CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Threats and Trends CISA is monitoring in Hawaii

JUNE 26 2024

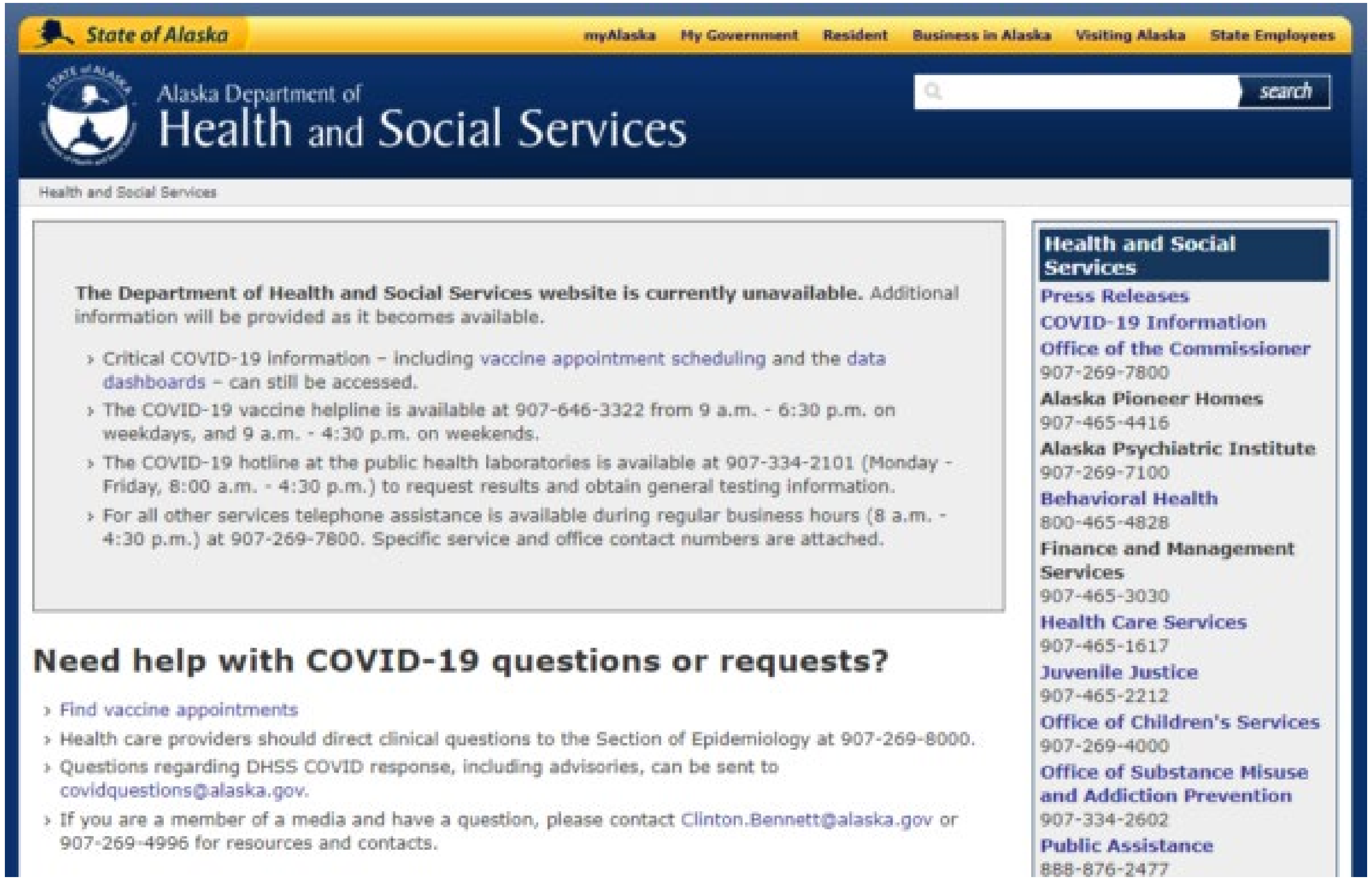
Mark Breunig

What Most People Think Of:

Or:

Mark Breunig
July 1, 2024

HSS & Courts:



Alaska Department of
Health and Social Services

The Department of Health and Social Services website is currently unavailable. Additional information will be provided as it becomes available.

- Critical COVID-19 information – including vaccine appointment scheduling and the data dashboards – can still be accessed.
- The COVID-19 vaccine helpline is available at 907-646-3322 from 9 a.m. - 6:30 p.m. on weekdays, and 9 a.m. - 4:30 p.m. on weekends.
- The COVID-19 hotline at the public health laboratories is available at 907-334-2101 (Monday - Friday, 8:00 a.m. - 4:30 p.m.) to request results and obtain general testing information.
- For all other services telephone assistance is available during regular business hours (8 a.m. - 4:30 p.m.) at 907-269-7800. Specific service and office contact numbers are attached.

