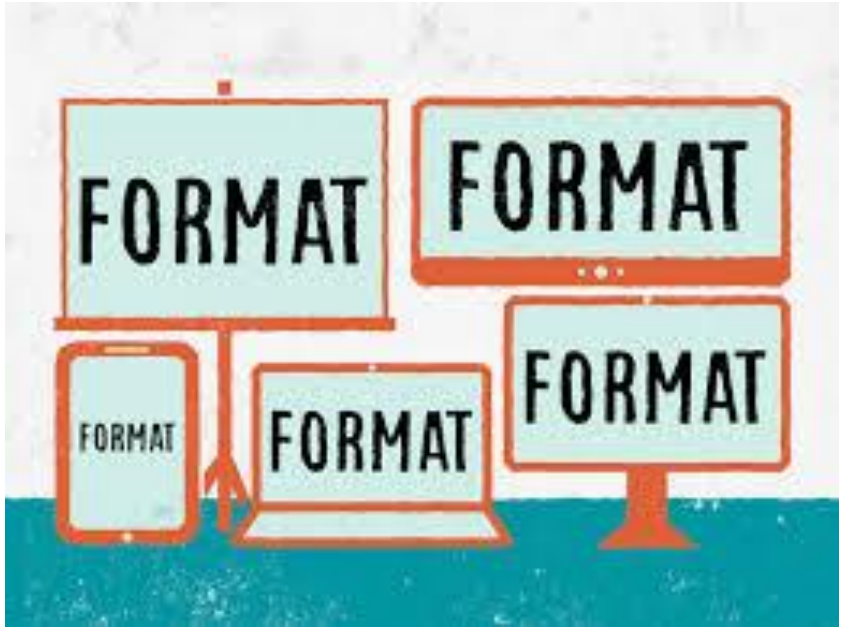
Threats to Water and Wastewater Systems

Association of Environmental Authorities

Briefing Format

- Insider Threat
- Insider Threat Case Studies
- Potential Impact
- Preventative Actions – Insider Threat
- Cyber Threat Case Studies
- China/Russia – Nation State Cyber Threats
- Third Party Attack
- Cyber Security Resources
- Preventative Actions – Cyber Intrusions



Insider Threat

Definition

Insider Threat

The potential for an individual who ***has or had authorized access*** to an organization's assets to use their access, ***either intentionally or unintentionally***, in a way that could negatively affect the organization, its resources, personnel, facilities, information, equipment, networks, or systems.

Case Study – Stoughton, MA

- Robert Bullock
- Former employee of the Water Department in Stoughton
- On the evening of Nov. 29, 2022, Bullock went into one of the Water Department's pumping stations and turned off the pump that introduces chlorine into drinking water

United States Attorney's Office
District of Massachusetts

About USAO-MA | Find Help | Contact Us

Search

About | Divisions | News | Outreach & Initiatives | Resources | Careers | Contact

Justice.gov > U.S. Attorneys > District of Massachusetts > Press Releases > Former Stoughton Water Department Employee Pleads Guilty To Tampering With Drinking Water

PRESS RELEASE

Former Stoughton Water Department Employee Pleads Guilty to Tampering with Drinking Water

Wednesday, March 26, 2025

Share

For Immediate Release

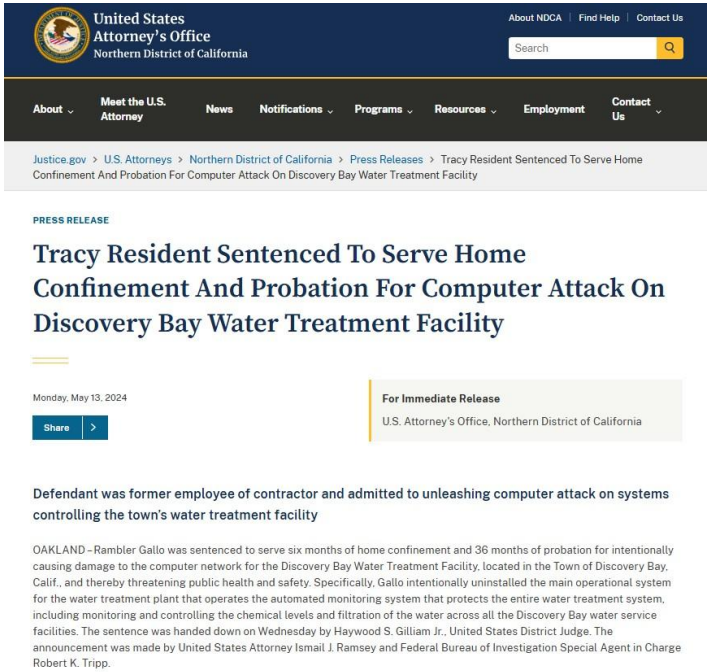
U.S. Attorney's Office, District of Massachusetts

BOSTON – A former Stoughton Water Department employee pleaded guilty today to tampering with the Stoughton drinking water supply.

