launches-test-module-alerting-on-fraud-activity https://www.crowdstrike.com/blog/wizard-spider-adds-new-feature-to-ryuk-ransomware/ https://labs.sentinelone.com/inside-a-trickbot-cobaltstrike-attack-server/ https://www.crowdstrike.com/blog/wizard-spider-lunar-spider-shared-proxy-module/ https://www.govcert.ch/blog/trickbot-an-analysis-of-data-collected-from-the-botnet/

Cyber Criminal Groups

Grim Spider

👤	Some believe Grim Spider has ties to FIN6, but not significantly documented
📍	Unknown
📄	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”.
✗	Various forms of phishing, RDP compromise, known vulnerability compromise; Often dropped by TrickBot
🔫	Ryuk ransomware
❤	Have targeted US healthcare frequently
$	2019 – Used to attack many US state and local government organizations
📖	https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/ https://n1ght-w0lf.github.io/malware%20analysis/ryuk-ransomware/ https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ryuk-ransomware-attack-rush-to-attribution-misses-the-point/ https://www.crowdstrike.com/blog/wizard-spider-adds-new-feature-to-ryuk-ransomware/ https://blog.intel471.com/2020/04/14/understanding-the-relationship-between-emotet-ryuk-and-trickbot/ https://www.crowdstrike.com/blog/timelining-grim-spiders-big-game-hunting-tactics/

Cyber Criminal Groups

Sodinokibi

Sodin, REvil
Unknown
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.picussecurity.com/blog/a-brief-history-and-further-technical-analysis-of-sodinokibi-ransomware https://www.cybereason.com/blog/the-sodinokibi-ransomware-attack https://healthitsecurity.com/news/new-ransomware-spotted-targeting-health-tech-orgs-via-supply-chain https://www.hhs.gov/sites/default/files/sodinokibi-aggressive-ransomware-impacting-hph-sector.pdf https://blog.malwarebytes.com/detections/ransom-sodinokibi/ https://portswigger.net/daily-swig/what-is-sodinokibi-the-ransomware-behind-the-travelex-attack

Cybercrime Trends

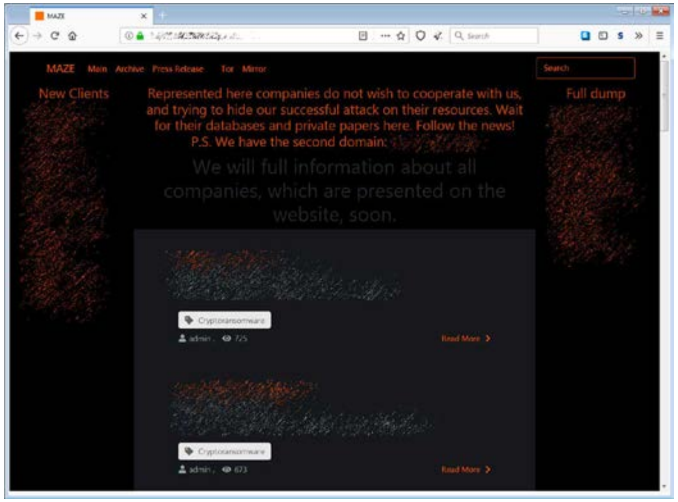
2019 – Cybercriminal modify tactics, techniques and procedures

- 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”

Image source: Bleeping Computer



[redacted]

Represented here companies do not wish to cooperate with us, and trying to hide our successful attack on their resources. Wait for their databases and private papers here. Follow the news! P.S. We have the second domain: [redacted]

We will full information about all companies, which are presented on the website, soon.

[redacted]

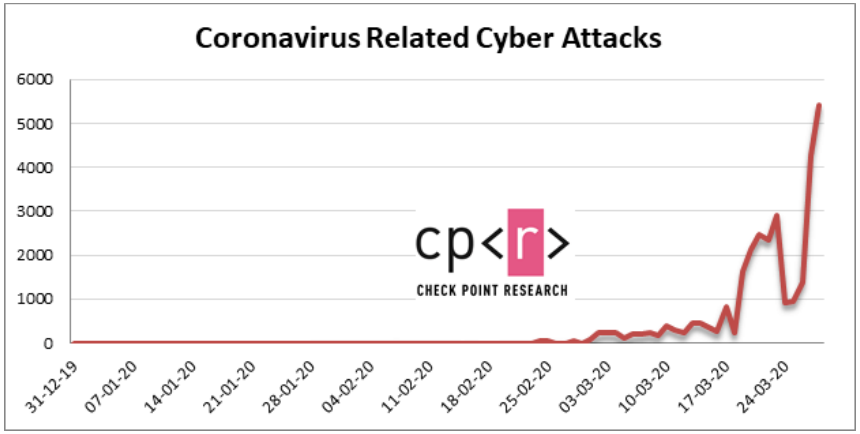
[redacted]

