CISA RANSOMWARE CAMPAIGN: REDUCE THE RISK OF RANSOMWARE

NIST NCCOE MANUFACTURING COMMUNITY OF INTEREST WEBINAR
FEBRUARY 25, 2021
We are the Nation’s Risk Advisors

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure.

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.
Ransomware Campaign Overview

REDUCE
THE RISK OF
RANSOMWARE
Ransomware Key Messages

- Keep Calm and Patch On
- Backing Up Is Your Best Bet
- Suspect Deceit? Hit Delete
- Always Authenticate
- Prepare & Practice Your Plan
- Your Data Will Be Fine If It’s Stored Offline...
- Secure Your Server Message Block (SMB)
- Paying Ransoms Doesn’t Pay Off
- Ransomware Rebuild and Recovery Recommendations
CISA Ransomware Resources

CISA.gov/ransomware
- Ransomware Guide
- CISA INSIGHTS: Ransomware Outbreak
- NEW! Toolkit, fact sheet, and images
- Alerts and Statements
  - US-CERT activity alerts on ransomware threats
  - Joint statements on ransomware with our partners
- Guides and Services
  - Cyber Hygiene Services
  - TTX Exercises
- 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
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.
Ransomware Response Checklist

Detection and Analysis
- Determine systems impacted, immediately isolate + triage impacted systems for restoration/recovery
- Engage internal/external stakeholders - help to mitigate, respond to, and recover from incident

Containment and Eradication
- Investigation: take a system image and memory capture of a sample of affected devices
- Research trusted guidance for ransomware variant + conduct examination of IDS/IPS and logs
- Conduct extended analysis to identify persistence mechanisms
- Rebuild systems based on a prioritization of critical services
- IT security authority declares the incident over
Ransomware Response Checklist

Recovery and Post-Incident Activity

- Reconnect systems, restore data from offline, encrypted backups based on critical services prioritization
- Document lessons learned from the incident
- Consider sharing lessons learned and relevant indicators of compromise (IOCs) with CISA and sector ISAC/ISAO
Who to Contact?

Federal Asset Response: CISA

CISA can assist with analysis at no cost to support your organization in understanding the root cause of the incident (CISA Advanced Malware Analysis Center and Remote Assistance request).

Federal Threat Response: FBI, USSS

For No-Cost Resources Contact:

Federal and SLTT Organizations: CyberLiaison_SLTT@cisa.dhs.gov

Private sector organizations: CyberLiaison_Industry@cisa.dhs.gov

Ransomware Campaign Resources: cisa.gov/Ransomware
Vulnerability Scanning

Scanning of internet-accessible systems for known vulnerabilities or potential points of exploit on a continuous basis. As potential vulnerabilities are identified, CISA notifies the organization via proactive notifications and weekly reports so that risk mitigation efforts may be implemented to avoid exploitation.

How to Sign Up

Email CISA at vulnerability_info@cisa.dhs.gov with the subject line “Request Vulnerability Scanning Services” to get started!
Known as a PCA, this service evaluates an organization’s susceptibility and reaction to phishing emails of varying complexity. Deliverable: Report that highlights organizational click rates for varying types of phishing emails and summarizes metrics related to proclivity of the organization to fall victim to phishing attacks and attempts.

**How to Sign Up**

Email CISA at vulnerability_info@cisa.dhs.gov with the subject line “Request Phishing Campaign Assessment Service” to get started!
Assessments

Cyber Resilience Review

- An interview-based assessment that evaluates an organization’s operational resilience and cybersecurity practices to provide an organization with greater awareness of its network posture. Evaluates the maturity of an organization in performing, planning, managing, measuring, and defining cybersecurity capabilities across 10 domains.

Cyber Infrastructure Survey

- This is used to assess an organization’s critical services against cybersecurity controls grouped into five domains. Organizations receive access to a user-friendly dashboard to review the results and findings of the survey.
Malicious Domain Blocking and Reporting

- MDBR is funded by CISA, our MS-ISAC and EI-ISAC partners provide the MDBR service at no-cost to members.

- Fully managed proactive security service (protective DNS resolver) that prevents IT systems from connecting to harmful web domains, which helps limit infections related to known ransomware, as well as other malware, phishing, and cyber threats.

- To sign up for MDBR, visit: https://www.cisecurity.org/ms-isac/services/mdbr/
Nationwide Cybersecurity Review

Nationwide Cybersecurity Review (NCSR)

• Conducted by MS-ISAC on CISA’s behalf, this review is based on NIST Cybersecurity Framework.

• Anonymous, annual self-assessment to measure gaps/capabilities of SLTT gov’t cybersecurity programs.

• Evaluates cybersecurity maturity across the nation while providing actionable feedback and metrics directly to individual respondents.

• Requirement for Homeland Security Grant Program recipients.

https://www.cisecurity.org/ms-isac/services/n csr
We recently released a new Ransomware Campaign Toolkit on our ransomware webpage!
For more information: 
cisa.gov/ransomware

Contact:
Amy.Nicewick@CISA.dhs.gov
(703) 203-0634