SECURE OUR WORLD

U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

WSU CYSER Spring 2024

Daniel Brown, CISSP, CISM
Cybersecurity Advisor (CSA)
Inland Northwest
Cybersecurity and Infrastructure Security Agency

Agenda

- What is CISA?
- CISA Initiatives:
  - SBOM
  - Secure By Design
- State of Cyber
- Volt Typhoon/State-Sponsored Actors
- CISA resource examples:
  - Self-Service Tools/templates
  - Advising & Assessments
- CISA Careers/Contact info

What is CISA?

Background: CISA

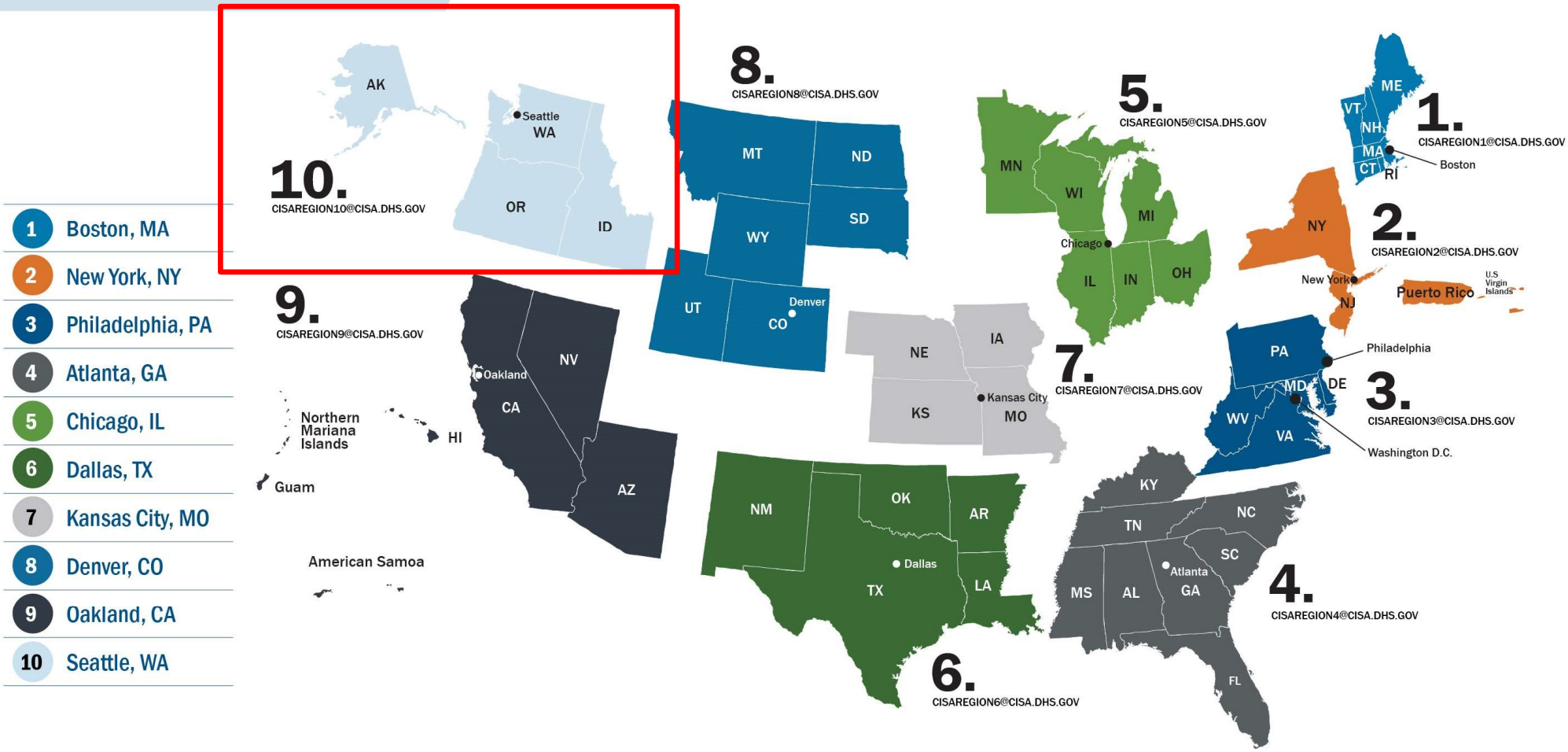
- The Cybersecurity and Infrastructure Security Agency (CISA) was established in 2018.

- The Cybersecurity and Infrastructure Security Agency (CISA) ***works with partners to defend against today's threats*** and collaborates with industry to ***build more secure and resilient critical infrastructure*** for the future.

- CISA coordinates security and resilience efforts using trusted partnerships across the private and public sectors and delivers ***technical assistance and assessments to federal stakeholders, as well as to infrastructure owners and operators nationwide.***

Region 10

CISA Regions



Critical Infrastructure Protection

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient critical infrastructure for the American people.

MISSION

Lead the national effort to understand and manage cyber and physical risk to our critical infrastructure.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Who We Are

CISA works with public sector, private sector, and government partners to share information, build greater trust, and lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

- FEDERAL NETWORK PROTECTION
- PROACTIVE CYBER PROTECTION
- INFRASTRUCTURE RESILIENCE & FIELD OPERATIONS
- EMERGENCY COMMUNICATIONS

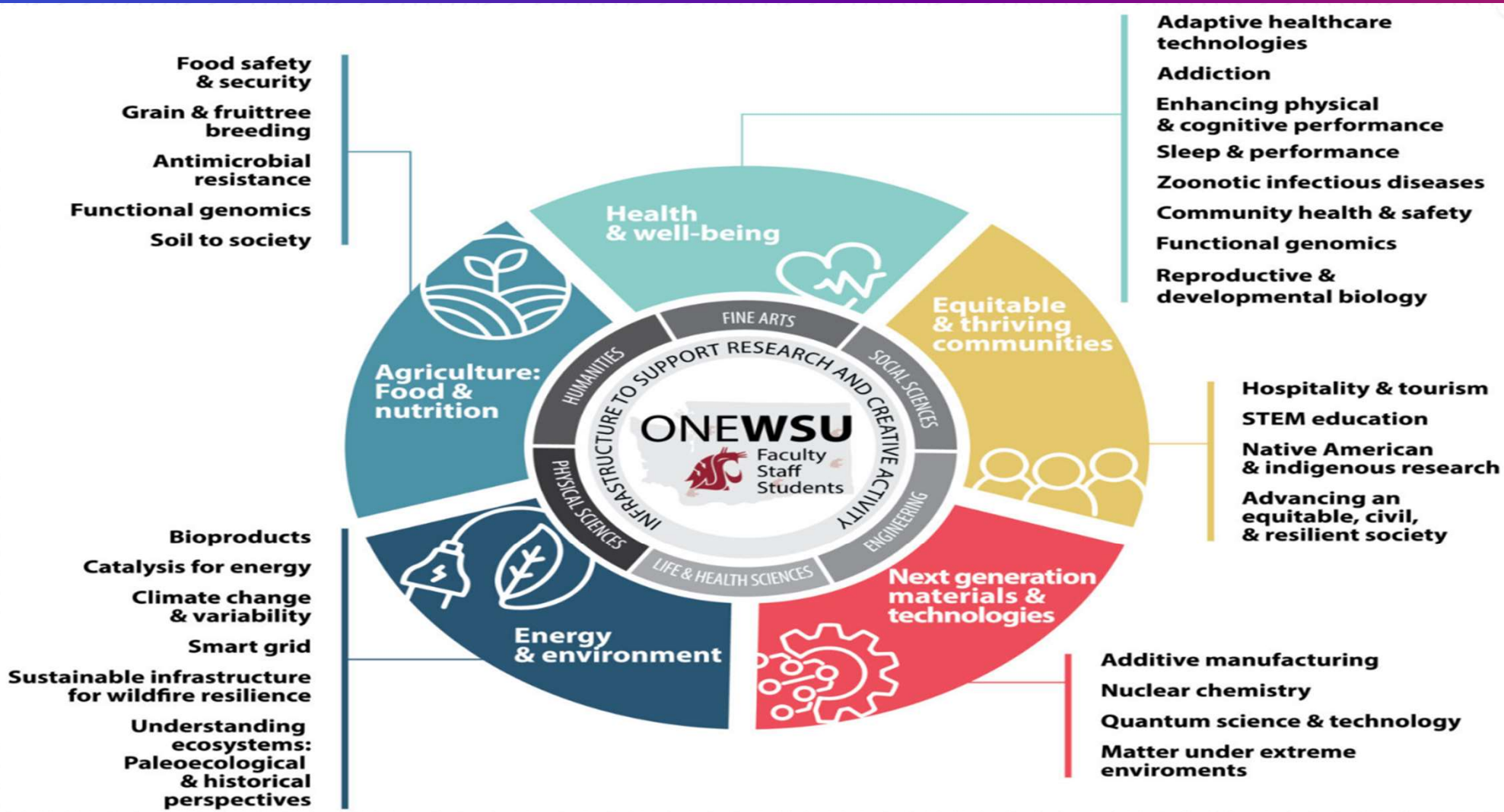
CISA Threat Intel Collaboration

Joint Cyber Defense Collaborative (JCDC)

- JCDC is a public-private cybersecurity collaborative that leverages new authorities granted by Congress in the 2021 NDAA.
- JCDC collaborates with over 100 international cyber defense organizations, often known as “CERTs,” to ensure that information about cyber threat is disseminated.
  - PNW Examples:
  - Initial Access Brokers selling credentials/access.
  - Breached data for sale.
  - Pre-Ransomware/Ransomware
  - Known Exploited Vulnerability (KEV) present on a system.

16 Critical Infrastructure Sectors
(primary agency)

WSU Research



CISA Initiatives

CISA Initiative Example

Software Bill of Materials (SBOM)

- Key building block in Software Security.
  - A SBOM is a nested inventory, a list of ingredients that make up software components.

SBOM resources

https://www.cisa.gov/sbom

Data Field	Description
Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version.
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y.
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.
Timestamp	Record of the date and time of the SBOM data assembly.

Secure by Design / Secure by Default

Secure by Design requirements include:

- The security of the customers is a core business requirement
- Security principles should be implemented during the design phase of a product's development lifecycle

Secure by Default features include:

- Products that are secure to use out of the box
- No additional cost for security features (i.e. MFA)
- Gather & log evidence of potential intrusions
- Control access to sensitive information

https://www.cisa.gov/securebydesign

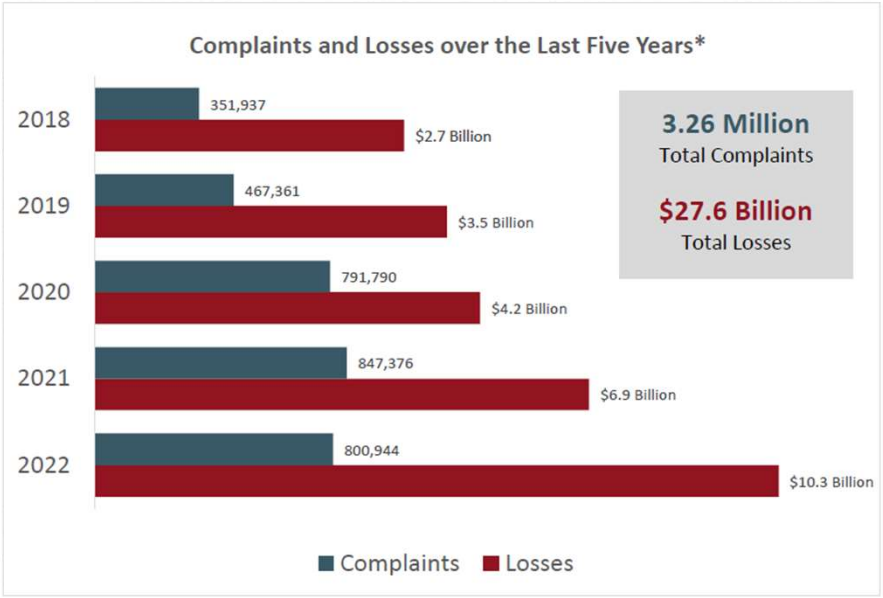
KEV's compared to CVE's

- Known Exploited Vulnerabilities (KEV)
  - CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild.
  - as of 5/16/2024 there were 1110 meticulously cataloged items (total)
  - 176 additions in the last year
- Common Vulnerabilities and Exposures (CVE)
  - As of February 2023 – 196,654
  - For 2024, estimated to be 34,888 – or 2900 per month
  - Previous estimates show around 2% exploited

State of Cyber

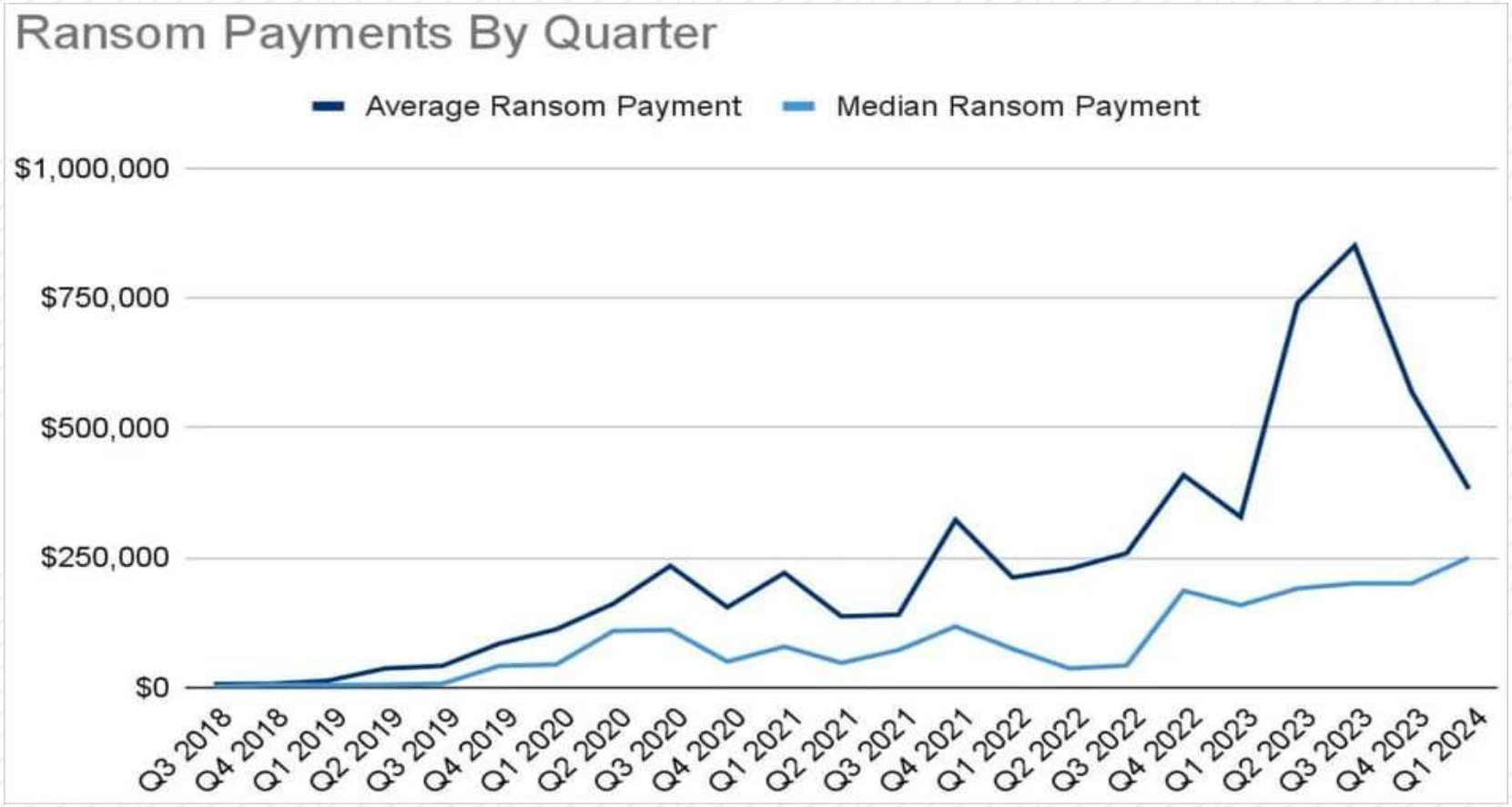
Cybersecurity statistics from FBI Internet Crime Complaint Center (IC3.gov)

- FBI IC3 2023 Report ➔
  - 3.26 million total complaints
  - $27.6 Billion Total Losses
    - Networth of YouTube ~$25 Billion
  - 870x Ransomware Victims
    1. Healthcare
    2. Critical Manufacturing
    3. Government Facilities
- Washington State was ranked 10th in terms of victim i the US.
- 58% increase in number of published vulnerabilities si 2017.
  - 2022 = ~25k Vulnerabilities.

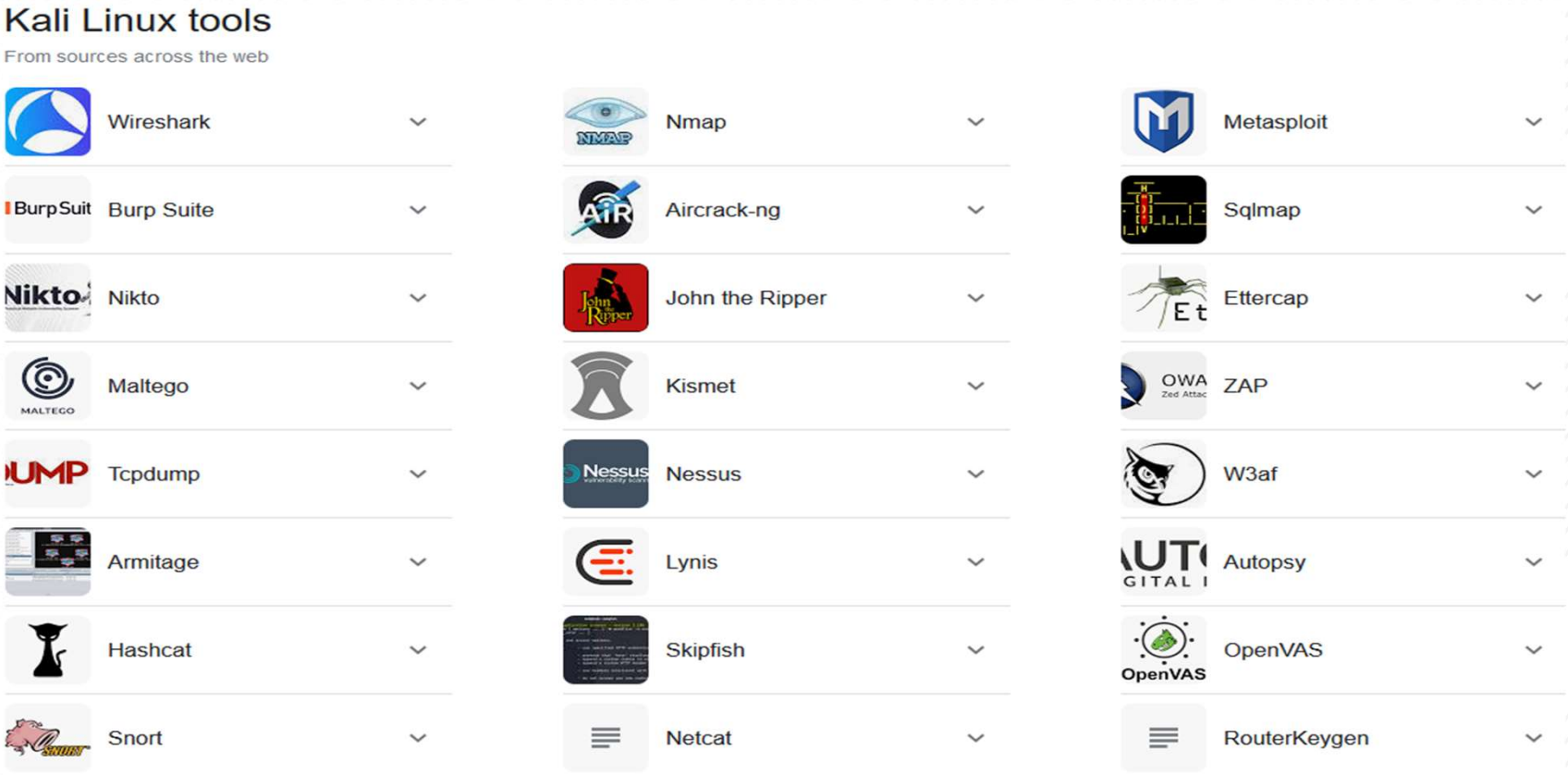


Ransomware payment rates

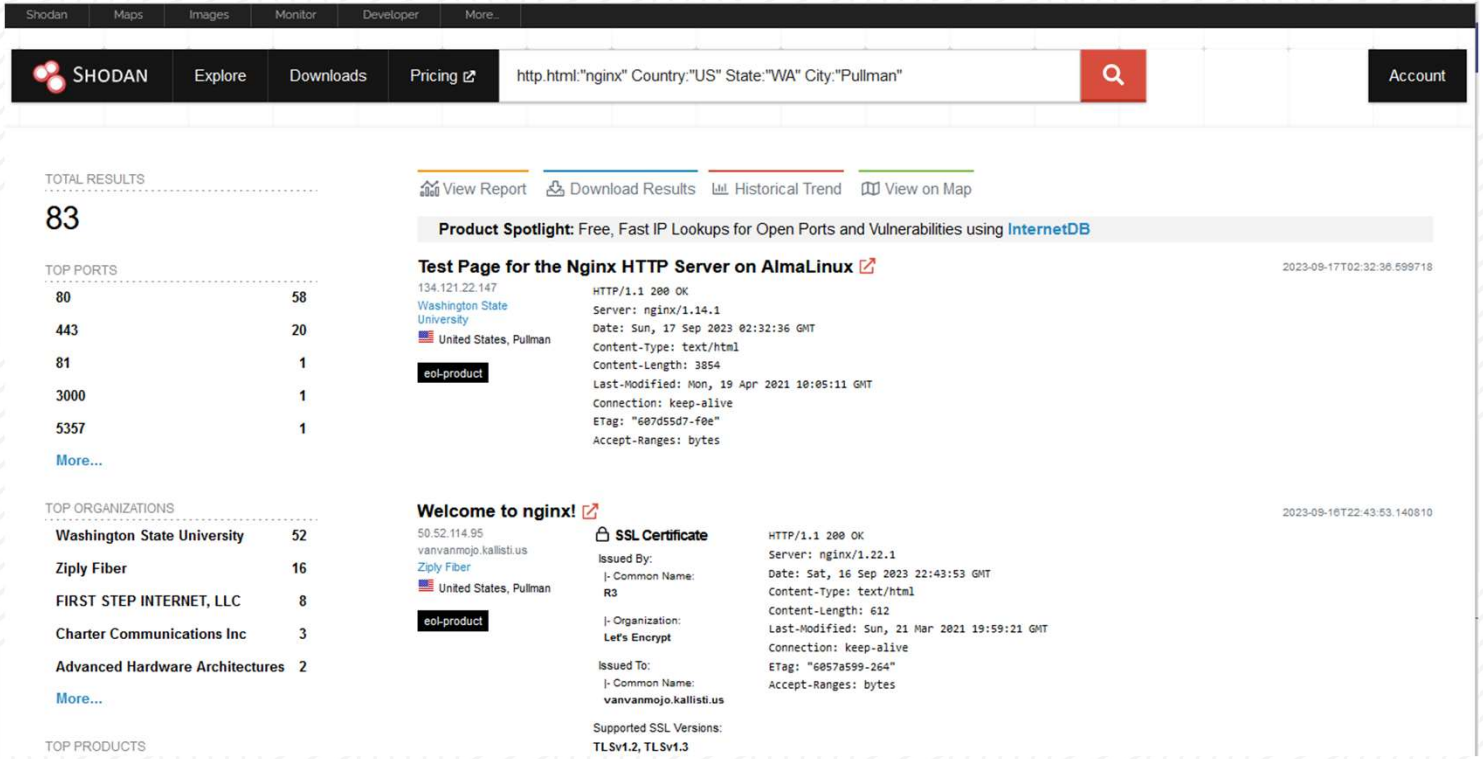
Ransomware payment amounts



Tools used by adversaries, or to protect from them



Shodan – search on metadata



Volt Typhoon/State-Sponsored Actors

Volt Typhoon

This CSA focuses on PRC-sponsored cyber actor, Volt Typhoon, targeting IT networks of communications, energy, transportation, water, and wastewater organizations in the U.S. and its territories.

Volt Typhoon - Living Off the Land (LOTL)

- Tactics involve using built-in tools that appear as normal activity and often do not set off alerts
- In some cases, the cyber actors have been living inside IT networks for years
- They are pre-positioned for disruptive or destructive cyberattacks against operational technology (OT) in the event of a major crisis or conflict with the United States.
- **Joint Guidance: Identifying and Mitigating Living off the Land Techniques**

Chinese Cyber Program

Capabilities:

- Highly capable, nimble operators; more sophisticated following public attribution
- Gain access via common vulnerabilities and zero-days
- Target software supply chains and Managed Service Providers
- Growing capability to engage in information operations

Intent:

- Targets a broad spectrum of U.S. interests, often for economic espionage
- Goal is to surpass Western industrial and defense capabilities
- Seeking to become less dependent on foreign technology
- Long-term strategy to gain advantage over the United States

China's cyber program supports economic and military development, primarily through espionage, and Beijing continues to develop cyber attack capabilities for wartime use.

Major Cyber Operations Attributed to China

- ***2011 -2013***: State-sponsored cyber actors conducts spearphishing and intrusion campaign targeting 23 US natural gas pipeline operators
- ***2013***: *IP Commission Report* highlights Chinese efforts at intellectual property theft efforts linked to an estimated $300 billion in business losses a year.
- ***2014-2015***: OPM is breached, exposing sensitive information for security background checks on 21 million federal employees.
- ***2017***: Chinese military hackers breach the networks of Equifax stealing the personal information of over 145 million Americans.
- ***2018***: Hackers breach servers of Marriot International, extracting information on 500 million guests.
- ***2020***: Suspected Chinese cyber actors exploited a known virtual private network vulnerability to compromise at least five federal agencies and entities in the defense, high-tech, transportation, and financial industries.
- ***2021***: APT 40 compromised as many as 100,000 e-mail servers worldwide in a range of industrial sectors, including infectious disease researchers, defense contractors, and more.

Russian Cyber Program

Capabilities:

- Assertive in its cyber operations even when detected
- Infiltrates software supply chains and broad campaigns exploiting vulnerabilities in networking devices
- Robust information operations program
- Historical precedent for targeting US and foreign elections

Intent:

- Collect information to support decision makers, influence military-political objectives
- Prep cyber environment for contingencies
- Divide and undermine US global standing and sow discord in US elections

Russia is aggressive in cyber ops—espionage and prepositioning for attack—against US government and critical infrastructure networks, including energy and transportation systems.

Major Cyber Operations Attributed to Russia

- ***2011-18***: Russian state-sponsored APT actors conducted a multi-stage intrusion campaign in which they gained remote access to U.S. and international Energy Sector networks, deployed ICS-focused malware, and collected and exfiltrated enterprise and ICS-related data.
- ***2015-16***: Russian state-sponsored APT actors conducted a cyberattack against Ukrainian energy distribution companies, leading to multiple companies experiencing power outages in 2015. In 2016, these actors conducted a cyber-intrusion campaign against a Ukrainian electrical transmission company and deployed malware designed to attack power grids.
- ***2016***: During the 2016 US presidential campaign, Russian operatives use cyber operations to seek vulnerabilities in election infrastructure, collect on political parties, and candidates and conduct influence operations using social media.
- ***2017***: NotPetya ransomware attack spills out of Ukraine affecting businesses globally.
- ***2018***: Russian cyber actors targeted the 2018 Winter Olympic Games' opening ceremony and deployed data deletion malware against Olympic related entities.
- ***2020***: Russian state-sponsored actors target state, local, tribal, and territorial (SLTT) governments and aviation networks.
- ***2020-2021***: A Russian software supply chain operation in 2020 distributed malware that compromised major US companies and multiple US federal agencies.

North Korean Cyber Program

Graphic is UNCLASSIFIED

Capabilities:

- Emphasis on Korean Peninsula, but history of successful cyber operations against US networks
- Have progressively developed their resources and operator capabilities
- Social engineering becoming increasingly sophisticated

Intent:

- Cyber criminal generation of revenue to support regime, its nuclear and ballist missile programs, and to counter international sanctions
- Signal to adversaries that they are capable of harm

North Korea uses cyber operations as a tool of coercion, espionage, attack, and a source of illicit financing via cyber criminal activities

Major Cyber Operations Attributed to DPRK

- ***2011-13***:
- ***2014***: North Korea conducts destructive attack against US-based Sony Pictures Entrainment
- ***2015***: North Korean-linked group use 5,986 phishing emails containing malicious code to gain access to noncritical systems at a South Korean nuclear power plant.
- ***2016***: North Korean groups are linked to an estimated $81 million cyber heist of Bangladesh's central bank account at the Federal Reserve Bank of New York.
- ***2017***: North Korea launches the WannaCry ransomware attack that infects over 300,000 computers in 150 countries; its effects include temporarily knocking some UK hospitals offline.
- ***2019***: A UN report concludes that North Korea used cyberattacks against financial institutions and cryptocurrency exchanges to steal and estimated $2 billion it used to fund its weapons of mass destruction program.
- ***2020-2021***: North Korean hackers target coronavirus vaccine developers.
- ***2021***: North Korean conducts social engineering campaign against cybersecurity researchers.

Iranian Cyber Program

Graphic is UNCLASSIFIED

Capabilities:

- Less sophisticated than Russian and Chinese counterparts but still able to disrupt and damage US networks
- Conducted disruptive and destructive cyberattacks on US financial institutions, companies, election infrastructure, other critical infrastructure, and academic institutions
- Research into Industrial Control Systems; capability to cause unspecified short-term effects
- Conducted malign influence operations targeting the US 2020 presidential election, including violence-related themes

Intent:

- Cyber operations are a tool for political retaliation and support its security priorities, including sanctions relief.
- "Eye for an eye" approach and response to provocations.

Iran's willingness to conduct aggressive cyber operations make it a significant threat to US networks and data; more recent demonstrations of cyber-enabled influence activities.

Major Cyber Operations Attributed to Iran

- ***2011-13***: Iran targeted 46 US financial institutions and a dam in Rye, New York, with distributed denial-of-service attacks.
- ***2012***: Iran conducted destructive attacks against the Saudi Arabian state-owned oil firm, Saudi Aramco, with Shamoon malware, which resulted in 30,000 computer rendered unusable and taken offline.
- ***2014***: Iranian hackers attacked the Sands Casino, infecting multiple systems and wiping hard drives.
- ***2017***: Iran launched Shamoon 2, affecting 15 government agencies and organizations in Saudi Arabia.
- ***2021***: Iranian government-sponsored APT actors leverage Microsoft Exchange and Fortinet vulnerabilities to gain initial access in advance of follow-on operations, which included deploying ransomware. They targeted a broad range of US critical infrastructure sectors, including a US municipal government, a US hospital, and the transportation sector.
- ***2021-22***: Iranian cyber actors observed leveraging the Log4j vulnerability.
- ***2022***: US Cyber Command connected actor MuddyWater to the Iranian Ministry of Intelligence and Security (MOIS) and noted open source tools they have recently leveraged to compromise US computer networks.

CISA No-cost Resources

On-site assessments and advising

- Cyber Protective Visit (CPV) – discuss your environment and your current systems, backups, and setup
- CPG, CIS, EDM, CRR, etc.
- Tabletop Exercises (TTX) – design scenarios to simulate an incident
- Incident Management/Response workshops and review
- Invite your PSA to review facilities and offer his (no-cost) services

Scanning services

- Cyber Hygiene (CyHy) – passive scanning of your external IP space for vulnerabilities
- Web Application Scanning (WAS) – will scan your web applications for vulnerabilities
- Remote Penetration Test (RPT)
- Remote Vulnerability Assessment (RVA)

Cybersecurity Advisor (CSA) Program

CISA mission: Lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure

In support of that mission: Cybersecurity Advisors (CSAs):

- **Assess**: Evaluate critical infrastructure cyber risk.
- **Promote**: Encourage best practices and risk mitigation strategies.
- **Build**: Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate**: Inform and raise awareness.
- **Listen**: Collect stakeholder requirements.
- **Coordinate**: Bring together incident support and lessons learned.

Joining CISA

- CISA.gov/careers
  - www.usajobs.gov
  - dhscs.usajobs.gov
  - StudentCareers@cisa.dhs.gov
- Resume Help
  - www.cisa.gov/careers/resume-application-tips
- Hiring Timeline
  - Depending on Job, 3-8 Months.

Cybersecurity/IT Jobs

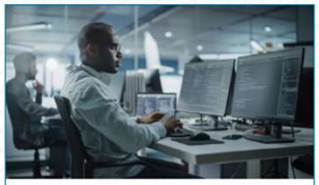
The demand for an experienced and qualified cyber workforce to protect our Nation's networks and information systems has never been higher.

Emergency Communications Jobs

Being able to communicate is critical during all emergencies. A rewarding career awaits knowing you had a hand in connecting first responders.

Infrastructure Security Jobs

These vital roles focus on the many critical infrastructure systems and places, working to make our people, spaces, data and networks more resilient and secure.



National Risk Management Jobs

For those who like to collect, collate, and analyze information! Work to identify and address the greatest risks to the Nation's critical infrastructure.

Stakeholder Engagement Jobs

Passionate about building connections? As threats continue to evolve, sustaining trusted and effective partnerships between government and the private sector helps to protect the nation's critical infrastructure.

Integrated Operations Jobs

In the matter of mitigating risks, it's critical to make the right decision at the right time. Joining Integrated Operations allows you to take part in preparing, planning, and managing operations and the delivery of CISA capabilities and services.

Mission Enabling Jobs

Support the mission! There are many other roles within the agency that support our mission of leading the National effort to understand, manage, and reduce risk to our critical infrastructure. Explore more careers at CISA.

Questions?

https://www.cisa.gov
https://www.cisa.gov/cyber-resource-hub

Daniel Brown
Region 10 (Inland Northwest)
Cybersecurity Advisor
(509) 981-9920
daniel.brown@cisa.dhs.gov

CISA Resources

Steve Neal
Region 10 (Eastern WA)
Protective Security Advisor
(509) 216-2534
steven.neal@cisa.dhs.gov