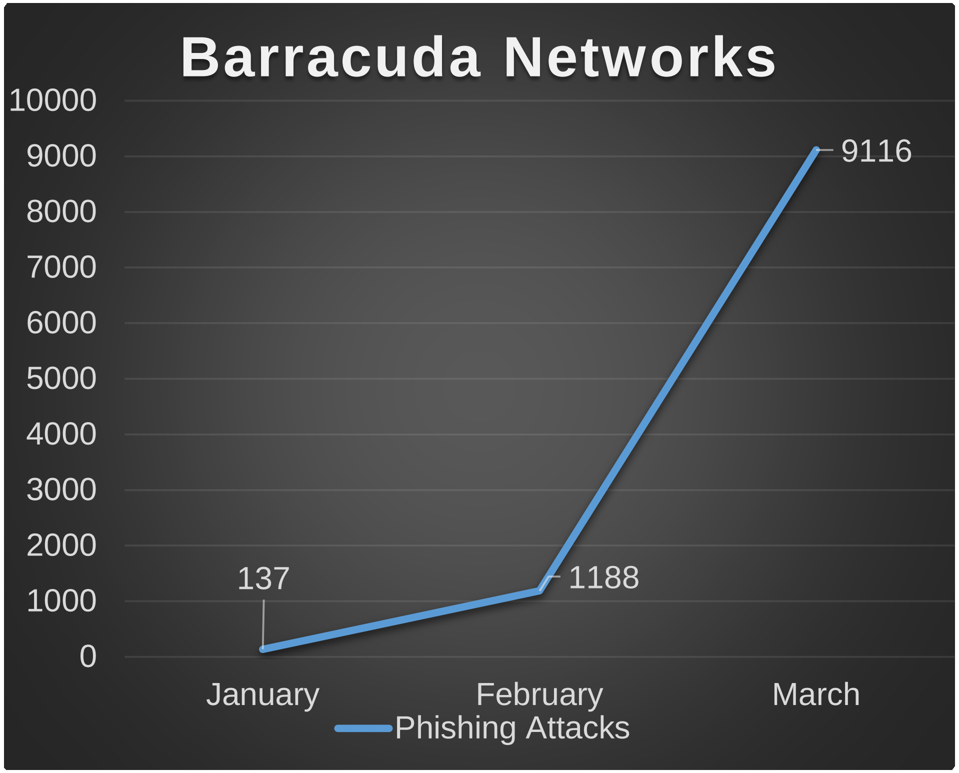
[redacted]

Cybercrime Trends (continued)

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."

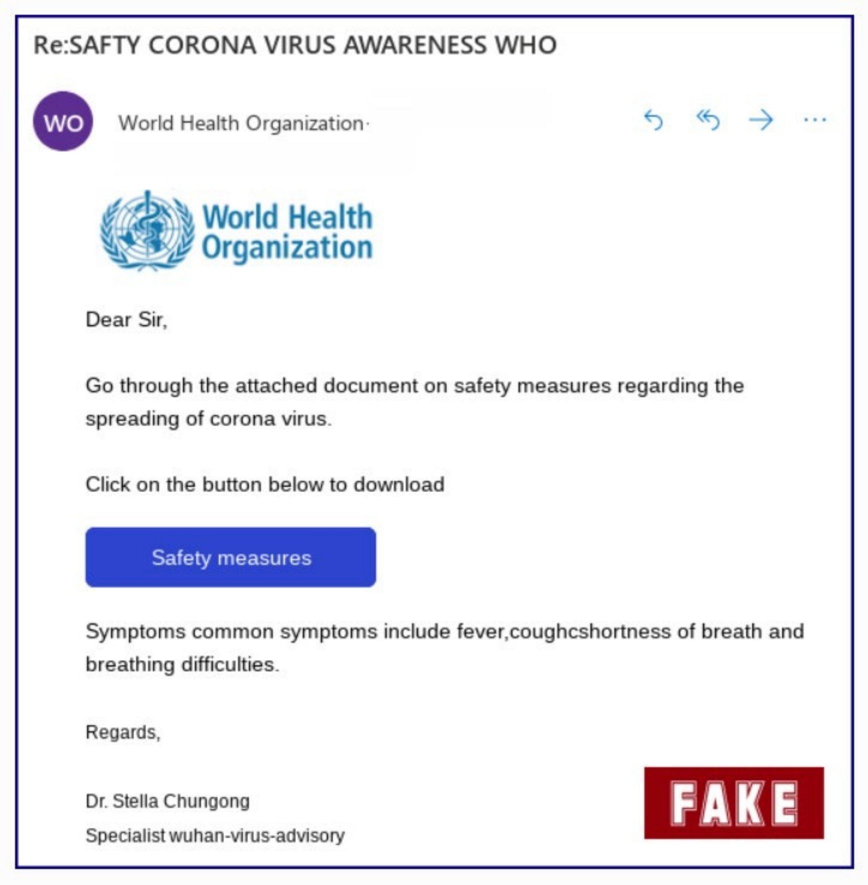
Michael D'Ambrosio, Head of the U.S. Secret Service Office of Investigations

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

WashingtonPost.com, April 14, 2020

Cybercrime Trends (continued)

Examples of COVID-related phishing e-mails



Re:SAFTY CORONA VIRUS AWARENESS WHO

WO 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

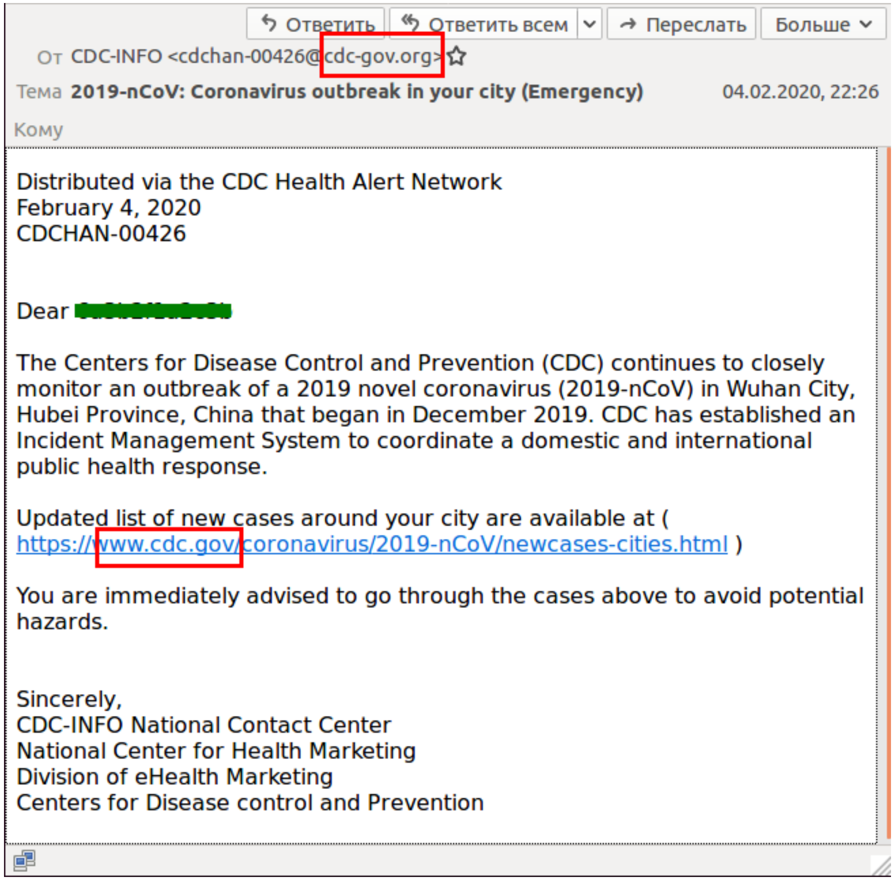
Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulties.

