LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

COVID-19 Cyber Threats

4/23/2020

Report #: 202004231000

Agenda

- Increasing Coronavirus-related cyberattacks
- Coronavirus-related domains
- Real-time Coronavirus infection tracking maps
- Fake Coronavirus maps and watering hole attacks
- Azorult overview
- Coronavirus-themed Phishing
- Cyberattacks on healthcare organizations
- Nation-state disinformation campaigns

Image source: teiss.co.uk

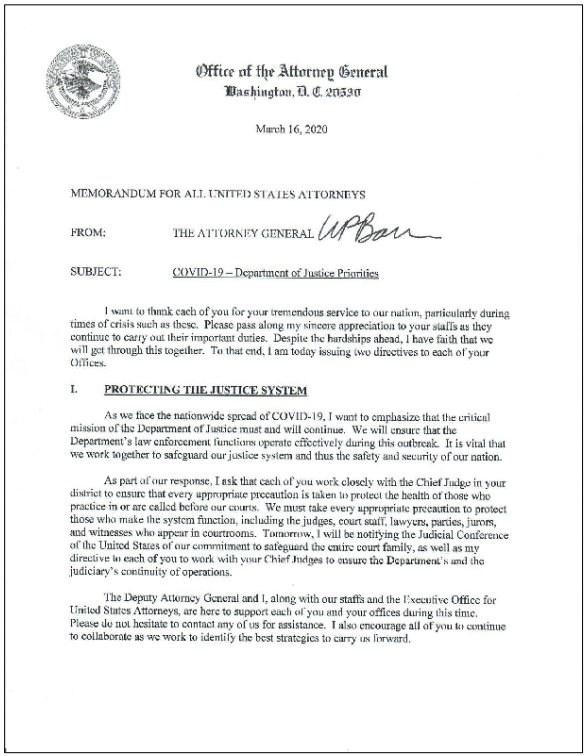
Slides Key:

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

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Coronavirus-related cyberattacks are prevalent!

Criminal cyber activity related to the Coronavirus pandemic has been rampant since the outbreak:



Office of the Attorney General
Washington, D. C. 20530

March 16, 2020

MEMORANDUM FOR ALL UNITED STATES ATTORNEYS

FROM: THE ATTORNEY GENERAL

SUBJECT: COVID-19 – Department of Justice Priorities

I want to thank each of you for your tremendous service to our nation, particularly during times of crisis such as these. Please pass along my sincere appreciation to your staffs as they continue to carry out their important duties. Despite the hardships ahead, I have faith that we will get through this together. To that end, I am today issuing two directives to each of your Offices.

I. PROTECTING THE JUSTICE SYSTEM

As we face the nationwide spread of COVID-19, I want to emphasize that the critical mission of the Department of Justice must and will continue. We will ensure that the Department's law enforcement functions operate effectively during this outbreak. It is vital that we work together to safeguard our justice system and thus the safety and security of our nation.

As part of our response, I ask that each of you work closely with the Chief Judge in your district to ensure that every appropriate precaution is taken to protect the health of those who practice in or are called before our courts. We must take every appropriate precaution to protect those who make the system function, including the judges, court staff, lawyers, parties, jurors, and witnesses who appear in courtrooms. Tomorrow, I will be notifying the Judicial Conference of the United States of our commitment to safeguard the entire court family, as well as my directive to each of you to work with your Chief Judges to ensure the Department's and the judiciary's continuity of operations.

The Deputy Attorney General and I, along with our staffs and the Executive Office for United States Attorneys, are here to support each of you and your offices during this time. Please do not hesitate to contact any of us for assistance. I also encourage all of you to continue to collaborate as we work to identify the best strategies to carry us forward.

US Attorney General William Barr sent a letter to US attorney offices across the country in mid-March, 2020, ordering them to investigate and prosecute "all criminal conduct related to the current pandemic."

"…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."

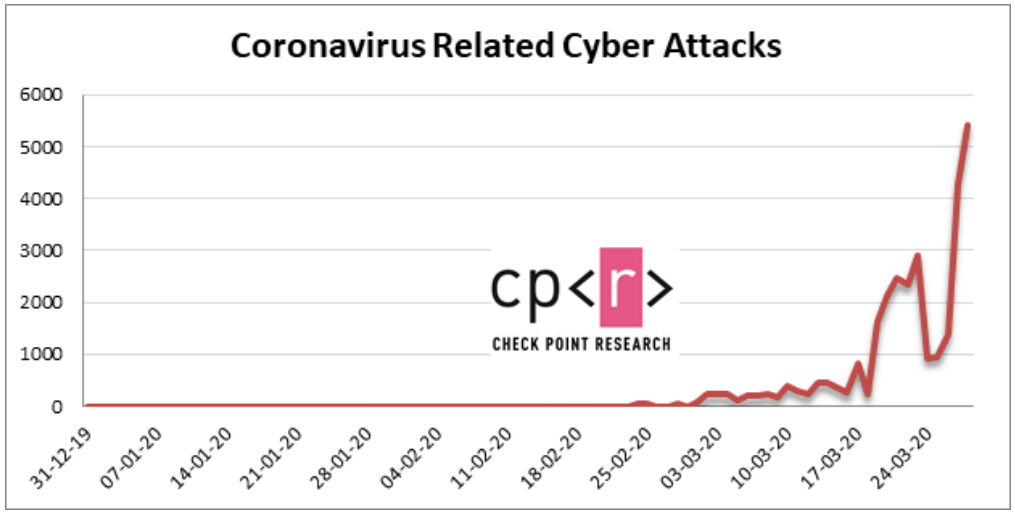
Michael D'Ambrosio, Head of the U.S. Secret Service Office of Investigations

