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 Fall 2022. 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 'policy 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** – Vanity Fair Profile
- **Tab 2** – Confido Slack Chat
- **Tab 3** – CIA Field Record
- **Tab 4** – Confido Email Chain
- **Tab 5** – Washington Post Article
- **Tab 6** – Tweets
- **Tab 7** – Interagency Memo

Tab 1 – Vanity Fair Profile

VANITY FAIR

Aleks Kozlov wants you to ditch your clunker (and with good reason too)

The founder and CEO of Nativus weighs in on the energy transition and where to find the best pelmeni.

BY MABEL EDWARDS
AUGUST 15, 2022

Aleks Kozlov is upset he can't get a hold of what he insists is the best pelmeni available in the United States. The CEO of Nativus and I are standing outside a twentieth century townhouse in the Kalorama neighborhood of Washington, DC that is home to one of just a handful of restaurants in the city serving Russian fare. According to Kozlov, Russia House makes the best pelmeni he's had in the United States. It also helps that its proximity to the Russian Embassy makes him feel a little less homesick when he finds himself in the nation's capital. Washington continues to use sanctions—perhaps its diplomatic tool of choice, but that's another story—on Russian officials and companies, but especially Russia's energy sector. One might think Kozlov would feel wary, nervous even in the nation's capital, but he insists he feels at home here. To Kozlov's dismay, Russia House closed its doors in response to the pandemic in 2020 and has yet to reopen.

Kozlov increasingly finds himself splitting his time between the United States, where Nativus has become a popular electric vehicle for Americans, and Nativus HQ in Moscow's Skolkovo Innovation Center. "This is largely the result of the Nativus team's deft navigation of the global chip shortage," says Kozlov modestly. "The Biden administration's Build Back Better Act's tax incentives on EVs also made a significant difference in our US sales."

Nativus' emphasis on and investments to support in-house software development have paid off. While many automobile companies still struggle to keep up with pent-up demand for new cars, especially fuel efficient and electric options, Nativus was able to circumvent chip shortages and lock in significant business deals. Zippee, the carsharing and car rental company, has purchased

75,000 Nativus vehicles and Kozlov is now trying his hand at making Nativus a software vendor, selling software to hospital systems electrifying their ambulance fleets. These contracts have made Kozlov a very wealthy man.

When asked about the newfound scrutiny on billionaires and corporation, Kozlov muses, "I work hard, pay taxes and am responsible for thousands of jobs around the globe. I'm not sure what it is that I'm doing wrong, if anything."

Advocacy organizations such as Patriotic Billionaires or Citizens for Tax Equity would probably disagree, citing the ballooning of some of the richest billionaires' wealth during the pandemic as income inequities were placed under a spotlight. Organizations like these have doubled down on their advocacy work, calling for the Biden administration and Congress to act on income inequality and the development of a just wealth redistribution mechanism.

Other groups take a harder line, with the Peoples' Militia taking their anti-capitalist and anti-institutional rhetoric to cyberspace with sporadic hack and leak operations. Another, younger, counterpart to the militia, dubbed Cyber Pleb, has threatened direct action against the "digital and physical infrastructures of modern tyranny," organizing a series of complex campaigns mobilizing thousands of people to divest from organizations such as Nativus, Amazon, Microsoft and more.

Kozlov is dismissive of the influence of these groups. "Can these patriotic billionaires or the so-called cyber plebs really claim to have improved the lives of working people, their families or their communities, the way I have?" We stop at a corner as he flips his hands in the air dismissively, sighs "mere matryoshkas," and moves on.

We make our way down Connecticut Avenue just as a Nativus Hermes zips by silently—it seems we will have to make do with Mari Vana today. Kozlov's demeanor is a far cry from headlines in 2020. Kozlov was spotted hosting a yacht party with Aleksey Mordashov near Zadar in May 2020 just as Croatia was extending its nationwide lockdown. Social media users were quick to criticize Kozlov's decisions. Kozlov responded at the time with a tweet brushing off the event and the rising number of infections in Eastern Europe and encouraging his followers to not live in fear since most COVID-19 deaths were result of pre-existing conditions.

"That wasn't the best move," Kozlov admits, looking over his menu at Mari Vana. "I still believe we mustn't live in fear over the pandemic but understand now that we all have a responsibility and a role to play in ending the pandemic—that's why I mandated vaccinations for all Nativus employees, myself included."

According to the World Health Organization, the COVID-19 pandemic's days are numbered as governments have doubled down on vaccination campaigns since the start of the year. Small outbreaks have cropped up periodically, but often contained to remote villages and towns where vaccine rates remain low. But while the pandemic is winding down, the past nearly three years have not been forgotten even as politicians pledge to build back better. The very persistent spotlight economic inequality finds itself under does not seem to be going anywhere.