Regards,

Dr. Stella Chungong

Specialist wuhan-virus-advisory

FAKE



От CDC-INFO <cdchan-00426@cdc-gov.org>

Тема **2019-nCoV: Coronavirus outbreak in your city (Emergency)** 04.02.2020, 22:26

Кому

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)

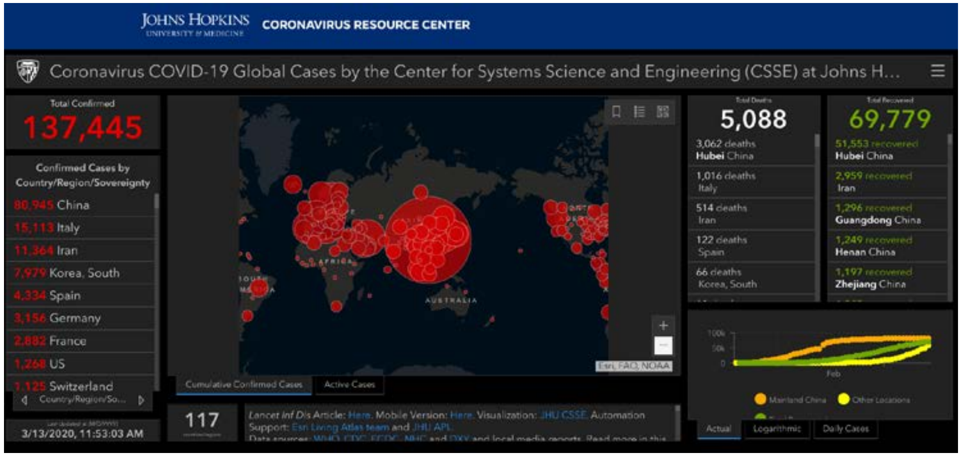
You are immediately advised to go through the cases above to avoid potential hazards.

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

Legitimate Map



Coronavirus COVID-19 Global Cases by the Center for Systems Science and Engineering (CSSE) at Johns H...

Total Confirmed
137,445

Confirmed Cases by Country/Region/Sovereignty

80,945	China
15,113	Italy
11,364	Iran
7,979	Korea, South
4,334	Spain
3,156	Germany
2,882	France
1,268	US
1,125	Switzerland

Country/Region/So...

Last Updated at (M/D/YYYY)
3/13/2020, 11:53:03 AM

117

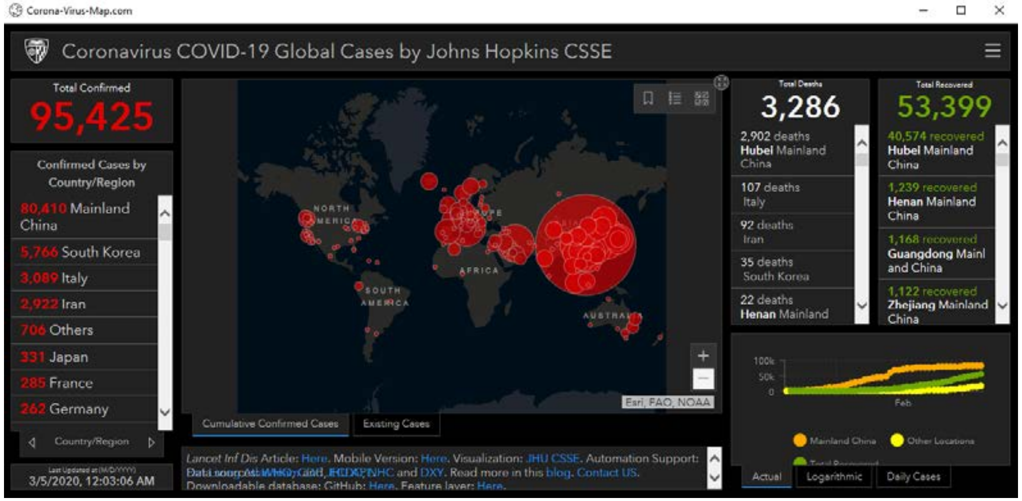
Lancet Inf Dis Article: Here. Mobile Version: Here. Visualization: JHU CSSE. Automation Support: Esri Living Atlas team and JHU APL.
Data sources: WHO, CDC, ECDC, NHC and DXY and local media reports. Read more in this

Total Deaths
5,088

- 3,062 deaths Hubei China
- 1,016 deaths Italy
- 514 deaths Iran
- 122 deaths Spain
- 66 deaths Korea, South

Total Recovered
69,779

- 51,553 recovered Hubei China
- 2,959 recovered Iran
- 1,296 recovered Guangdong China
- 1,249 recovered Henan China
- 1,197 recovered Zhejiang China



Coronavirus COVID-19 Global Cases by Johns Hopkins CSSE

Total Confirmed
95,425

Confirmed Cases by Country/Region

80,410	Mainland China
5,766	South Korea
3,089	Italy
2,922	Iran
706	Others
331	Japan
285	France
262	Germany

Country/Region

Last Updated at (M/D/YYYY)
3/5/2020, 12:03:06 AM

Lancet Inf Dis Article: Here. Mobile Version: Here. Visualization: JHU CSSE. Automation Support: Data sources: WHO, CDC, ECDC, NHC and DXY. Read more in this blog. Contact US.
Downloadable database: GitHub: Here. Feature layer: Here.