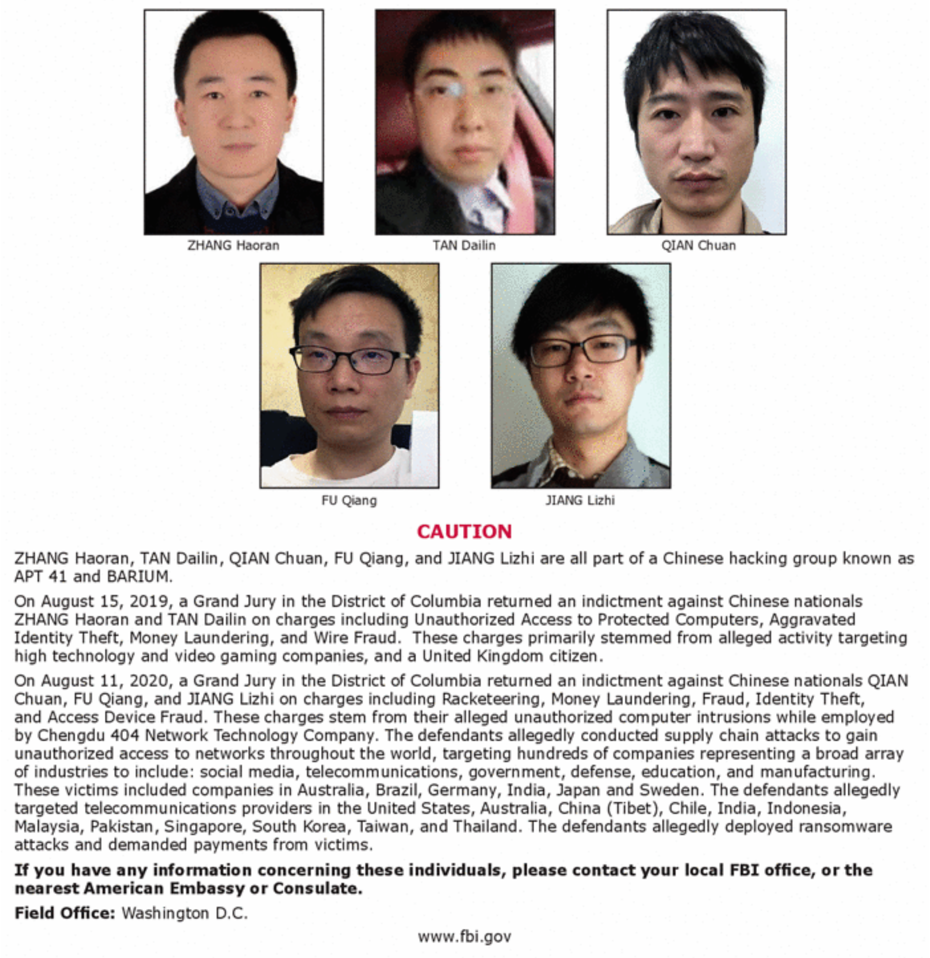
Need help with COVID-19 questions or requests?

- Find vaccine appointments
- Health care providers should direct clinical questions to the Section of Epidemiology at 907-269-8000.
- Questions regarding DHSS COVID response, including advisories, can be sent to covidquestions@alaska.gov.
- If you are a member of a media and have a question, please contact Clinton.Bennett@alaska.gov or 907-269-4996 for resources and contacts.

Health and Social Services

Press Releases
COVID-19 Information
Office of the Commissioner
907-269-7800
Alaska Pioneer Homes
907-465-4416
Alaska Psychiatric Institute
907-269-7100
Behavioral Health
800-465-4828
Finance and Management Services
907-465-3030
Health Care Services
907-465-1617
Juvenile Justice
907-465-2212
Office of Children's Services
907-269-4000
Office of Substance Misuse and Addiction Prevention
907-334-2602
Public Assistance
888-876-2477

Meet Your Attackers:



ZHANG Haoran

TAN Dailin

QIAN Chuan

FU Qiang

JIANG Lizhi

CAUTION

ZHANG Haoran, TAN Dailin, QIAN Chuan, FU Qiang, and JIANG Lizhi are all part of a Chinese hacking group known as APT 41 and BARIUM.

On August 15, 2019, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals ZHANG Haoran and TAN Dailin on charges including Unauthorized Access to Protected Computers, Aggravated Identity Theft, Money Laundering, and Wire Fraud. These charges primarily stemmed from alleged activity targeting high technology and video gaming companies, and a United Kingdom citizen.

On August 11, 2020, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals QIAN Chuan, FU Qiang, and JIANG Lizhi on charges including Racketeering, Money Laundering, Fraud, Identity Theft, and Access Device Fraud. These charges stem from their alleged unauthorized computer intrusions while employed by Chengdu 404 Network Technology Company. The defendants allegedly conducted supply chain attacks to gain unauthorized access to networks throughout the world, targeting hundreds of companies representing a broad array of industries to include: social media, telecommunications, government, defense, education, and manufacturing. These victims included companies in Australia, Brazil, Germany, India, Japan and Sweden. The defendants allegedly targeted telecommunications providers in the United States, Australia, China (Tibet), Chile, India, Indonesia, Malaysia, Pakistan, Singapore, South Korea, Taiwan, and Thailand. The defendants allegedly deployed ransomware attacks and demanded payments from victims.

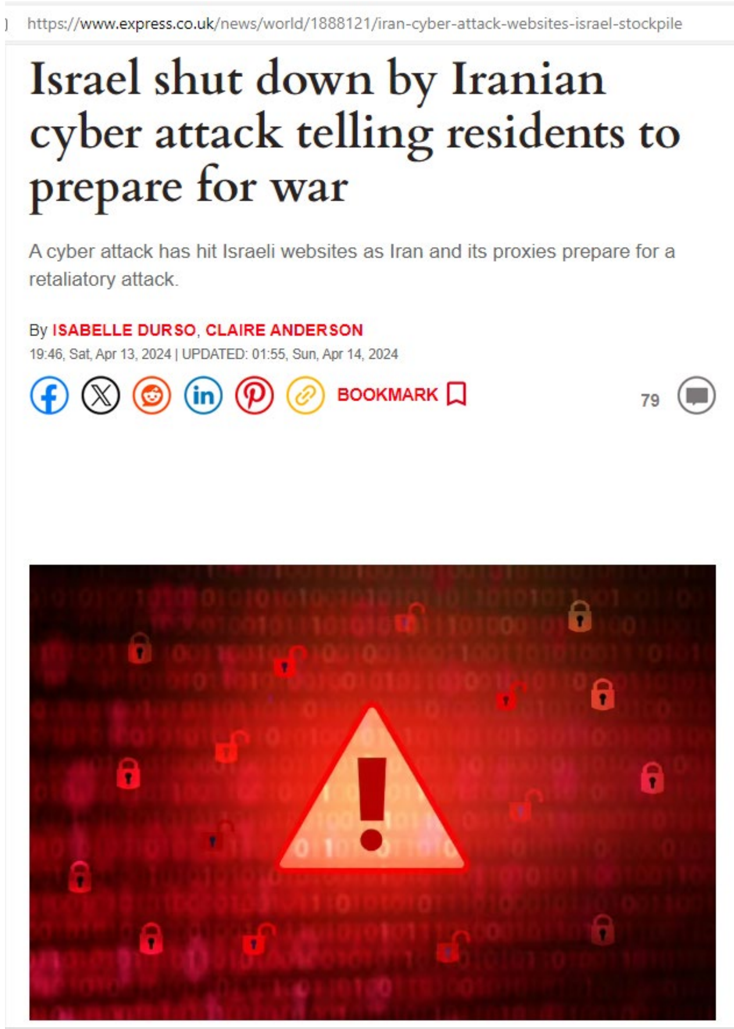
If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Field Office: Washington D.C.