Continued on Page 32

Tab 2 – Confido Slack Chat

#Fracti2.0.3
14SEP2022

B. Vo 9:05 AM
Hey team--big day (or night) this Friday! I know everyone has been working hard and I wanted to check in with the teams and see how we're getting along before we drop update 2.0.3. @Ms. Reveille I things have been good up until now – is there anything you need, or any support needed?

Ms. Reveille 11:29 AM
Howdy Bo, we haven't run into any problems so far. Most of the work for is done, but right now we're just in the testing phase just to make sure everything is set for Friday!

B. Vo 11:35 AM
Thanks Rev! I know Mike's out this week, but if there's anything you need in the next couple days, just let us know. Happy to help. @Earl Rudder how's logistics for the update? Were we able to send out the reminder update to our clients for Friday evening? Also, how many have responded saying they received the notice of the update?

Earl Rudder 1:30 PM
We sent the initial announcement about the update early last week, and we got a pretty good response rate. We scheduled the reminder email to be sent this Monday and a couple more of our clients responded. So far most of our clients who are receiving the update for Fracti have responded and we're happy with where we're at.

B.Vo 1:33 PM
Okay, I wanted to confirm – are all of the companies who have responded to the notice primed to receive the update?

Earl Rudder 1:34 PM
Yep! We've tested the distribution list and everyone who is scheduled to receive an update will, regardless of whether they confirm receipt or not.

B.Vo 1:35 PM
Great. Is there anything I can help either of y'all with, or any resources personnel that would help before the push on Friday?

Ms. Reveille 1:36 PM
Software dev. is good with the support we have. We have a couple of work items ahead of us before we push out the update, but other than that, there's no outstanding needs for support or additional staff. No one on our teams has seen any problems and we're just finishing up. In short, no support needed for us!

Earl Rudder 1:40 PM
I would agree with Ms. Rev, logistics is working well, finishing up some last-minute tasks, and no support needed for us as far as I know. I will ask the team, and if anything comes up I'll make sure to update ASAP.

B.Vo 1:50 PM
Thanks y'all! I'll check in again before we push the update at 23:59 on Friday just to make sure.

Tab 3 – CIA Field Record

SUSPECT: MRAT aka Marat Pavlychko
AFFILIATION: Speculated affiliation with Mined Mischief, an Eastern European cybercrime group.
LAST SIGHTING: Odessa, Ukraine on January 7, 2022.
OPERATOR NOTES: Identified MINED MISCHIEF members are speculated to communicate using in-game chat features in a popular MMO videogame.

User	Message
	<Mrat has joined the channel by invitation>
Mrat	is everyone here?
Nangs	we are waiting for AlterEgo
Mrat	tell them to hurry up
Nangs	ok
	<AlterEgo has joined the chat>
Mrat	where were you?
AlterEgo	literally working on tomorrow's event
Mrat	Is Fracti all set for tomorrow?
AlterEgo	Well i was working on it when i was interrupted
EndersToi	pretty sure we're set. even if no, not much we can do. they're testing and would notice anything funny at this point
AlterEgo	no one asked you
Mrat	stoy. we're here to do the job. EndersToi, are our friends talking about this?
EndersToi	yes, regular amplification of years of Western sanctions and undermining of Russian energy. also some chatter about the beagle who drove a car into the Voronezh.
AlterEgo	I missed the one about Masha the beagle. this wouldn't have happened if the car had dog mode.
Mrat	Good. Let's see how their economy fares when we're done with them. AlterEgo can you confirm the compromise of the update and who will be affected?
AlterEgo	I will get back to you.
	<AlterEgo has left the chat.>
Mrat	Nangs you're certain we will be able to follow up with ransom post-update?
Nangs	Of course I am.
	<AlterEgo has entered the chat.>
AlterEgo	we're good
Nangs	k
Mrat	Good. Closing lobby and DCing

// Recorded on 9/15/2022 //

Tab 4 – Confido Email Chain

From: Sam Loom <SLoom@confidotech.com>
To: Ben Vo <BVo@confidotech.com>; Keiko Reveille <KReveille@confidotech.com>; Earl Rudder <ERudder@confidotech.com>
Date: Saturday, September 17, 2022 at 12:23 AM
Subject: Fracti Update 2.0.3

Hey all,

Was doomscrolling on twitter and caught wind of some manufacturing plants shuttering operations. Anyone else seeing this?

www.twitter.com/frechdachs82530/status/2190328325359

Sam

From: Keiko Reveille <KReveille@confidotech.com>;
To: Sam Loom <SLoom@confidotech.com>; Ben Vo <BVo@confidotech.com>; Earl Rudder <ERudder@confidotech.com>
Date: Saturday, September 17, 2022 at 12:24 AM
Subject: RE:Fracti Update 2.0.3

Is this legit? Seems iffy to me…

From: Ben Vo <BVo@confidotech.com>
To: Sam Loom <SLoom@confidotech.com>; Keiko Reveille <KReveille@confidotech.com>; Earl Rudder <ERudder@confidotech.com>
Date: Saturday, September 17, 2022 at 12:26 AM
Subject: RE:Fracti Update 2.0.3

Hmmm I think this might real outages for Freya Industries, Chalybe, Voluble, and Winchester Colony Corp.

This isn't good.

From: Keiko Reveille <KReveille@confidotech.com>
To: Sam Loom <SLoom@confidotech.com>; Ben Vo <BVo@confidotech.com>; Earl Rudder <ERudder@confidotech.com>
Date: Saturday, September 17, 2022 at 12:27 AM
Subject: RE:Fracti Update 2.0.3

Anybody else notice that this looks an awful lot like a list of our clients? 😐

From: Earl Rudder <ERudder@confidotech.com>
To: Sam Loom <SLoom@confidotech.com>; Ben Vo <BVo@confidotech.com>; Keiko Reveille <KReveille@confidotech.com>
Date: Saturday, September 17, 2022 at 12:29 AM
Subject: RE:Fracti Update 2.0.3

Bad news bears. I'll get in touch with the security team. Let's hope this isn't us.

- ER

From: Ben Vo <BVo@confidotech.com>;
To: Sam Loom <SLoom@confidotech.com>; Keiko Reveille <KReveille@confidotech.com>; Earl Rudder <ERudder@confidotech.com>
Date: Saturday, September 17, 2022 at 12:30 AM
Subject: RE:Fracti Update 2.0.3

I'll ping my cousin. They work at Winchester Colony's facility in Westerville and might have some clues.

From: Keiko Reveille <KReveille@confidotech.com>;
To: Sam Loom <SLoom@confidotech.com>; Ben Vo <BVo@confidotech.com>; Earl Rudder <ERudder@confidotech.com>
Date: Saturday, September 17, 2022 at 12:32 AM
Subject: RE:Fracti Update 2.0.3

….Earl and Ben, keep me posted? I'm getting a bunch of calls from panicked customers. What exactly happened here and do we need to deploy an expedited patch?

From: Sam Loom <SLoom@confidotech.com>;
To: Ben Vo <BVo@confidotech.com>; Keiko Reveille <KReveille@confidotech.com>; Earl Rudder <ERudder@confidotech.com>
Date: Saturday, September 17, 2022 at 12:33 AM
Subject: RE:Fracti Update 2.0.3

Keiko, there's a process for this and it'll take time in order for us to get it right.

From: Keiko Reveille <KReveille@confidotech.com>;
To: Sam Loom <SLoom@confidotech.com>; Ben Vo <BVo@confidotech.com>; Earl Rudder <ERudder@confidotech.com>
Date: Saturday, September 17, 2022 at 12:35 AM
Subject: RE:Fracti Update 2.0.3

I know that but we have to take *some* action before this gets more attention. It's been a slow news cycle.

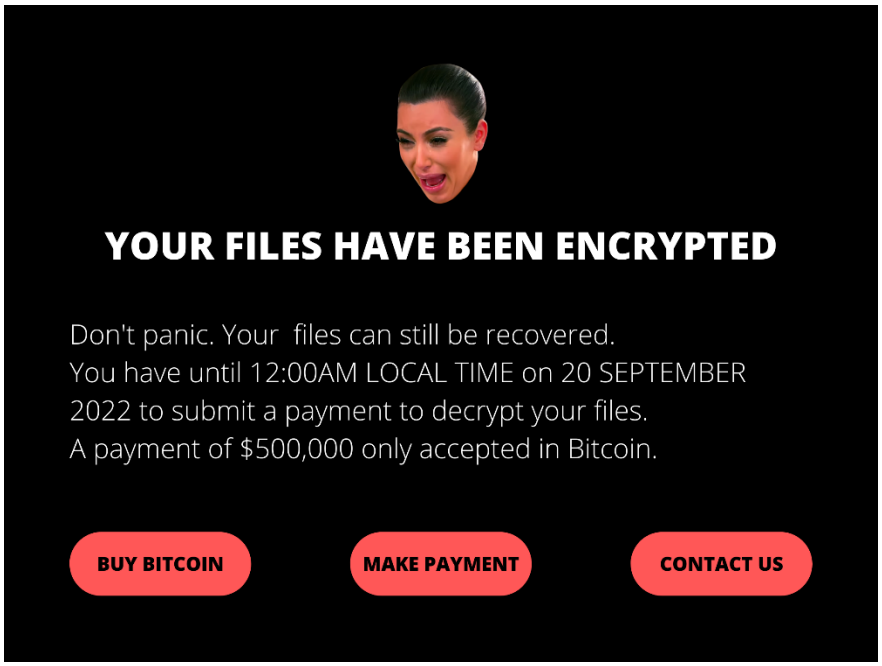
From: Ben Vo <BVo@confidotech.com>;
To: Sam Loom <SLoom@confidotech.com>; Keiko Reveille <KReveille@confidotech.com>; Earl Rudder <ERudder@confidotech.com>
Date: Saturday, September 17, 2022 at 12:38 AM
Subject: RE:Fracti Update 2.0.3

Hey guys—just got off the phone with my cousin at Winchester Colony. They say things are fine at their Westerville facility.

From: Sam Loom <SLoom@confidotech.com>
To: Ben Vo <BVo@confidotech.com>; Keiko Reveille <KReveille@confidotech.com>; Earl Rudder <ERudder@confidotech.com>
Date: Saturday, September 17, 2022 at 12:39 AM
Subject: RE: Fracti Update 2.0.3

Are they sure? I'm seeing some posts from Chalybe and Freya employees that this showed up on their screens shortly after update 2.0.3 was released.

But no ransom notes for Nativus or Voluble which is weird.



From: Earl Rudder <ERudder@confidotech.com>
To: Sam Loom <SLoom@confidotech.com>; Ben Vo <BVo@confidotech.com>; Keiko Reveille <KReveille@confidotech.com>; Cressida Hayat <CHayat@confidotech.com>
Date: Saturday, September 17, 2022 at 12:41 AM
Subject: RE:Fracti Update 2.0.3

Just got off the phone with the security and product teams and they're looking into some fixes that might be able to go into testing.

Looping in @Cressida from product to coordinate. We're going to need to look into what might've gone awry with 2.0.3.

We'll need to get this on legal's radar. Keep an eye out for a separate note to Jen/general counsel.

From: Ben Vo <BVo@confidotech.com>;
To: Sam Loom <SLoom@confidotech.com>; Keiko Reveille <KReveille@confidotech.com>; Earl Rudder <ERudder@confidotech.com>
Date: Saturday, September 17, 2022 at 12:42 AM
Subject: RE:Fracti Update 2.0.3

Hey sorry I spoke too soon. Turns out my cousin isn't even in Westerville. Something about PTO and Daytona Beach.

Please don't hate me.

From: Keiko Reveille <KReveille@confidotech.com>;
To: Sam Loom <SLoom@confidotech.com>; Ben Vo <BVo@confidotech.com>; Earl Rudder <ERudder@confidotech.com>; Cressida Hayat <CHayat@confidotech.com>
Date: Saturday, September 17, 2022 at 12:43 AM
Subject: RE:Fracti Update 2.0.3

Shouldn't we notify our customers that something might be wrong? What about working with public relations to work on an external comms plan?

From: Cressida Hayat <CHayat@confidotech.com>
To: Sam Loom <SLoom@confidotech.com>; Ben Vo <BVo@confidotech.com>; Keiko Reveille <KReveille@confidotech.com>; Earl Rudder <ERudder@confidotech.com>
Date: Saturday, September 17, 2022 at 12:45 AM
Subject: RE:Fracti Update 2.0.3

Hey hey, something's definitely off about update 2.0.3.

In the meantime, pump the brakes on anything related to external comms and customers. We need to get synced internally on what exactly happened and, by the looks of twitter, go to legal.

From: Ben Vo <BVo@confidotech.com>
To: Sam Loom <SLoom@confidotech.com>; Keiko Reveille <KReveille@confidotech.com>; Earl Rudder <ERudder@confidotech.com>; Cressida Hayat <CHayat@confidotech.com>

Date: Saturday, September 17, 2022 at 12:48 AM
Subject: RE:Fracti Update 2.0.3

What about briefing the board? Or notifying feds?

From: Cressida Hayat <CHayat@confidotech.com>
To: Sam Loom <SLoom@confidotech.com>; Ben Vo <BVo@confidotech.com>; Keiko Reveille <KReveille@confidotech.com>; Earl Rudder <ERudder@confidotech.com>
Date: Saturday, September 17, 2022 at 12:50 AM
Subject: RE:Fracti Update 2.0.3

Again, let's slow down and figure out what exactly is going on and we'll move forward from there.

Earl, just got your note with Jen and Sam—thanks for that.