- As a result, insufficiently disinfected water was introduced into the drinking water system

Case Study – Discovery Bay, CA

- Rambler Gallo:
- Gallo, Company A employee, installed software into his own PC and into Company A's private internal network to gain **remote access to municipal Water Treatment facility computer network**
- Gallo resigned from Company A on November 25, 2020, giving two weeks' notice.
- Approximately five weeks later, Gallo **accessed the facility's computer system remotely and transmitted a command to uninstall certain software** which was designed to perform as the main hub of the facility's computer network
- Specifically, Gallo intentionally uninstalled the main operational system for the water treatment plant that operates the automated monitoring system that protects the entire water treatment system, including monitoring and controlling the chemical levels and filtration of the water across all the Discovery Bay water service facilities.



United States Attorney's Office
Northern District of California

About NDCA | Find Help | Contact Us

Search

About | Meet the U.S. Attorney | News | Notifications | Programs | Resources | Employment | Contact Us

Justice.gov > U.S. Attorneys > Northern District of California > Press Releases > Tracy Resident Sentenced To Serve Home Confinement And Probation For Computer Attack On Discovery Bay Water Treatment Facility

PRESS RELEASE

Tracy Resident Sentenced To Serve Home Confinement And Probation For Computer Attack On Discovery Bay Water Treatment Facility

Monday, May 13, 2024

Share

For Immediate Release

U.S. Attorney's Office, Northern District of California

Defendant was former employee of contractor and admitted to unleashing computer attack on systems controlling the town's water treatment facility

OAKLAND – Rambler Gallo was sentenced to serve six months of home confinement and 36 months of probation for intentionally causing damage to the computer network for the Discovery Bay Water Treatment Facility, located in the Town of Discovery Bay, Calif., and thereby threatening public health and safety. Specifically, Gallo intentionally uninstalled the main operational system for the water treatment plant that operates the automated monitoring system that protects the entire water treatment system, including monitoring and controlling the chemical levels and filtration of the water across all the Discovery Bay water service facilities. The sentence was handed down on Wednesday by Haywood S. Gilliam Jr., United States District Judge. The announcement was made by United States Attorney Ismail J. Ramsey and Federal Bureau of Investigation Special Agent in Charge Robert K. Tripp.

Insider Threat - Preventative Actions

- Employee / Staff Education on Insider Threat
- Ensuring all employees know procedure for reporting suspicious activity, including surveillance, recon
- Regular contact with first responder organizations, including familiarization tour/briefing for local law enforcement/New Jersey State Police/DHS CISA PSA/FBI WMD SA/IA
- Create Anonymous Reporting Avenues for Employees
- Require Ongoing Personnel Suitability
  - Changes in Employee Performance
  - Concerning Behaviors (Indicators)
- Remove or Reassess Accesses of Unsuitable Employees

Physical Threats

WATER ISAC

2025 Q1
INCIDENT REPORT SUMMARY

Physical Security Incidents

PHYSICAL SECURITY SUMMARY

22% Of respondents reported at least one physical security incident during the reporting period. Notable details of anonymized reports are presented below.

- **Theft** continues to be the highest reported threat
- **Sabotage** incidents continue to be reported, leading to operational impacts
- **Threat of Harm**
  - Bomb threats
  - Threats of poison
  - Assault and threats of harm against utility workers

Most notable incidents or activity reported this quarter:

- Two cases of bomb threats directed at water and wastewater utilities. In one case, a former disgruntled utility employee was charged by law enforcement for allegedly making a bomb threat at the utility and for threatening to poison the utility's water supply.
- A sabotage/tampering incident where unknown perpetrator(s) tampered with two fire hydrants, which led to approximately 30,000 liters of untreated sewage leaking into a nearby major river.
- Two incidents involved threats to poison a utility's water supply, including one where a suspect was charged with domestic terrorism.

Cyber Threats

WATER ISAC

2025 Q1
INCIDENT REPORT SUMMARY

Cybersecurity Incidents

CYBERSECURITY SUMMARY

19% Of respondents reported at least one cybersecurity incident during the reporting period. Notable details of anonymized reports are presented below.

Top Types of Cyber Incidents Reported

- **26%** involved **Industrial Control Systems**
- **55%** involved a social engineering component, often leading to system compromise
- This quarter's reported incidents saw a significant rise in distributed denial-of-service (DDoS) attacks

Hacktivisim Continues to be a Prevalent Threat

- Russian Affiliated Group, Z-Pentest Alliance appeared again this quarter
- Several lone-wolf hacktivist attacks
- False claims and extortion attempts caused disruptions

Most notable cyber incidents or activity for the reporting period:

- The Russian-affiliated hacktivist group Z-Pentest Alliance posted an 11-second video to Telegram to demonstrate alleged compromise of an industrial control system interface.
- An employee from a third-party engineering firm that had a contractual relationship with a medium-sized wastewater utility, reported to WaterISAC partners that it suspected the utility's wastewater controls system was compromised.
- Multiple threat actors operating under various aliases posted to the dark web claiming to have compromised OT systems at different water utilities, sometimes advertising compromised credentials.
- A large drinking water utility was impacted by the Cityworks exploitation that occurred in early February. WaterISAC sent an **advisory** to members on February 3rd regarding incidents in the water and wastewater sector resulting from vulnerabilities in Cityworks software.
- A very large, combined utility identified a typosquatting attack where four lookalike domains closely resembled its official domain.

Cyber Intrusions

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ALERT

Threat Actors Continue to Exploit OT/ICS through Unsophisticated Means

Release Date: September 25, 2024

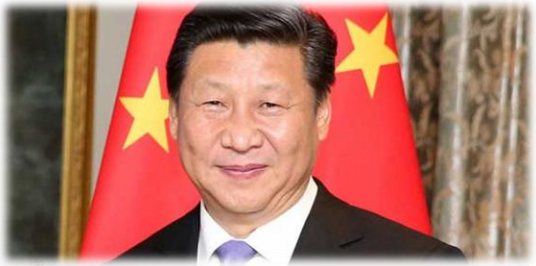
CISA continues to respond to active exploitation of internet-accessible operational technology (OT) and industrial control systems (ICS) devices, including those in the Water and Wastewater Systems (WWS) Sector. Exposed and vulnerable OT/ICS systems may allow cyber threat actors to use default credentials, conduct brute force attacks, or use other unsophisticated methods to access these devices and cause harm.

Russia - China

Seeking a Multi-Polar World, Limited US Economic/Political Power

Cyber and Information Operations to Boost Limited Military Capability

Russian troops in Georgia



China

Russian Troops in Crimea

Russian aid arrives in Dayr az Zawr

Xi – Strategic Objectives

- **First** – Regime stability and maintaining CCP's grip on power
- **Second** - make China whole again by **regaining territories lost in earlier eras of internal upheaval and foreign aggression**: Hong Kong and **Taiwan.**
- **Third** - create a regional sphere of influence in which China is supreme because outside actors, especially the United States, are pushed to the margins
- **Fourth** - Achieving global power and, eventually, global primacy. State media and party officials….**an increasingly powerful China cannot comfortably reside in a rules-based system led by the United States**. **Xi has talked of creating a global "community of common destiny" that would involve "all under heaven being one family"—and presumably obeying the fatherly guidance of the CCP**

Source: What Does China Want?, Foreign Policy, Hal Brands - Aug 13, 2022

CHINA

Cyber

- **The PRC remains the most active and persistent cyber threat to US government, private-sector, and critical infrastructure networks**

- The PRC's campaign to **preposition access on critical infrastructure for attacks during crisis or conflict, tracked publicly as Volt Typhoon**, and its more recently identified **compromise of US telecommunications infrastructure, also referred to as Salt Typhoon**, demonstrates the growing breadth and depth of the PRC's capabilities to compromise U.S. infrastructure

- If Beijing believed that a major conflict with Washington was imminent, **it could consider aggressive cyber operations against U.S. critical infrastructure and military assets.** Such strikes would be designed to deter US military action by impeding US decision-making, inducing societal panic, and interfering with the deployment of US forces.

PRC –Taiwan Tensions

- (U) According to an April 2023 Politico article, the PRC is expected to launch cyber attacks against CONUS critical infrastructure systems as part of a Taiwan invasion, with the chair of the House Select Committee on China, Representative Mike Gallagher (R, Wis.) claiming, "**If Xi Jinping moves on Taiwan, we should assume he'll launch cyberattacks against the United States as part of the operation…on our electrical grid, water systems and communications infrastructure — especially near key military installations.**"

- (U) A 2020 DoD report on the "Military and Security Developments Involving the People's Republic of China," also stated the PRC prefers leveraging **cyberattacks that physically disrupt critical infrastructure targets such as power systems to at the initial stages of conflict in order to delay military intervention.**

(U) Cyberattack on Civilian Critical Infrastructures in a Taiwan Scenario –CSIS, AUG 2023 -Targets

- (U) The most probable targets fall into three categories:

- (U) The first would be electrical power facilities.

- (U) The second would be the pipelines and railroads in the continental United States that connect to these locations.

- (U) The third would be the logistics and communications networks, including those that support supply chains for manufacturing precision-guided munitions and military aircraft.

- **(U) Primary targets would include telecommunications systems in cities and regions where naval and air bases are located, such as California, Hawaii, and Washington State**. All are logical targets for cyber disruption, and many are located on the United States' Pacific Rim. Disruptions at such targets would provide near-term, tangible military advantage and would be conducted in parallel with Chinese cyber actions against military targets, such as information systems and advanced weapons.

PRC Cyber Attacks on Critical Infrastructure

The PLA-related cyber intrusions known as "Volt Typhoon"…JAN-FEB 2024 press reported **attacks targeted critical US infrastructure, including water utility systems in Hawaii, major ports on the West Coast, and an oil and gas pipeline**, according to experts…intrusions part of a broader effort to develop ways to sow chaos or snarl logistics in the event of a US-China conflict in the Pacific

Volt Typhoon: Chinese hackers allegedly sow chaos in US critical infrastructure

Plus: VR goggle for mice, space-based gas stations, tires with instant snow chain deployment

15 hours ago

the blueprint
BY INTERESTING ENGINEERING

As geopolitical tensions with China worsen, **hackers with suspected ties to the nation's military** have penetrated computer networks regulating vital US dams, pipelines, and power stations.