Total Deaths
3,286

- 2,902 deaths Hubei Mainland China
- 107 deaths Italy
- 92 deaths Iran
- 35 deaths South Korea
- 22 deaths Henan Mainland

Total Recovered
53,399

- 40,574 recovered Hubei Mainland China
- 1,239 recovered Henan Mainland China
- 1,168 recovered Guangdong Mainl and China
- 1,122 recovered Zhejiang Mainland China

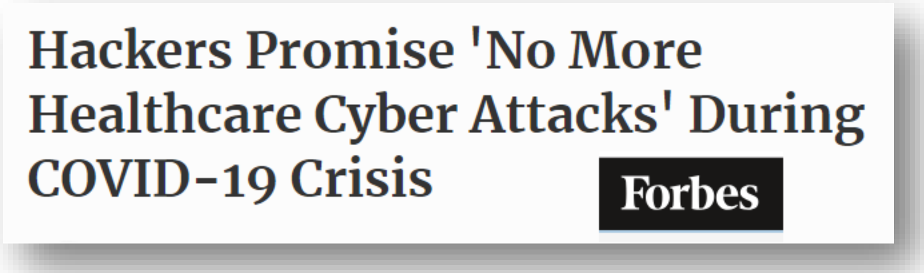
Fake Map

Fake Coronavirus tracking map drops AZORult on victim systems.

Cybercrime Trends (continued)

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



Hackers Promise 'No More Healthcare Cyber Attacks' During COVID-19 Crisis

Forbes

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…

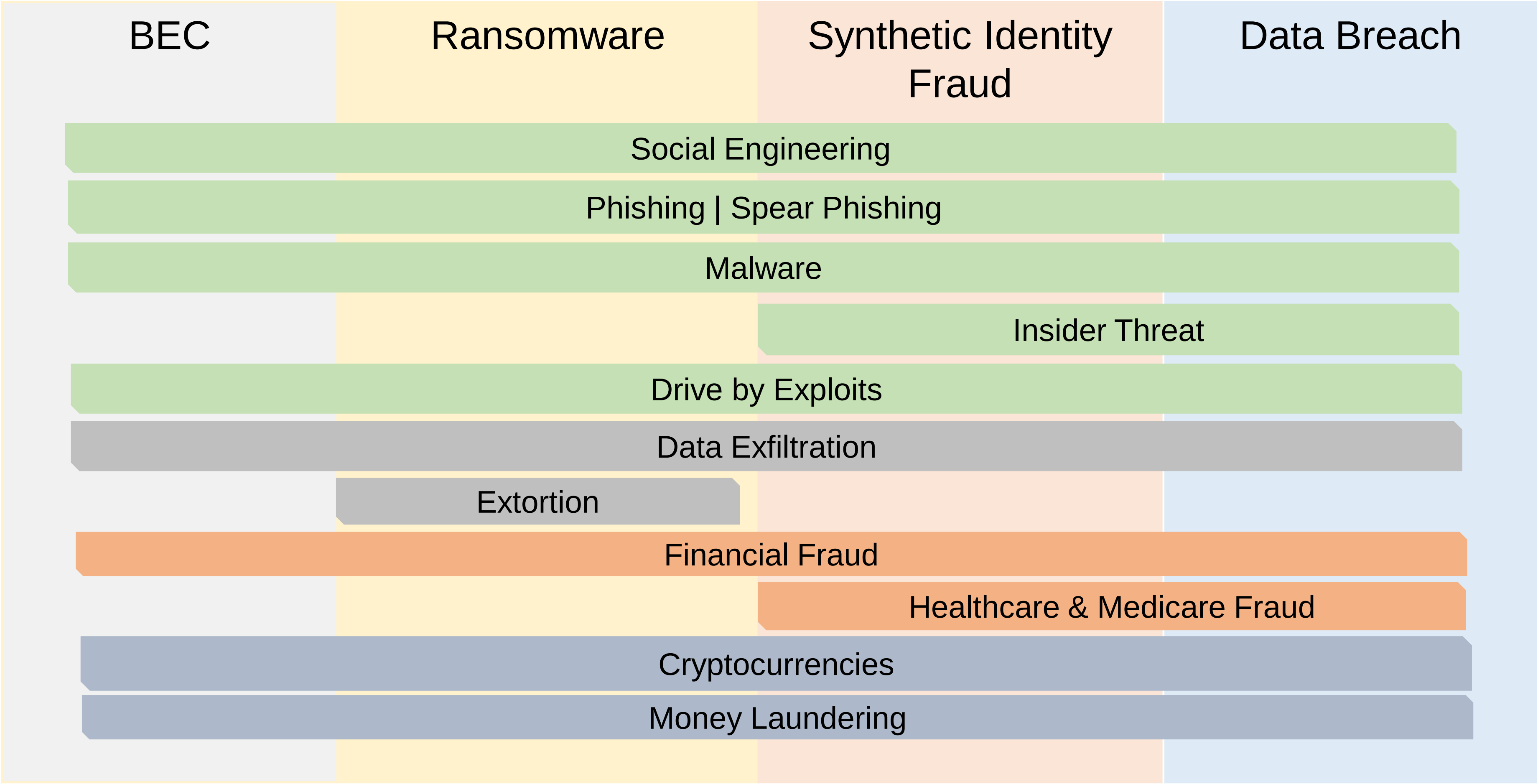
Maze attacked a London-based medical research company

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



BEC

Ransomware

Synthetic Identity Fraud

Data Breach

Social Engineering

Phishing | Spear Phishing

Malware

Insider Threat

Drive by Exploits

Data Exfiltration

Extortion

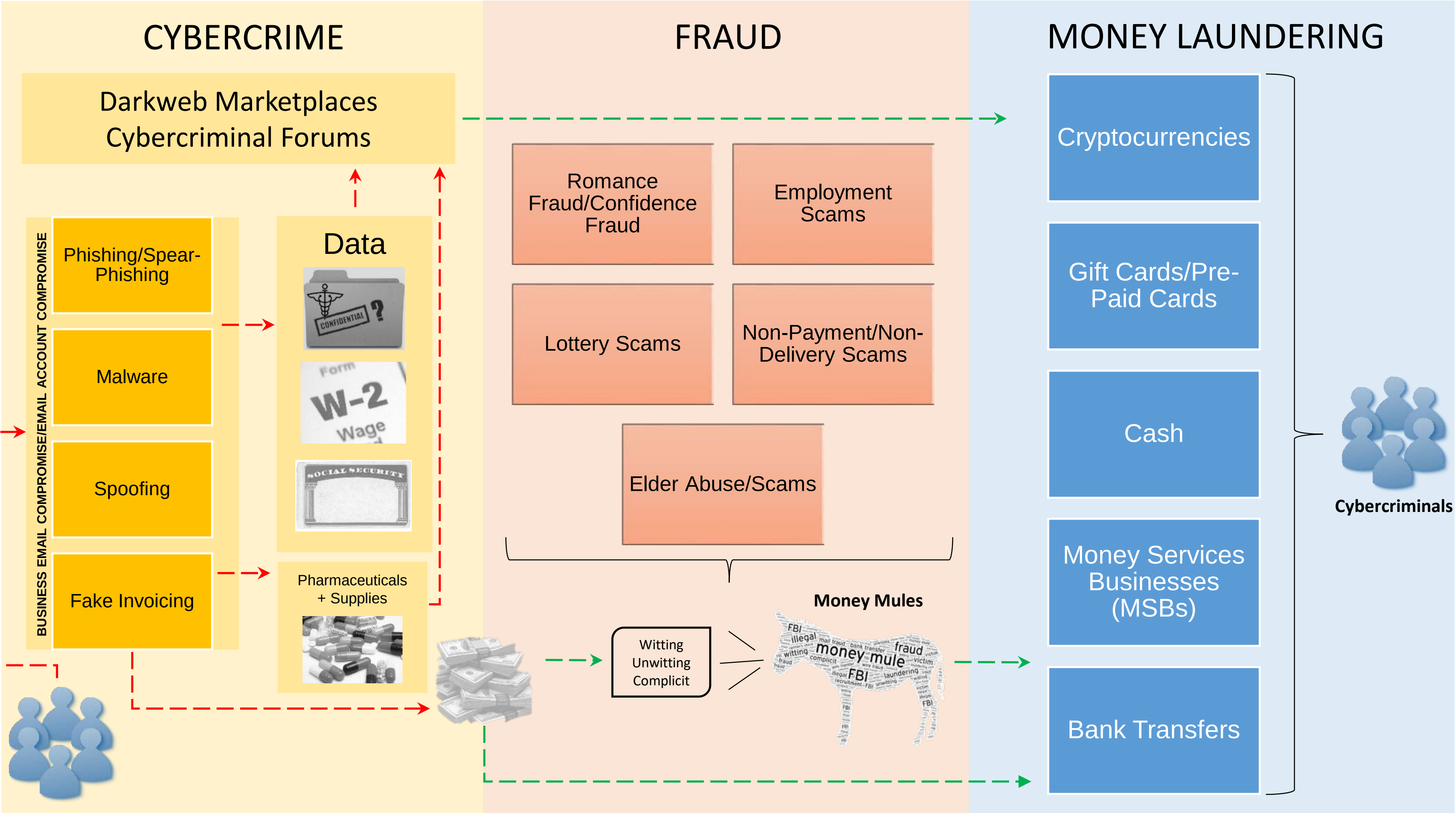
Financial Fraud

Healthcare & Medicare Fraud

Cryptocurrencies

Money Laundering

BEC in the Health Sector



CYBERCRIME

Darkweb Marketplaces
Cybercriminal Forums