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

WashingtonPost.com, April 14, 2020

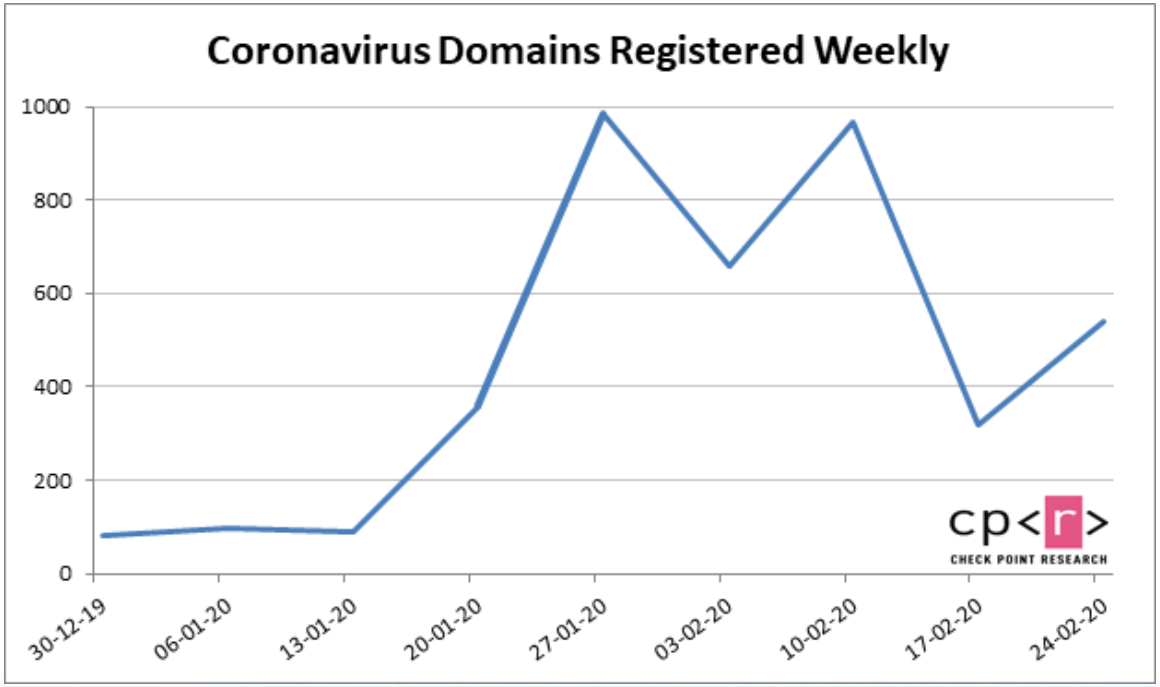
"...the risk to this sector will be elevated throughout this crisis."

- FireEye, as part of analysis of cyber threats to the healthcare industry during the Coronavirus pandemic



Fake COVID-19/Coronavirus-related domains

- These domains in many cases will host malware. The attack vector can be any number of options such as phishing, watering hole and typosquatting
- According to Checkpoint, new coronavirus-related domains are being registered at very high rates and many of them are malicious
  - Over 4000 Coronavirus-related domains registered in Jan. and Feb.
  - Coronavirus-themed domains are 50% more likely to be malicious than other domains
  - Over 6000 Coronavirus-related domains registered in the third week in March