Rather than immediately vandalize these **critical infrastructure controls**, officials say the infiltrations provide Chinese forces with a ready-made way to **remotely trigger disruption** of civilian infrastructure if armed warfare ever breaks out in the Pacific theater.

There is now an urgent effort to locate and remove all pre-positioned cyberweapons from the critical systems that modern societies depend upon. Jump to today's **Must Read** to understand the ongoing battle to eradicate the means to spark mayhem in cities across the US.

(U) VOLT TYPHOON

- (U) The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI) assess that **People's Republic of China (PRC) state-sponsored cyber actors are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States.**

(U) VOLT TYPHOON

- (U) The U.S. authoring agencies have confirmed that Volt Typhoon has compromised the IT environments of multiple critical infrastructure organizations—**primarily in Communications, Energy, Transportation Systems, and Water and Wastewater Systems Sectors—in the continental and non-continental United States and its territories, including Guam.**
- (U) Volt Typhoon's choice of targets and pattern of behavior is not consistent with traditional cyber espionage or intelligence gathering operations, and the **U.S. authoring agencies assess with high confidence that Volt Typhoon actors are pre-positioning themselves on IT networks to enable lateral movement to OT assets to disrupt functions.** The U.S. authoring agencies are concerned about the potential for these actors to use their **network access for disruptive effects in the event of potential geopolitical tensions and/or military conflicts.**

(U) VOLT TYPHOON -LOTL

- (U) As the authoring agencies have previously highlighted, the **use of living off the land (LOTL) techniques is a hallmark of Volt Typhoon** actors' malicious cyber activity when targeting critical infrastructure. The group also relies on valid accounts and leverage strong operational security, which combined, allows for long-term undiscovered persistence.

- LOTL: Unlike traditional malware attacks, which leverage signature files, LOTL attacks are fileless, meaning **they do not require an attack to install any code or scripts on the target system…attacker uses tools already present**, like PowerShell, Windows Management Instrumentation(WMI) or the password-saving tool Mimikatz to carry out the attack.

- (U) In fact, the U.S. authoring agencies have recently observed indications of Volt Typhoon actors maintaining access and footholds within some victim IT environments for at least five years. Volt Typhoon actors conduct extensive pre-exploitation reconnaissance to learn about the target organization and its environment; tailor their tactics, techniques, and procedures (TTPs) to the victim's environment; and dedicate ongoing resources to maintaining persistence and understanding the target environment over time, even after initial compromise.

RUSSIA: STRATEGIC OVERVIEW

- **Russia views its ongoing war in Ukraine as a proxy conflict with the West, and its objective to restore Russian strength and security in its near abroad against perceived US and Western encroachment** has increased the risks of unintended escalation between Russia and NATO.
- Regardless of how and when the war in Ukraine ends, Russia's current geopolitical, economic, military, and domestic political trends underscore its resilience and enduring potential threat to US power, presence, and global interests.
- **Despite having paid enormous military and economic costs in its war with Ukraine, Russia has proven adaptable and resilient, in part because of the expanded backing of China, Iran, and North Korea.** Russia is also increasing military cooperation with Iran and North Korea, which will continue to help its war effort and enhance U.S. adversary cooperation and collective capacity.
- Finally, Moscow is increasingly willing to play spoiler in Western-centric forums such as the UN and use non-Western organizations like Brazil, Russia, India, China, and South Africa (BRICS) group to press policies such as de-dollarization.

RUSSIA

Cyber

- Russia's advanced cyber capabilities, its repeated success compromising sensitive targets for intelligence collection, and **its past attempts to pre-position access on US critical infrastructure make it a persistent counterintelligence and cyber attack threat**
- Moscow's unique strength is the practical experience it has gained integrating cyber attacks and operations with wartime military action, almost certainly amplifying its potential to focus combined impact on US targets in time of conflict
- Russia has demonstrated real-world disruptive capabilities during the past decade, including gaining experience in attack execution by relentlessly targeting Ukraine's networks with disruptive and destructive malware

RUSSIA

TLP:CLEAR

Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity

MS-ISAC Multi-State Information Sharing & Analysis Center

Communications Security Establishment / Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications / Centre canadien pour la cybersécurité

National Cyber Security Centre, a part of GCHQ

Overview

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), Environmental Protection Agency (EPA), Department of Energy (DOE), United States Department of Agriculture (USDA), Food and Drug Administration (FDA), Multi-State Information Sharing and Analysis Center (MS-ISAC), Canadian Centre for Cyber Security (CCCS), and United Kingdom's National Cyber Security Centre (NCSC-UK)—hereafter referred to as "the authoring organizations"—are disseminating this fact sheet to highlight and safeguard against the continued malicious cyber activity conducted by pro-Russia hacktivists against operational technology (OT) devices in North America and Europe.

Actions to take today:

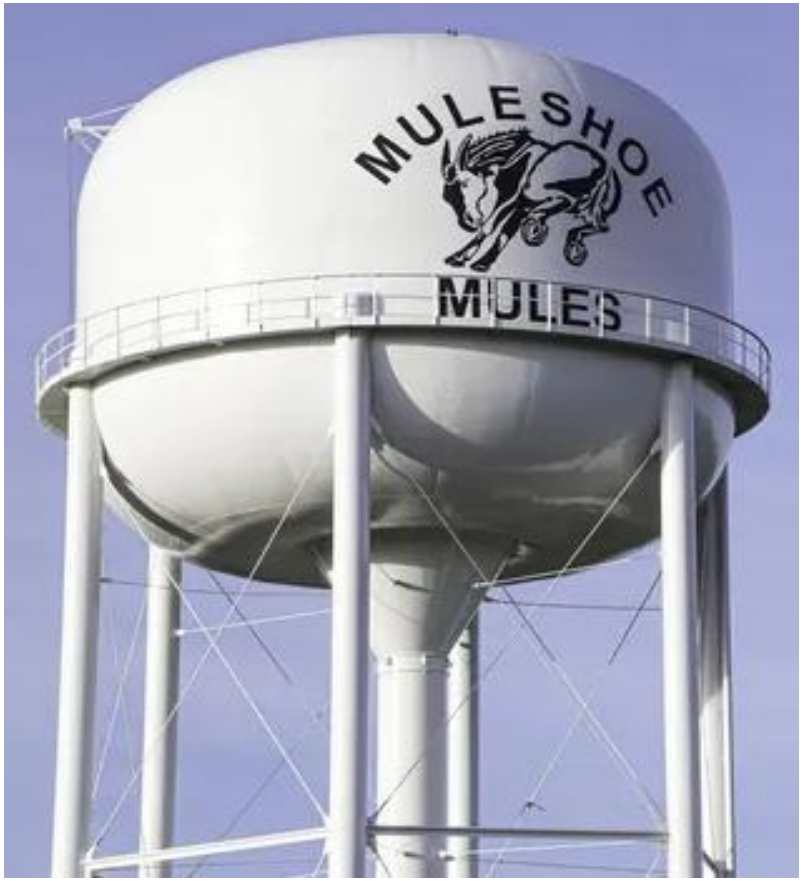
- Immediately change all default passwords of OT devices (including PLCs and HMIs), and use strong, unique passwords.
- Limit exposure of OT systems to the internet.
- Implement multifactor authentication for all access to the OT network.

The authoring organizations are aware of pro-Russia hacktivists targeting and compromising small-scale OT systems in North American and European Water and Wastewater Systems (WWS), Dams, Energy, and Food and Agriculture Sectors. These hacktivists seek to compromise modular, internet-exposed industrial control systems (ICS) through their software components, such as human machine interfaces (HMIs), by exploiting virtual network computing (VNC) remote access software and default passwords.

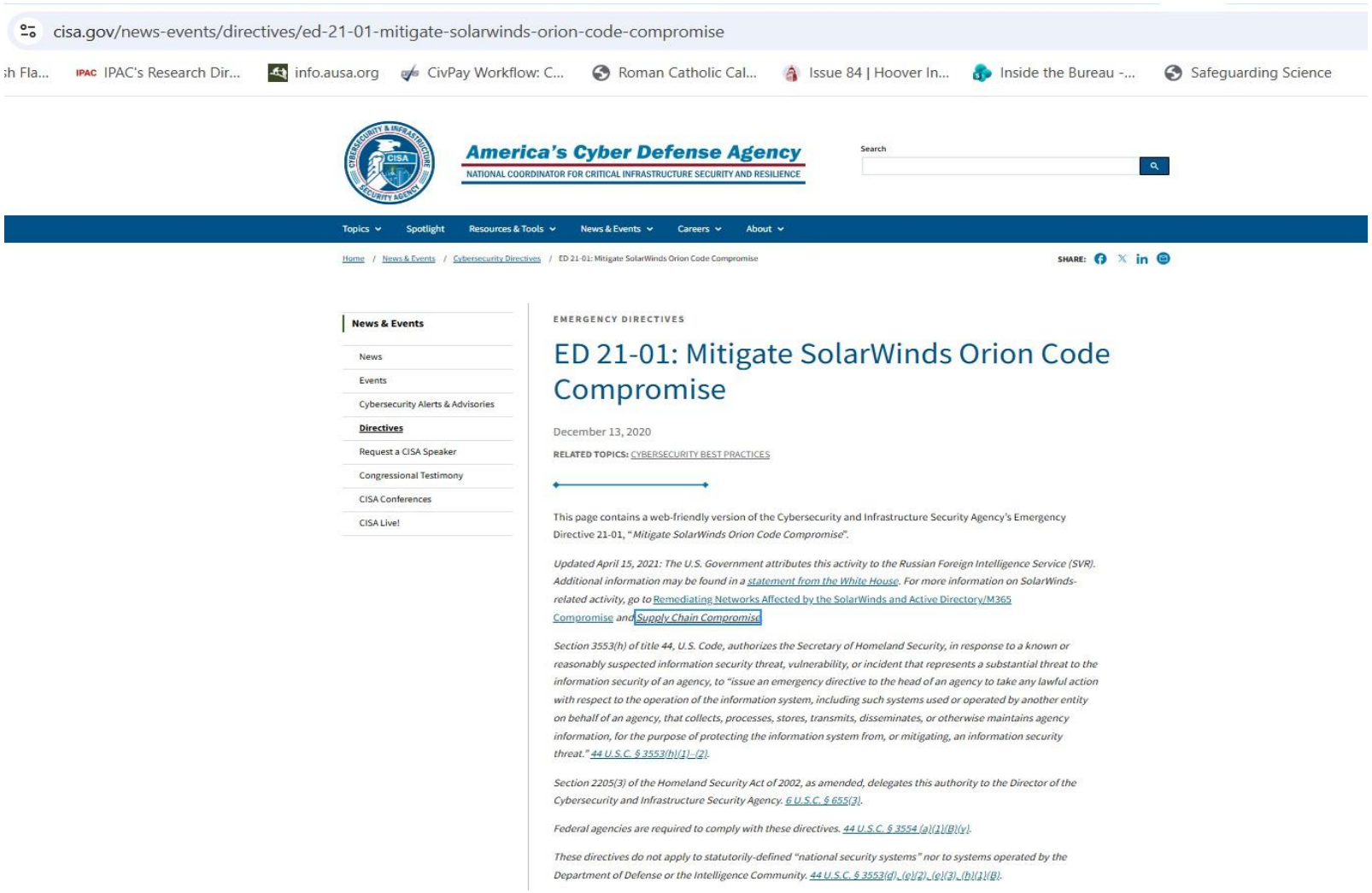
Pro-Russia Hacktivist Activity

- In early 2024, the authoring organizations observed pro-Russia hacktivists targeting vulnerable industrial control systems in North America and Europe. CISA and the FBI have responded to several U.S.-based WWS victims who experienced limited physical disruptions from an unauthorized user remotely manipulating Human Machine Interfaces (HMIs)
- Specifically, pro-Russia hacktivists manipulated HMIs, causing water pumps and blower equipment to exceed their normal operating parameters. In each case, the hacktivists maxed out set points, altered other settings, turned off alarm mechanisms, and changed administrative passwords to lock out the WWS operators
- Some victims experienced minor tank overflow events; however, most victims reverted to manual controls in the immediate aftermath and quickly restored operations.

Case Study – Muleshoe, TX



Supply Chain – Third Party Attack: Solar Winds



cisa.gov/news-events/directives/ed-21-01-mitigate-solarwinds-orion-code-compromise

ish Fla... IPAC IPAC's Research Dir... info.ausa.org CivPay Workflow: C... Roman Catholic Cal... Issue 84 | Hoover In... Inside the Bureau -... Safeguarding Science

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics Spotlight Resources & Tools News & Events Careers About

Home / News & Events / Cybersecurity Directives / ED 21-01: Mitigate SolarWinds Orion Code Compromise

SHARE:

News & Events

- News
- Events
- Cybersecurity Alerts & Advisories
- **Directives**
- Request a CISA Speaker
- Congressional Testimony
- CISA Conferences
- CISA Live!

EMERGENCY DIRECTIVES

ED 21-01: Mitigate SolarWinds Orion Code Compromise

December 13, 2020

RELATED TOPICS: CYBERSECURITY BEST PRACTICES

This page contains a web-friendly version of the Cybersecurity and Infrastructure Security Agency's Emergency Directive 21-01, "*Mitigate SolarWinds Orion Code Compromise*".

Updated April 15, 2021: The U.S. Government attributes this activity to the Russian Foreign Intelligence Service (SVR). Additional information may be found in a statement from the White House. For more information on SolarWinds-related activity, go to Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise *and Supply Chain Compromise.*

Section 3553(h) of title 44, U.S. Code, authorizes the Secretary of Homeland Security, in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, to "issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat." 44 U.S.C. § 3553(h)(1)–(2).

Section 2205(3) of the Homeland Security Act of 2002, as amended, delegates this authority to the Director of the Cybersecurity and Infrastructure Security Agency. 6 U.S.C. § 655(3).

Federal agencies are required to comply with these directives. 44 U.S.C. § 3554 (a)(1)(B)(v).

These directives do not apply to statutorily-defined "national security systems" nor to systems operated by the Department of Defense or the Intelligence Community. 44 U.S.C. § 3553(d), (e)(2), (e)(3), (h)(1)(B).

Supply Chain – Third Party Attack: Solar Winds

What is SolarWinds?

- SolarWinds is a major software company based in Tulsa, Okla., which provides system management tools for network and infrastructure monitoring, and other technical services to hundreds of thousands of organizations around the world

- Among the company's products is an IT performance monitoring system called Orion.

Supply Chain – Third Party Attack: Solar Winds

- Suspected nation-state hackers that have been identified as a group known as **Nobelium by Microsoft -- often simply referred to as the SolarWinds Hackers** -- gained access to the networks, systems and data of thousands of SolarWinds customers. The breadth of the hack is unprecedented and one of the largest, if not the largest, of its kind ever recorded.

- More than 30,000 public and private organizations -- including local, state and federal agencies -- use the Orion network management system to manage their IT resources -- **SolarWinds inadvertently delivered the backdoor malware as an update to the Orion software in March 2020 to these organizations and compromised their data, networks and systems**

- SolarWinds customers weren't the only ones affected. Because the hack exposed the inner workings of Orion users, the hackers could potentially gain access to the data and networks of their customers and partners as well -- enabling affected victims to grow exponentially from there.

Supply Chain – Third Party Attack: Solar Winds

- The hackers used a method known as a supply chain attack to insert malicious code into the Orion system. A supply chain attack works by targeting a third party with access to an organization's systems rather than trying to hack the networks directly.

- SolarWinds Orion Platform creates a backdoor through which hackers can access and impersonate users and accounts of victim organizations. The malware could also access system files and blend in with legitimate SolarWinds activity without detection, even by antivirus software.

- SolarWinds was a perfect target for this kind of supply chain attack. Because their Orion software is used by many multinational companies and government agencies, all the hackers had to do was install the malicious code into a new batch of software distributed by SolarWinds as an update or patch.

Cyber Intrusions - Preventative Actions

- Air-Gap Network
- Keep Software Updated
- Set Unique Passwords / Routinely Change Passwords
- Restrict Port Access / Restrict Software Downloads / Restrict Software Removal
- Regular contact with cyber first responder organizations, including network familiarization with NJCICC, DHS CISA Cyber PSA, FBI WMD/Cyber

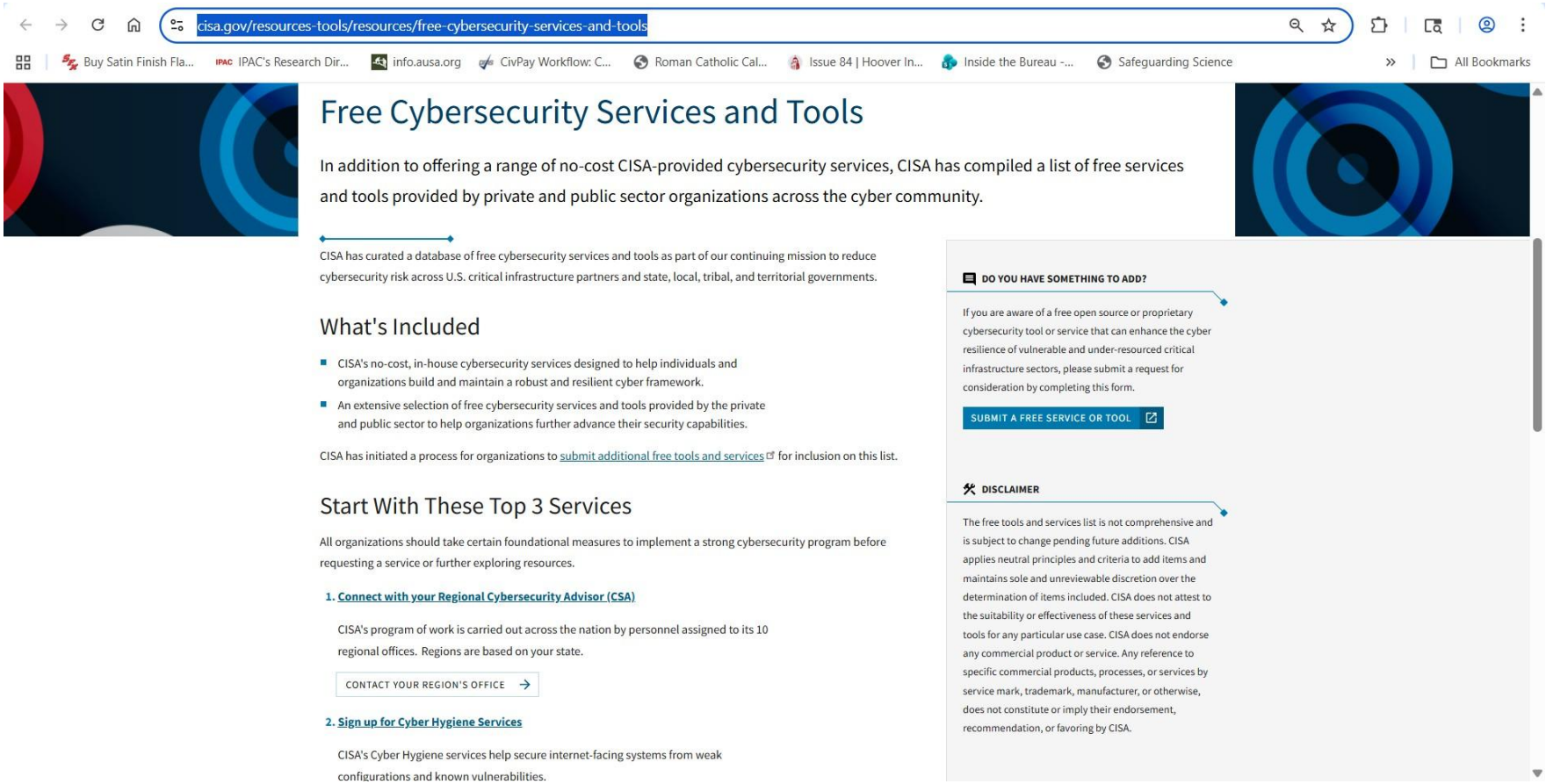
CISA Cyber Threats and Advisories

- https://www.cisa.gov/topics/cyber-threats-and-advisories

CISA Resources

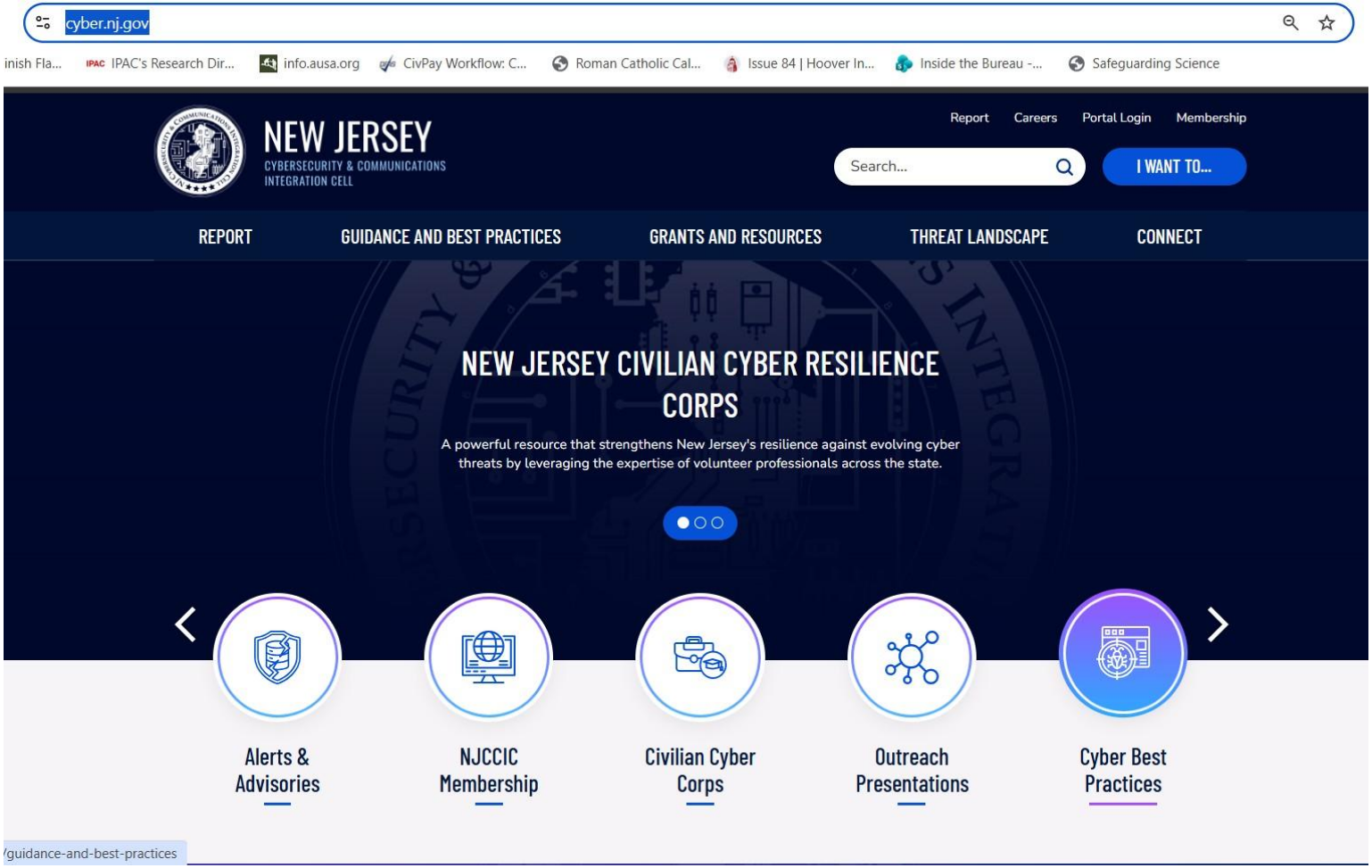
- https://www.cisa.gov/resources-tools/all-resources-tools

CISA Services/Tools



- https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools

New Jersey Cybersecurity and Communications Integration Cell



- https://www.cyber.nj.gov/

Recap

- Insider Threat
- Insider Threat Case Studies
- Potential Impact
- Preventative Actions – Insider Threat
- Cyber Threat Case Studies
- Preventative Actions – Cyber Intrusions