MS-ISAC®
Multi-State Information Sharing & Analysis Center®

No Cost Resources with the MS-ISAC

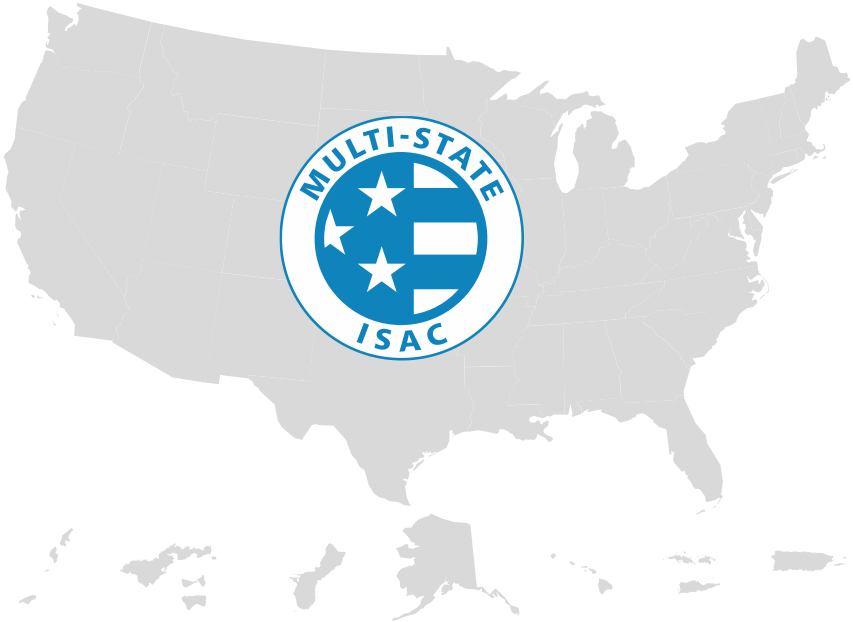
Kyle Bryans
Regional Engagement Manager

Multi-State Information Sharing & Analysis Center®

The MS-ISAC®

- Designated by the Cybersecurity & Infrastructure Security Agency (CISA) as a key resource for cyber threat prevention, protection, response and recovery for all U.S. State, Local, Tribal and Territorial (SLTT) governments.
- A division of the Center for Internet Security® (CIS®), a 501(c)(3) nonprofit.

https://learn.cisecurity.org/ms-isac-registration



Who We Serve

State, Local, Tribal, and Territorial Governments

- 50 State Governments
- 15,000 Local Governments
- 6 Territorial Governments
- 146 Tribal Governments
- 80 DHS-recognized Fusion Centers

Local Governments include

- 177 Total Members in State of SC
- 25 SC Cities and Towns
- 31 SC Counties
- 30 K-12 School Districts

MS-ISAC®
EI-ISAC

Security Operations Center

24x7x365

Support

Network Monitoring Services
+
Research and Analysis

Analysis & Monitoring

Threats, Vulnerabilities
+
Attacks

Reporting

Cyber Alerts & Advisories

Web Defacements

Account Compromises

To report an incident or request assistance:

Phone: 1-866-787-4722

Email: soc@cisecurity.org

Intelligence Sources

180+ Open Source & Commercial Vendors

International Intelligence Partners

FS-ISAC

CROWDSTRIKE

National Cyber Security Centre
a part of GCHQ

MCAP

AVIATION ISAC

FIREEYE

ACSC Australian Cyber Security Centre

Albert
CIS Network Monitoring

H-ISAC
HEALTH - ISAC

FLASHPOINT

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

Akamai

21 National Council of ISAC Members

U.S. Federal & SLTT Government Sources

Internal Research & Member Submissions

Monitoring of IP Range & Domain Space

IP Monitoring

- Signs of Compromise
- Malicious Activity

Domain Monitoring

- Notifications on compromised user credentials

Send Public IPs and Domains to soc@cisecurity.org

Malicious Domain Blocking and Reporting (MDBR)

Security Focused DNS service:

Blocks malicious domain requests before a connection is even established!

Simple Implementation:

No new hardware or software required

Helps limit infections related to:

- Known Malware
- Ransomware
- Phishing
- Other cyber threats

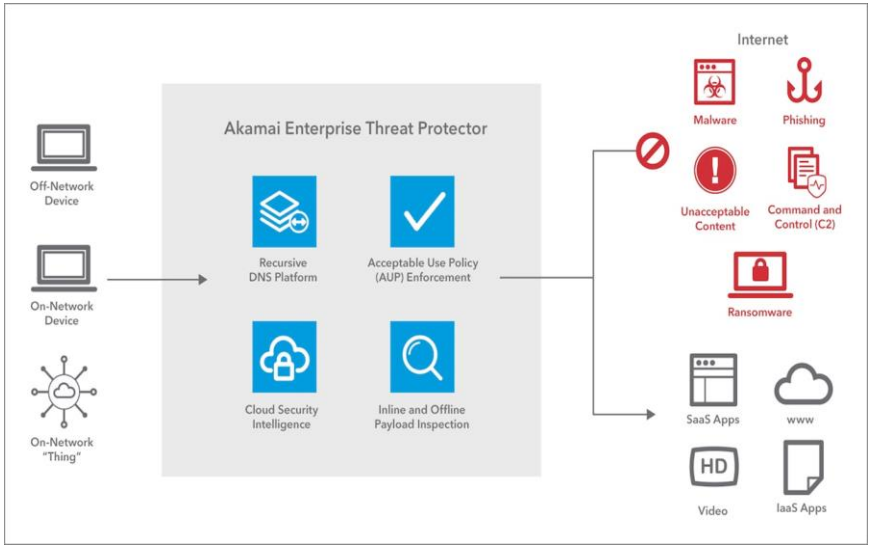
Akamai Enterprise Threat Protector (ETP)

Built on the global Akamai Intelligent Edge Platform and Akamai's carrier-grade recursive DNS service.

Akamai Intelligent Edge Platform manages up to 30% of global web traffic and delivers up to 2.2 trillion DNS queries daily (2/3 of the world's DNS traffic).

Requested domains are checked against Akamai's real-time domain risk scoring threat intelligence.

Quick-to-configure and easy-to-deploy.



Simple Implementation

Can be implemented in minutes, on existing infrastructure, with no new hardware or software required.

MDBR service requires configuring your organization's DNS infrastructure to use Akamai's recursive servers as its primary and secondary DNS forwarders. When reconfiguring your DNS infrastructure, you have two options:

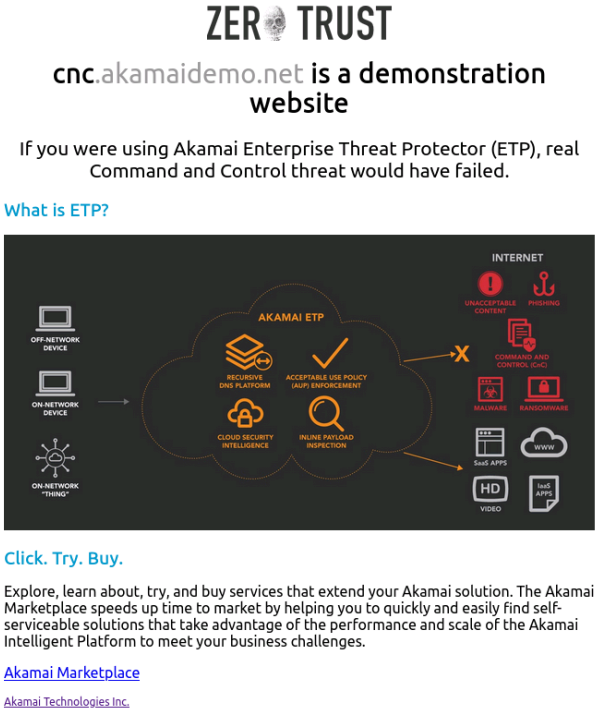
Option 1

DNS forwarders point to Akamai's primary and secondary forwarders only

Option 2

- Akamai's primary and secondary forwarders
- Tertiary and quaternary forwarders (3rd party)

Implementation Testing

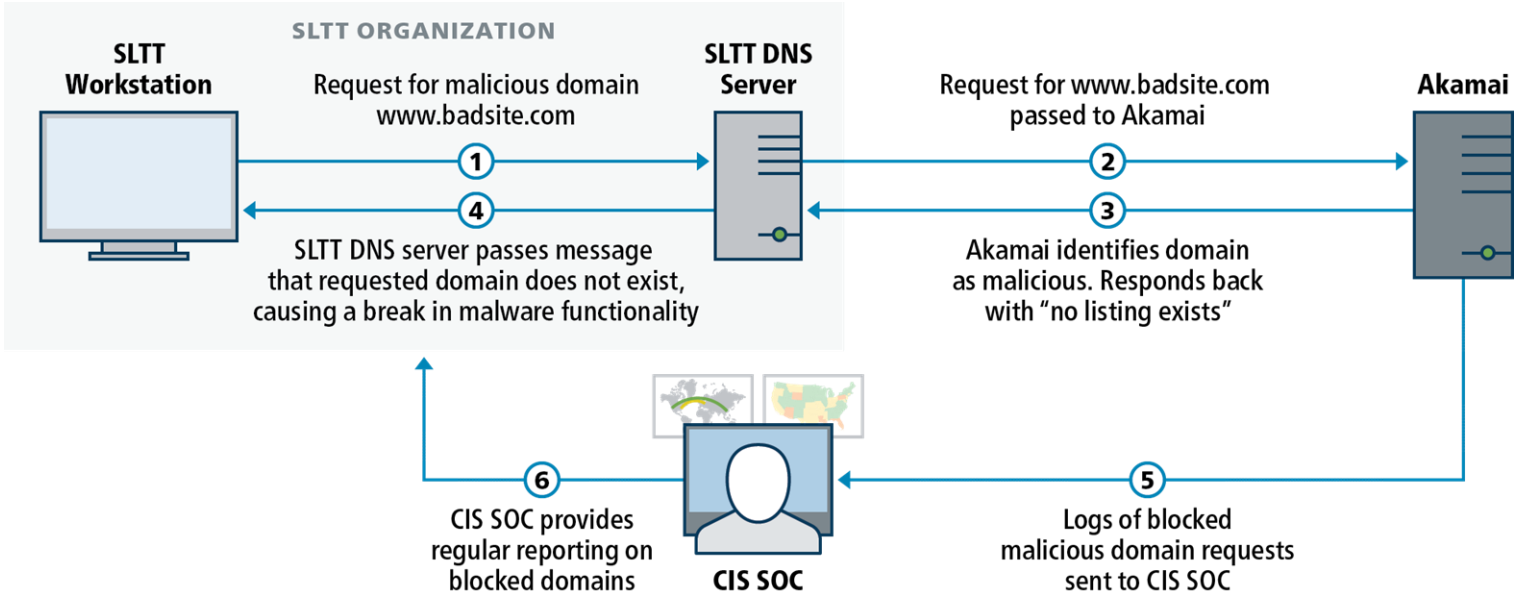


Test Domains:

akamaietpcnctest.com
akamaietpphishingtest.com
akamaietpmalwaretest.com

Configured Correctly:

Reporting Data Flow



MDBR Reporting

Top 10 Blocked Malicious Domains for the Past Week

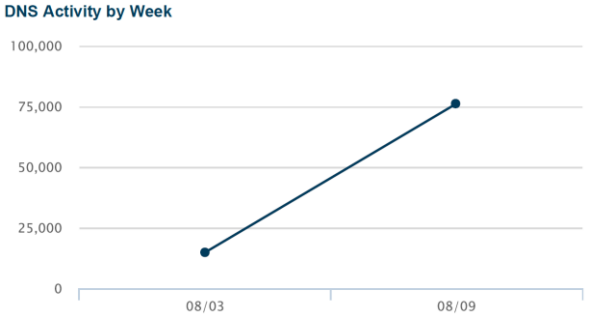
Domain	Total
(akamaietpcnctest[.]com[.])	7
(akamaietpmalwaretest[.]com[.])	3
(akamaietpphishingtest[.]com[.])	3

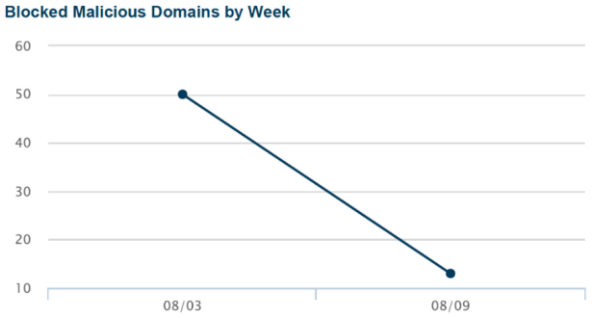
Summary PDF reports and associated blocked logged data will be sent on a weekly basis, identifying both high-level and detailed information on blocked requests, broken down by:

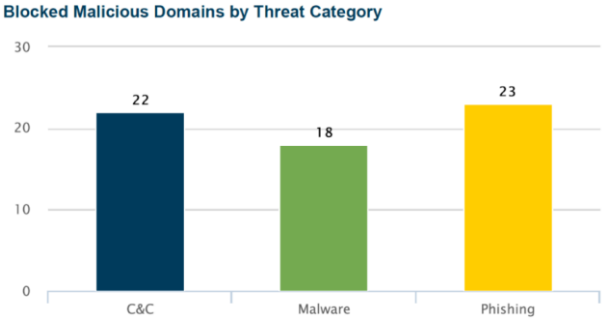
- Severity
- Threat type and category
- Top domains blocked
- Number of blocked requests
- Confidence level (known or suspected)

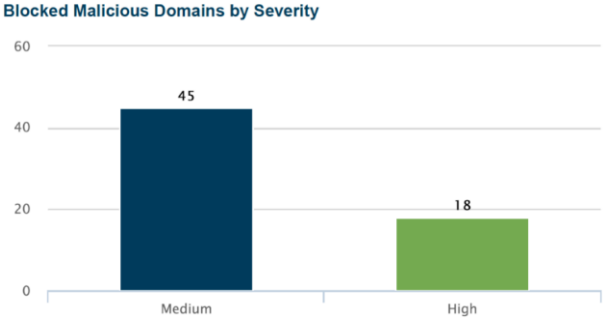
Number of Blocked Requests: 33,518
Description: phishing domains from cyberthreatcoalition
Threat: Corona Phishing, Known CNC
Threat Category: C&C, Phishing

MDBR Reporting









Cyber Incident Response Team (CIRT)

- Incident Response
- Malware Analysis
- Log Analysis

To report an incident or request assistance:

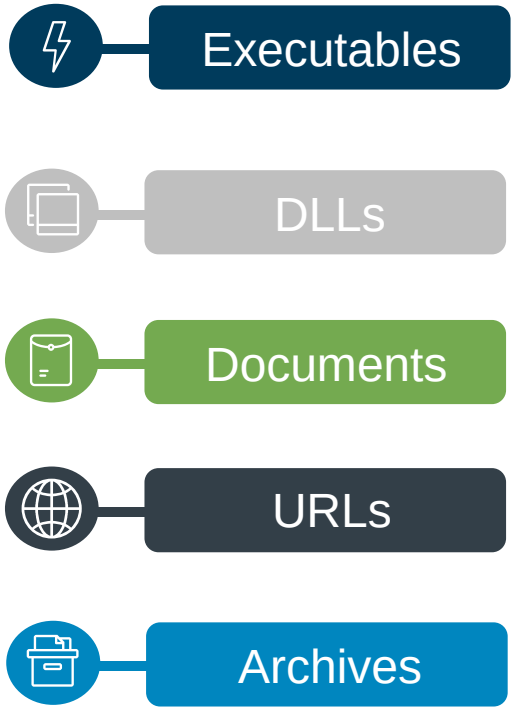
Phone: 1-866-787-4722

Email: soc@cisecurity.org

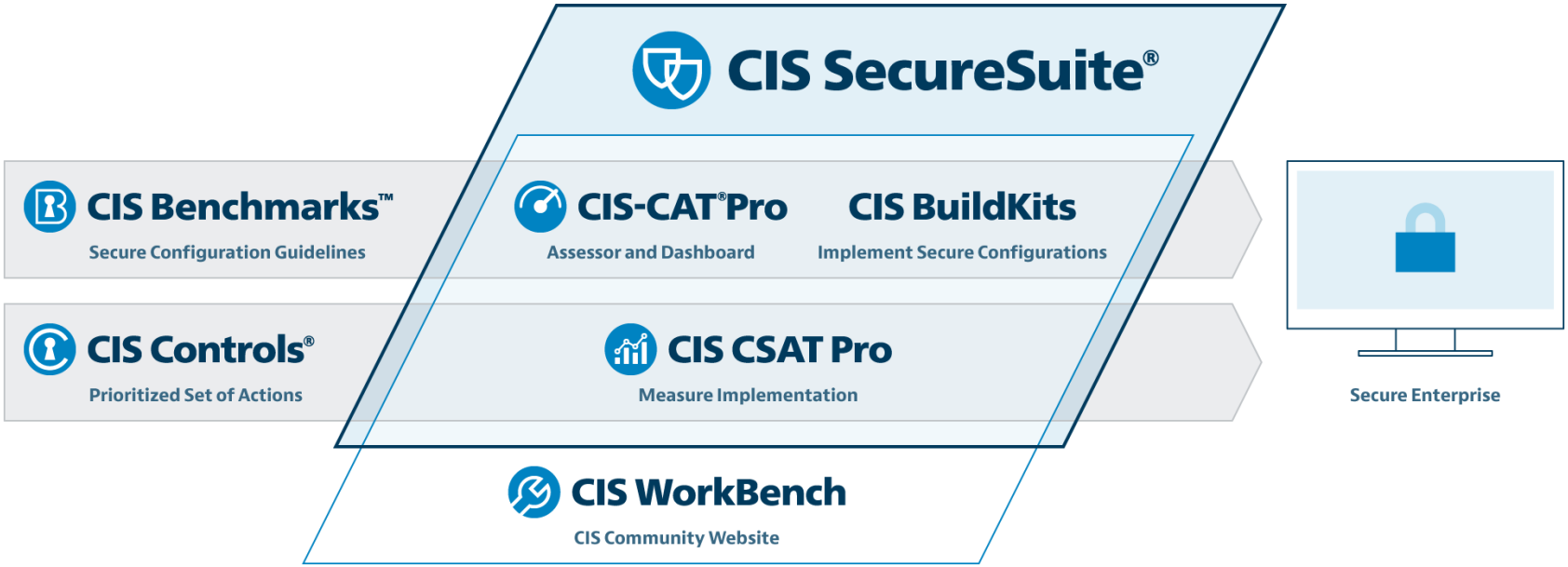
Malicious Code Analysis Platform (MCAP)

A web based service used to submit and analyze suspicious files

To request an account:
mcap@cisecurity.org



CIS SecureSuite Membership



Start Secure. Stay Secure.®

CIS SecureSuite Membership

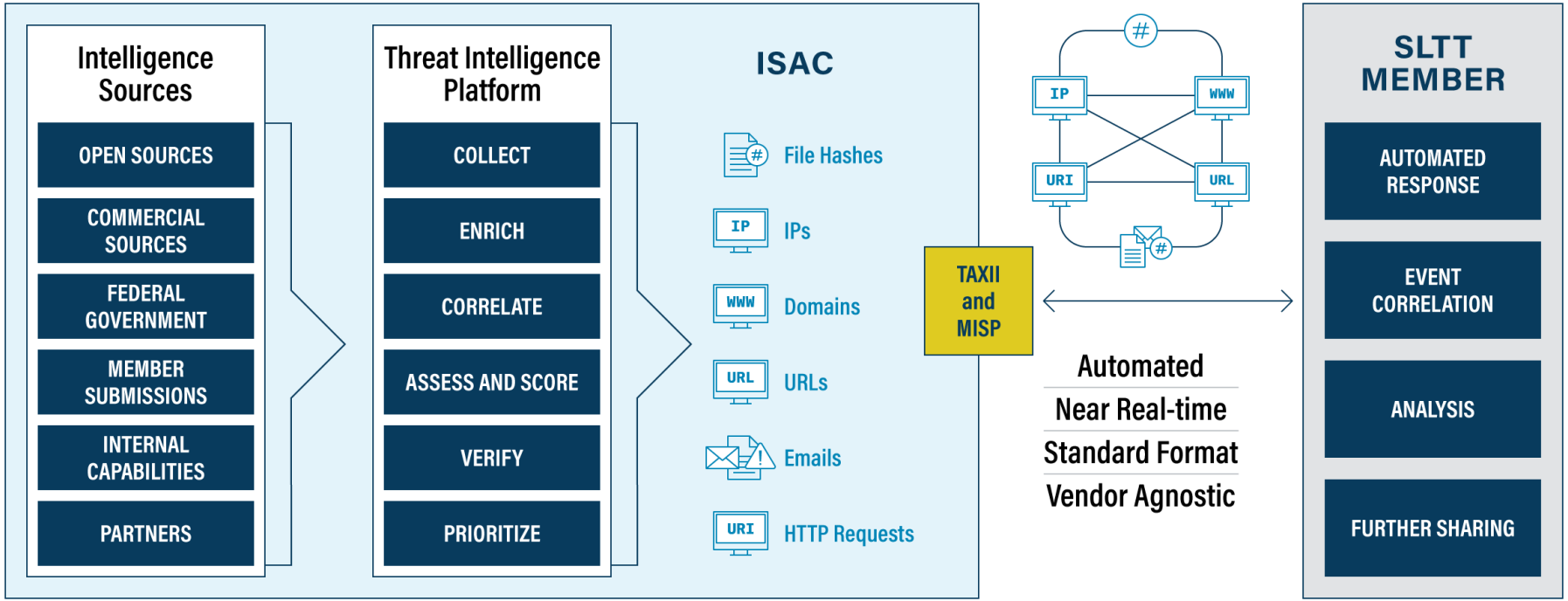
Getting Started is Easy!

1. **Log into CIS Workbench:**
   - https://workbench.cisecurity.org
2. **Download CIS-CAT Pro Assessor to scan against your target system's configuration:**
   - https://workbench.cisecurity.org/files/2151
3. **Learn more – visit the Support Center:**
   - https://workbench.cisecurity.org/support-center

- **Contact Us:**
  - freesecuresuite@cisecurity.org

Indicator Sharing Program

OperationsSupport@cisecurity.org



Foundational Assessment

- **Looking to get started with an assessment? Start here!**
  - 32 question assessment to evaluate essential activities within a cybersecurity program
- **Next Steps**
  - Complete the Nationwide Cybersecurity Review (NCSR) for a wholistic review of your cybersecurity program.

Foundational Assessment

Sign up

- **Request access to the Foundational Assessment:**
  - **foundationalassessment@cisecurity.org**
- **Please include the following details in the email:**
  - Subject: Foundational Assessment Access
  - First Name, Last Name
  - State/Territory
  - Public Organization Name (*i.e. State – ABC County*)
  - Email Address

Nationwide Cybersecurity Review (NCSR)

- Annual, self-Assessment
- NIST Framework
- Cybersecurity Roadmap

For More Information:

https://www.cisecurity.org/ms-isac/services/ncsr

- **2022 NCSR**
  - Currently Open for Registration
  - Available to Complete through February 28, 2023
- **Registration & Resources**
  - Located on NCSR Webpage
  - End-User Guidance
  - Results & Reporting Templates

Best Practice Resources

https://www.cisecurity.org/ms-isac/services/ncsr

Cyber Threat Intelligence Products

Reports

- Assessment Based
- Probability Focused
- Analytic Confidence


MS-ISAC
Multi-State Information Sharing & Analysis Center

Cyber Threat Intelligence
Long-Form Analytic Report

Cyber Threats to the Healthcare Industry

Analysis Across Trends from 2019-2021

February 2021 • LFAR-2021-0002
TLP: WHITE

Executive Summary

Protected health information (PHI) represents highly valuable data for cybercriminals on dark web markets. Constrained financial resources, system sprawl, and varied cybersecurity awareness among staff are primary factors for the majority of healthcare-related breaches. In 2019, attacks against healthcare institutions increased by 75%, and these trends will likely increase due to pandemic-related telework vulnerabilities, increasing integration of innovative technology into legacy systems, and profitable return for exfiltrated data within the healthcare sector. This publication aims to illuminate current targeted data and identify key cybersecurity trends between 2019-2020 to highlight major threats and vulnerabilities for healthcare industries in 2021.