www.fbi.gov

Attacks (Actual and Potential)

Attacks (Recent)



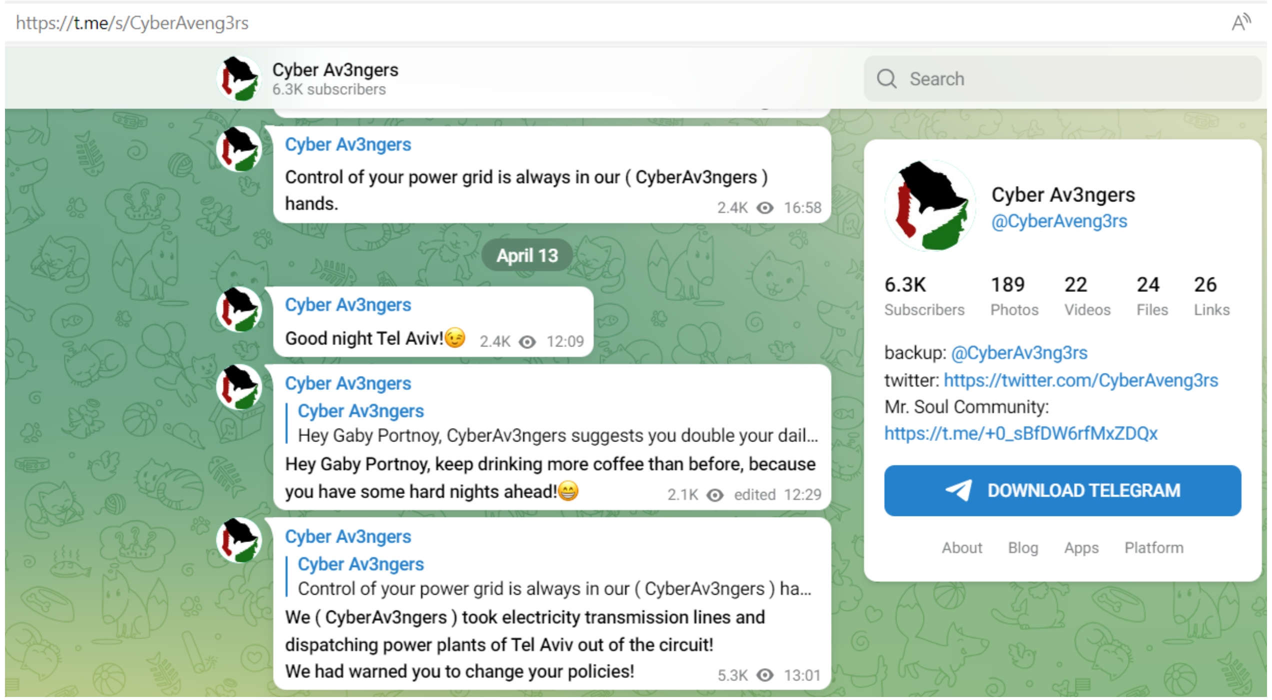
https://www.express.co.uk/news/world/1888121/iran-cyber-attack-websites-israel-stockpile

Israel shut down by Iranian cyber attack telling residents to prepare for war

A cyber attack has hit Israeli websites as Iran and its proxies prepare for a retaliatory attack.

By ISABELLE DURSO, CLAIRE ANDERSON

19:46, Sat, Apr 13, 2024 | UPDATED: 01:55, Sun, Apr 14, 2024



https://t.me/s/CyberAveng3rs

Cyber Av3ngers
6.3K subscribers

Cyber Av3ngers
Control of your power grid is always in our (CyberAv3ngers) hands.
2.4K 16:58

April 13

Cyber Av3ngers
Good night Tel Aviv!😉 2.4K 12:09

Cyber Av3ngers
Cyber Av3ngers
Hey Gaby Portnoy, CyberAv3ngers suggests you double your dail...
Hey Gaby Portnoy, keep drinking more coffee than before, because you have some hard nights ahead!😁
2.1K edited 12:29

Cyber Av3ngers
Cyber Av3ngers
Control of your power grid is always in our (CyberAv3ngers) ha...
We (CyberAv3ngers) took electricity transmission lines and dispatching power plants of Tel Aviv out of the circuit!
We had warned you to change your policies!
5.3K 13:01

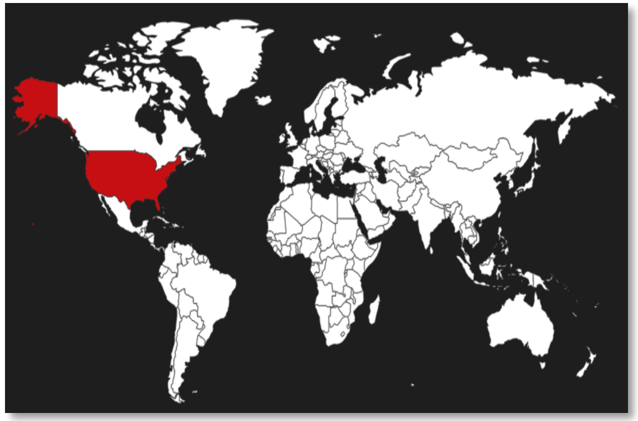
Cyber Av3ngers
@CyberAveng3rs

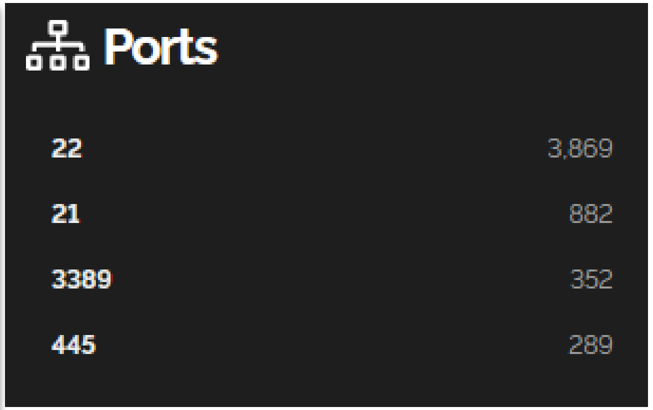
6.3K	189	22	24	26
Subscribers	Photos	Videos	Files	Links

backup: @CyberAv3ng3rs
twitter: https://twitter.com/CyberAveng3rs
Mr. Soul Community:
https://t.me/+0_sBfDW6rfMxZDQx

General Cyber Threats – Attack Surface

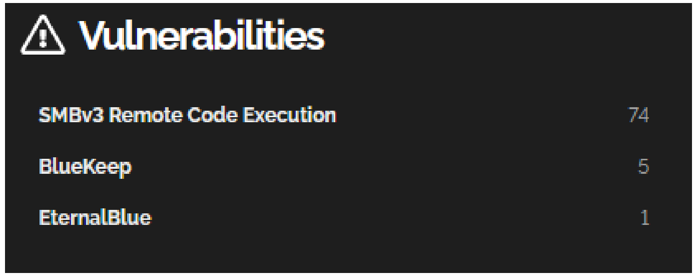
- **Default Open Ports to Internet:**
  - **22-SSH, 21-FTP, 445-SMB, 3389-RDP**
- **Open ports and misconfigured services are exposed to the internet.**
  - This is one of the most common vulnerability findings. Cyber actors use scanning tools to detect open ports and often use them as an initial attack vector. RDP, Server Message Block (SMB), Telnet, and NetBIOS are high-risk services.
- **Remote services, such as a virtual private network (VPN), lack sufficient controls to prevent unauthorized access.**
  - During recent years, malicious threat actors have been observed targeting remote services. Network defenders can reduce the risk of remote service compromise by adding access control mechanisms, such as enforcing MFA, implementing a boundary firewall in front of a VPN, and leveraging intrusion detection system/intrusion prevention system sensors to detect anomalous network activity.
  - Weak Security Controls and Practices Routinely Exploited for Initial Access | CISA





Ports

22	3,869
21	882
3389	352
445	289

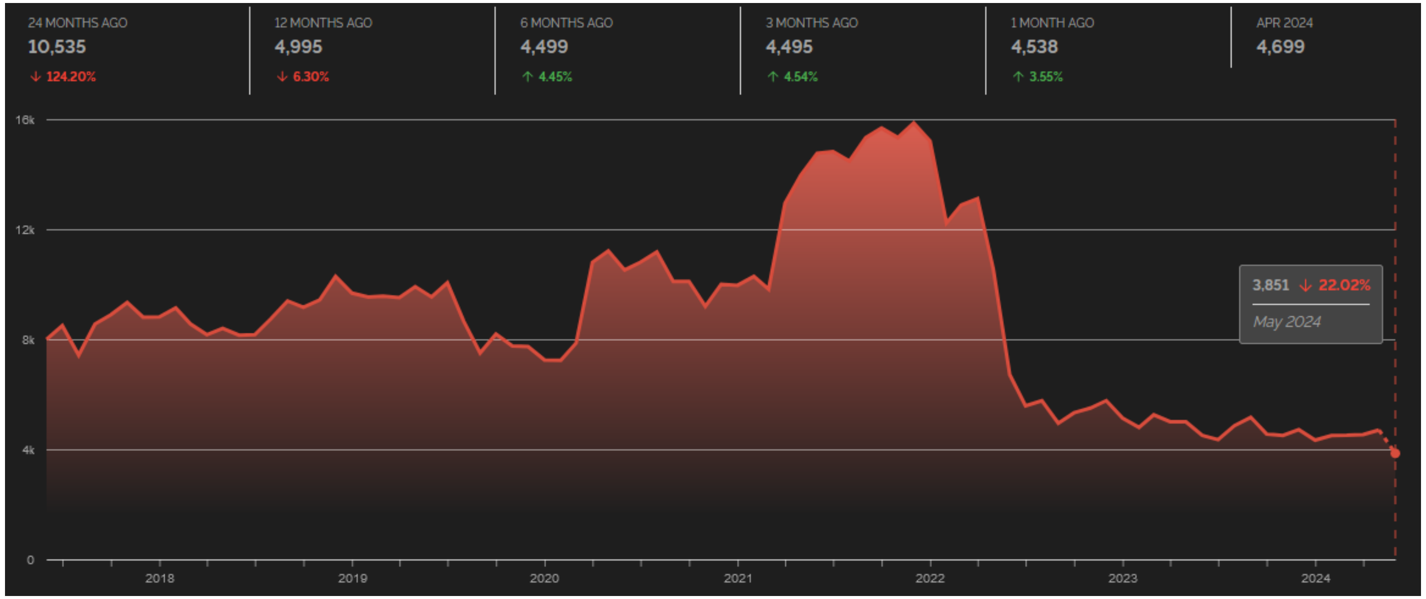


Vulnerabilities

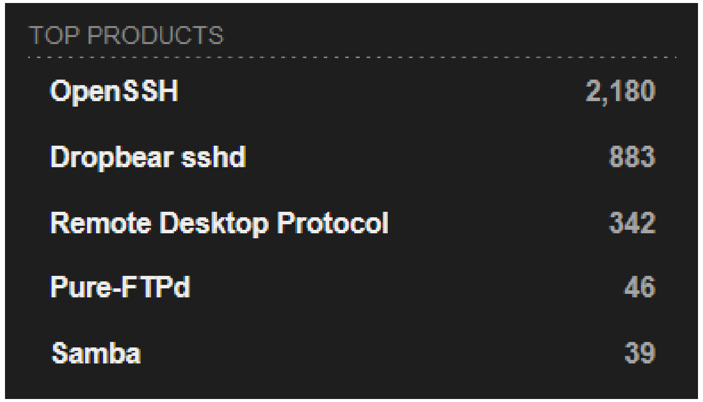
SMBv3 Remote Code Execution	74
BlueKeep	5
EternalBlue	1

