COVID19 Related Nation-State and Cyber Criminal Targeting of the Healthcare Sector

5/14/2020

Agenda

- Recent Activity

- Sophisticated Cyber Campaigns

- Disinformation

- Mitigation Techniques

- Questions

Slides Key:

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

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

Recent Activity

Cybersecurity and Infrastructure Security Agency (CISA) Alert (AA20-099A) COVID-19 Exploited by Malicious Cyber Actors (April 8, 2020)

APT groups are using the COVID-19 pandemic as part of their cyber operations:

- Masquerade as trusted entities
- Use coronavirus-themed phishing messages or malicious applications
- Their goals and targets are consistent with long-standing priorities such as espionage and "hack-and-leak" operations.

Cybercriminals are using the pandemic for commercial gain, deploying a variety of ransomware and other malware.
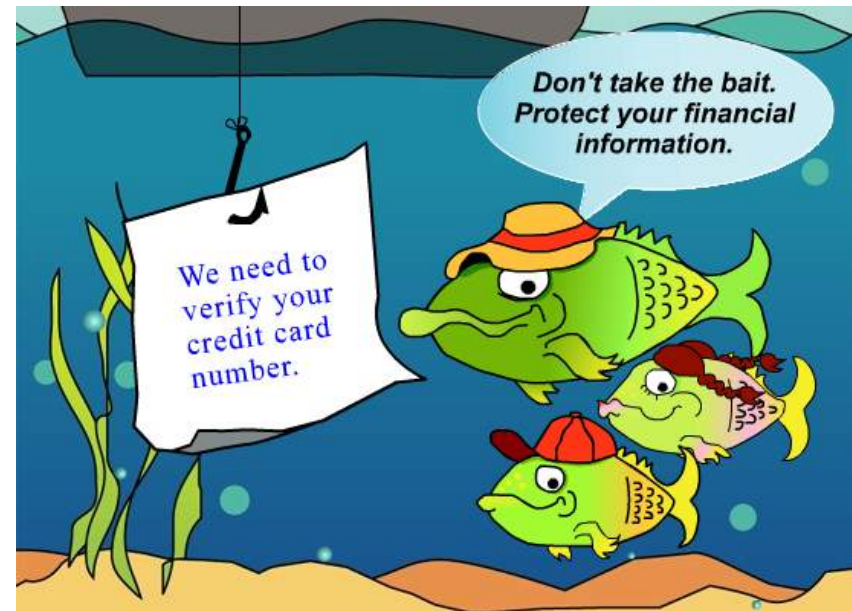
CISA Alert (AA20-099A) APT Groups Target Healthcare and Essential Services (May 5, 2020)

APT actors are targeting organizations involved in national and international COVID-19 responses.

Targeting organizations in order to collect bulk:

- personal information
- intellectual property
- intelligence that aligns with national priorities

Actors view supply chains as a weak link that they can exploit to obtain access to better-protected targets.

Sophisticated Cyber Campaigns

Early February, Unknown Cyber Actors Target Companies' Logistics

AZORult phishing campaign targeting Japanese-speakers originating from Russia or Eastern Europe.

The attackers were not an APT but, "clearly understand the economic concerns surrounding the Coronavirus."

The campaign exploited a two-and-a-half-year-old vulnerability and targeted industries "particularly susceptible to shipping disruptions".

Those industries in order of most targeted are:

1. Manufacturing
2. Industrial
3. Finance
4. Transportation
5. **Pharmaceutical**
6. Cosmetic Companies

Sophisticated Cyber Campaigns (cont.)

Mid-February Russian APT 28 (Fancy Bear) linked, Hades group Targets Ukraine

1. Emails containing malicious attachments appearing to be Coronavirus information from the Center for Public Health of the Ministry of Health of Ukraine to targets in Ukraine.

2. Mass Coronavirus-themed spam email campaign targeted Ukrainian citizens

3. Social media accounts spread "scaremongering" messages that the virus had reached the country.

In March, Russian Linked Cyber Criminals Target Biotech Firm

Evil Corp infected the U.S.-based biotech firm, 10x Genomics with the Sodinokibi aka REvil ransomware.

10x Genomics is "part of an international alliance sequencing cells from patients who've recovered from the Coronavirus, in an effort to fuel the discovery of potential treatments."

Angry protests greet Ukrainians evacuated from China for coronavirus quarantine

FEB. 21, 2020 / 00:54

Local residents clashed with police as more than 70 people evacuated from China were taken to quarantine in central Ukraine.

00:05 / 00:54

Disinformation

Intent

- Create a lack of trust by U.S. citizens in their government

- Russian disinformation campaigns are used over the long-term to create a larger political impact

- "Russia's intent is to sow discord and undermine US institutions and alliances from within, including through covert and coercive malign influence campaigns,"
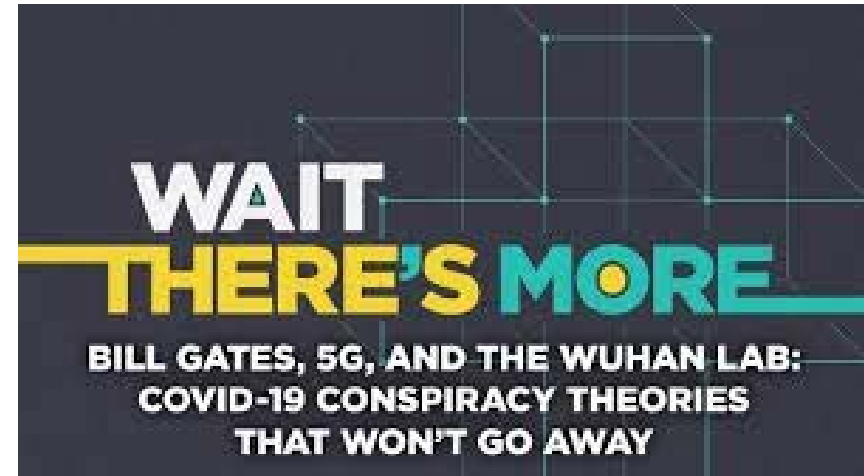

Historical

- Blamed the United States Government (USG) for the creation of the AIDs, SARs, and Ebola epidemics

- Disinformation referenced as fact today

- Victim Beliefs:
  - Targeted by the USG because of their race
  - Used as "guinea pigs" for the USG's furtherance of developing vaccines for the ailment they were infected with

Chinese Embassy in South Africa
@ChineseEmbSA

More evidence suggests that the virus was not originated at the seafood market in Wuhan at all, not to mention the so called "made in China". twitter.com/zlj517/status/...

Lijian Zhao 赵立坚 @zlj517
This article is very much important to each and every one of us. Please read and retweet it. COVID-19: Further Evidence that the Virus Originated in the US. globalresearch.ca/covid-19-furth...

♡ 1,991   3:27 AM - Mar 16, 2020

💬 4,067 people are talking about this

Disinformation

Current

- Effort to identify COVID19 disinformation

- Suspect news sources and legitimate Russian owned news running stories that place the blame for the Coronavirus on the USG

- Stories "amplified" in social media by Russian-based accounts reposting and commenting on the disinformation

- Russian COVID19 Message: Portraying "American officials as downplaying the health alarms and thus posing serious threats to public safety."

WAIT THERE'S MORE

BILL GATES, 5G, AND THE WUHAN LAB: COVID-19 CONSPIRACY THEORIES THAT WON'T GO AWAY

Operation INFEKTION

The opening salvo of the AIDS disinformation campaign was fired on 17 July 1983, when an obscure newspaper in India, the *Patriot*, printed an anonymous letter headlined "AIDS may invade India: Mystery disease caused by US experiments." The letter, allegedly written by a "well-known American scientist and anthropologist" in New York, claimed that "AIDS...is believed to be the result of the Pentagon's experiments to develop new and dangerous biological weapons." It went on to state that the United States was about to transfer these experiments to sites in Pakistan, where they would pose a grave threat to neighboring India.

CGTN
1.61M subscribers

SUBSCRIBE

Russia is again accusing the United States of running a clandestine biological weapons lab in Georgia. Moscow says Washington is flouting international conventions and posing a direct threat to Russia. During a press conference in Beijing, a question was raised on the claim to China's Foreign Ministry.

Then **Now**

[Russian Social Media] Posts reportedly included claims that the virus was a bid to "wage economic war on China," that it was a bioweapon engineered by the CIA, and that it was fostered "to push anti-China messages."

Chinese Propaganda News Amplifies U.S.

Conspiracy Theorist

GLOBAL TIMES
DISCOVER CHINA, DISCOVER THE WORLD

HOME | CHINA | SOURCE | WORLD | OPINION | LIFE | ARTS | SCI-TECH | ODD | SPORT | METRO

HOME >> CHINA

US urged to release health info of military athletes who came to Wuhan in October 2019

By Leng Shumei and Wan Lin Source:Global Times Published: 2020/3/25 0:48:40

US urged to release military athlete info

TruthLeaks - Investigative Journalist George Webb
@GeorgWebb

March 23rd, 2020. Origins of CoronaVirus - Metadata Says Ft. Detrick youtu.be/PIF8HBFWMyU via @YouTube

9:26 PM · Mar 23, 2020 · Twitter Web Client

124 Retweets **149** Likes

TruthLeaks - Investigative Journalist George Webb
@GeorgWebb

Replying to @abask_cat

Yes, I am trying to get to what killed people in the CoronaVirus-like deaths in the US for vaping deaths in Sept 2019.   Ft Detrick also was closed for sloppy Bioweapon handling in Aug 2019. Maatje Benassi may have contracted Corona at Ft Belvoir Comm. Hospital where she works.

6:17 AM · Mar 28, 2020 · Twitter for iPhone

An American journalist claimed one US military athlete in the delegation could be patient zero of the deadly new disease.

George Webb, an investigative journalist in Washington, DC claimed in recent videos and tweets that he believes Maatje Benassi, an armed diplomatic driver and cyclist who was in Wuhan in October for the cycling competition in the Military World Games, could be patient zero of COVID-19 in Wuhan.

In a report by the US Department of Defense official website on October 25, Maatje Benassi has participated 50-mile cycling road race in Wuhan.

Mitigation Techniques

The following actions could mitigate the risk posed by APTs and cybercriminals:

1. An understanding of APT and associated cybercriminals tactics, techniques, and procedures (TTPs) to include, historical attacks and targeted vulnerabilities.

2. Keep systems updated with the most recent patches and prioritize patching for the most at risk systems based on the TTPs identified in bullet "1".

3. Increase the identification and ingestion of APT and associated cybercriminal unit IOCs.

4. Have and practice an incident response plan.

General understanding of historical disinformation campaigns:

• Simplistic scapegoating

• Endless repetition

• Mixing of lies and half-truths with undeniable facts

Reference Materials

- Alert (AA20-099A) - COVID-19 Exploited by Malicious Cyber Actors
  - https://www.us-cert.gov/ncas/alerts/aa20-099a

- Alert (AA20-126A) - APT Groups Target Healthcare and Essential Services
  - https://www.us-cert.gov/ncas/alerts/AA20126A

- Another COVID-19 Research Firm Targeted by Ransomware Attack
  - https://healthitsecurity.com/news/another-covid-19-research-firm-targeted-by-ransomware-attack

- State-sponsored hackers are now using coronavirus lures to infect their targets
  - https://www.zdnet.com/article/state-sponsored-hackers-are-now-using-coronavirus-lures-to-infect-their-targets/

- Putin's Long War Against American Science
  - https://www.nytimes.com/2020/04/13/science/putin-russia-disinformation-health-coronavirus.html

- US Pushes Back Against Russian, Chinese, Iranian Coronavirus Disinformation
  - https://www.voanews.com/covid-19-pandemic/us-pushes-back-against-russian-chinese-iranian-coronavirus-disinformation

- US accuses Russia of spreading conspiracies about the Wuhan coronavirus, including that it's a CIA biological weapon
  - https://www.businessinsider.com/us-officials-claim-russian-coronavirus-disinformation-campaign-2020-2?r=US&IR=T

- Russia accuses U.S. of running weapons lab in Georgia
  - https://www.youtube.com/watch?v=tHfTe4P7FQY

- Soviet Bloc Intelligence and Its AIDS Disinformation Campaign
  - https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no4/pdf/U-%20Boghardt-AIDS-Made%20in%20the%20USA-17Dec.pdf

- How coronavirus disinformation caused chaos in a small Ukrainian town
  - https://www.nbcnews.com/news/world/how-coronavirus-disinformation-caused-chaos-small-ukrainian-town-n1146936

- Locals oppose quarantine of Ukrainians evacuated from China amid coronavirus concerns
  - https://www.nbcnews.com/video/locals-oppose-quarantine-of-ukrainians-evacuated-from-china-amid-coronavirus-concerns-79139909949

- China's Global Times plays a peculiar role
  - https://www.economist.com/china/2018/09/20/chinas-global-times-plays-a-peculiar-role

- TruthLeaks - Investigative Journalist George Webb (@GeorgWebb)
  - https://twitter.com/GeorgWebb/status/1242261391416774656
  - https://twitter.com/GeorgWebb/status/1243844539397353477

Questions

Questions

Upcoming Briefs

- Web Shell Malware Threats and Mitigations

- Maze Ransomware

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.**

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.

Contact

Health Sector Cybersecurity Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV