



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



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:

Contraction of the second		Office of the Attorney General Washington, D. C. 20530	
		March 16, 2020	
	MEMORANDI	M FOR ALL UNITED STATES ALTORNEYS	
	MEMORALIZE		
	FROM:	THE ATTORNEY GENERAL WBar	
	SUBJECT:	COVID-19 - Department of Justice Priorities	
	times of crisis su continue to carry	think each of you for your tremendous service to our raism, particularly during oth as these. Please pass along my sincere appreciation to your satifs as they out their important duries. Despite the hardships aback, I have faith that we this together. To that end, I am today issuing isso directives to each of your	
	L PROTE	CTING THE JUSTICE SYSTEM	
	mission of the D Department's lay	ce the nationwide spread of COVID-19, I want to emphasize that the critical opartmet of Justice must and will continue. We will ensure that the we unforcement functions operate cfriceively during this outbreak. It is viral that to safegaated our justice system and thus the safety and security of our antion.	
	district to ensure practice in or are those who make and witnesses who of the United Sta directive to each	f our response, I ask that each of you work closely with the Chief Judge in your that every appropriate precention is taken to protect the health of those who called before our corns. We must take every appropriate precation to protect the system function, including the judges, court satif, lawyers, parties, jurors, to appear in courtons. Two more way, will be notifying the Jadical Coefference tack of our commitment to asteguard the entire court family, as well as my of you to work, with your Chief Judges to ensure the Department's and the mity of operations.	
	United States At Please do not he	any Attomps General and L along with our staffs and the L'scentifice Office for formers, see here to support each of you and your offices during this time, ittlet to comman any of us for meristance. I also encourage all of you to continue we work to identify the best stategies to carry us forward.	
			1

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



P FOR IT SECURITY & PRIVACY ACROSS HHS CYBERSECURITY PROGRAM

- 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







- 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
 - <u>https://www.kff.org/global-health-policy/fact-sheet/coronavirus-tracker/</u>
 - HealthMap
 - <u>https://www.healthmap.org/covid-19/</u>

ADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS HAS CYBERSECURITY PROGRAM

- SharedGe0
 - <u>https://uscovid-19map.org/</u>
- Microsoft Bing:
 - <u>https://www.bing.com/covid</u>
- University of Washington
 - <u>https://hgis.uw.edu/virus/</u>



TLP: WHITE, ID# 202004231000

Image source: Forbes

Legitimate Johns Hopkins Coronavirus Map



HHS CYBERSECURITY & PRIVACY ACROSS HHS

AZORult

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)

ERSECURITY PROGRAM

- Screenshots
- Data Exfiltration/Communication
 - Pushes to a command-and-control server

EADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

Executes files via remote backdoor commands





COVID-related phishing

EADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS HHS CYBERSECURITY PROGRAM

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.

Re:SAFTY CORONA VIRUS AWARENESS WHO	⑦ Ответить ⑦ Ответить Всем マ → Переслать Больше ~ От CDC-INFO <cdchan-00426@cdc-gov.org>☆</cdchan-00426@cdc-gov.org>
Wo World Health Organization $5 \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	Тема 2019-nCoV: Coronavirus outbreak in your city (Emergency) 04.02.2020, 22:26 Кому
World Health Organization	Distributed via the CDC Health Alert Network February 4, 2020 CDCHAN-00426
Dear Sir,	Dear Guilte Charles
Go through the attached document on safety measures regarding the spreading of corona virus.	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
Click on the button below to download	public health response.
Safety measures	Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)
Symptoms common symptoms include fever, cough cshortness of breath and breathing difficulties.	You are immediately advised to go through the cases above to avoid potential hazards.
Regards,	Sincerely, CDC-INFO National Contact Center National Center for Health Marketing
Dr. Stella Chungong	Division of eHealth Marketing Centers for Disease control and Prevention
Specialist wuhan-virus-advisory	
Image source: FTC.gov	Image source: Kaspersky
	inage source. Raspersky

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



Non-Coronavirus Themed Malicious Email Detections

O FIREEYE





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







- 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

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

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

FA30D-Readme - Notepad	
File Edit Format View Help	
Hil Your files are encrypted. All encrypted files for this computer has extension: .fa30d	^
If for some reason you read this text before the encryption ended, this can be understoad by the fact that the computer slows down, and your heart rate has increased due to the ability to turn it Off, then we recommend that you move amay from the computer and accept that you have been compromised, reboting/shutdown will cause you to lose files without the possibility of recovery and even god will not be able to help you, it could be files on the network belonging to other users, sure you want to take that responsibility?	
Our encryption algorithms are very strong and your files are very well protected, you can't hope to recover them without our help The only way to get your files back is to cooperate with us and get the decrypter program. Do not try to recover your files without a decrypt program, you may damage them and then they will be impossible to recover.	
we advise you to contact us as soon as possible, otherwise there is a possibility that your files will never be returned. For us this is just business and to prove to you our seriousness, we will decrypt you some files for free. but we will not wait for your letter for a long time, mail can be abused, we are moving on, hurry up with the decision.	
Contact us: 1.sevenoneone@cock.li 2.kavariusingštutanota.com	
Den't forget to include your code in the email: [code_a51546f_fa10d: [ec2.0KucvM4/UMG/g5XRDL1+el]]WettSwMsedwj7+LpDUMY SSUMU7+RuKSkenynCogoCTScog15W1La3k5(c);18907U8692Rf owsUCKKVVLdj18F7J00gR0pLXkC938cr7TjG7385NNsg23jGeZ ArCKK15B0czEfniwdigTruKY7cacZtyKRSyQmFj2FFwc+EN D7]KrY901gaPZJZZDXc67P0R3JCHTKf1CCpZrwf3JUu0tMHye T119yg8g2aHcSyGVTivtf3SUVDSMd7D_	
4	۰. F

Image source: Carbon Black



REvil/Sodinokibi #Ransomware group claiming they took 1TB worth of data from 10x Genomics (@10xGenomics), American biotechnology company that is traded on NASDAQ.

-posted samples, Will publish more files in 3 days if not paid. -10x Genomics appear to be working on #coronavirus.



Image source: Govinfosecurity.com



- 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

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.

FBI official says foreign hackers have targeted COVID-19 research

Source: ZDNet

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

Russian media 'spreading Covid-19 disinformation'







- Phishing Attacks Increase 350 Percent Amid COVID-19 Quarantine
 - <u>https://www.pcmag.com/news/phishing-attacks-increase-350-percent-amid-covid-19-quarantine</u>
- Limited Shifts in the Cyber Threat Landscape Driven by COVID-19
 - <u>https://www.fireeye.com/blog/threat-research/2020/04/limited-shifts-in-cyber-threat-landscape-driven-by-covid-19.html</u>
- FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic
 - <u>https://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic</u>
- #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/

- 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
 - <u>https://hgis.uw.edu/virus/</u>
- Coronavirus phishing
 - <u>https://www.kaspersky.com/blog/coronavirus-phishing/32395/</u>
- Coronavirus-Related Domain Registrations Rise 6,000 in a Week
 - <u>https://www.cbronline.com/news/coronavirus-related-domains</u>
- 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
 - <u>https://www.businessinsider.com/scammers-are-creating-shady-new-websites-with-coronavirus-domains-2020-4</u>
- Coronavirus domains 50% more likely to infect your system with malware
 - <u>https://thenextweb.com/security/2020/03/05/coronavirus-domains-malware-infect/</u>
- Update: Coronavirus-themed domains 50% more likely to be malicious than other domains
 - <u>https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/</u>
- Coronavirus update: In the cyber world, the graph has yet to flatten
 - <u>https://blog.checkpoint.com/2020/04/02/coronavirus-update-in-the-cyber-world-the-graph-has-yet-to-flatten/</u>
- Security News This Week: Ransomware Groups Promise Not to Hit Hospitals Amid Pandemic
 - https://www.wired.com/story/ransomware-magecart-coronavirus-security-news/



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





- 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
 - <u>https://unit42.paloaltonetworks.com/covid-19-themed-cyber-attacks-target-government-and-medical-organizations/</u>
- Limited Shifts in the Cyber Threat Landscape Driven by COVID-19
 - <u>https://www.fireeye.com/blog/threat-research/2020/04/limited-shifts-in-cyber-threat-landscape-driven-by-covid-19.html</u>
- APTs and COVID-19: How advanced persistent threats use the coronavirus as a lure
 - <u>https://blog.malwarebytes.com/threat-analysis/2020/04/apts-and-covid-19-how-advanced-persistent-threats-use-the-coronavirus-as-a-lure/</u>
- COVID-19 pandemic opens up new frontiers for health data privacy
 - <u>https://www.healthcareitnews.com/news/europe/covid-19-pandemic-opens-new-frontiers-health-data-privacy</u>
- 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
 - <u>https://www.darkreading.com/8-phishing-lures-preying-on-pandemic-panic/d/d-id/1337495</u>





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



- COVID-19 increases vulnerability of hospitals to ransomware, says Microsoft
 - https://www.dotmed.com/news/story/50712
- There's another coronavirus crisis brewing: Fraud
 - <u>https://www.washingtonpost.com/opinions/2020/04/14/theres-another-coronavirus-crisis-brewing-fraud/</u>
- Report examines COVID-19 cyber threats
 - <u>https://homelandprepnews.com/stories/47280-report-examines-covid-19-cyber-threats/</u>
- 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
 - <u>https://www.digitalshadows.com/blog-and-research/how-cybercriminals-are-taking-advantage-of-covid-19-scams-fraud-misinformation/</u>
- The Cybersecurity 202: Hospitals face a surge of cyberattacks during the novel coronavirus pandemic
 - <u>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/</u>
- Penn Medicine CISO offers tips for COVID-19 cybersecurity response
 - <u>https://www.healthcareitnews.com/news/penn-medicine-ciso-offers-tips-covid-19-cybersecurity-response</u>





- Hospital Hackers Seize Upon Coronavirus Pandemic
 - https://www.nextgov.com/cybersecurity/2020/04/hospital-hackers-seize-upon-coronaviruspandemic/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
 - <u>https://www.forbes.com/sites/thomasbrewster/2020/04/15/iran-linked-group-caught-spreading-covid-19-disinformation-on-facebook-and-instagram/#29ae56361f21</u>



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 <u>HC3@HHS.GOV</u>.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to <u>HC3@HHS.GOV</u> 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



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

Products

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 <u>HC3@HHS.GOV</u> 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