Open-Source Intel (OSINT) - Shodan

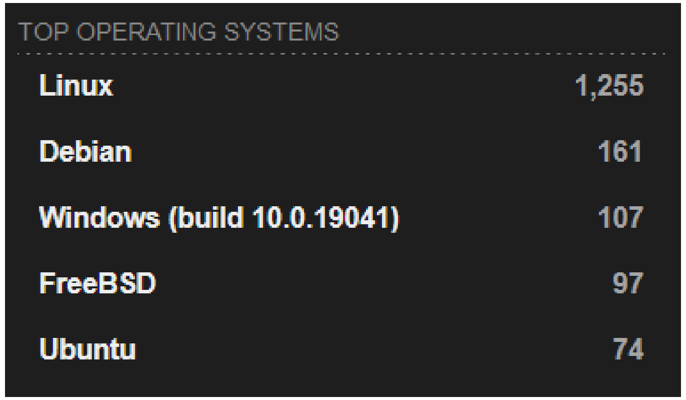
- Trends dropped 22.02% since April 2024
- Telecommunications/broadband services show most vulnerabilities
- RCE top vulnerability
- Shodan Search Engine



24 MONTHS AGO	12 MONTHS AGO	6 MONTHS AGO	3 MONTHS AGO	1 MONTH AGO	APR 2024
10,535	4,995	4,499	4,495	4,538	4,699
↓ 124.20%	↓ 6.30%	↑ 4.45%	↑ 4.54%	↑ 3.55%	



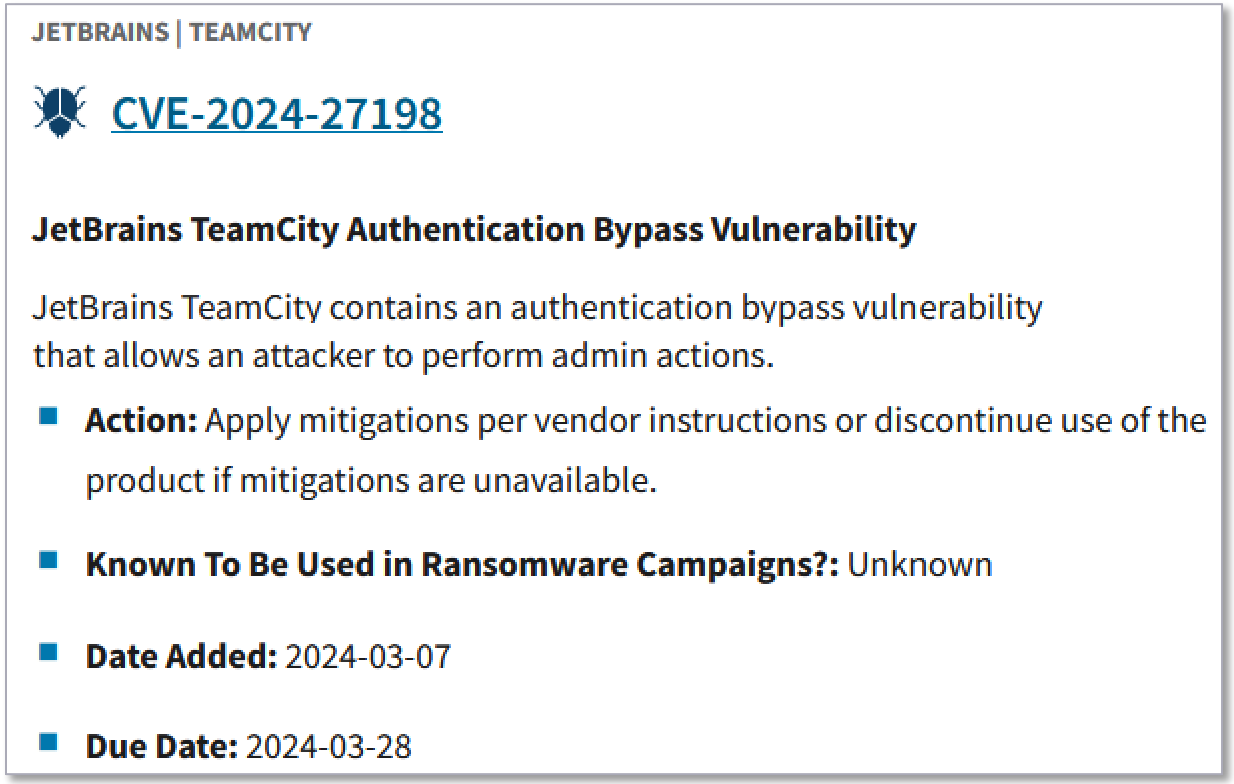
TOP PRODUCTS	
OpenSSH	2,180
Dropbear sshd	883
Remote Desktop Protocol	342
Pure-FTPd	46
Samba	39



TOP OPERATING SYSTEMS	
Linux	1,255
Debian	161
Windows (build 10.0.19041)	107
FreeBSD	97
Ubuntu	74

New KEV Entries

- The most pressing recent KEV is CVE-2024-27198 for JetBrains TeamCity, a CI/CD application for managing software build pipelines.
  - Please patch! The BOD 22-01 deadline for this TeamCity issue is March 28, 2024, but don't wait that long. This bug is very attractive for nation-state actors.
- Other current KEVs are concerned with Android, Microsoft, and MacOS. You're probably patching those automatically anyway.



JETBRAINS | TEAMCITY

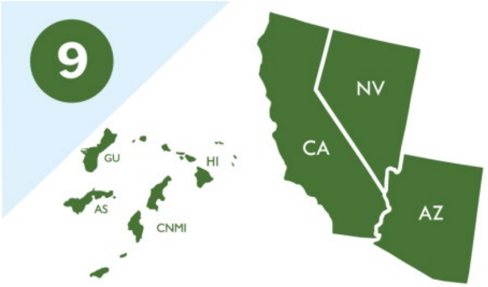
CVE-2024-27198

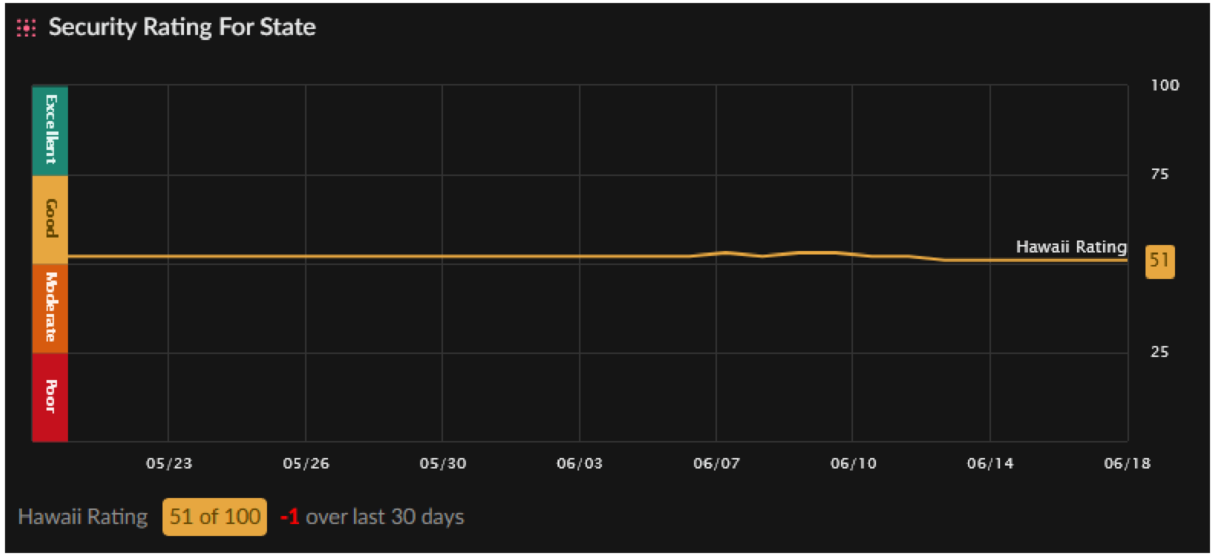
JetBrains TeamCity Authentication Bypass Vulnerability

JetBrains TeamCity contains an authentication bypass vulnerability that allows an attacker to perform admin actions.

- **Action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
- **Known To Be Used in Ransomware Campaigns?:** Unknown
- **Date Added:** 2024-03-07
- **Due Date:** 2024-03-28

Cyber Hygiene (CyHy) Zones - HI

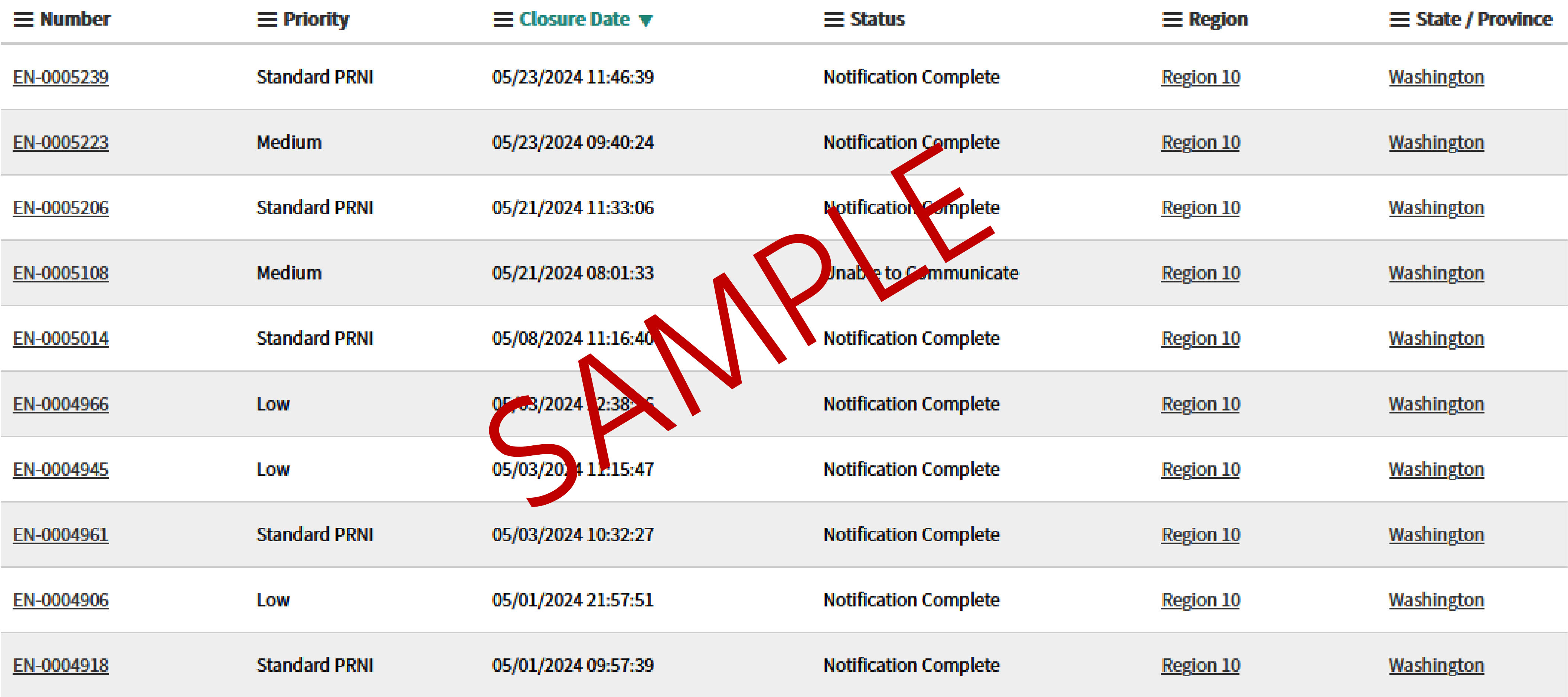




Hawaii Rating 51 of 100 -1 over last 30 days

- Most KEV violations are from SonicWallSonicOS (320)
- Tracked and labeled in the CISA KEV catalog
- CyHy last observed June 17, 2024
- Known Exploited Vulnerabilities Catalog | CISA

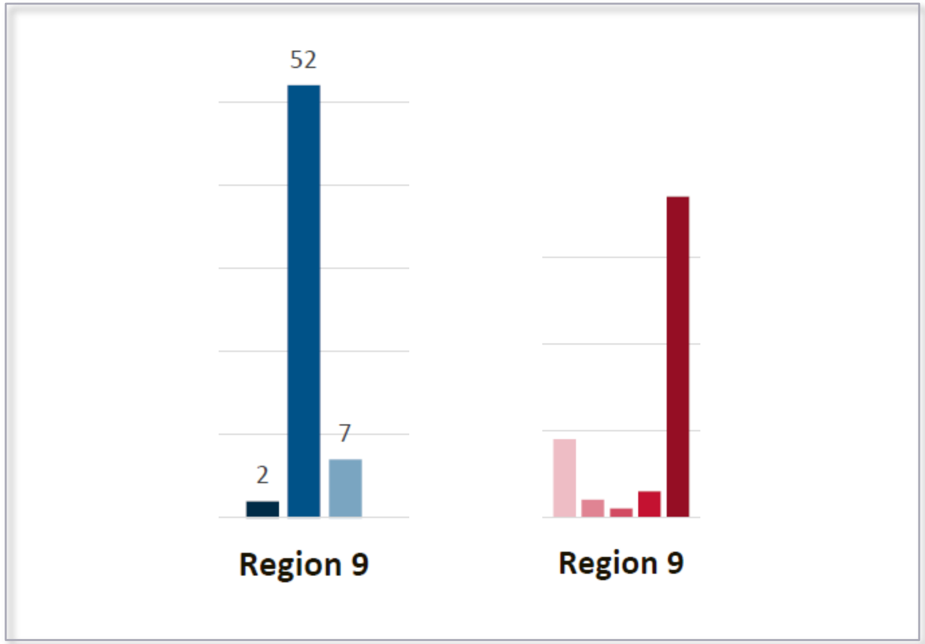
X Entity Notifications – HI – FY24



☰ Number	☰ Priority	☰ Closure Date ▼	☰ Status	☰ Region	☰ State / Province
EN-0005239	Standard PRNI	05/23/2024 11:46:39	Notification Complete	Region 10	Washington
EN-0005223	Medium	05/23/2024 09:40:24	Notification Complete	Region 10	Washington
EN-0005206	Standard PRNI	05/21/2024 11:33:06	Notification Complete	Region 10	Washington
EN-0005108	Medium	05/21/2024 08:01:33	Unable to Communicate	Region 10	Washington
EN-0005014	Standard PRNI	05/08/2024 11:16:40	Notification Complete	Region 10	Washington
EN-0004966	Low	05/03/2024 12:38:[illegible]6	Notification Complete	Region 10	Washington
EN-0004945	Low	05/03/2024 11:15:47	Notification Complete	Region 10	Washington
EN-0004961	Standard PRNI	05/03/2024 10:32:27	Notification Complete	Region 10	Washington
EN-0004906	Low	05/01/2024 21:57:51	Notification Complete	Region 10	Washington
EN-0004918	Standard PRNI	05/01/2024 09:57:39	Notification Complete	Region 10	Washington

R9 EN Data Unavailable – R10 Used as Sample

0 ADMIN SUBPOENA – HI – FY24



During the month, the CISA Regions conducted a total of:

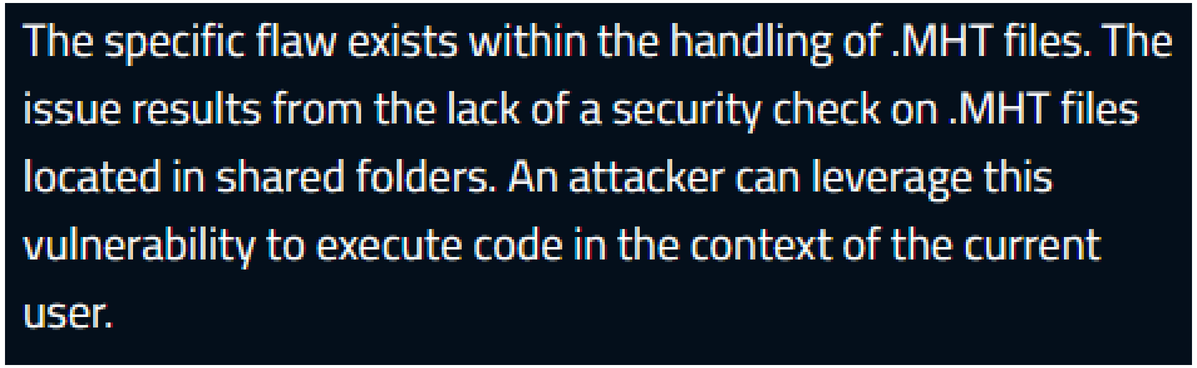
- **420 notifications**, including
  - **25 Admin Subpoenas**
  - **355 Cyber Activity**
  - **40 Vulnerability**

A breakdown of total notifications by region.

🟥 PRNI 🟥 TH - Barracuda Follow-Up 🟥 TH - Citrix 🟥 TH - Ivanti 🟥 TH - Other 🟥 TH - Restricted

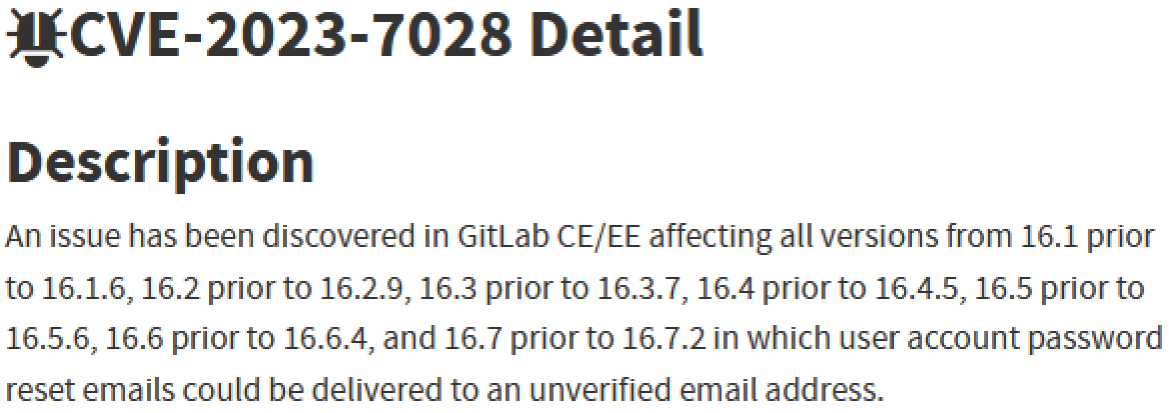
New KEV Entries

- CVE-2024-29988: Microsoft SmartScreen Bypass (due May 21, 2024)
  - MHT files (a web archive format) can bypass Mark of the Web checks
  - See the ZDI writeup for (slightly) more



The specific flaw exists within the handling of .MHT files. The issue results from the lack of a security check on .MHT files located in shared folders. An attacker can leverage this vulnerability to execute code in the context of the current user.

