Asia-Pacific Cybersecurity Community Collaboration and Joint Defense

Tom Millar, US Cybersecurity and Infrastructure Security Agency (CISA)

1. A Little Bit About CISA
2. The Top Threat to US Critical Infrastructure
3. Fighting The Top Threat
4. Working Collaboratively
5. Questions & Answers

What is CISA?

- CISA is the “Nation’s Risk Advisor”
- Not a Cyber Regulator
- Not a Law Enforcement Agency
- Our stakeholders include US Federal Government agencies and US Critical Infrastructure

The #1 Threat To Critical Infrastructure

… is Ransomware.

- Ransomware is intentionally disruptive.
- Recovery to full operations can take weeks (whether the victim pays the ransom or not).
- Recent severe incidents have affected the energy sector, food and agriculture supply chain, and hospital networks.
- Attacks occur daily across all sectors.

Defeating Ransomware Together

CISA works together with its sister agencies and with private sector partners to combat the ransomware threat.

- Law Enforcement Agencies and the Treasury Department disrupt operations and their payment schemes.
- Defense, Law Enforcement, Diplomatic and Intelligence Agencies work to take the fight to the enemy.
- CISA leads the effort to harden targets – making systems more secure and resilient.

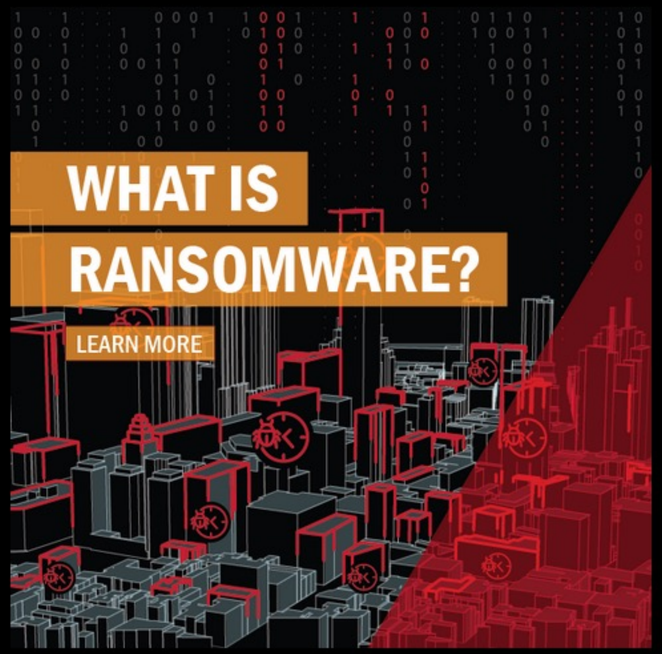
https://www.cisa.gov/stopransomware

An official website of the United States government Here's how you know

STOP RANSOMWARE

Search

RESOURCES NEWSROOM ALERTS REPORT RANSOMWARE



https://www.cisa.gov/BadPractices

An official website of the United States government Here's how you know

EMAIL US CONTACT SITE MAP

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Search

COVID Questions

Report Cyber Issue

CYBERSECURITY | INFRASTRUCTURE SECURITY | EMERGENCY COMMUNICATIONS | NATIONAL RISK MANAGEMENT | ABOUT CISA | MEDIA

Cybersecurity > Bad Practices

Cybersecurity

- Cybersecurity Training & Exercises
- Cybersecurity Summit 2020
- Cyber QSMO Marketplace
- Combating Cyber Crime
- Securing Federal Networks
- Protecting Critical Infrastructure
- Cyber Incident Response

BAD PRACTICES

As recent incidents have demonstrated, cyberattacks against critical infrastructure can have significant impacts on the critical functions of government and the private sector. All organizations, and particularly those supporting designated

https://us-cert.cisa.gov/ncas/alerts/aa21-291a

An official website of the United States government Here's how you know

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Search

CISA.gov Services Report

Alerts and Tips Resources Industrial Control Systems

National Cyber Awareness System > Alerts > BlackMatter Ransomware

Alert (AA21-291A)

More Alerts

BlackMatter Ransomware

Original release date: October 18, 2021

Print Tweet Send Share

Summary

Note: *this advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, version 9. See the ATT&CK for Enterprise for all referenced threat actor tactics and techniques.*

This joint Cybersecurity Advisory was developed by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) to provide information on BlackMatter ransomware. Since July 2021, BlackMatter ransomware has targeted multiple U.S. critical infrastructure entities, including two U.S. Food and Agriculture Sector organizations.

Actions You Can Take Now to Protect Against BlackMatter Ransomware

- *Implement and enforce backup and restoration policies and procedures.*
- *Use strong, unique passwords.*
- *Use multi-factor authentication.*

https://github.com/cisagov/cset/releases

Why GitHub? Team Enterprise Explore Marketplace Pricing Search / Sign in Sign up

cisagov / cset Public

Notifications Star 713 Fork 133

Code Issues 25 Pull requests 43 Actions Projects Wiki Security Insights

Releases Tags

Latest release

v10.3.0.0

c0748ac

Compare

Ransomware Readiness Assessment CSET v10.3

inlguy released this on Jun 28

The download the installer file

Download CSETStandAlone.exe

Algorithm : SHA256
Hash : D7FBBEE8542D81B40E8E1D7D4AB1DC65D4EDBCB63248B1A080DE953D77BCA90B
Path : CSETStandAlone.exe

Accessing the Ransomware Readiness Assessment (RRA)

To use the RRA first follow the CSET installation instructions to properly install CSET.

Global Collaboration

Critical infrastructure is global and international collaboration is key to succeeding against this threat.

- International partnerships have helped alert potential victims and minimizing impact.
- Sharing timely alerts and detection methods is critical.
- This is done via various trust communities using different channels, from formal Information Sharing and Analysis Centers (ISACs) to volunteer groups.

Thank You!