Tab 5 – Interagency Memo

FROM: Director, Cybersecurity and Infrastructure Security Agency (CISA) and Deputy Director, Federal Bureau of Investigation (FBI)
FOR: National Security Advisor
RE: Software Supply Chain Attack on US Manufacturing
DATE: September 18, 2022

PACKET SUMMARY: Coordinated investigations by CISA and FBI report serious exploitation of a routine software update deployed by Confido Technologies' Fracti software. Hundreds of companies across the United States and in allied and partner governments in Europe may be impacted, with the potential to disrupt international supply chains and economic output. The techniques, and processes (TTPs) employed in the attack are consistent with TTPs previously utilized by the Main Intelligence Directorate (GRU) of the Russian Federation. However, NSA has made no medium confidence or better attribution at this time. Potential for grave economic harm from these incidents, and unclear further scope, warrants significant further investigation and appropriate response.

ITEM #1
CONTENTS: Confido Technologies and CISA have conducted a thorough analysis of Fracti Update 2.0.3. The certificates utilized in the software update appear to have been forged by a malicious actor. By forging the certificates, the malicious actor hijacked the Fracti software update, gaining access to Confido Technologies customer systems.

ITEM #2
CONTENTS: Four Fracti customers are known to have been impacted, including Freya Industries, an industrial chemical producer; Winchester Colony Corporation, a food processor; and Chalybe and Voluble, the two largest ball bearing manufacturers in the United States. Victims have reported activity on their networks, and the infection of ransomware, halting operations. The malware encrypts the organization's data and demands a ransom of $500,000 is paid within 72 hours of infection via BitCoin. While four companies are known to have been compromised, CISA anticipates more have been impacted. FBI has advised these organizations to abstain from paying the ransom.

ITEM #3
CONTENTS: Hundreds of companies in the United States and Europe rely on Confido Technologies' Fracti software for the management of Industrial Control Systems (ICS) utilized in manufacturing. Considering the companies impacted, especially ball bearing manufacturers, the economic and national security impacts of this incident have the potential to be severe.

Tab 6 – Washington Post Article

The Washington Post

National Security Foreign Policy Justice Military

Confido Drops the Ball, Manufacturers Scramble

By Kevin Parker
September 19, 2022 at 11:15 ET

Bikes, blenders, photocopiers, and cars. What do they have in common? Well, they all rely on ball bearings to reduce friction.

On Saturday, a software update was disseminated to customers of Confido Technologies' software, Fracti. Fracti is depended on for industrial control systems (ICS) used in manufacturing facilities across the US and Europe. However, shortly after the update was released, four Fracti customers—Freya Industries, Chalybe, Voluble and Winchester Colony Corporation—noticed strange activity on their networks and soon enough were forced to halt operations due to ransomware. Initially, no other organizations from Confido's extensive list of customers reported a compromise but that has quickly changed with Nativus, Mayflower Pride and many more organizations across the United States and Europe reporting they have been experienced a ransomware attack.

After last year's ransomware attack against Kaseya customers, software vendors have been wary of compromised updates leveraged by criminal groups and nation-state actors alike. The Fracti compromise, has much more directly observable effects. ICS systems used in the manufacturing of automobiles and ball bearings—specifically, Chalybe and Voluble, the two largest ball bearing manufacturers in the United States. As companies that rely on Fracti are unable to operate and companies and policymakers are bracing themselves for major supply chain challenges. It is reported that Confido was unaware of the compromised update as the company had conducted iterative testing of Fracti prior to releasing the update on Friday evening. The full impact of the attack is not yet known, but Confido has confirmed they are coordinating with the Cybersecurity and Infrastructure Security Agency.

Amidst the scramble to resume operations, one company stands out as a victim—Nativus. While Nativus so deftly navigated the chip shortage during the COVID-19 pandemic, it has been forced to halt operations in its facilities in the United States, as well as Togliatti. Nativus was established in 2013 by Russian billionaire Aleks Kozlov, who has come under scrutiny as his net worth nearly doubled this year as post-COVID economies are still in recovery.

It remains unknown if the attack was executed by a criminal group or a nation-state actor, such as North Korea, which has a track record of engaging in revenue-generating activities like ransomware attacks. A government source, who agreed to speak under the condition of anonymity, claims the incident was reported to the National Security Council within twenty-four hours, a timeframe established by the White House last year. This disclosure to the NSC reportedly confirmed the attack was possibly connected to the Main Intelligence Directorate (GRU) of the Russian Federation.

This is a developing story and will be updated.

Tab 7 – Twitter Thread

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 Fall 2022. 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 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 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 2022. 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** – City of San Francisco Press Release
- **Tab 2** – Internal FBI Memo
- **Tab 3** – Social Media Post
- **Tab 4** – News Article
- **Tab 5** – Cyber Pleb Website

- **Tab 6** – FBI Email Chain
- **Tab 7** – News Article

Tab 1 – City of San Francisco Press Release

News Releases

The latest news and announcements from Mayor Deborah Nachtnebel

Repairs Underway for Public EV Charging Stations

Posted Date: Monday, September 19, 2022

Mayor Deborah Nachtnebel and San Francisco Municipal Transportation Agency Launch Plan to Repair Hundreds of Public Electric Vehicle Charging Stations

San Francisco, CA — Today, Mayor Deborah Nachtnebel and San Francisco Municipal Transportation Agency (SFMTA) Director Laszlo Madhav released a plan to repair hundreds of public electric vehicle (EV) charging stations across San Francisco.

Over the weekend, SFMTA received reports of malfunctioning and broken EV charging stations across the city. SFMTA and the San Francisco Department of Technology have been working around the clock to respond to this incident and repair charging stations.

The City of San Francisco has committed to achieve 100 percent emission-free ground transportation by 2040. Part of our strategy has been to invest millions of dollars in the installation of public EV charging stations to reduce transportation sector greenhouse gas emissions. In 2022 alone, the City has installed over one hundred stations with a special focus on neighborhoods with high concentrations of low-income households.

Since 2019, the SFMTA has installed hundreds of charging stations, addressing air pollution and reducing emissions in the process. We remain committed to investing in our goal of becoming a net zero emissions city by 2050.

###

Tab 2 – Internal FBI Memo

TO: SAMANTHA DELGADO
DEPUTY DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

FROM: ESTE KARO
ASSISTANT DIRECTOR, CYBER DIVISION
CRIMINAL, CYBER, RESPONSE, AND SERVICES BRANCH
FEDERAL BUREAU OF INVESTIGATION

CC: FILIPPA TOL
SPECIAL AGENT IN CHARGE, COLORADO FIELD OFFICE
FEDERAL BUREAU OF INVESTIGATION

DATE: SEPTEMBER 20, 2022

RE: CYBER PLEB OPERATIONS

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.

The purpose of this memorandum is to advise you of a recent information provided to us from an informant tied to Cyber Pleb, an activist group. Cyber Pleb was established in the United States in the Summer of 2020 in response to high unemployment rates and a contracting economy. Initially, Cyber Pleb focused on social media campaigns to boycott companies led by or connected to billionaires. Recently, Cyber Pleb has successfully expanded its operations to target the infrastructure of corporations and high net worth individuals they believe to be exacerbating income inequality.

The individual, Kasia Turner, was apprehended by City of Denver Police after getting lodged in an automobile window while attempting to steal shrimp cocktail platters located in the car. While in custody, Turner notified Denver Police of her connection to Cyber Pleb and had information on recent operations.

In the ensuing interviews, officers leveraged knowledge of Turner's activities relating to Cyber Pleb. During the course of the interviews, Turner confirmed that Cyber Pleb had successfully launched a cyber campaign targeting Nativus, a Russian electric vehicle company founded by Aleks Kozlov, a billionaire frequently criticized by Cyber Pleb. The campaign successfully rendered Nativus electric vehicles (EV) and EV chargers inoperable.

Turner informed Denver Police that Cyber Pleb has identified a critical vulnerability in software used in Nativus vehicles. When exploited, Cyber Pleb is able to upload malware to the vehicles, impeding their ability to take charge when connected to a charging station.

An Agent immediately investigated the validity of these claims and found that they match Turner's statement, and furthermore, the malware also infects the connected charging station's communications stack. As a result, both public and private charging stations that connect with Nativus vehicles can no longer provide power to connected EVs.

We believe this incident is connected to recent reports of malfunctioning and broken EV charging stations across the United States. The full report, including the Denver Police files on Turner, including her full statement, was sent to the FBI Cyber Division and Filippa Tol, the SAIC in the Colorado Field Office.

The Cyber Division has launched an investigation into the claims made by Turner and will focus investigative efforts on identifying senior members of Cyber Pleb connected to this incident. As this incident directly impacts US transportation infrastructure, we are also in close coordination with contacts at the Cybersecurity and Infrastructure Security Agency. I will keep you informed as this investigation continues.

Tab 3 – Social Media Post

r/electricvehicles · Posted by u/mitsubishimacchiato 3 hours ago

177

I should've bought a diesel

Image

180 Comments Share Save Hide Report 89% Upvoted

Log in or sign up to leave a comment Log In Sign Up

scrmteddy 3 hours ago

as luck would have it, i bought an EV just last week. i'm worried to take it anywhere not knowing if i'll be able to charge it.

coupstorybro 3 hours ago

we have hundreds of charging stations in DC and only a handful seem to be functioning. i should've taken metro today…

wonderdog2010 3 hours ago

Anyone else reminded of their first generation iPod touch whose charging port Would…just…break?

plusbellepizza 2 hours ago

Okay so here's the deal--DO NOT CONNECT YOUR NATIVUS TO A CHARGING STATION. My coworker hooked up their Nativus and it's now a forty thousand dollar brick *plus* they seem to have broken the last functioning charging station at work.

303mountaineer 1 hour ago

^ what they said. not even kidding, it seems like Nativus cars are breaking all the charging stations. told yall to buy Tesla ¯_(ツ)_/¯

Tab 4 – News Article

THE WALL STREET JOURNAL.

ECONOMY | U.S. ECONOMY

Global Supply Chain Pressure Expected to Peak in Coming Weeks

By Melissa Fleming
Sep. 22, 2022 | 9:30 am ET

Around the world, consumers are finding more and more store shelves devoid of goods. Online purchases are taking days, if not weeks, longer to be fulfilled.

The post-pandemic economy was beginning to improve. Global shortages and shipping logistics were slowly improving, especially as pandemic restrictions eased across China. But as luck would have it, manufacturing around the globe, especially in the United States and Europe, would be severely curtailed.

A hijacked update of the software Fracti, developed by Confido Technologies, has brought the operations of some of the largest ball bearing manufacturers around the world to a sudden halt. The effects of the shortage of ball bearings are now being felt around the globe but especially in Western Europe and North America. Since the incident, companies have struggled to fail gracefully as manufacturers work around the clock to resume operations.

Several consumer good companies, including Vitamix, Accor and Miele have tried to circumvent shortfalls caused by expediting parts, investing in demand forecasting and eliminating single points of failure in manufacturing.

Other firms such as Lasko and Nestle have announced the establishment of shortage taskforces in their respective organizations, an action criticized by investors as hand-waving in the face of a trade catastrophe.

These efforts have yet to produce any meaningful impact on international trade and experts predict shortages will worsen before they improve. In the wake of what might be the worst software supply chain attack since SolarWinds, the United States, the S&P 500 index finished last week down 1.2% and in Tokyo, the Nikkei 225 was down 1.46%. Meanwhile, France and Germany's economies have been hit hardest by this cyber incident and its economic fallout. Protests have been reported in the industrial cities of Strasbourg and Stuttgart, criticizing consumer good shortages, plummeting stocks and rising prices. Analysts predict an economic crisis in the European Union if action is not taken soon by Berlin and Paris.

German Chancellor Olaf Scholz is expected to meet with French President Emmanuel Macron to discuss a joint economic and diplomatic response to the cyber incident with reaching economic impacts. Whatever comes of this meeting, the United States' perceived slow response to the cyber incident is sure to be on the agenda.

Tab 5 – Cyber Pleb Website

Tab 6 – FBI Email Chain

From: Este A. Karo <eakaro@fbi.gov>
To: Samantha G. Delgado <sgdelgago@fbi.gov>
Cc: Dinesh B. Chugtai <dbchugtai@fbi.gov>; Bertram M. Gilfoyle <bmgilfoyle@fbi.gov>
Date: Friday, September 23, 2022 at 8:33 AM
Subject: Update on Fracti Incident

Dear Deputy Director Delgado,

Thank you for taking time to connect this morning. To recap, our team has obtained the keys necessary to decrypt the systems of organizations impacted by the hijacked Fracti update. Still, we currently do not have plans to share the keys as this is an open investigation, we risk losing access to evidence and this may impact affected organizations if Mined Mischief becomes aware.

At this stage, we believe it's most prudent to notify the Director of this development and obtain their input on how we can elevate this decision to the White House.

In the meantime, we will continue to coordinate with CISA as they provide incident response support to impacted organizations, with a special focus on manufacturing.

We will inform Interpol of our decision to focus on incident response instead of sharing or utilizing the keys at this time.

Best regards,
Este

Este A. Karo
Assistant Director, Cyber Division
Criminal, Cyber, Response, and Services Branch
Federal Bureau of Investigation
eakaro@fbi.gov | ext. 8529

From: Samantha G. Delgado <sgdelgador@fbi.gov>
To: Este A. Karo <eakaro@fbi.gov>
Cc: Dinesh B. Chugtai <dbchugtai@fbi.gov>; Bertram M. Gilfoyle <bmgilfoyle@fbi.gov>
Date: Friday, September 23, 2022 at 8:37 AM
Subject: Update on Fracti Incident

Este,

Thanks for the call this morning. I'll raise this with Director Gallagher shortly.

Samantha

Samantha Delgado
Deputy Director
Federal Bureau of Investigation
sgdelgado@fbi.gov

Tab 7 – News Article

POLITICO
FOREIGN POLICY

Berlin and Paris Threaten to Recall Ambassadors

French President Emmanuel Macron and German Chancellor Olaf Schulz during a meeting in October 2021. | dpa

By **MAISA MCKINNEY**
09/24/2022 | 11:27 AM EDT

The French and German Ambassadors to the United States may be recalled following a meeting between French President Emmanuel Macron and German Chancellor Olaf Schulz. The meeting, held earlier this week in Paris, reportedly focused on the significant economic impacts of an American software company, Confido Technologies,' and its recent hijacked update for its Fracti software.

Fracti is an industrial control systems (ICS) software that is used by many manufacturing companies in the United States and Europe, particularly ball bearing manufacturers. Both European governments have raised serious concerns over the lack of urgency from the US government in assisting or driving a response from Fracti, given the impact on companies around the world.

The French and German embassies in Washington, DC have linked a slow response to the incident by US Government to bottlenecked and halted manufacturing in the US and Europe, impacting global supply chains and precipitating a looming economic crisis. Furthermore, the economic impacts of the incident have had outsized impact in Western Europe, causing social unrest in industrial cities such as Strasbourg, Lille, Stuttgart and Hanover.

A spokesperson for the German Embassy confirmed German law enforcement is no longer cooperating with the Federal Bureau of Investigation on the incident and a decision regarding the Ambassador's recall will be made in the coming week. The French Embassy in Washington did not immediately respond for a comment.

This is a developing story and will be updated.

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 Fall 2022. 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: 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 2022. 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** – Hospital Press Release

Tab 1 – News Article

CNN US World Politics Business Opinion Health Entertainment Style Travel Sports Videos

Destructive winds and rain to hit the Gulf Coast as Hurricane Tobias makes landfall

By William Klein
Updated 11:37a.m. ET, September 25, 2022

Houston, Texas following Hurricane Harvey in 2017, where the city experienced nearly three feet of precipitation in a four-day period.

(CNN) – Hurricane Tobias is expected to make landfall this evening in Corpus Christi. Over six million residents in cities along the coast of Texas have been ordered to evacuate the area by this morning. Texas Governor Greg Abbott issued dire warnings about the hurricane, imploring residents in evacuation zones to not leave their homes at the last moment.

"Once the storm begins, there will be very little to be done. Please stay safe," Abbott said at a press conference in Houston on Friday.

The National Hurricane Center has been monitoring Hurricane Tobias and upgraded the storm to Category 4 on Saturday, anticipating sustained winds of over 130 mph.

In the midst of a mass evacuation, residents who rely on electric vehicles (EV) for transportation have received software updates increasing vehicle ranges to accommodate thousands of customers in evacuation zones—that is, if one is a Tesla, Volvo or Volkswagen owner. Nativus owners are effectively stranded after a bug in Nativus software rendered Nativus EVs inoperable, infecting charging stations across the country. Repairs to public and private chargers remain underway.

"We are committed to our customers during this difficult time. The Nativus team is working around the clock to develop and deploy a patch. At this time, we ask for our customers' understanding and that those in Hurricane Tobias' path remain safe," Aleks Kozlov, Founder and CEO of Nativus said in a statement. Nativus stock recovered modestly from an all-time low on Friday, September 23 when the FBI announced the arrest of two senior Cyber Pleb operatives connected to exploitation of a critical vulnerability in Nativus software.

EV owners in evacuation zones have been encouraged to not wait for charger repairs and rideshare to safety instead. It is estimated that thousands of residents along the Gulf Coast may need to reevaluate their evacuation and secure an alternate mode of transportation.

A 2019 AAA survey, found that unsettling twenty one percent of respondents would choose to not evacuate their home in the event of an evacuation order.

Tab 2 – Hospital Press Release

Mobile County Hospital to Divert Patients in the Wake of Hurricane Tobias

September 27, 2022

(MOBILE, ALABAMA) In the wake of the devastating Hurricane Tobias, Mobile County Hospital will be diverting patients for the foreseeable future.

In February 2022, Mobile County Hospital invested in a fleet of electric-powered ambulances as part of a broader effort to become more environmentally friendly. Our ambulance fleet rely on Nativus software and have been directly impacted by recent cybersecurity incident involving Nativus.

A patient of Mobile County Health passed away this morning when they were unable to be transferred to Springfield Hospital for immediate care.

"Our medical team went to greats lengths to care for this patient. We are deeply saddened by their passing and empathize with their family," Mobile County Hospital CEO Chloe Nguyen said. "During a time like this, we are working with partners institutions to ensure patients get the care they need."

###