BUSINESS EMAIL COMPROMISE/EMAIL ACCOUNT COMPROMISE

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

Data

Pharmaceuticals + Supplies

FRAUD

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

Witting
Unwitting
Complicit

Money Mules

MONEY LAUNDERING

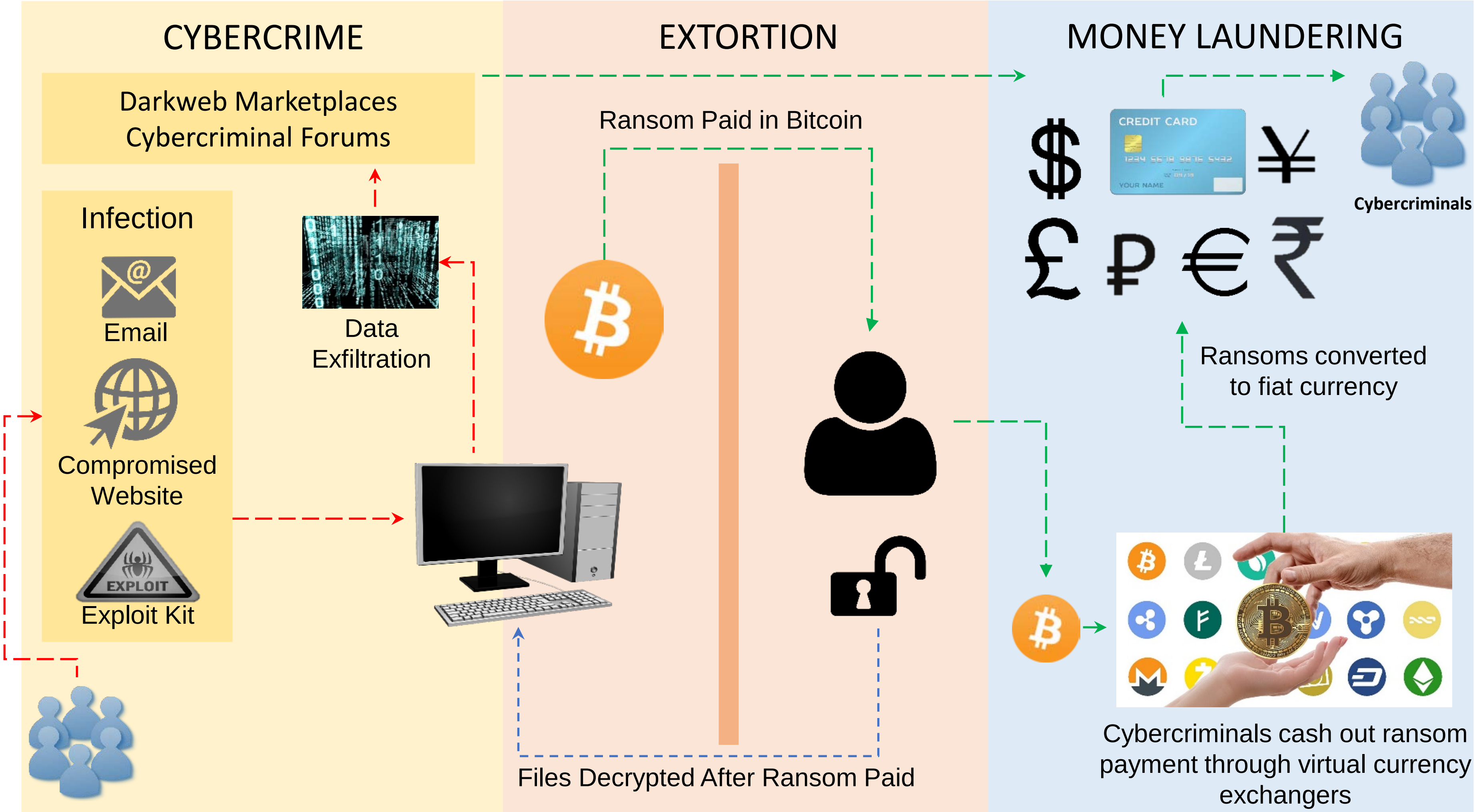
- Cryptocurrencies
- Gift Cards/Pre-Paid Cards
- Cash
- Money Services Businesses (MSBs)
- Bank Transfers

Cybercriminals

(CISA, 2009) (IC3, 2019)

Images Sources:
Creative Commons & FBI

Ransomware in the Health Sector



CYBERCRIME

Darkweb Marketplaces
Cybercriminal Forums

Infection

Email

Compromised Website

Exploit Kit

Data Exfiltration

EXTORTION

Ransom Paid in Bitcoin

Files Decrypted After Ransom Paid

MONEY LAUNDERING

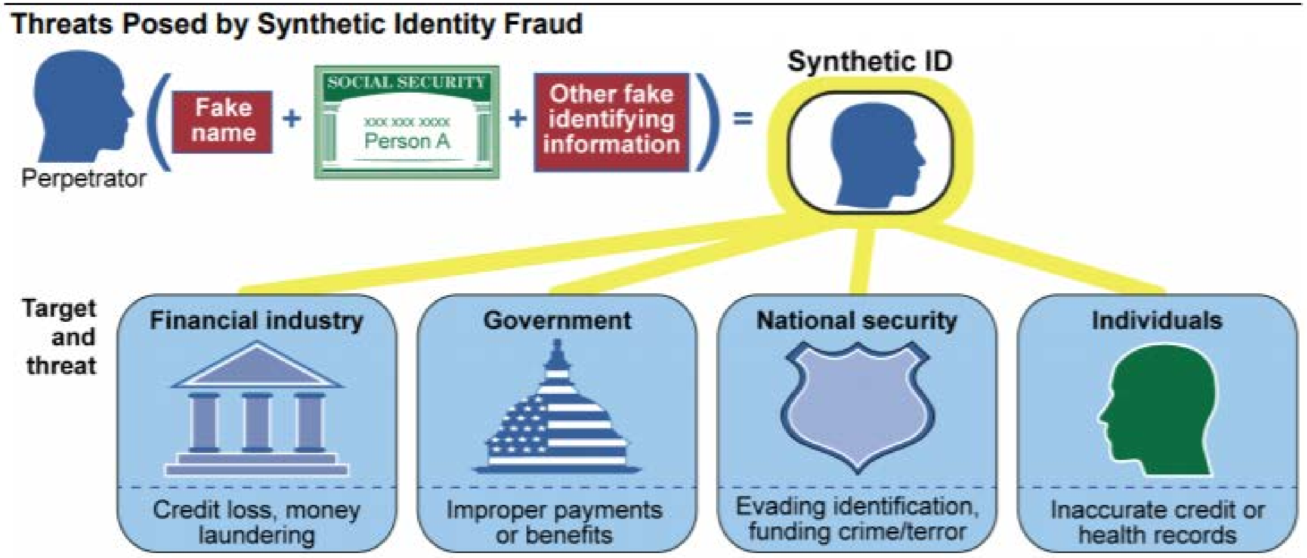
Cybercriminals

Ransoms converted to fiat currency

Cybercriminals cash out ransom payment through virtual currency exchangers

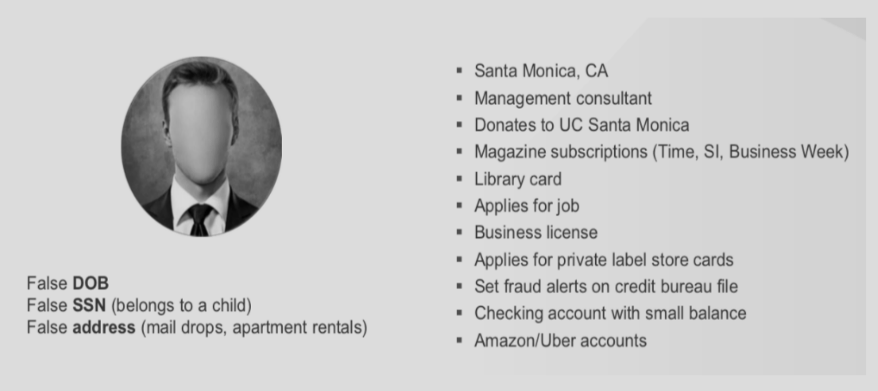
Image Source: Creative Commons

Synthetic Identity Fraud in the Health Sector


Threats Posed by Synthetic Identity Fraud
Perpetrator
Fake name
+
SOCIAL SECURITY
XXX XXX XXXX
Person A
+
Other fake identifying information
=
Synthetic ID
Target and threat
Financial industry
Credit loss, money laundering
Government
Improper payments or benefits
National security
Evading identification, funding crime/terror
Individuals
Inaccurate credit or health records

Source: GAO. | GAO-17-708SP

By leveraging synthetic identities and shell corporations, cybercriminals target healthcare organizations, insurers, and programs like Medicaid and Medicare for financial gain.

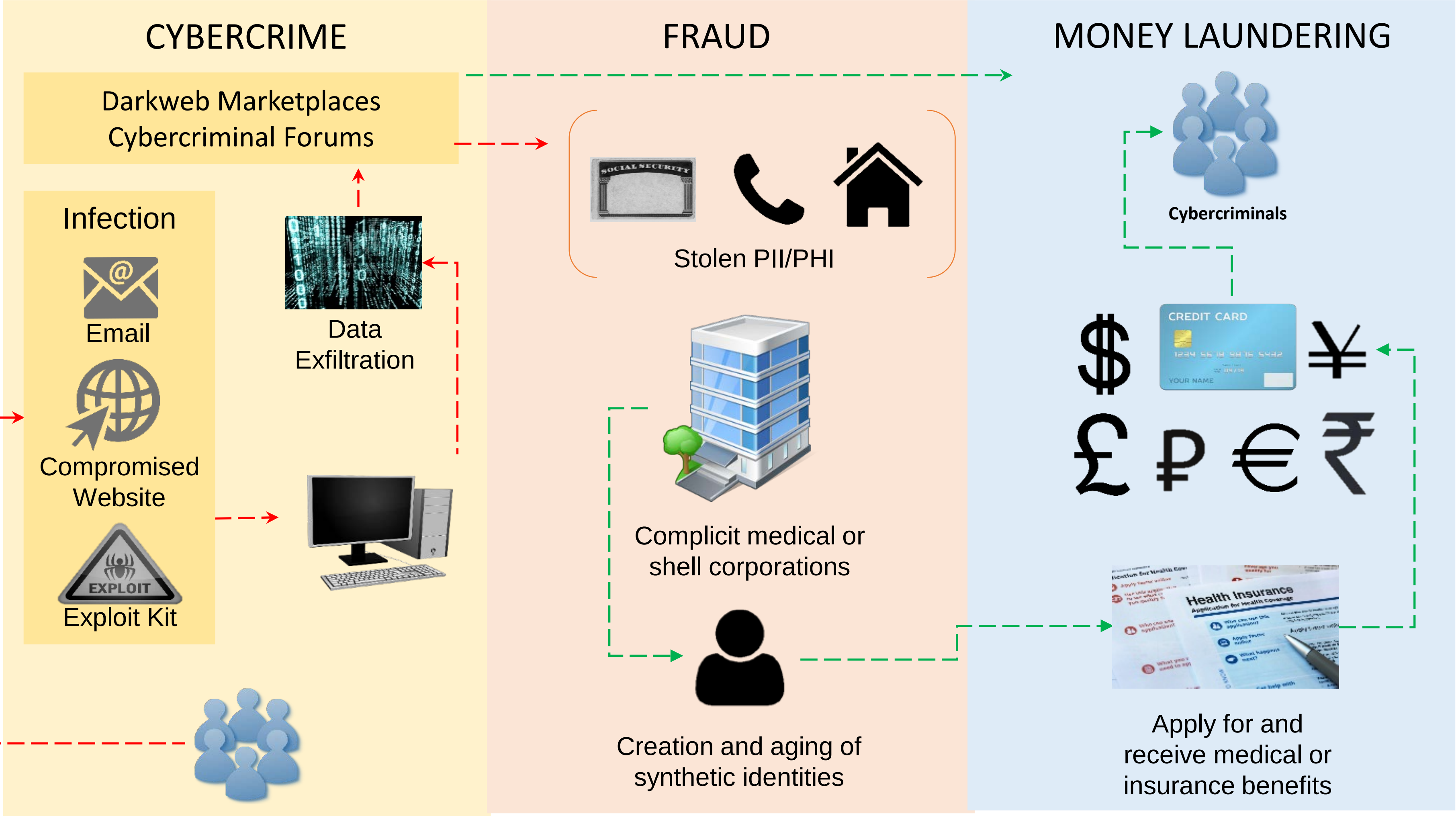


False **DOB**
False **SSN** (belongs to a child)
False **address** (mail drops, apartment rentals)

- Santa Monica, CA
- Management consultant
- Donates to UC Santa Monica
- Magazine subscriptions (Time, SI, Business Week)
- Library card
- Applies for job
- Business license
- Applies for private label store cards
- Set fraud alerts on credit bureau file
- Checking account with small balance
- Amazon/Uber accounts

Image Source: Alegeus.com and US GAO

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

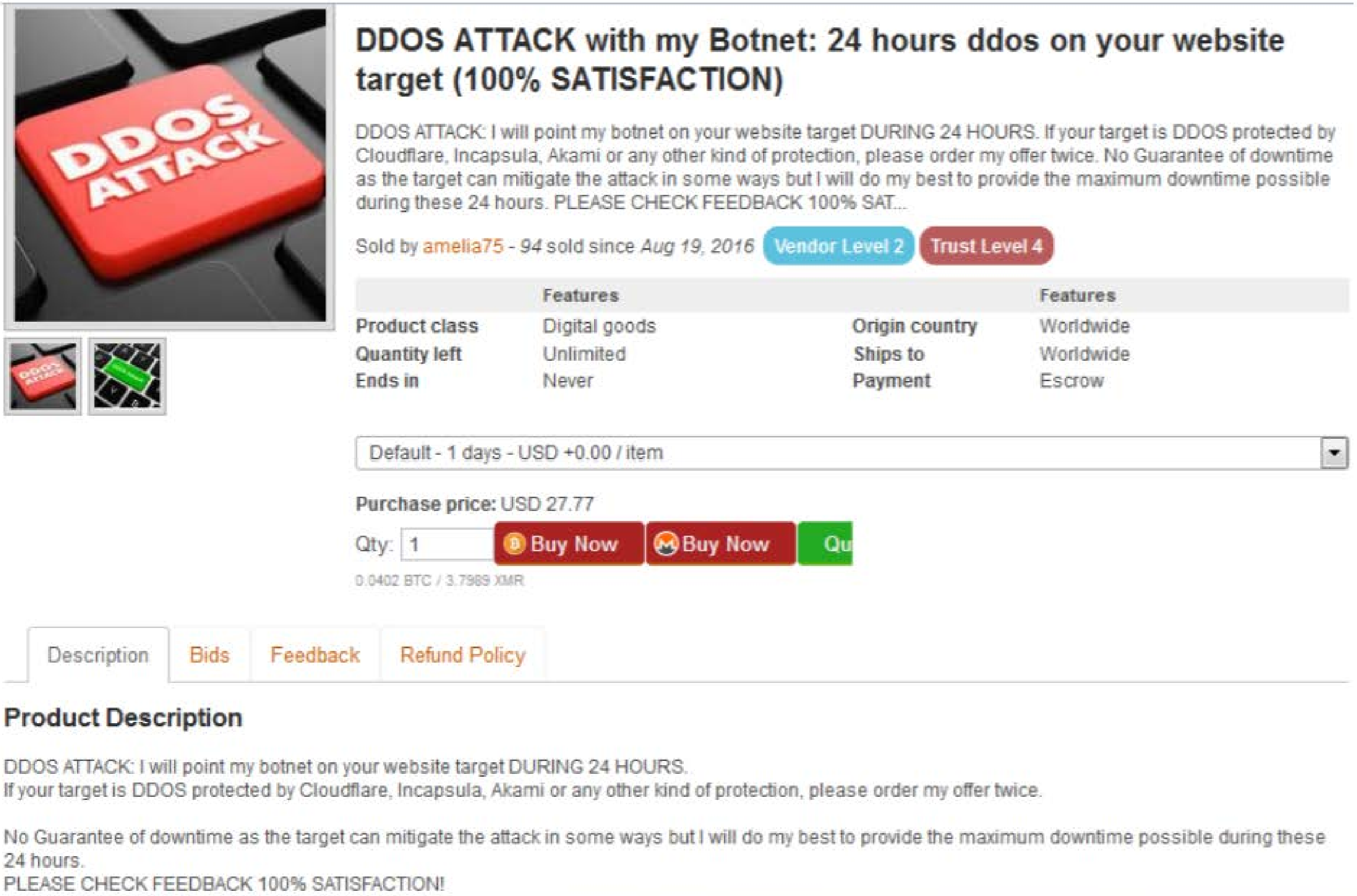
MONEY LAUNDERING

Cybercriminals

Apply for and receive medical or insurance benefits

Image Source: Creative Commons

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

	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 27.77

Qty: 1

0.0402 BTC / 3.7989 XMR

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!

Image Source: ICIT

DDoS in the Health Sector

Darkweb: DDoS-as-a-Service

Distraction: DDoS as a misdirect for additional attacks

Impact: DDoS for political, hacktivism, and extortion goals

Technique	Targets	OSI Layer	Description	Examples
HTTP Flood	Application	Layer 7: FTP, HTTP, POP3, & SMTP	This technique uses simple or complex methods of harnessing IP addresses to target URLs using random referrers and user agents to flood the server	**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
SYN Flood	Infrastructure	Layers 3 & 4: IP, ICMP, ARP, RIP, TCP, & UDP	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	
DNS Amplification	Bandwidth	Layers 3 & 4: IP, ICMP, ARP, RIP, TCP, & UDP	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	

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

Image Source: Creative Commons

Reference Materials

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
  - https://www.nytimes.com/2020/02/09/technology/ransomware-attacks.html
- 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
  - https://www.aoa.org/news/practice-management/healthcare-cybersecurity
- 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
  - https://healthitsecurity.com/news/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.

PDF

HC3 Customer Feedback

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

Questions

Contact

Health Sector Cybersecurity
Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV