Dave Sonheim
Cybersecurity Advisor
Region VIII | Colorado, South Dakota, North Dakota
Cybersecurity and Infrastructure Security Agency (CISA)

A secure and resilient critical infrastructure for the American People
Agenda

- Current Threats and RaaS Trends
- Definition of a Cyber Threat Actor
- Cyber and Ransomware Terms
- Anatomy of a Cyber Attack
- Notable Recent Cyber Attacks
- Common Themes – Take Away Items
- CISA Ransomware Resources / Guides
- CISA Cybersecurity Service Offerings Overview
- Q&A
Current Cybersecurity Threats

REDUCE THE RISK OF RANSOMWARE
Hackers

Threat actors are sophisticated and well funded.

Threat = Capability + Intent + Motivation
The New Face of Organized Crime

Hackers are no longer lone wolves. They’re now banding together to run fewer—yet much larger—attacks, similar to the traditional crime rings of the 20th century.

80% of cyber-attacks are driven by organized crime rings, in which data, tools, and expertise are widely shared.
Anatomy of a Cyber Attack

7 Phases of a Cyber Criminal's Methodology:

1. Reconnaissance
2. Weaponisation
3. Delivery
4. Exploitation
5. Command & Control
6. Internal Reconnaissance
7. Maintain
Recent Significant RaaS Attacks

- **Kaseya**: 2 July 21, Cybercriminal group REvil (Raas) targeted a flaw in Kaseya’s code on their Virtual Server Agent (VSA) which is among the World’s most popular remote monitoring and management (RMM) for managed service providers worldwide. More than 60 Kaseya customers and 1,500 downstream businesses were impacted by a poisoned VSA update which the threat actor used to infect downstream organizations. The Russian-based Advanced Persistent Actor demanded $70 million in Bitcoin for a universal decryptor. (Sodinokibi)

- **JBS S.A. Meat Processing**: 1 June 21, REvil (RaaS) conducted a ransomware attack against business networks of meat processor JBS who supplies one-fifth of meat globally, receiving a ransom demand of $11 million dollars. The attack shut down global business networks which directly impacted their meat production operations. Due to 2nd & 3rd order impacts of business automation within their networks meat tagging and shift scheduling were interrupted which in-turn impacted supply chains and their ability to fully operate their meat production lines.  
  **Result**: $11 million Ransom, Disruption in the global meat production supply chain

- **Colonial Pipeline**: 7 May 21, Cybercriminals known a DarkSide (RaaS) conducted a ransomware attack against the largest refined products pipeline in the United Sates, with a capacity to transport 2.5 million barrels a day from the Gulf coast to markets in the southern and eastern US. Colonial proactively shut down its OT pipeline systems to contain and mitigate the ransomware spread. Due to business automation integration the ransomware event on their business IT Systems directly impacted their tracking and billing automation within their pipeline distribution network. Disrupting the fuel supply chain network across multiple States and vendors for several days resulting in the most significant pipeline outage in due to a cyber event in history.  
  **Result**: More than $4.3 million in Ransom and millions more in lost revenue
- **Large Scale Ransomware Attacks Likely to Continue**: Adversaries have developed effective business models and through their expansion into a Ransomware as a Service (RaaS) it is highly likely we will continue to see these significant and large scale attacks on US business to include critical infrastructure in the near term.

- **Common Attack Tactics** – Regardless of the RaaS gang we typically see them use similar attack paths: Phishing Email to gain credentials and install malicious script files, Leverage vulnerabilities in Remote Desktop, Server Message Block, and VPN related security flaws. This includes other software vulnerabilities where the most current patches have not been applied as well a Remote Code execution vulnerabilities allowing an attacker to inject arbitrary code and execute on the impacted system.

- **Command & Control (C2)**: Attackers typically employ a technique called a C2 Beacon – This means they install a program that creates a hidden backdoor that communicates out to third party servers they control in order issue follow on commands and execution instructions which blend in with normal activity. (C2 domain leverages cloud infrastructure based in the US to avoid US authority investigating US based infrastructure.

- **Biggest Take Away**: These incidents underscore the threat that ransomware poses to organizations regardless of size or sector. All organizations should take immediate action to review and strengthen their Cybersecurity posture before they become a victim. Once encrypted, it becomes very difficult to recover data and any backups that were not stored in an off-line solution. Cyber Incident responders will have limited tools to assist with any decryption efforts and without detailed security logs to conduct forensic analysis recovery could be a lengthy and challenging process.
Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. In recent years, ransomware incidents have become increasingly prevalent among the Nation’s state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations.

Malicious actors continue to adjust and evolve their ransomware tactics over time, and CISA analysts remain vigilant in maintaining awareness of ransomware attacks and associated tactics, techniques, and procedures across the country and around the world: See CISA’s Awareness Briefings on Combating Ransomware, Joint Ransomware Statement, and CISA Insights – Ransomware Outbreak.
Ransomware Guide

Joint CISA and MS-ISAC Ransomware Guide

This Ransomware Guide includes recommendations, best practices, recommended incident response policies and procedures, cyber hygiene services, and several checklists that organizations can use to help protect against or response to ransomware attacks.
CISA Ransomware Resources

Ransomware Campaign Toolkit | CISA

CISA.gov/ransomware

- Ransomware Guide (CISA & MS-ISAC)
- CISA INSIGHTS: Ransomware Outbreak
- Activity Alerts and Analysis Reports
  - US-CERT activity alerts on ransomware threats
  - Joint statements on ransomware with our partners
- Guides and CISA Cyber Services
  - Cyber Assessments (CRR, EDM, CIS)
  - Cyber Hygiene Vulnerability Scanning Services
  - TTX Exercises & Workshops
- Factsheets and Infographics
  - Protect Your Center From Ransomware poster
  - Ransomware: What It Is and What To Do About It
- Training and Webinars
  - Trends and Predictions in Ransomware (Cyber Summit 2020)
  - CDM Training
  - Incident Response Training Series
  - Combating Ransomware Webinar

RANSOMWARE GUIDANCE AND RESOURCES

Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by a victim unknowingly visiting an infected website.

CISA has observed continuing ransomware attacks across the country and around the world: See CISA’s Awareness Briefings on Combating Ransomware, Joint Ransomware Statement, and CISA Insights – Ransomware Outbreak. Below, please find resources on CISA’s redesigned ransomware information page to better connect you with helpful resources and tools you and your organization need to guard against the ransomware threat.

Looking to learn more about this growing cyber threat? With industry best practices and individualized checklists, the NEW Ransomware Guide is a great place to start. The guide, released in September 2020, represents a joint effort between CISA and the Multi-State Information Sharing and Analysis Center (MS-ISAC). The joint Ransomware Guide is a customer-centered, one-stop resource with best practices and ways to prevent, protect and/or respond to a ransomware attack.

In addition to reviewing the Ransomware Guide, we invite you to click on resources below to find additional Ransomware-related information. These resources are designed to help individuals and organizations prevent attacks that can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services.
CISA Cybersecurity No Cost Offerings

Denver Federal Center Based
CISA Cybersecurity Advisor Facilitated

- Preparedness Activities
  - Information/Threat Indicator Sharing
  - Cybersecurity Training and Awareness
  - Cyber Exercises and “Playbooks”
  - National Cyber Awareness System (US-CERT)
  - Vulnerability Notes Database (MITRE CVE)
  - Ransomware Guide / Playbook
- Cybersecurity Service Offerings
  - Cyber Resilience Reviews (CRR)
  - External Dependency Management (EDM)
  - Cyber Infrastructure Surveys (C-IST)
  - Cyber Security Evaluation Tool (CSET)

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)
- Red Team Assessment (RTA)
- Validated Architecture Design (VADR)
- Critical Product Evaluation (CPE)
- CISA Qualification Initiative (CQI)

CISA HQ Response Assistance

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

Denver Based Protective Security Advisors

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

DAVE SONHEIM
Cybersecurity Advisor Region VIII (CO, SD, ND)
Cyber & Infrastructure Security Agency (CISA)
EMAIL: David.Sonheim@hq.dhs.gov
MOBILE: (720) 661-1643

Process Management and Improvement

August 4, 2021
R8 All State Call
Q & A

- Are these attackers targeting specific sectors or casting a wide net?
- Are all of the Cyber attacks that we hear about Criminal in Nature?
- Is the intent of these threat actors to disrupt critical infrastructure or cause physical harm to the US public?
- Are only large corporations at risk of these attacks?
- Why are we now hearing about these attacks on a daily basis has ransomware increased significantly in recent months?
- If organizations have a suspected incident what are the immediate actions? (Disconnect, Contain, & Report)
- If organizations experience a cyber incident who should they contact first?
CISA REGION VIII

DAVE SONHEIM
Cybersecurity Advisor Region VIII
(CO, SD, ND)
Cybersecurity and Infrastructure
Security Agency (CISA)
CISA.GOV

EMAIL: david.sonheim@hq.dhs.gov
MOBILE: (720) 661-1643