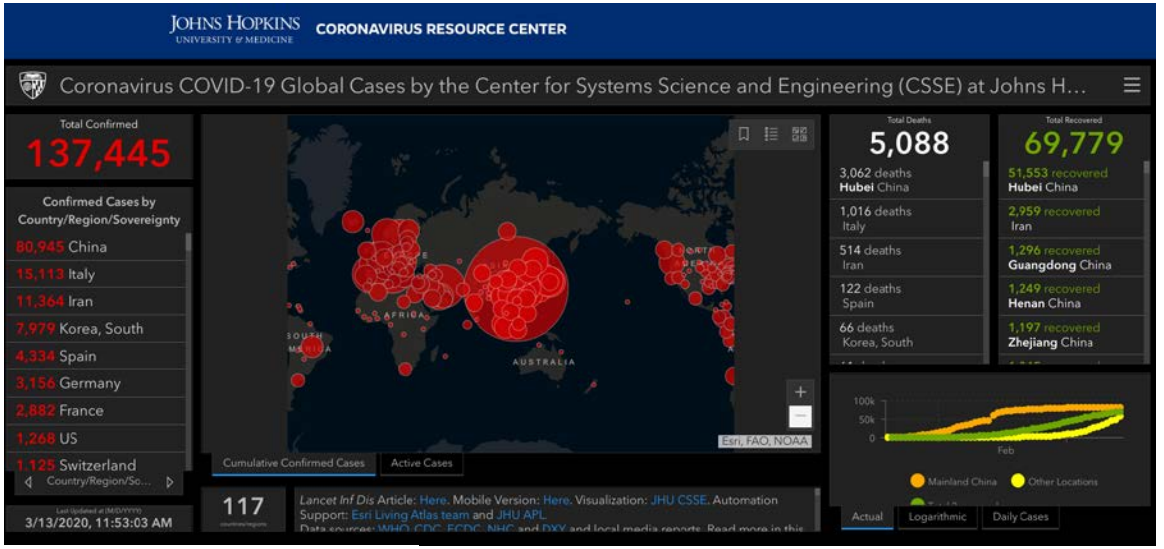
Real-time infection maps

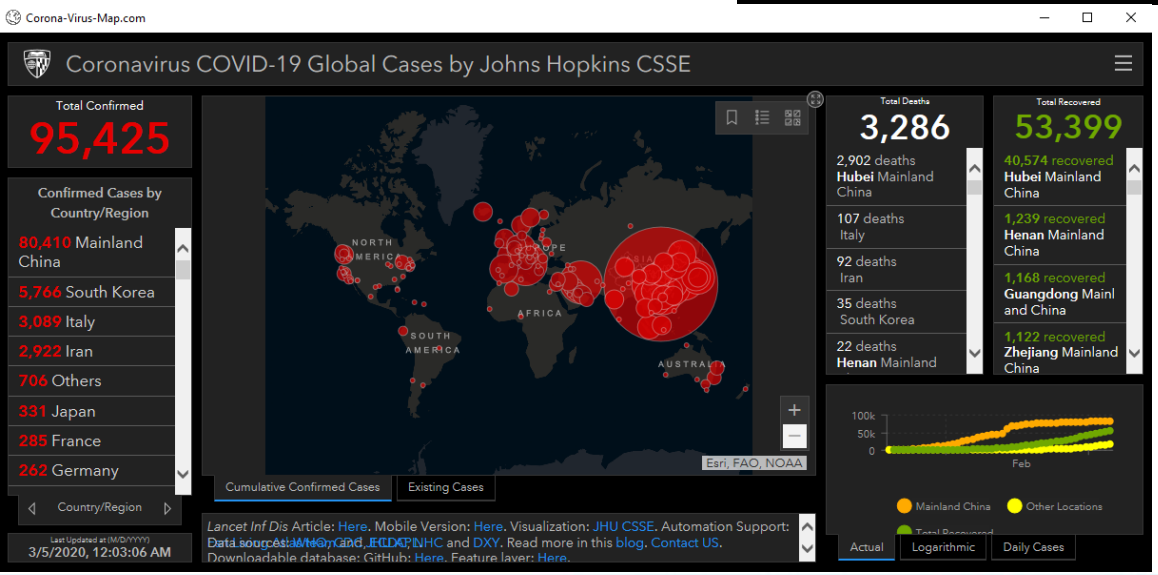
- As the Coronavirus/COVID-19 pandemic spread, several real-time infection maps have been stood up:
  - Johns Hopkins University
    - https://coronavirus.jhu.edu/map.html
  - World Health Organization
    - https://who.sprinklr.com/
  - Kaiser Family Foundation
    - https://www.kff.org/global-health-policy/fact-sheet/coronavirus-tracker/
  - HealthMap
    - https://www.healthmap.org/covid-19/
  - SharedGe0
    - https://uscovid-19map.org/
  - Microsoft Bing:
    - https://www.bing.com/covid
  - University of Washington
    - https://hgis.uw.edu/virus/

Image source: Forbes

Legitimate Johns Hopkins Coronavirus Map

Legitimate Map





Fake Map

Fake Coronavirus tracking map drops AZORult on victim systems:

AZORult

Image source: NJCCIC

AZORult:

- Malware – Information stealer and cryptocurrency theft
- Very common; Sold on Russian hacker forums for ~$100
- Can both be dropped or serve as a dropper (first or second stage)
- Constantly changing/evolving infection vectors and attack stages and capabilities
  - System login credentials
  - System reconnaissance info (GUID, system architecture and language, username and computer name, operating system version, system IP address
  - Cryptocurrency wallets
    - Monero, uCoin, and bitcoin cryptocurrencies
    - Electrum, Electrum-LTC, Ethereum, Exodus, Jaxx and Mist wallets
    - Steam and Telegram credentials; Skype chat history and credentials
  - Payment card numbers
  - Cookies and other sensitive browser-based data (especially autofill)
- Screenshots
- Data Exfiltration/Communication
  - Pushes to a command-and-control server
- Executes files via remote backdoor commands

COVID-related phishing

Phishing: A social engineering attack using a fake e-mail, often with a theme, to elicit interaction (clicking a link or opening an attachment) to deposit malware on the target system.

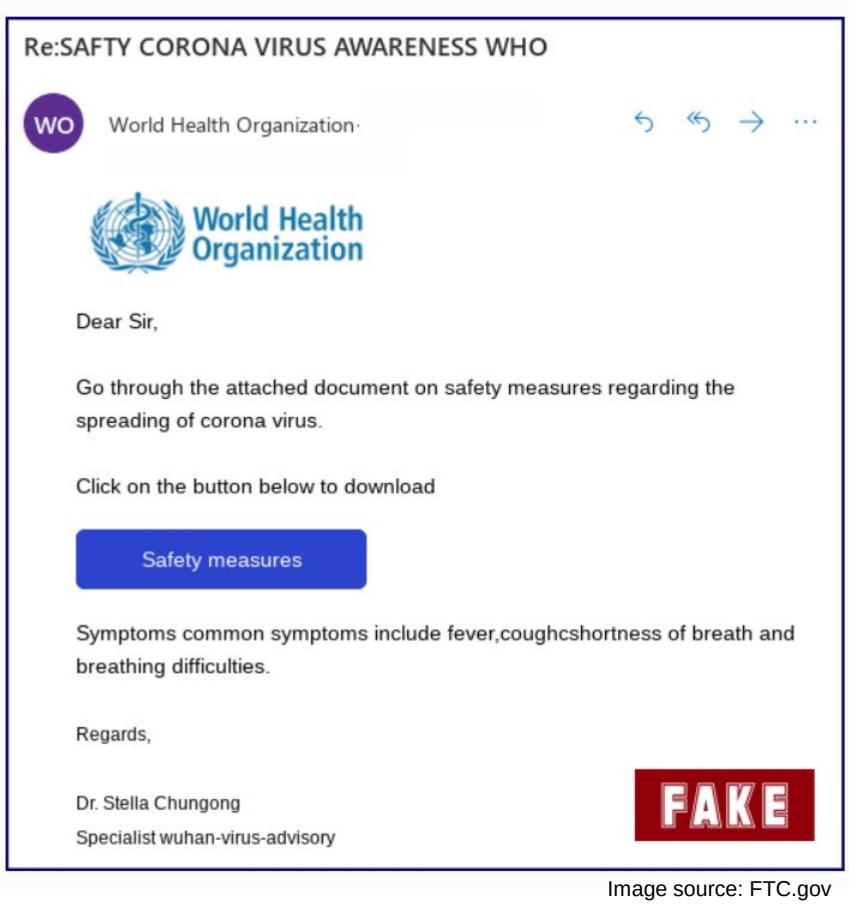


Image source: FTC.gov

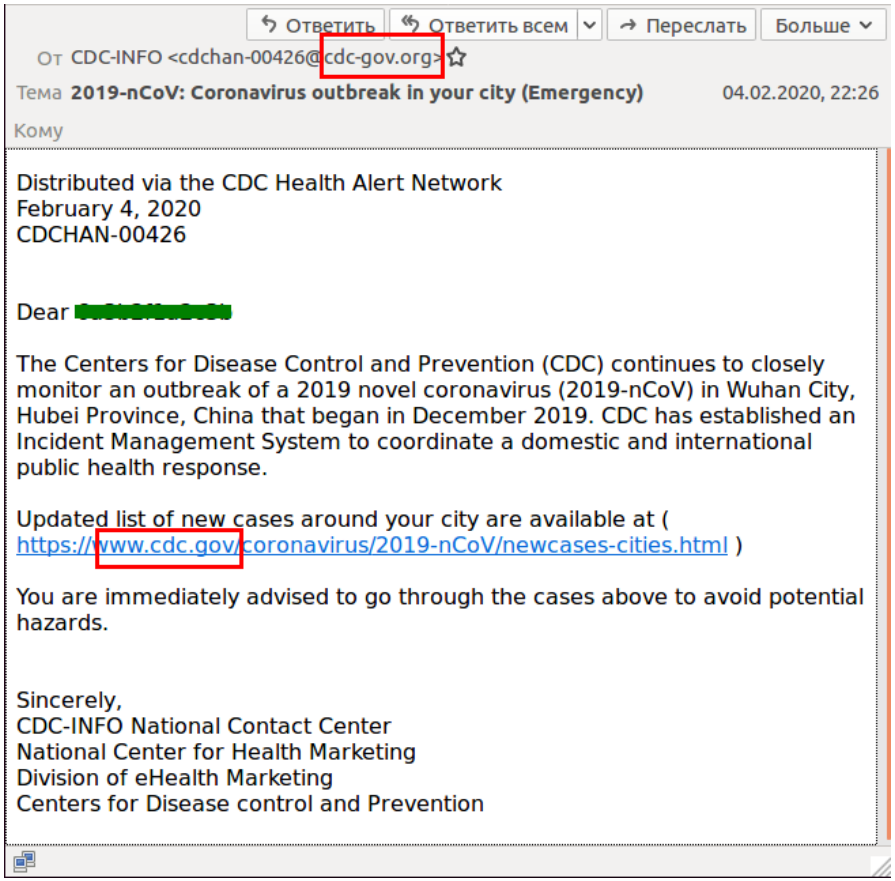


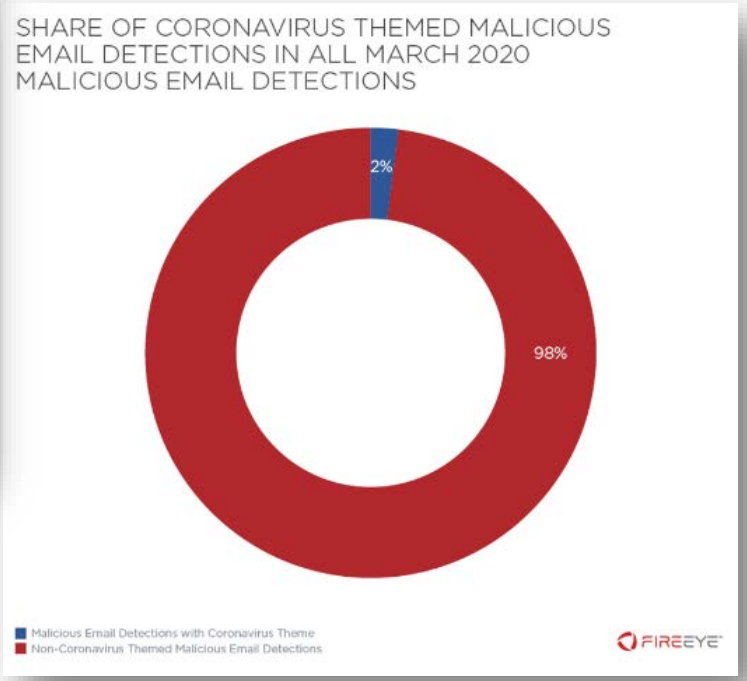
Image source: Kaspersky

Coronavirus-themed Phishing

We already noted the increasing number of Coronavirus-themed domains being registered

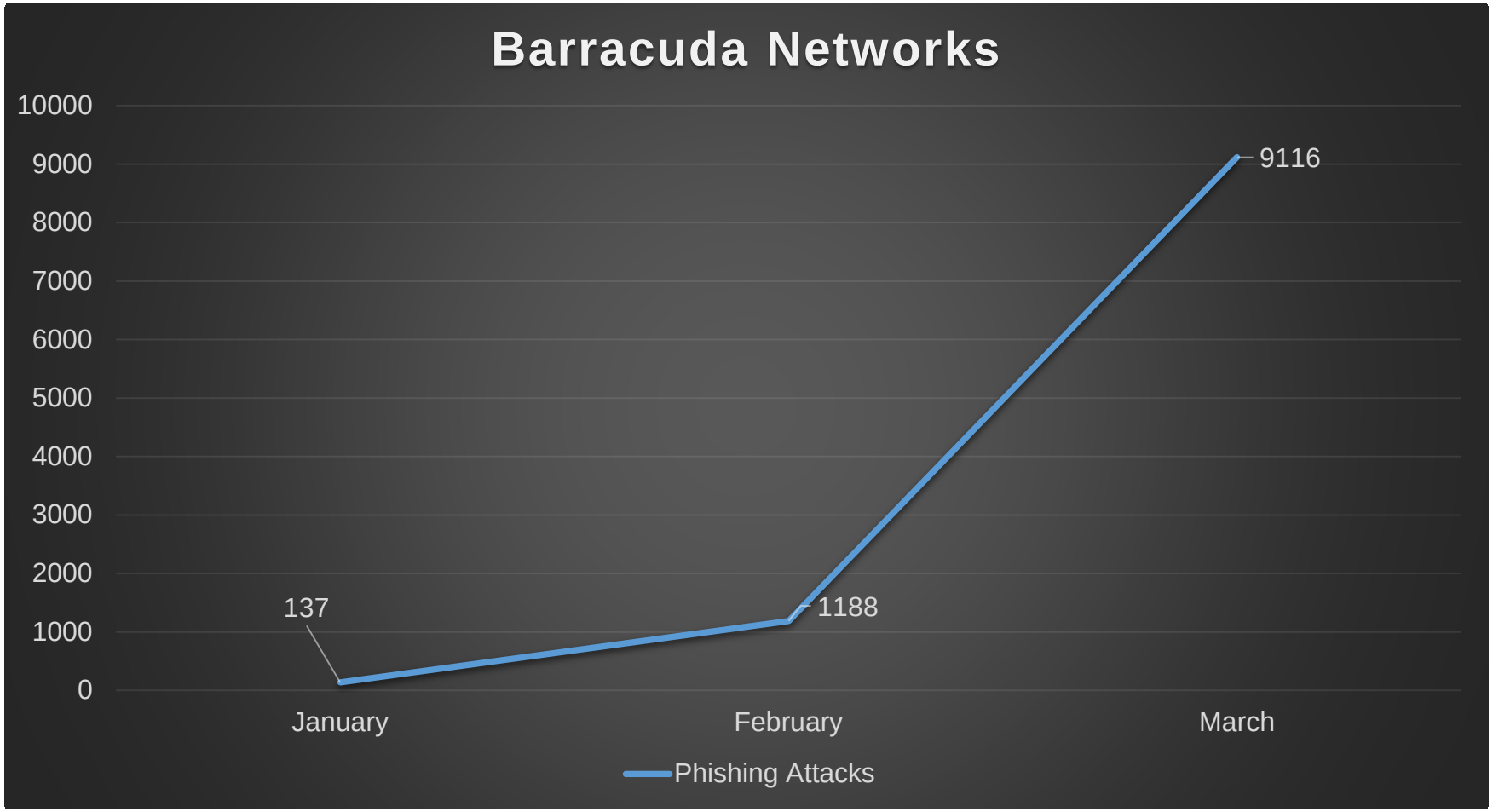
- Many of them are being setup for phishing
- Coronavirus-related phishing is becoming prevalent

Image source: PC Mag Raw data: Google



Coronavirus-related phishing

8X increase in Coronavirus related phishing from Jan. to Feb., and again from Feb. to Mar.



Attacks vs. hospitals and other healthcare orgs.

- 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

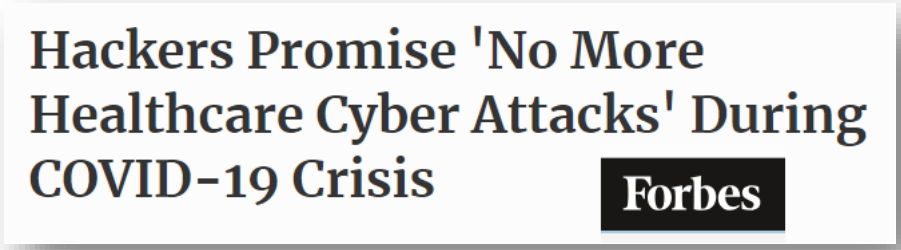


Image source: Datanami

Promises made, Promises broken

The result:

WRONG!

> "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

The Maze ransomware group has published personal and medical details of thousands of former patients of a London-based medical research company after a failed attempt to disable the firm's computer systems

Source: Carbon Black

Example Netwalker ransom note, used to attack Champaign-Urbana Public Health District in Illinois

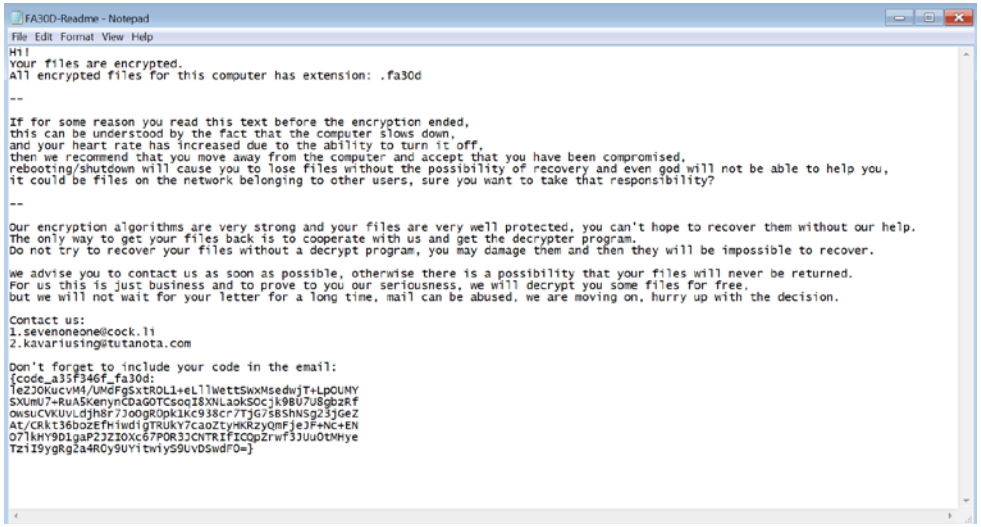


Image source: Carbon Black

Image source: Govinfosecurity.com

Nation-state threats

- Nation states also have agendas which make them threats:
  - Collection of research
    - Why invest the resources and wait for results when you can steal them?
    - Bioweapons and other medical research have national security/defense implications
  - Disinformation and propaganda
    - The pandemic is having a significant global impact which makes it inherently political
    - There are also significant implications for the economies of the world as well as the readiness of troops of many nations

Source: ZDNet

FBI official says foreign hackers have targeted COVID-19 research

Iran-Linked Group Caught Spreading COVID-19 'Disinformation' On Facebook And Instagram

Chinese COVID-19 disinformation campaigns commenced as early as January: Stanford

This culminated in a Chinese government official accusing the US military of starting the outbreak on social media.

Russian media 'spreading Covid-19 disinformation'

Reference Materials

References

- Phishing Attacks Increase 350 Percent Amid COVID-19 Quarantine
  - https://www.pcmag.com/news/phishing-attacks-increase-350-percent-amid-covid-19-quarantine
- Limited Shifts in the Cyber Threat Landscape Driven by COVID-19
  - https://www.fireeye.com/blog/threat-research/2020/04/limited-shifts-in-cyber-threat-landscape-driven-by-covid-19.html
- FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic
  - https://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic
- #COVID19 Drives Phishing Emails Up 667% in Under a Month
  - https://www.infosecurity-magazine.com/news/covid19-drive-phishing-emails-667
- Johns Hopkins University real-time Coronavirus infection map
  - https://coronavirus.jhu.edu/map.html
- World Health Organization real-time Coronavirus infection map
  - https://who.sprinklr.com/
- Kaiser Family Foundation real-time Coronavirus infection map
  - https://www.kff.org/global-health-policy/fact-sheet/coronavirus-tracker/
- HealthMap real-time Coronavirus infection map
  - https://www.healthmap.org/covid-19/

References

- SharedGe0 real-time Coronavirus infection map
  - https://uscovid-19map.org/
- Microsoft Bing real-time Coronavirus infection map
  - https://www.bing.com/covid
- University of Washington real-time Coronavirus infection map
  - https://hgis.uw.edu/virus/
- Coronavirus phishing
  - https://www.kaspersky.com/blog/coronavirus-phishing/32395/
- Coronavirus-Related Domain Registrations Rise 6,000 in a Week
  - https://www.cbronline.com/news/coronavirus-related-domains
- Thousands of shady websites with 'coronavirus' or 'covid' in their domain have popped up since January — and it reflects how eagerly scammers are trying to cash in on the epidemic
  - https://www.businessinsider.com/scammers-are-creating-shady-new-websites-with-coronavirus-domains-2020-4
- Coronavirus domains 50% more likely to infect your system with malware
  - https://thenextweb.com/security/2020/03/05/coronavirus-domains-malware-infect/
- Update: Coronavirus-themed domains 50% more likely to be malicious than other domains
  - https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/
- Coronavirus update: In the cyber world, the graph has yet to flatten
  - https://blog.checkpoint.com/2020/04/02/coronavirus-update-in-the-cyber-world-the-graph-has-yet-to-flatten/
- Security News This Week: Ransomware Groups Promise Not to Hit Hospitals Amid Pandemic
  - https://www.wired.com/story/ransomware-magecart-coronavirus-security-news/

References

- Hackers Promise 'No More Healthcare Cyber Attacks' During COVID-19 Crisis
  - https://www.forbes.com/sites/daveywinder/2020/03/19/coronavirus-pandemic-self-preservation-not-altruism-behind-no-more-healthcare-cyber-attacks-during-covid-19-crisis-promise/#76a7a20e252b
- Ransomware Gangs to Stop Attacking Health Orgs During Pandemic
  - https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/
- Hackers Promise 'No More Healthcare Cyber Attacks' During COVID-19 Crisis
  - https://www.forbes.com/sites/daveywinder/2020/03/19/coronavirus-pandemic-self-preservation-not-altruism-behind-no-more-healthcare-cyber-attacks-during-covid-19-crisis-promise/#29dc4eb9252b
- Ransomware Gangs to Stop Attacking Health Orgs During Pandemic
  - https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/
- Security News This Week: Ransomware Groups Promise Not to Hit Hospitals Amid Pandemic
  - https://www.wired.com/story/ransomware-magecart-coronavirus-security-news/
- No COVID-19 Respite: Ransomware Keeps Pummeling Healthcare
  - https://www.govinfosecurity.com/no-covid-19-respite-ransomware-keeps-pummeling-healthcare-a-14072
- COVID-19 Complication: Ransomware Keeps Hitting Healthcare
  - https://www.govinfosecurity.com/covid-19-complication-ransomware-keeps-hitting-hospitals-a-13941

References

- Sodinokibi Ransomware Gang Appears to Be Making a Killing
  - https://www.govinfosecurity.com/sodinokibi-ransomware-gang-appears-to-be-making-killing-a-13269
- Cyberattacks Target Healthcare Orgs on Coronavirus Frontlines
  - https://threatpost.com/cyberattacks-healthcare-orgs-coronavirus-frontlines/154768/
- Malicious Attackers Target Government and Medical Organizations With COVID-19 Themed Phishing Campaigns
  - https://unit42.paloaltonetworks.com/covid-19-themed-cyber-attacks-target-government-and-medical-organizations/
- Limited Shifts in the Cyber Threat Landscape Driven by COVID-19
  - https://www.fireeye.com/blog/threat-research/2020/04/limited-shifts-in-cyber-threat-landscape-driven-by-covid-19.html
- APTs and COVID-19: How advanced persistent threats use the coronavirus as a lure
  - https://blog.malwarebytes.com/threat-analysis/2020/04/apts-and-covid-19-how-advanced-persistent-threats-use-the-coronavirus-as-a-lure/
- COVID-19 pandemic opens up new frontiers for health data privacy
  - https://www.healthcareitnews.com/news/europe/covid-19-pandemic-opens-new-frontiers-health-data-privacy
- Critical VPN Security for Telehealth, Remote Access Amid COVID-19
  - https://healthitsecurity.com/news/critical-vpn-security-for-telehealth-remote-access-amid-covid-19
- 8 Phishing Lures Preying on Pandemic Panic
  - https://www.darkreading.com/8-phishing-lures-preying-on-pandemic-panic/d/d-id/1337495

References

- Keeping the DNS Secure During the Coronavirus Pandemic
  - https://www.icann.org/news/blog/keeping-the-dns-secure-during-the-coronavirus-pandemic
- Network Data Shows Spikes, Vulnerability of Work-at-Home Shift
  - https://www.darkreading.com/perimeter/network-data-shows-spikes-vulnerability-of-work-at-home-shift/d/d-id/1337552
- Covid-19 / CoronaVirus Domains: a looming threat?
  - http://garwarner.blogspot.com/2020/04/covid-19-coronavirus-domains-looming.html
- COVID-19: Remote Workforce Security Strategies
  - https://www.databreachtoday.com/covid-19-remote-workforce-security-strategies-a-14012
- The Cyber Threat Impact of COVID-19 to Global Business
  - https://wow.intsights.com/rs/071-ZWD-900/images/Cyber%20Threat%20Impact%20of%20Covid19.pdf
- Hackers Targeting Critical Healthcare Facilities With Ransomware During Coronavirus Pandemic
  - https://thehackernews.com/2020/04/ransomware-hospitals-coronavirus.html
- US consumers report $12M in COVID-19 scam losses since January
  - https://www.bleepingcomputer.com/news/security/us-consumers-report-12m-in-covid-19-scam-losses-since-january/
- Free COVID-19 Threat List - Domain Risk Assessments for Coronavirus Threats
  - https://www.domaintools.com/resources/blog/free-covid-19-threat-list-domain-risk-assessments-for-coronavirus-threats /

References

- COVID-19 increases vulnerability of hospitals to ransomware, says Microsoft
  - https://www.dotmed.com/news/story/50712
- There's another coronavirus crisis brewing: Fraud
  - https://www.washingtonpost.com/opinions/2020/04/14/theres-another-coronavirus-crisis-brewing-fraud/
- Report examines COVID-19 cyber threats
  - https://homelandprepnews.com/stories/47280-report-examines-covid-19-cyber-threats/
- Battling Cybercrime During the COVID-19 Crisis
  - https://www.bankinfosecurity.com/interviews/battling-cybercrime-during-covid-19-crisis-i-4655
- How Cybercriminals Are Taking Advantage of COVID-19: Scams, Fraud and Misinformation
  - https://www.digitalshadows.com/blog-and-research/how-cybercriminals-are-taking-advantage-of-covid-19-scams-fraud-misinformation/
- The Cybersecurity 202: Hospitals face a surge of cyberattacks during the novel coronavirus pandemic
  - https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/04/15/the-cybersecurity-202-hospitals-face-a-surge-of-cyberattacks-during-the-novel-coronavirus-pandemic/5e95fbc9602ff10d49ae4ba4/
- Penn Medicine CISO offers tips for COVID-19 cybersecurity response
  - https://www.healthcareitnews.com/news/penn-medicine-ciso-offers-tips-covid-19-cybersecurity-response

References

- Hospital Hackers Seize Upon Coronavirus Pandemic
  - https://www.nextgov.com/cybersecurity/2020/04/hospital-hackers-seize-upon-coronavirus-pandemic/164605/
- COVID-19 Isn't the Only Virus to Fear: Cybersecurity Attackers Target Hospitals Amidst COVID-19
  - https://www.lexology.com/library/detail.aspx?g=e72251ad-db6e-43f0-a942-642412012b76
- Iran-Linked Group Caught Spreading COVID-19 'Disinformation' On Facebook And Instagram
  - https://www.forbes.com/sites/thomasbrewster/2020/04/15/iran-linked-group-caught-spreading-covid-19-disinformation-on-facebook-and-instagram/#29ae56361f21

Questions

Upcoming Briefs

- Threat Modeling for Mobile Health Systems
- Quantitative Risk Management

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to **HC3@HHS.GOV**.

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.**

Health Sector Cybersecurity Coordination Center (HC3) Background

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.

Contact

Health Sector Cybersecurity Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV