Cyber 9/12 Strategy Challenge

Intelligence Report I

INSTRUCTIONS

Please read these instructions carefully. They have changed from previous years.

Your team will take on the role of experienced policy advisers, part of a hypothetical cybersecurity task force, preparing to brief the National Security Council (NSC). This packet contains fictional information on the background and current situation involving a major cyber incident affecting US systems. The attacks notionally take place in Spring 2021. The scenario presents a fictional account of political developments and public reporting surrounding the cyber incident.

The NSC needs information on the full range of response options available regarding this incident. Your team has been tasked with developing an appropriate course of action for recommending to the NSC.

You are to consider as facts the following pages for formulating your response.

You will use the fictional scenario material presented to perform three tasks:

Written Situation Assessment and Policy Brief: Your first task is to write an analytical policy brief that provides a concise assessment of the situation, addresses potential impacts and risks, and discusses the implications of the cyber incident. Describe policy considerations for different potential state and non-state actors. Be clear regarding the advantages and disadvantages of various policy options and explore the course of action you are recommending in depth. The length of the brief is limited to two single-sided pages.

Oral Policy Brief (Day 1): For the first day of the competition, prepare a ten-minute oral presentation outlining your impact and risk assessment, as well as your suggested course of action. You will present to a panel of judges playing the role of the NSC.
Decision Document (Day 1): Teams will also be required to submit a "decision document" accompanying their oral presentation at the beginning of the competition round. The "decision document" will be a maximum of one single-sided page in length, outlining the team's response options, decision process, and recommendations. The teams should note that the document is not intended to summarize every detail of the recommendations, but to help the judges follow the oral presentation, and the judges will be given only 2 minutes to read it before the presentation begins. The document should be written with the goal of assisting busy senior officials to quickly grasp your team's recommendations and analysis.

Keep these tips in mind as you are reading and considering your policy response alternatives:

- *Analyze the issues.* The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of potentially conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.

- *Engage the scenario.* Believe that the universe we have created is plausible and that the events that happen in it are realistic. Nevertheless, remember to think critically about the intelligence you have been provided and its provenance.

- *Think multi-dimensionally*. When analyzing the scenario, remember to consider implications for other organizations and domains (e.g. private sector, military, law enforcement, different levels of government, diplomatic) and incorporate these insights along with cybersecurity.

- *Consider who you are, and who you're briefing.* You are experienced cyber policy professionals briefing the National Security Council. As such, you should be ready to answer questions on agency responsibility, provide justifications for your recommendations, and have potential alternatives ready.

- *Be creative.* Cyber policy is an evolving discourse, and there is no single correct course of action to the scenario information provided. There are many ideas to experiment with in responding to the crisis.

- *Don't fight the scenario*. Unless stated otherwise, assume all inter-state relations, policies, and treaties have remained the same as they were in December 2019. Explore the implications of that information, not the plausibility.

Given the unclear nature of the threat, the NSC requests that your team prepare a concise assessment of the ongoing situation and reporting. Your assessment should include:

- How or where the relevant systems could be vulnerable to exploit, and what steps can be made to mitigate these vulnerabilities;
- An assessment of potential risks and impacts to consider if the vulnerabilities are successfully exploited; and
- Responses the NSC can or should consider addressing these vulnerabilities, taking into account the severity and likelihood of the threat.

To provide this assessment and policy recommendations, you will apply your understanding of the technologies involved, cybersecurity, law, foreign policy, international relations, and security theory to
synthesize useful policy measures from limited information. Your recommendation must analyze the possible strengths, weaknesses, opportunities, and threats of your proposed response.

In formulating your response, you will be expected to have considered, at a minimum:

- All stakeholders when determining an action or recommendation, including the role of the government and private sector;
- The long and short-term impacts of your recommendation;
- Which agency will be responsible for the action you have recommended;
- Appropriate recommendations for local vs. federal government;
- Whether you can, or should, attribute the threat; and

- The covert or overt nature of your response.

Additionally, this message is accompanied by several documents that may assist your team in preparing the assessment and policy brief for the NSC:

- **Tab 1** – New York Times Article
- **Tab 2** – CNN News Article
- **Tab 3** – CISA Advisory
- **Tab 4** – Think Tank Report
- **Tab 5** – NSA Report to NSC
- **Tab 6** – Facebook Blog
- **Tab 7** – Panel Discussion Transcript

Tab 1 – New York Times Article

The New York Times

Ransomware: To pay, or not to pay?

New York Presbyterian-Weill Cornell Medical Center *by ecksunderscore, CC BY-SA 2.0 via Wikimedia Commons*

By James Hoya
Mar. 10, 2021, 14:19 ET

It was just past midday on February 27, and Nicole Paisley had just returned from her regular lunchtime walk around New York Presbyterian-Weill Cornell on East 70th Street. She keyed in her password as she sat down at her workstation at the ER admission desk and did a double-take to the screen. When she tried to log in, the system booted her out. She checked her password and tried again, but again was kicked off the machine. She turned to her colleague who, like her, was starting his shift at the ER. His system was down too.

A siren caused Ms. Paisley's years of experience to kick in. New York City was experiencing a surge of coronavirus and flu cases due to a record cold-wave that had battered the city with freezing temperatures and forcing New Yorkers indoors. More and more ambulances were arriving filled with coronavirus patients and others suffering from respiratory distress. After failing to log in a third time, Ms. Paisley

dug out paper admission forms from a filing cabinet, “I wasn’t panicking,” she said, “but I did start worrying when the phones stopped working.”

The cyberattack on New York Presbyterian-Weill Cornell became the latest in a parallel pandemic as cybercriminals have targeted hospitals treating coronavirus patients, demanding multimillion-dollar ransoms for the return of a healthcare systems. This attack through the Plaguerizer ransomware – a recently discovered derivative of Ryuk which plagued hospitals last year - crippled access to patient records, blocked access to email, and disrupted internal systems to access MRI and CT scans.

Ms. Paisley, like the rest of the nursing staff, fell back on written notes and faxes to find and locate vital patient information. “I’ve never felt more powerless,” she said. “We had to turn away hundreds of patients from the ER, cancel procedures and redirect incoming critical cases. We just couldn’t care for them, things took us so long.”

The hospital agreed to pay an eight-figure ransom to the attackers, a decision it affirmed was done in the interest of patient care and public service. The attack would still result in the death of seventeen patients – fifteen of who were in critical care due to the coronavirus.

A preliminary investigation would conclude that half of the deaths at New York Presbyterian-Weill Cornell occurred within the first twenty-four hours, before the hospital could contact the criminals and begin negotiations. It would also state that twelve of the deaths could have been prevented had all systems been operational. Nellie James, Attorney General of New York, stated that her office would investigate if criminal homicide charges could be brought on the criminals.

“When dealing with the coronavirus which does affect the respiratory system among others, imaging systems play a critical role,” said Dr. Stephen Mooney a pulmonologist at New York Presbyterian-Weill Cornell. “It is challenging to accurately diagnose and gauge treatment for COVID-19 with no way to visualize within the body – especially if their condition deteriorates.”

Cybersecurity experts believe that criminals can see the light at the end of the coronavirus tunnel and are focused on extorting as much money as possible before the pandemic subsides.

This renewed pressure has brought additional government scrutiny. An advisory from the U.S. Treasury in early October 2020 indicated that ransomware payments to cybercriminal groups in nations like North Korea may be illegal for violating U.S. sanctions.

This presents a serious dilemma for hospitals, which are bracing for another wave of ransomware campaigns once the coronavirus vaccine rolls out. “How can they

chastise the victim for paying their own ransom?" Ms. Paisley said, "We have a job to do. An illegal payment means nothing if we can save a 57-year old coding in the ICU."

Tab 2 – CNN News Article

CNN health Food Fitness Wellness Parenting Vital Signs

New Strain of COVID-19 Threatens Phase Two of Vaccine Rollout

By **Vince Bowie**, CNN
Updated 10:20 AM ET, Mon April 5, 2021

(CNN) - This month, the next phase of the U.S. COVID-19 vaccine rollout is expected to commence.

Following the four-phase plan announced by the National Academies of Sciences, Engineering, and Medicine committee, since late December 2020 approximately 21 million healthcare workers, 3 million long-term health facility residents, and 50 million essential workers have been vaccinated with one of the available vaccines from Moderna, Pfizer, AstraZeneca, and Johnson & Johnson. The vaccine has also been made available to Americans at higher morbidity and mortality risk, particularly those with pre-existing conditions and those over the age of 65, and essential workers who are at higher risk of infection and transmission.

With the additions of the AstraZeneca and Johnson & Johnson vaccines, as well as the Novavax vaccine, which is currently under the FDA approval process, vaccine production has increased to a level which will allow this next phase to include a larger portion of the general populace. Despite these advances, young adults and children should not expect to receive a vaccine until June at the earliest. The focus of this stage of vaccinations will continue to be on essential workers, those

with pre-existing conditions, and older Americans – groups whose combined population amounts to about 250 million Americans.

As of April 1, 2021, the United States has lost over 400,000 Americans to the COVID-19 epidemic. Due to the efforts of the Biden administration, in partnership with the Centers for Disease Control and state and local authorities, the infection curve has flattened, allowing the country to avoid another larger spike in COVID-19 infections and deaths. The universal mask mandate in combination with federal guidelines are credited with slowing the spread of the virus, helping to cap the holiday season-surge in infection cases.

According to Dr. Anthony Fauci, director of the National Institute of Allergy and Infectious Diseases, reaching herd immunity will only be possible if an "overwhelming majority of people" are vaccinated, hopefully by the end of June. "Somewhere between 75% and 80% of the people [need] to get vaccinated in order to get a real umbrella of protection over the community — the 'community' being the United States of America," Dr. Fauci said. "And hopefully that can get done worldwide so that we globally crush this outbreak."

A larger portion of phase two vaccinations will rely not on employers, but voluntary inoculation. Polls have shown a steady increase in the likelihood of Americans seeking out vaccination, from 50% in September 2020 to 61% in March 2021. This increase is a reassuring sign that Americans increasingly trust in the effectiveness and safety of the various vaccines and in federal and state government efforts towards mass vaccination. However, these numbers do not yet appear sufficient to eradicate the virus.

The US federal government and its state and local partners must continue to push the importance of vaccinations if we hope to put an end to this pandemic any time soon. Adding an additional layer of concern, there have been reports of a potential evolution of the virus itself. There is increasing evidence that COVID-19 has jumped the animal to human barrier once again in a mutated form from infected livestock and mink. This possibility is particularly worrisome following the actions of the Danish government in November 2020, who moved to cull 17 million Minks after discovering the transmission of a mutated COVID-19 virus to over 200 people.

While the earlier mutation of the COVID-19 virus proved to be a more infectious strain, studies have shown that it not more lethal. With the possibility of a new strain of COVID-19, the question of whether this mutation is also a relatively simple one, or a more lethal form of the already deadly virus remains. If the mutation has created a virus from the original strain, there is a possibility that this new strain may be removed enough from the dominant strain to substantially lower vaccine effectiveness.

"We have seen mutations of this virus before, and as in those cases," said Dr. Elizabeth Bertoni, "research is needed on the possible consequences on the effectiveness of the COVID-19 vaccines."

Tab 3 – CISA Advisory

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Alert (AA21-343A)

Plaguerizer Ransomware Targeting the Healthcare and Public Health Sector

Original release date: April 7, 2021

Summary

This joint cybersecurity advisory provides an update to a previous report (AA20-302A) on ransomware threats to the healthcare and public health sector. With the roll out of the COVID-19 vaccine, there has been a significant uptick of related ransomware activity. This sector is uniquely vulnerable to shock due to the fact that its operations have been running over capacity for a prolonged period and frequently rely on legacy systems and diverse supply chains. Throughout the COVID-19 pandemic, ransomwares – such as Ryuk, Conti, TrickBot, and now Plaguerizer – have been leveraged for cybercrimes against the healthcare and public health sectors, especially hospitals. When affected, these institutions are unable to operate, as patient dataas well as key hospital systems are locked out. These attacks have proven lucrative for cyber criminals seeking financial gain.

This advisory describes the tactics, techniques, and procedures (TTPs) used by cybercriminals against targets in the Healthcare and Public Health Sector (HPH) to infect systems with ransomware for financial gain. CISA, FBI, and HHS have credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers. CISA, FBI, and HHS are sharing this information to provide warning to healthcare providers to ensure that they take timely and reasonable precautions to protect their networks from these threats.

Key Findings

- CISA, FBI, and HHS assess malicious cyber actors are targeting the HPH Sector, often leading to ransomware attacks, data theft, and the disruption of healthcare services.
- These issues will be particularly challenging for organizations during the COVID-19 pandemic; therefore, administrators will need to consider this risk when determining their cybersecurity investments.

Technical Details

Threat Details

With global efforts for a COVID-19 vaccine coming to fruition, cybercriminal operators have continued to develop and update new ransomware to target and financially extort HPHs. The newest ransomware, Plaguerizer, has continued to develop new functionality and tools, increasing the ease, speed, and profitability of victimization. These threat actors increasingly use loaders—like Plaguerizer—as part of their malicious cyber campaigns. Cybercriminals disseminate Plaguerizer via phishing campaigns that contain either links to malicious websites that host the malware or attachments containing the malware. Loaders start the infection chain by distributing the payload; they deploy and execute the backdoor from the C2 server and install it on the victim's machine.

Plaguerizer Ransomware

Plaguerizer has emerged as a new payload being used by Trojans such as TrickBot, appearing for sale as recently as December 2020. Plaguerizer appears to be a derivative of Ryuk, which itself was a derivate of the Hermes 2.1 ransomware. Plaguerizer, however, has received some bespoke modifications such as a Ctrl+Delete function to increase its effectiveness against targets in the HPH sector. These modifications have added the ability for the ransomware to deploy during the initial booting process and target firmware and RTOS based devices which can be used to permanently disable hardware. This new function increases the seriousness of the attack, since HPH victims are now faced with the possibility of building entirely new systems and losing all their data if the ransom is not paid.

While navigating the victim network, Plaguerizer actors will commonly use commercial off-the-shelf products – such as Cobalt Strike and PowerShell Empire—to gain access to the network and move laterally in order to steal credentials. Both frameworks are robust and are highly effective dual-purpose tools, allowing actors to dump clear text passwords or hash values from memory with the use of Mimikatz. This allows the actors to inject malicious dynamic-link library into memory with read, write, and execute permissions. In order to maintain persistence in the victim environment, Plaguerizer has been used to scheduled tasks and service creation.

Threat actors employing Plaguerizer will quickly map the network in order to understand the scope of the infection. To limit suspicious activity and possible detection, the actors choose to live off the land and, if possible, use native tools—such as net view, net computers, and ping—to locate mapped network shares, domain controllers, and active directory. Native tools, like PowerShell, Windows Management Instrumentation (WMI), and Windows Remote Management, and Remote Desktop Protocol (RDP), also allow movement laterally throughout the network. Once dropped, Plaguerizer uses AES-256 to encrypt files and an RSA public key to encrypt the AES key. Plaguerizer also drops a .bat file that attempts to delete all backup files and Volume Shadow Copies (automatic backup snapshots made by Windows), preventing the victim from recovering encrypted files without the decryption program.

In addition, the attackers will attempt to shut down or uninstall security applications on the victim systems that might prevent the ransomware from executing. Plaguerizer actors designate a ransom amount only after the victim makes contact. The victim is told to pay the specified amount to a specific Bitcoin wallet for the decryptor and is provided two decrypted forms of proof.

Initial testing indicates that files affected by Plaguerizer will not decrypt properly without the decryption script. Furthermore, Plaguerizer actors have been reported sending a modified decryption script that will render systems inoperable if they believe the victim is consulting with law enforcement or delays past established deadlines for ransom payment.

General Ransomware Mitigations —HPH Sector

Follow Ransomware Best Practices

Refer to the best practices and references below to help manage the risk posed by ransomware and support your organization's coordinated and efficient response to a ransomware incident. Apply these practices to the greatest extent possible based on availability of organizational resources.

- It is critical to maintain offline, encrypted backups of data and to regularly test your backups. Backup procedures should be conducted on a regular basis. It is important that backups be maintained offline or in separated networks as many ransomware variants attempt to find and delete any accessible backups. Maintaining offline, current backups is most critical because there is no need to pay a ransom for data that is readily accessible to your organization.
    - Use the 3-2-1 rule as a guideline for backup practices. The rule states that three copies of all critical data are retained on at least two different types of media and at least one of them is stored offline.
    - Maintain regularly updated "gold images" of critical systems in the event they need to be rebuilt. This entails maintaining image "templates" that include a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.

    - Retain backup hardware to rebuild systems in the event rebuilding the primary system is not preferred.
        - Hardware that is newer or older than the primary system can present installation or compatibility hurdles when rebuilding from images.
        - Ensure all backup hardware is properly patched.
- In addition to system images, applicable source code or executables should be available (stored with backups, escrowed, license agreement to obtain, etc.). It is more efficient to rebuild from system images, but some images will not install on different hardware or platforms correctly; having separate access to necessary software will help in these cases.
- Create, maintain, and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident.
- The Ransomware Response Checklist, available in the CISA and MS-ISAC Joint Ransomware Guide, serves as an adaptable, ransomware-specific annex to organizational cyber incident response or disruption plans.
- Review and implement as applicable MITRE's Medical Device Cybersecurity: Regional Incident Preparedness and Response Playbook.
- Develop a risk management plan that maps critical health services and care to the necessary information systems; this will ensure that the incident response plan will contain the proper triage procedures.
- Plan for the possibility of critical information systems being inaccessible for an extended period of time. This should include but not be limited to the following:
    - Print and properly store/protect hard copies of digital information that would be required for critical patient healthcare.
    - Plan for and periodically train staff to handle the re-routing of incoming/existing patients in an expedient manner if information systems were to abruptly and unexpectedly become unavailable.
    - Coordinate the potential for surge support with other healthcare facilities in the greater local area. This should include organizational leadership periodically meeting and collaborating with counterparts in the greater local area to create/update plans for their facilities to both abruptly send and receive a significant number of critical patients for immediate care. This may include the opportunity to re-route healthcare employees (and possibly some equipment) to provide care along with additional patients.
- Consider the development of a second, air-gapped communications network that can provide a minimum standard of backup support for hospital operations if the primary network becomes unavailable if/when needed.
- Predefine network segments, IT capabilities and other functionality that can either be quickly separated from the greater network or shut down entirely without impacting operations of the rest of the IT infrastructure.
- Legacy devices should be identified and inventoried with highest priority and given special consideration during a ransomware event.

- See CISA and MS-ISAC's Joint Ransomware Guide for infection vectors including internet-facing vulnerabilities and misconfigurations, phishing, precursor malware infection, and third parties and managed service providers.
- HHS/HC3 tracks ransomware that is targeting the HPH Sector. This information can be found at http://www.hhs.gov/hc3.

Tab 4 – Think Tank Report

The Decade of the Cyber Mercenary

Dr. Mabel Edwards

If the past decade has been characterized by the nation-states' domination of cyberspace, then we should expect for the following decade to be the decade of the cyber mercenary. In the past few years, there has been an emergence of private firms who blur the line between state-level operations and hackers for hire or state-sponsored advanced persistent threats (APTs). The privatization of cyber operations and capabilities pulls governments and companies into uncharted territory regarding cyber defense, cyber offense, and attribution.

In international relations, as well as cyberspace, government actors rely on treaties, alliances, and norms in order to maintain stable and positive relations with one another. While responsible states rely on diplomatic tools in cyberspace, nonstate actors often conduct operations with little regard for norms and treaties, instead motivated by ideology and financial gain.

In spite of this ambiguity, there has been an unprecedented trend of governments outsourcing their cyber operations to private firms. Government motivations for outsourcing are twofold—first, due to the global cyber skills shortage, and second, to advance strategic goals with impunity. There remains a dire shortage of cybersecurity experts and practitioners, and yet, a high demand from governments for cybersecurity skills and services. When governments are unable to tap into a domestic cyber workforce,

they have little choice but to turn to private, foreign firms.

While many governments may rely on private and foreign firms for cyber defense services, there will be governments who seek to take advantage of the additional complexity and obfuscation that private firms can provide them for offensive operations that are at odds with international cyber norms. These new transactions may facilitate the proliferation of capabilities such as vulnerability research and exploitation, malware payload development, technical or operational command and control, as well as training on offensive cyber programs. Repressive and authoritarian regimes may seek to hire private firms to support or execute their dirty work such as surveilling human rights activists, journalists, and political dissidents.

The use of private firms for malicious and offensive cyber operations introduces a number of challenges around attribution and promoting responsible state behavior in cyberspace. Attribution, as difficult as it is to obtain, encourages actors to adhere to norms in cyberspace. With more and more governments turning to private firms for cyber operations, attribution may now point to a nonstate actor, acting on behalf of a government, instead of the government procuring the services in question. There may be a very near future where we may be unable to discern whether a company or an actor is American, Israeli, Russian, or Chinese, and who is engaging in what operations.

Even more worrisome is the potential for the growth of self-regulated illicit and semi-regulated commercial marketplaces for cyber knowledge, personnel, and skills needed for offensive cyber operations, tailored for and marketed to governments with vast resources.

What is certain, is that private firms are hiring and searching for the experience and skillsets that often come with being a former government employee. These former employees will naturally bring the tactics, techniques, and procedures characteristic of their government's cyber operations to these private firms, further complicating attribution and the future of responsible state behavior in cyberspace.

Tab 5 – NSA Report to NSC

National Security Agency

Ransomware Threat to American Hospitals; April 2021 (TS//SI//OC/REL TO USA, FVEY/FISA)

(U//FOUO) INTELLIGENCE PURPOSES ONLY: (U//FOUO) The information in this report is provided for intelligence purposes only but may be used to develop potential investigative leads. No information contained in this report, nor any information derived therefrom, may be used in any proceeding (whether criminal or civil), to include any trial, hearing, or other proceeding before any court, department, agency, regulatory body, or other authority of the United States without the advance approval of the Attorney General and/or the agency or department that originated the information contained in this report. These restrictions apply to any information extracted from this document and used in derivative publications or briefings.

SUMMARY (U)

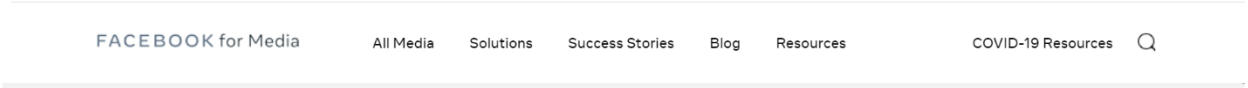
[redacted] (TS//SI//OC/REL TO USA, FVEY/FISA) On April 9 2021, under NSC recommendation, CIA and NSA increased operational surveillance of a threat actor targeting organizations in the United States with ransomware. Organizations targeted have included hospitals, clinics, and public health organizations. When targeting hospitals, the threat actor has targeted hospitals of varying sizes, including rural hospitals who often do not have sufficient security staff or budget to respond to a ransomware attack and are operating near capacity with COVID-19 and seasonal influenza cases.

Threat actor is targeting a Windows software vulnerability in [redacted] devices present at hospitals and ultra-cold freezers manufactured by InfiniChill. The vulnerability allows for the ransomware to obtain a foothold and then spread on the organization's network.

Assumption with MEDIUM confidence that the threat actor is linked to the Russian Federation due to the financial motivation of the attacks and the TTPs used in operations. TTPs used have also been previously linked to operations by Sobornost, a company based in Nicosia, Cyprus with ties to Russian Federation government personnel and bank accounts. Sobornost was established by Kremlin-linked oligarchs Leonid Loomischenkov and Ioann Malkin who receive coverage under appropriate programs.

In order to increase the confidence level for attribution, more surveillance will need to be conducted. Due to the trend of private cyber companies adopting TTPs previously only linked to governments, attribution of this threat actor may be delayed.

Tab 6 – Facebook Blog



Fighting Misinformation on COVID-19 Vaccinations

By Zhao Qiqiang, Head of Health

Everyone wants the COVID-19 pandemic to end as soon as possible, and to minimize the number of those affected by the virus. Misinformation can erode trust at a time when trust is most important. Our platform in the past few months has seen a steady rise of discourse and conversations surrounding the efficacy of the various COVID-19 vaccines.

Specifically, we see allegations that the COVID-19 vaccines produced by Pfizer, Moderna, AstraZeneca, and Johnson & Johnson are ineffective against the virus and even potentially dangerous. We have tracked an increase in activity that encourages users to ignore CDC and government COVID-19 guidelines, including calls to ignore the universal mask mandate and ignore social distancing restrictions. Such posts are hosted on a wide number of private pages and Facebook groups, and do not appear to be centrally guided.

This kind of COVID-19 misinformation is especially dangerous in this pivotal stage of vaccine rollout. The CDC has warned that these attitudes and narratives could result in an increase in infections and hospitalizations, as well as decrease public trust, at a time when most Americans need to trust public health officials and experts in order to end the pandemic.

We at Facebook will be continuing our efforts towards tracking and minimizing misinformation surrounding the dangers of COVID-19 and the safety of the COVID-19 vaccine. We have continued our policy of rejecting ads that specifically discourage people from getting the vaccine. These takedowns focus on known vaccines hoaxes, as identified by leading public health entities, such as the World Health Organization (WHO) and the US Centers for Disease Control and Prevention (CDC).

We also expanded this effort to include individual posts that violate this policy. This process is being undertaken with extreme care to ensure that we are responsible partners in supporting the spread of accurate and helpful information on COVID-19, while respecting our users' ability to use our platforms. To promote the spread on accurate information regarding COVID-19 and its vaccines, and to make it easier for our users to access this information, we will continue to update our Coronavirus (COVID-19) Information Center.

Tab 7 – Panel Discussion Transcript

The Hatchet School of Law and Diplomacy

Panel Discussion: Collaborating with Allies and Countering Adversaries in Cyberspace

April 13, 2021

Panelists:
Jackie Fischer, *Adjunct Faculty, Schwarzenegger Center for Conflict Studies*

Max Crockett, *Principal, KPMG; Former FBI Special Investigator*

Stanley Smythe, *Senior Professional Staff Member, House Committee on Foreign Affairs, U.S. House of Representatives*

Katherine Taylor, *Senior Fellow, Institute for Cyber Peace Studies*

Amira Bhatt, *Associate Counsel, CrowdFire*

Moderator: Diego Meza, *Associate Professor, Hatchet School of Law and Diplomacy*

[Truncated Transcript]

Diego Meza:	I'd like to turn us over to Q&A. At the start of the event, we'd asked students and guests to drop their questions in the chat. We'll start with a few that have already come in, and if you've got additional questions, please drop them in there along with your name and affiliation. If you can address it to a specific panelist that will keep Q&A moving smoothly. Our first question is from Luke Peters.
Luke Peters:	Thanks, this has been a really interesting panel. Really liked the point brought by Katherine about how there needs to be clearer rules of the road when it comes to infrastructure takedowns. I was wondering whether the panelists could elaborate on why certain actions work for some countries, but not for others?
Diego Meza:	Thanks Luke, before I throw it to the panelists, where are you from?
Luke Peters:	Oh, sorry about that Professor Meza! I'm a 2nd year JD student at Hatchet. Thanks!

Diego Meza: Right, Katherine, since Luke's question referred to your point, why don't we start with you?

Katherine Taylor: Of course, thanks for your question Luke. So just to quickly recap, at present, there are two separate processes for takedowns that can occur. To take a pretty recent example, TrickBot was initially disrupted by a military operation conducted by US Cyber Command, while, almost concurrently, there was a disruption conducted by private actors – namely Microsoft, ESET, the FS-ISAC and others. They use two very different tools to conduct their actions. What Cyber Command did was a military operation to protect the election – and there are a slew of legal authorities, executive orders, and laws that allow them to conduct such an operation in cyberspace without needing sign off from Congress or the President. Cyber Command's approach was a deliberate, and technical, disruption of how Trickbot infections received updates and communicated with their operators. On the flipside, the takedown led by Microsoft started in the courts. As a private actor, Microsoft had to make a substantive case that certain domains and infrastructure were being used for criminal and malicious purposes, and by applying copyright law and that massively long terms of service agreement that few of us read – secured legal authority to stop the botnets – but only those domains located in the US. Those takedowns were delivered at the end of a court order, not a malicious update. Now I can go on for days, but I think I'll stop here and get my fellow panelists in on this.

Max Crockett: Diego, if it's alright, I'd like to jump in?

Diego Meza: Sure thing, go ahead.

Max Crockett: Katherine is correct, there have been two if not three variations to this operational formula. You've got the private sector leveraging the courts to get approvals to conduct takedown operations, then you've got Cyber Command which has been using the yet-undisclosed NSPM-13 to great effect to conduct operations presumably like takedowns. There have also been collaborative operations, typically in emergencies, like when Mirai was setting stuff on fire, where everyone is just like, "who needs what and how do we get it done?" Having been part of the FBI during the Mirai takedown, it was an amazing sight to see, but my experience has also shown that there are places where additional frictions emerge, like when the infrastructure is in Russia or the operator is Chinese. Those are expected frictions given the kind of geopolitical tapestry that exists, and I'd imagine that will only build up as countries try and find a silver bullet for this problem.

Jackie Fischer: I think if there's a gold standard for us to be aiming for its that Cyber Command takes the reigns in embodying that principle of Defending Forward. That means finding the infrastructure, locating the bad guys, and taking them out with military precision. It shouldn't matter whether its China, Russia or North Korea – if someone is attacking the United States, especially during a crisis where they are specifically targeting

hospitals, the US should have every justification to disrupt their operations.

Stanley Smythe: I don't think that --

Jackie Fischer: No one is saying-- Oh sorry Stanley, I'll just leave it on this last point. Cyber Command's focus is to disrupt operations and that is what we should focus on. Everyone's a bit more experienced with cyber now, and there's a clear difference between a disruptive operation and an offensive operation like a Stuxnet.

Stanley Smythe: At the same time, the gold standard shouldn't be for the US to march across the internet and kick down doors in cyberspace. That can only result in a resentment which will cost the US in the long run. I think it is worth remembering the complexities in the relationships that exist. And keeping in mind the number of new cyber players that are emerging. North Korea launches a ransomware attack? The response for that is comparatively straightforward as compared to if it was an attack conducted by China's MSS or if the attack originated from a democratic state like India. For China, there are economic concerns, a cyber response could be met with severe economic or geopolitical consequences. And for India, it's a democratic nation and an ally! Even if there's a malicious actor present within its borders, it's impossible for us to suggest that the US marches in and takes down C2 infrastructure.

Jackie Fischer: I'd like to clarify that I'm not suggesting that the United States becomes this cyber bully as some might infer, but rather, as per Katherine's original point, there should be clear rules of the road so that if a takedown has to occur, it is done by law enforcement and by military authorities. The idea of having the private sector – these net states – so intrinsically linked to the defense of our domestic and international cyberspace should be something that gives us pause.

Amira Bhatt: I guess that leaves me with the last word! So, I'm going to quickly piggyback on what Max said about finding a silver bullet. He's right that everyone will look for one, but thing is that there isn't one. When Cyber Command conducts a disruption type of takedown, think of it like them applying force to the botnet infrastructure. They might knock the C2 offline, they might sinkhole the bots with some credential hacking, both are great! But without taking out the infrastructure entirely – the operators are always going to find a way to come back. I mean, we all saw how Trickbot recovered!

That's why the collaborative operations are so important. We may not like it, but private companies can have a lot of international trust. That means when they go to another country's law enforcement and say "Look we've got this evidence; this is what we want to remove, can you help us," they're likely to get a yes. For Necurs, Microsoft worked with law enforcement, ISP providers, domain name registries and government CERTs across *six* different countries. I don't think any Cyber Command from the US or anywhere else could have taken down that infrastructure without creating massive international backlash – especially if it was

revealed they operated against an ally like France to takedown – not disrupt – a botnet operated from Russia!
That was a lot more than a word – sorry Diego.

Diego Meza: No, those were some good points from all our panelists. Clearly, we could have had an entire panel on this! However, in the interest of time, let's move onto another question.

Cyber 9/12 Strategy Challenge

Intelligence Report II

INSTRUCTIONS

Please read these instructions carefully. They have changed from previous years.

Your team will take on the role of experienced policy advisers, part of a hypothetical cybersecurity task force, preparing to brief the National Security Council (NSC). This packet contains fictional information on the background and current situation involving a major cyber incident affecting US systems. The attacks notionally take place in Spring 2021. The scenario presents a fictional account of political developments and public reporting surrounding the cyber incident.

The NSC needs information on the full range of response options available regarding this incident. Your team has been tasked with developing an appropriate course of action for recommending to the NSC.

You are to consider as facts the following pages for formulating your response.

You will use the fictional scenario material presented to perform two tasks:

Oral Policy Brief (Day 2): For Day 2 of the competition, prepare a ten-minute oral presentation outlining your impact and risk assessment, as well as your suggested course of action. You will present to a panel of judges playing the role of the NSC.
Decision Document (Day 2): Teams will also be required to submit a "decision document" accompanying their oral presentation at the beginning of the competition round. The "decision document" will be a maximum of one single-sided page in length, outlining the team's response options, decision process, and recommendations. The teams should note that the document is not intended to summarize every detail of the recommendations, but to help the judges follow the oral presentation, and the judges will be given only 2 minutes to read it before the presentation begins. The document should be written with the goal of assisting busy senior officials to quickly grasp your team's recommendations and analysis.

Keep these tips in mind as you are reading and considering your policy response alternatives:

- *Analyze the issues.* The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of potentially conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.

- *Engage the scenario.* Believe that the universe we have created is plausible and that the events that happen in it are realistic. Nevertheless, remember to think critically about the intelligence you have been provided and its provenance.

- *Think multi-dimensionally*. When analyzing the scenario, remember to consider implications for other organizations and domains (e.g. private sector, military, law enforcement, different levels of government, diplomatic) and incorporate these insights along with cybersecurity.

- *Consider who you are, and who you're briefing.* You are experienced cyber policy professionals briefing the National Security Council. As such, you should be ready to answer questions on agency responsibility, provide justifications for your recommendations, and have potential alternatives ready.

- *Be creative.* Cyber policy is an evolving discourse, and there is no single correct course of action to the scenario information provided. There are many ideas to experiment with in responding to the crisis.

- *Don't fight the scenario*. Unless stated otherwise, assume all inter-state relations, policies, and treaties have remained the same as they were in January 2021. Explore the implications of that information, not the plausibility.

Given the unclear nature of the threat, the NSC requests that your team prepare a concise assessment of the ongoing situation and reporting. Your assessment should include:

- How or where the relevant systems could be vulnerable to exploit, and what steps can be made to mitigate these vulnerabilities;
- An assessment of potential risks and impacts to consider if the vulnerabilities are successfully exploited; and
- Responses the NSC can or should consider addressing these vulnerabilities, taking into account the severity and likelihood of the threat.

To provide this assessment and policy recommendations, you will apply your understanding of the technologies involved, cybersecurity, law, foreign policy, international relations, and security theory to
synthesize useful policy measures from limited information. Your recommendation must analyze the possible strengths, weaknesses, opportunities, and threats of your proposed response.

In formulating your response, you will be expected to have considered, at a minimum:

- All stakeholders when determining an action or recommendation, including the role of the government and private sector;
- The long and short-term impacts of your recommendation;
- Which agency will be responsible for the action you have recommended;
- Appropriate recommendations for local vs. federal government;
- Whether you can, or should, attribute the threat; and
- The covert or overt nature of your response.

Additionally, this message is accompanied by several documents that may assist your team in preparing the assessment and policy brief for the NSC:

- **Tab 1** – Hospital Administrator Email Chain
- **Tab 2** – Salt Lake Tribune News Article
- **Tab 3** – Interagency Memo

- **Tab 4** – NextDoor Post
- **Tab 5** – Email Chain with Digital Wells Hosting
- **Tab 6** – US State Department Teams Chat
- **Tab 7** – Rabinara Group Report
- **Tab 8** – Diplomatic Cable

Tab 1 – Hospital Administrator Email Chain

From: Elliott Bleeker <elliott.bleeker@COHealth.org>
Sent: Friday, April 16, 2021 at 2:36 p.m.
To: Cara Lane <cara.lane@COHealth.org>
Cc: Nathalie Ahles <nathalie.porter@COHealth.org>; Forrest Edwards<forrest.edwards@COHealth.org>
Subject: URGENT - Network Activity

Hi Cara,

I hope you've had a good week. I'm reaching out as the team is noticing some strange activity on COHealth networks.

Nurses in the Pediatrics Department have reported being locked out of devices and are unable to access patient records.

I can be reached at my extension.

Best,
Elliott

Elliott Bleeker
Director, IT & Information Systems
Colorado Health
elliott.bleeker@COHealth.org | Ext. 2395

From: Cara Lane <cara.lane@COHealth.org>
Sent: Friday, April 16, 2021 at 2:42 p.m.
To: Elliott Bleeker <elliott.bleeker@COHealth.org>
Cc: Nathalie Ahles <nathalie.porter@COHealth.org>; Forrest Edwards<forrest.edwards@COHealth.org>
Subject: Re: URGENT - Network Activity

Elliott,

I just got off the phone with a couple of my contacts at Mountain Healthcare and Cheyenne Medical in Utah and Wyoming and they've been experiencing similar activity. Mountain Healthcare's devices in their Surgery Department have been bricked so they're diverting priority patients to Valley Hospital and rescheduling everything they can.

More when I call you in a sec.

Cara Lane
Vice President, Information Services
Colorado Health
cara.lane@COHealth.org | Ext. 1453

From: Cara Lane <cara.lane@COHealth.org>
Sent: Friday, April 16, 2021 at 3:13 p.m.
To: Elliott Bleeker <elliott.bleeker@COHealth.org>; Randy DiCoco <randolph.dicoco@COHealth.org>
Cc: Nathalie Ahles <nathalie.porter@COHealth.org>; Forrest Edwards <forrest.edwards@COHealth.org>; Mel Wagner <mel.wagner@ COHealth.org>; Li Zhang <li.zhang@COHealth.org>
Subject: Re: URGENT - Network Activity

Hi all,

Looping in Randy and the rest of the team at the Office of the CIO.

Randy, IT has been investigating an incident at the Pediatrics Department where staff have been locked out of devices and are unable to access patient records.

The Neurology and Radiology Departments are now also reporting similar activity. I'm convinced we're experiencing something like what's going on at Mountain Healthcare and Cheyenne Medical. My contacts there have reported some devices being rendered useless.

I propose we reach out to our contact at H-ISAC to get in touch with CISA and the FDA before the weekend.

Cara

Cara Lane
Vice President, Information Services
Colorado Health
cara.lane@COHealth.org | Ext. 1453

Tab 2 – Salt Lake Tribune News Article

The Salt Lake Tribune

Utah appeals to Moferza to combat new strain of COVID virus

(Rick Egan | The Salt Lake Tribune) Covid-19 testing at Mountain Healthcare Center, on Dec. 11, 2020.

Editor's note: *The Salt Lake Tribune is providing free access to critical stories about the coronavirus. Sign up for* our Top Stories newsletter*, sent to your inbox every weekday morning. To support journalism like this, please* donate *or become a* subscriber*.*

By Melanie Cruz | April 19, 2021 15:56 | Updated: 32 mins ago

While Utah is in the throes of a serious surge in coronavirus cases, a race for the vaccine is underway despite several recent cases of individuals admitted to hospitals for treatment after already received a COVID-19 vaccine as part of the state-wide drive back in March.

Utah is expected to receive a new shipment of Moferza's COVID-19 vaccine by the end of the week in a bid to offset a new strain of the virus, a state official said on Monday.

The additional 12,450 doses are slated to be stored at Mountain Healthcare Center in Salt Lake City as the hospital has become the primary vaccine storage and distribution hub for much of the state. The surge in COVID-19 cases has already resulted in 30 deaths and has hospitalized 432 more people.

In a joint statement last week, the U.S. Department of Agriculture and the National Institute of Allergy and Infectious Diseases (NIAID) confirmed that a previous outbreak of the COVID-19 virus among Utah's mink was capable of transmission to humans.

The Department of Agriculture had confirmed the existence of the virus in mink back in December 2020, following concerns out of Denmark which was forced to cull more than ten thousand of the animals as a preventive measure. No culling was authorized in Utah at the time.

An NIAID spokesperson said investigators had localized the outbreak to the Salt Lake City area as well as several of Colorado's Front Range cities. The spokesperson went on to reiterated that the Moferza vaccine was still a viable preventive measure against the new strain, and that no changes to the vaccine rollout are being planned.

State officials urged the public to voluntarily return to 2020 COVID-19 protection measures. "That means wearing a mask and staying six feet apart," the statement on Twitter read.

"We've made an appeal to Moferza to prioritize our vaccines, and asked the President's COVID-19 Task Force to ensure that Utahns get the attention needed to prevent this from becoming a new pandemic," the statement on Twitter continued.

Tab 3 – Interagency Memo

U.S. Department of Heath and Human Services

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

FROM: Cybersecurity and Infrastructure Security Agency (CISA) and Department of Health and Human Services (HHS)
FOR: National Security Council Cyber Response Group
RE: Coordinated Ransomware Attacks against the Healthcare and Public Health Sector
DATE: April 20, 2021

PACKET SUMMARY: Coordinated investigations by CISA and HHS report serious ongoing effects of ransomware attacks against the Healthcare and Public Health sector in Utah, Colorado, and Wyoming. These attacks have severely impacted hospital operations during a spike in COVID-19 cases and administrators fear the ransomware attacks may lead to additional fatalities. According to CISA reports, the malicious activity appears to be emanating from IP addresses located in Spain. However, CISA stresses that at this time, attribution remains unclear. Given the potential lethality of the attacks, items were compiled and fast-tracked for NSC review in context.

ITEM #1

CONTENTS: The Department of Health and Human Services has conducted a thorough analysis of the current and potential effects of the ongoing ransomware attacks against hospitals in Utah, Colorado, and Wyoming. Many of these hospitals are currently over capacity due to the recent surge in COVID-19 cases. Hospitals are often the nexus of distribution for the COVID-19 vaccine in local communities. However, studies suggest that the available vaccines are not effective against this second strain of COVID-19 identified in these states. This second strain has quickly exhausted available hospital capacity. This report found that hospitals affected by the ransomware attacks do not have the capability to operate over half-capacity under the restraints inflicted by the attack in combination with COVID-19-related stresses. Access to patient health information, crucial to diagnosis and treatment, is unavailable, but doctors, nurses, and administrators have switched to less efficient but effective offline documentation methods.

These attacks have also targeted the physical infrastructure of victimized hospitals, including elevators and medical devices, such as MRI machines. Several hospitals have made the decision to temporarily stop admitting new patients, instead rerouting the load to nearby hospitals. As yet, no deaths have been positively linked to offline medical devices to hospital's response to this crisis. The effects of these ransomware attacks have been greatly exacerbated by the increasing severity of the COVID-19 outbreak in these states.

ITEM #2

CONTENTS: CISA earlier this month released a public advisory to the Healthcare and Public Health sector warning of a new type of ransomware, Plaguerizer, targeting U.S. hospitals. Analysts have continued to investigate these ransomware attacks which utilize a combination of TTPs to target hospital operations and data. This aggregate of TTPs does not appear to align with any known state or organization. It is possible that the actor responsible has assimilated use of new TTPs in an effort to mask their identity. While that segment of the investigation is still underway, examination has shown that large portions of the infrastructure used to launch this series of attacks are located in Spain. The attacker used IP address 2.17.134.[redacted] as a command-and-control IP address. Specifically, this Spanish IP address was used to access the compromised servers at each affected hospital. Additionally, the Cruce wiper component was identified as a module in the ransomware attacks – which has been observed in other malware attacks emanating from Spain. It is unclear the extent to which the Spanish government is aware of its infrastructure's connection to these attacks. There has not been any public acknowledgement by the Spanish government.

Tab 4 – NextDoor Post

nextdoor

Safety

Add new

Updates Tips & Resources

Your neighborhood + 20 nearby. View

Catherine Parr

Greeley, CO • April 20, 2021

IMPORTANT – The outbreak of the second strain of COVID is NOT limited to mink! IT IS ALSO SPREAD THROUGH LIVESTOCK. My husband was just diagnosed with COVID even though we have been social distancing and do not own Mink. He started feeling sick last week, so we talked to our neighbors who also own cattle and they told us that the second, deadlier strain of COVID can be spread through interaction with livestock, not just Mink. I took Mike to the hospital yesterday morning and it took 7 hours to get tested. We waited in our cars in line with about a hundred other people who also needed the test. This is bad guys, I know we thought we were nearing the finish line with the vaccines, but I don't think this is gonna be over any time soon.

Like 113 Comments Share 102

See 50 previous comments

Jack Ullman • Kelim, CO

I've heard that too, I've been telling all my friends who work in ranching that they should get tested ASAP. I know the government keeps saying that this new covid only passes through mink, but now I'm not so sure.

Danny Derwent • Evans, CO

The CDC still says that this second strain ONLY passes to humans from Mink, not livestock. Please stop spreading rumors. Just stay inside and STOP overcrowding hospitals.

Winnifred Hatfield • Greeley, CO

I agree **@Jack Ullman** we have to protect ourselves when the government won't.

Georgia Hallorann • Lucerne, CO

I know this is awful guys, but this just isn't true! Our community's doctors and nurses are already overwhelmed, and the only way to get through this is to let them work and STAY AT HOME

Tab 5 – Email Chain with Digital Wells Hosting

From: Rainn Schrute <rschrute@fbi.gov>;
Sent: Wednesday, April 21 2021 8:27 EST
To: James Halpert <jhalpert@dwhosting.com>;
CC: Erica Kessler <erica.kessler@kesslerbernard.com>; Michael Dent <mdent@cisa.dhs.gov>; Jessie Wesley <j.wesley@microsoft.com>;
Subject: URG: Takedown Notice

Dear Mr. Halpert,

We wanted to provide you with an update on our ongoing investigation and our recent request to Digital Wells Hosting to cooperate with law enforcement to isolate servers in Texas supporting the Plaguerizer campaign and bring them offline. Please call me when you receive this. I can still be reached at the number I provided you.

Many thanks,
R Schrute
<<UNCLASSIFIED>>

From: James Halpert <jhalpert@dwhosting.com>
Sent: Wednesday, April 21 2021 9:57 EST
To: Rainn Schrute <rschrute@fbi.gov>;
CC: Erica Kessler <erin.kessler@kesslerbernard.com>; Michael Dent <mdent@cisa.dhs.gov>; Jessie Wesley <j.wesley@microsoft.com>; Stanley Baker <sbaker@dwhosting.com>; Mihir Kapoor <mkapoor@dwhosting.com>
Subject: URG: Takedown Notice

Morning Agent Schrute,

Just got in.

As Erica had explained, we as a company that takes pride with our bulletproof hosting, it's incredibly difficult for us to comply with your directive. I believe when we first put across our position, we were informed that we'd be hearing from Microsoft's legal team after they secured a preemptive order from a Federal judge. Frankly, that would move things along considerably. Stanley from legal could process it, and Mihir who coordinates our technical facilities could comply.

Calling now. Thanks!
J
Assistant Vice President, Central - North America
Digital Wells Hosting

From: Stanley Baker <sbaker@dwhosting.com>;
Sent: Wednesday, April 21 2021 10:29 EST

To: James Halpert <jhalpert@dwhosting.com>; Rainn Schrute <rschrute@fbi.gov>;
CC: Erica Kessler <erin.kessler@kesslerbernard.com>; Michael Dent <mdent@cisa.dhs.gov>; Jessie Wesley <j.wesley@microsoft.com>; Mihir Kapoor <mkapoor@dwhosting.com>
Subject: URG: Takedown Notice

Just letting everyone know. I will be out of office on Thursday and Friday for pre-approved PTO.

From: Michael Dent <mdent@cisa.dhs.gov>;
Sent: Wednesday, April 21 2021 11:11 EST
To: Rainn Schrute <rschrute@fbi.gov>; James Halpert <jhalpert@dwhosting.com>;
CC: Erica K <erin.kessler@kesslerbernard.com>; Jessie Wesley <j.wesley@microsoft.com>; Mihir Kapoor <mkapoor@dwhosting.com>; Stanley Baker <sbaker@dwhosting.com>;
Subject: URG: Takedown Notice

Just wanted to summarize our call with James for the benefit of those on the chain.

CISA has found evidence that the origin of these attacks is emanating from IP ranges tied to a colocation facility near Barcelona owned and operated by Digital Wells Hosting . We're going to be following up with our counterparts at the Cybercrime Central Unit of the Guardia Civil in Spain and hope that this doesn't disrupt the response process that DW Hosting already has underway. This malware is extremely destructive, and it is important that the infrastructure supporting it is taken offline.

Jessie's team from Microsoft will continue their appeals to secure an emergency TRO through the Fifth Circuit.

Regards,
Michael S.

<<UNCLASSIFIED>

From: James Halpert <jhalpert@dwhosting.com>;
Sent: Wednesday, April 21 2021 13:54 EST
To: Rainn Schrute <rschrute@fbi.gov>; Michael Dent <mdent@cisa.dhs.gov>;
CC: Erin K <erin.kessler@kesslerbernard.com>; Jessie Wesley <j.beesley@microsoft.com>; Mihir Kapoor <mkapoor@dwhosting.com>; Stanley Baker <sbaker@dwhosting.com>;
Subject: URG: Takedown Notice

After discussing this with you both and with Erica. I'm reading this as - Erica, please let me know if I'm wrong - Digital Wells Hosting shouldn't expect a legal notice, and legally has no requirement for further action which might impact our commitments to our customers.

J

Tab 6 – US State Department Teams Chat

----------April 21, 2021----------

Jake 18:57 PM
Evening folks! Edwarda can you rename this channel and give me admin access? Given the briefing we've got, and the strong confidence from CISA and other IC partners that this *isn't* North KoreaI think you and the others from EAP can leave this channel to declutter your Teams app

// Edwarda *renamed the channel to* ***TF: Plaguerizer (S/CCI-EUR)*** //

Edwarda 18:58 PM
Cool. Good luck team. While I'm glad it's not NK, knowing how grey CCI's issues get, I'm not sure I envy the work you have ahead. I've asked Tiffany to stay in this channel – she's handled our responses to NK when they've used ransomware before and would be useful to the Coordinator on Cyber Issues work on this.

// Edwarda made Jake an admin //
// Edwarda, Matthew, John, *left the channel. Bye Bye!* //

Jake 19:00 AM
Thanks Edwarda & Tiffany, looking forward to your inputs on this. @August, can you start adding those contacts from EUR that might be needed on this? Especially folks that have dealt with ES law enforcement and Europol

August 19:06 AM
Sure thing. Going to rope in two folks from the DC office. Stuart has experience working with our counterparts in ES and Jenny has worked with Europol before.

// *August added* Stuart *and* Jenny *to the channel. Say Hi!* //

August 19:26 AM
@Jake, I've briefed Stuart and Jenny on the situation but feel free to add some useful CCI tidbits. Guys, if you have any questions for Jake, please drop it in.

Jenny 19:29 AM
Hi! Could I get some clarification on what's happening with the hosting firm in Austin, TX? Has there been any progress from the FBI? Is there anything for State to pick up from there?

Jake 19:34 PM

That's a big negative on progress Jenny. According to the FBI/CISA team, it's a mess because the company's stance is that since they advertise bulletproof hosting they will refuse to cooperate unless they get a legal notice that will force them. That said, since this we're confident this is now coming from Spain we might have more options. Erica was right in that Spain's an ally, which alters our typical approach. I'm interested in what this team thinks - channel is open to your suggestions.

Tiffany

NK has always been difficult to engage with diplomatically, so we've responded with a heavier hand. Our responses have always been measured to the threat. That said, the last thing we should be is too soft and have these guys slip away. I'm probably wrong, but didn't Spain have issues prosecuting Mariposa actors back in 2010?

Tab 7 – Rabinara Group Report

Emergence of A New Non-State Actor

For several months, the Rabinara Group has tracked the activity of what appears to be a new and aggressive non-state threat actor. In cyberspace, non-state actors have the potential to be much more effective and wield greater influence than in other traditional domains. The decentralized and malleable structure of the domain belies traditional notions of wholly state-centered control. Indeed, the cyber domain is primarily operated by non-state actors, namely private corporations. In this environment, malicious non-state actors have identified and exploited niches where their capabilities align with their primary motivation. These axes range from groups operating simple phishing scams for monetary gain to groups building and deploying sophisticated malware toward politically-driven targets.

This group, as yet unnamed, does not appear to have a significant political motivation despite its focus on targets within the United States. The group's primary purpose appears to be monetary gain. Our investigations have found that this group is responsible for numerous attacks on hospitals and care facilities throughout the United States. This group has capitalized on the fact that, due to the COVID-19 pandemic, US hospitals can ill-afford the time and efficiency loss caused by ransomware or botnet attacks. Therefore, the cost-benefit analysis of hospital administrators has been forced to shift towards providing prompt payment to those demanding payment of ransoms.

Attribution of this group has proven to be a slow process. The actor has displayed an inconsistent amalgamation of tactics, techniques, and procedures (TTP), some of which have previously been associated with advanced persistent threat (APT) groups tied to several different states. The presence of these capabilities within a single group raises serious concerns as to the potential proliferation of advanced TTPs. As the Rabinara Group continues our investigation, we are prioritizing understanding this actor's technical and operational command and control (C2) structure to determine the existence and reach of a new pathway of capability-spread amongst non-state actors. This should also provide more significant indicators for attribution.

Tab 8 - Diplomatic Cable

DATE 2021-04-22

SOURCE Embassy Madrid

CLASSIFICATION SECRET / / NOFORN

S E C R E T SECTION 01 OF 01 MADRID 204187

SUBJECT: U.S. ACCESS TO SPANISH PORTS AND MILITARY BASES

CLASSIFIED BY: NAME, U.S. Embassy Madrid, Department of State

REASON 5.1 (b)

1. Summary: During a meeting, the Spanish Minister of Foreign Affairs informed [redacted] the Spanish government is concerned with recent events surrounding ransomware attacks originating from Spain targeting U.S. hospitals.

   Madrid is considering financial penalties on firms that falsely accuse Spain of involvement in such a crime against U.S. infrastructure.

   The Minister also raised the possibility of blocking U.S. access to Spanish ports. Such a move would have immediate and adverse impacts on American freight and shipping logistics in addition to commerce and trade.

Cyber 9/12 Strategy Challenge

Intelligence Report III

INSTRUCTIONS

Please read these instructions carefully. They have changed from previous years.

Your team will take on the role of experienced policy advisers, part of a hypothetical cybersecurity task force, preparing to brief the National Security Council (NSC). This packet contains fictional information on the background and current situation involving a major cyber incident affecting US systems. The attacks notionally take place in Spring 2021. The scenario presents a fictional account of political developments and public reporting surrounding the cyber incident.

The NSC needs information on the full range of response options available regarding this incident. Your team has been tasked with developing an appropriate course of action for recommending to the NSC.

You are to consider as facts the following pages for formulating your response.

You will use the fictional scenario material presented to perform one task:

Oral Policy Brief (Final Round): For the final round of the competition, prepare a ten-minute oral presentation outlining your impact and risk assessment, as well as your suggested course of action. You will present to a panel of judges playing the role of the NSC.

Keep these tips in mind as you are reading and considering your policy response alternatives:

- *Analyze the issues.* The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of potentially conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.

- *Engage the scenario.* Believe that the universe we have created is plausible and that the events that happen in it are realistic. Nevertheless, remember to think critically about the intelligence you have been provided and its provenance.

- *Think multi-dimensionally*. When analyzing the scenario, remember to consider implications for other organizations and domains (e.g. private sector, military, law enforcement, different levels of government, diplomatic) and incorporate these insights along with cybersecurity.

- *Consider who you are, and who you're briefing.* You are experienced cyber policy professionals briefing the National Security Council. As such, you should be ready to answer questions on agency responsibility, provide justifications for your recommendations, and have potential alternatives ready.

- *Be creative.* Cyber policy is an evolving discourse, and there is no single correct course of action to the scenario information provided. There are many ideas to experiment with in responding to the crisis.

- *Don't fight the scenario*. Unless stated otherwise, assume all inter-state relations, policies, and treaties have remained the same as they were in January 2021. Explore the implications of that information, not the plausibility.

Given the unclear nature of the threat, the NSC requests that your team prepare a concise assessment of the ongoing situation and reporting. Your assessment should include:

- How or where the relevant systems could be vulnerable to exploit, and what steps can be made to mitigate these vulnerabilities;
- An assessment of potential risks and impacts to consider if the vulnerabilities are successfully exploited; and
- Responses the NSC can or should consider addressing these vulnerabilities, taking into account the severity and likelihood of the threat.

To provide this assessment and policy recommendations, you will apply your understanding of the technologies involved, cybersecurity, law, foreign policy, international relations, and security theory to
synthesize useful policy measures from limited information. Your recommendation must analyze the possible strengths, weaknesses, opportunities, and threats of your proposed response.

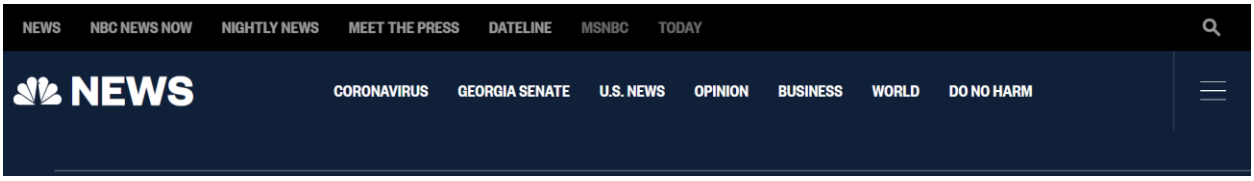
In formulating your response, you will be expected to have considered, at a minimum:

- All stakeholders when determining an action or recommendation, including the role of the government and private sector;
- The long and short-term impacts of your recommendation;
- Which agency will be responsible for the action you have recommended;
- Appropriate recommendations for local vs. federal government;
- Whether you can, or should, attribute the threat; and
- The covert or overt nature of your response.

Additionally, this message is accompanied by several documents that may assist your team in preparing the assessment and policy brief for the NSC:

- **Tab 1** – News Article
- **Tab 2** – Digital Wells Hosting Teams Chat
- **Tab 3** –NSA Intelligence Report on Dark Node Forum Thread

Tab 1 – News Article



Six Killed as a Result of Colorado Ransomware Attacks - Ransomware Continues to Spread

April 22, 2021, 10:20 am EST

By Andi Jameson

In the early afternoon of April 16, 2021, administrators across multiple hospital and health service facilities in Colorado, Utah, and Wyoming detected suspicious activity on their networks. Hospital administrators and medical personnel at affected hospitals were disconnected from patient record databases and a large number of medical devices were rendered inoperable. IT staff discovered that these effects were the result of a coordinated ransomware attack, called Plaguerizer, and that a malicious actor had encrypted data on the hospital networks barring control and access by staff.

Hospital leadership notified the Federal Bureau of Investigation of the attack and also reached out to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency and the Food and Drug Administration for expertise and support on incident response.

Due to the loss of access to patient records and medical device functionality, administrators at affected hospitals made the decision to reroute incoming medical emergencies and transfer severe cases, where possible, to nearby hospitals. This decision is notable not only due to the dangers inherent in the transportation of ill patients, but also because all area hospitals are dealing with an exceptional spike in hospitalizations due to an outbreak of a second strain of the COVID-19 virus. These extreme stresses on the operation of hospitals have severely limited COVID-19 testing, treatment and vaccine distribution.

Six individuals to date have died as a direct consequence of this ransomware attack. These deaths were the result of the closure of surgical departments and, in one case, of increased transfer time to an emergency room. These deaths may mark some of the first incidents of fatalities directly linked to a cyberattack.

_____

The latest in a series of concerning developments, reports from hospital administrators in Nevada and California appear to show that this ransomware has spread west to five additional hospitals. Initial investigation by FBI cyber action team suggests that the vector facilitating the spread of the ransomware in these cases are the control systems of hospitals ultra-cold freezers, manufactured by InfiniChill. As these freezers are crucial for the preservation of Pfizer COVID-19 vaccine doses, response teams are currently investigating whether the actor behind these ransomware attacks might have the capability to manipulate freezer storage conditions and whether this capability was exercised.

With six lives already lost as a result of this attack, hospital staff across Nevada and California as well as state and local officials, are preparing for a severe reduction of hospital functionality and corresponding impact on COVID-19 testing, vaccination and treatment.

The spread of this ransomware endangers thousands, if not millions, more lives and raises a larger question: are our hospitals prepared to operate in the digital world? Medical personnel have embraced new technologies that allow them to diagnose, track, and treat patients with increased accuracy and effectiveness. But are the benefits of new medical technologies worth the potential loss of human life? Ransomware attacks against hospitals are not a new phenomenon, neither are ransomware attacks against hospitals during the COVID-19 pandemic. What has remained consistent in these cases is this sector is ill-prepared for this type of crisis and its potential and dire consequences.

VA emergency physician Dr. Nora Haig suggests that ransomware attacks will continue to be "a recurring challenge as we try to maintain trust in digitized healthcare." An alternative, she offered, is that Centers for Medicare and Medicaid Services and VA Medical Centers revert to an analog-primary system preemptively until the spread of this ransomware is contained.

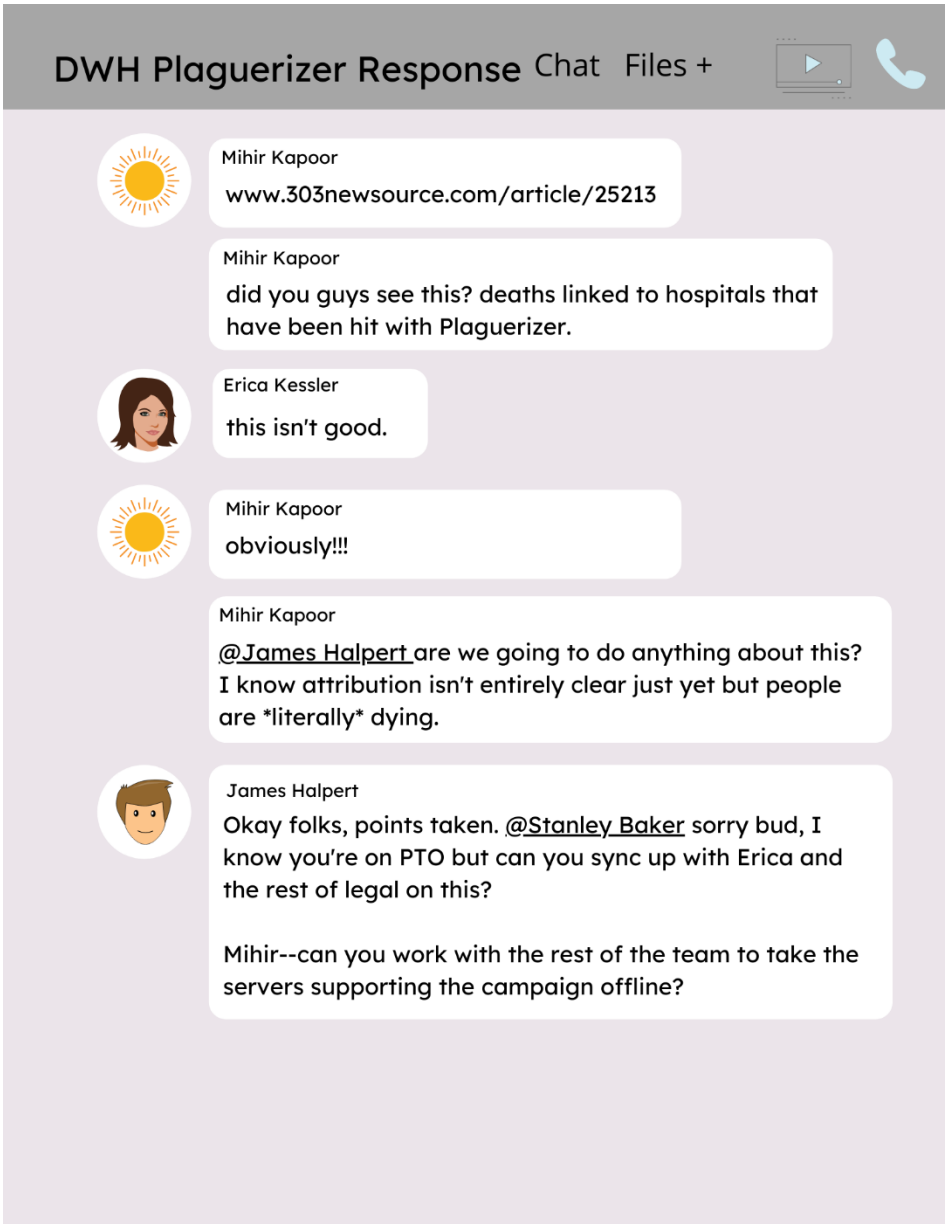
"Doctors cannot perform at peak level," Haig insisted. "When crisis upon crisis is unlooked for and unprepared for continue to batter us down – start using safe systems now, before an emergency requires it."

_____

As deaths continue to climb more than a year after the first cases of COVID-19 were reported in the country, this attack and its consequences are adding fuel to the fire of misinformation and conspiracy theories. On April 19, a second strain of COVID-19, which had jumped the barrier to humans from Mink, was officially confirmed, though rumors of this strain have been circling since March. In an absence of confirmed information, misinformation spread alleging that developed vaccines were no longer effective and that this strain could spread through livestock as well.

The ransomware attack on regional hospitals, as noted above, significantly reduced the ability to distribute vaccines to at-risk groups. Additionally, the potential compromise of ultra-cool freezers has paused distribution of Pfizer vaccines until their viability is reconfirmed. The resulting decrease in vaccinations has led some to mistakenly conclude that hospitals are choosing to slow distribution because COVID-19 vaccines are not now, or never have been, effective. The snowballing misinformation will likely continue after the direct effects of these ransomware attacks have been dealt with and will likely further elongate the plan to create herd immunity through mass inoculation.

Tab 2 – Digital Wells Hosting Teams Chat (Mobile)



Tab 3 – NSA Intelligence Report on Dark Node Forum Thread

Intelligence Packet: NSA Market Monitor Program ID #54814304

Threat Level	**ELEVATED**
Admiralty Code	**C4**
Event Date	**19-20 April 2021**
Source	**DarkNode "Hackers Who Care" Forum**
Threat Actor (TA)	**Unknown, suspected Cyber Praetoriae**
TA's Language	**English**
Targeted Geography	**United States**
Analysts	**Jacqueline Zagorski**

Key Points

1. **Abstract: During routine network monitoring, analysts came across an English language thread on a dark web forum, DarkNode, hosted in the Asia-Pacific. The thread linked to potential future Cyber Praetoriae operations on U.S. hospitals affected by the Plaguerizer ransomware campaign. Might provide insight into this cyber vigilante group's organizational structure, network preferences, and future operations.**

2. **Audience: U.S. law enforcement agencies, U.S. and international intelligence agencies.**

3. **Source and Validation: DarkNode has a mixed record of providing legitimate intelligence. It has been used as a marketplace for malware and credit card information before, and it has hosted forums used to coordinate illegal online activity. However, it is also a popular anonymous message board for privacy minded internet users and has hosted discussions from Cyber Praetoriae in the past, often focused on launching operations on cyber matters that touch public safety.**

4. **Mitigation Summary: We suggest increased monitoring of known Cyber Praetoriae networks and malware marketplaces and preparation for a potential counterattack in response to the Plaguerizer campaign.**

5. **<u>IOCs and Attachments:</u> No Relevant IOCs were found.**

Source Report: Text of DarkNode forum discussion

1. **TA's post on 19-20 April 2021:**

19/04/2021 2351EST

trajan117> have you seen the reports of the hospitals?

goodemperor5> of course i have. it's everywhere.

goodemperor5> such a shame. it shouldn't be like this.

trajan117> it doesn't have to be.

20/04/2021 0008EST

goodemperor5> what do you even mean?

trajan117> what i'm saying is that this is a failure. people are not just dying from the pandemic but now from a ransomware attack.

trajan117> government has failed. companies have failed. people are at a loss for who's the adult in the room. who's looking out for them.

goodemperor5> i know. this is terrible but i'm still torn about what we should do.

20/04/2021 0032EST

trajan117> we do what we do best. if no one's going to stop the ransomware campaign and the killing, we will. we have a moral imperative to act.

goodemperor5> you have a point. let's take this offline.