- CVE-2023-7028: GitLab Password Reset (due May 22, 2024)
  - Attacker can supply their own email for a password reset request
  - See the GitLab bug for (a lot) more



CVE-2023-7028 Detail

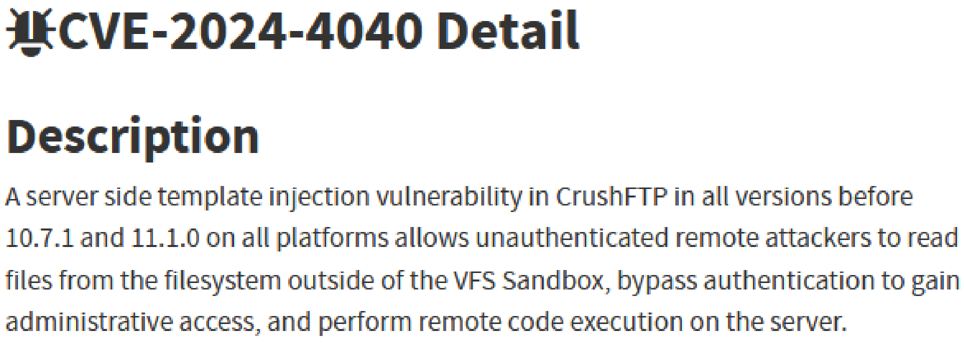
Description

An issue has been discovered in GitLab CE/EE affecting all versions from 16.1 prior to 16.1.6, 16.2 prior to 16.2.9, 16.3 prior to 16.3.7, 16.4 prior to 16.4.5, 16.5 prior to 16.5.6, 16.6 prior to 16.6.4, and 16.7 prior to 16.7.2 in which user account password reset emails could be delivered to an unverified email address.

Other Recent KEVs

- CVE-2024-20353 & CVE-2024-20359: Cisco ASA vulnerabilities.
  - Remote,unauth reboot and a local privsec from Admin to root
  - See the Cisco Talos blog for more.

- CVE-2024-4040:CrushFTP
  - Unauthserver-side template inclusion (SSTI)
  - Much worse than originally thought, see the AttackerKB analysis for more.



CVE-2024-4040 Detail

Description

A server side template injection vulnerability in CrushFTP in all versions before 10.7.1 and 11.1.0 on all platforms allows unauthenticated remote attackers to read files from the filesystem outside of the VFS Sandbox, bypass authentication to gain administrative access, and perform remote code execution on the server.

CISA Resources

CISA Cybersecurity Regional Advisors

Preparedness Activities

- Information/Threat Indicator Sharing
- Cybersecurity Training, Workshops, Tabletops
- Cyber Exercises and “Playbooks” Review
- National Cyber Awareness System (US-CERT)
- Incident Management Workshops
- Ransomware Guide / Playbook
- **Cybersecurity Assessment Services**
  - Cyber Performance Goals (**CPG**)
  - Cyber Resilience Essentials (**CRE**)
  - External Dependency Management (**EDM**)
  - Cyber Infrastructure Surveys (**C-IST**)
  - Cyber Security Evaluation Tool (**CSET**)
  - Ransomware Readiness (**RRA**)

Delivered by CISA HQ Vulnerability Mgt Team

- Phishing Campaign Assessment (**PCA**)
- Cyber Hygiene Scanning (**CyHy**)
- Web Application Scanning (**WAS**)
- Remote Penetration Testing (**RPT**)
- Risk & Vulnerability Assessment (**RVA**)

CISA HQ Response Assistance

- Remote / On-Site Assistance
- Malware Analysis
- Hunt and Incident Response Teams
- Incident Coordination

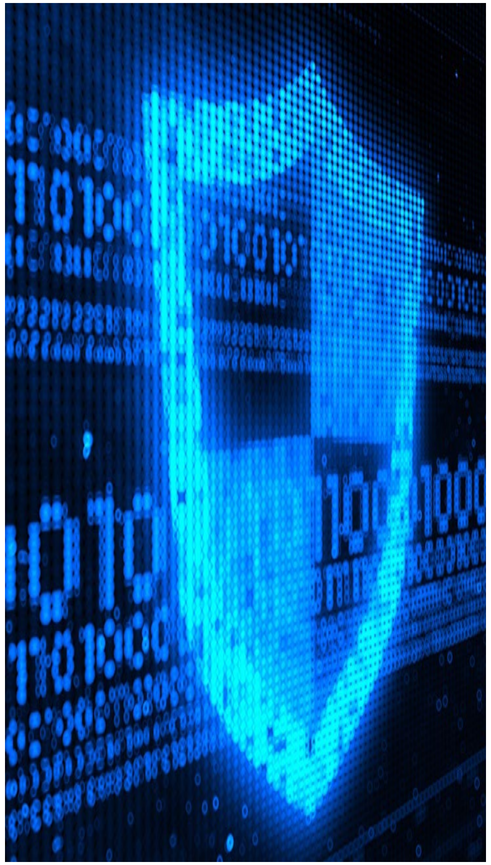
State Based Protective Security Advisors

- Physical Security Assessments
- Incident liaisons between government and private sector for CI protection

Protected Critical Infrastructure Information

Protected Critical Infrastructure Information (PCII)
Program Guards Your Information

- Sensitive critical infrastructure information voluntarily given to CISA is ***protected*** by law from
  - Public release under Freedom of Information Act (FOIA) requests,
  - Public release under State, local, tribal, or territorial disclosure laws,
  - Use in civil litigation and
  - Use in regulatory purposes.
- Find out more: https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program



Questions?

mark.breunig@cisa.dhs.gov
(907) 795-5673

CYBERSECURITY & INFRASTRUCTURE

CISA

SECURITY AGENCY