Key Findings

An increase in ransomware campaigns and secondary infections, through long-term campaigns against digital healthcare supply chains, marks a notable shift from 2019-2020. COVID-19 vaccine research makes an attractive target for nation-state cyber threat actors (CTAs), while COVID-19-themed phishing lures offer cybercriminals an opportunity to capitalize on hospitals in need of personal protective equipment (PPE), such as N95 masks.

- Estimated total financial losses for U.S. health systems and facilities at $323.1 billion in 2020. [1]
- Seventy-five percent increase in reports of ransomware attacks on healthcare entities in 2019. [2]
- Stolen medical records can sell for 10 to 20 times more than credit card or social security numbers. [3]
- COVID-19-related phishing attempts increased by 700% worldwide in 2020. [4]

Substantive Analysis

Most successful data breaches stem from human error or adversaries preying upon human behavioral patterns of trust, fear, and urgency. [5] With hospitals and healthcare providers rushing to acquire PPE, contain COVID-19 within their facilities, and minimizing staff to reduce spread, cybercriminals are provided many windows of opportunity to leverage human error. Errors can range from misconfigured systems, susceptibility to phishing, and improperly secured data. The Multi-State Sharing and Analysis Center's (MS-ISAC) Cyber Threat Intelligence (CTI) team assesses with high confidence cybercriminals will likely increase targeting hospitals and healthcare providers in 2021. The CTI team bases this assessment on current reported profitable returns for PHI, [6] wider attack surfaces due to integration of legacy systems with internet-of-things (IoT) devices, increased telemedicine practices; and the cost associated with an inability to care for patients [7] or store limited vaccine supply. [8]

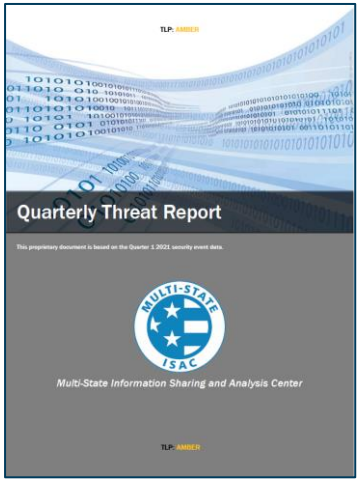
Targeted Data

Medical identity theft, which includes using a victim's personal information to fraudulently obtain medical services or prescriptions alongside standard identity theft actions, represents a critical threat to patients and providers

1

Strategic Assessments

- Deeply Researched
- Forward Looking
- Trends & Patterns


TLP: AMBER

Quarterly Threat Report

This proprietary document is based on the Quarter 1 2021 security event data.

Multi-State Information Sharing and Analysis Center

TLP: AMBER

Briefs & Blogs

- Simple or Complex
- Technically Focused
- Threat Driven


CIS Center for Internet Security

Why TikTok is the Latest Security Threat

TikTok and Data Collection

Collection of PII and User Data

Violations of COPPA

Censorship

What Can Be Done?

MS-ISAC Advisories & Cyber Alerts

MS-ISAC Advisory Michael Aliperti Thu 3:38

UPDATED - MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in F5 BIG-IP and BIG-IQ Products Could Allow for Arbitrary Code Exe...

Retention Policy Default 2 year move to archive (2 years) Expires 3/25/2023

This message was sent with High importance.

Action Items + Get more add-in

TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2021-035 - **UPDATED**

DATE(S) ISSUED:
03/10/2021
03/20/2021 - UPDATED
03/25/2021 - UPDATED

SUBJECT:
Multiple Vulnerabilities in F5 BIG-IP and BIG-IQ Products Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in F5 products, the most severe of which could allow for remote code execution.

- BIG-IP and BIG-IP Advanced WAF/ASM are a family of products covering software and hardware designed around application availability, access control, and security solutions.
- BIG-IQ enables administrators to centrally manage BIG-IP infrastructure across the IT landscape. It discovers, tracks, manages, and monitors physical and virtual BIG-IP devices - in the cloud, on premise, or co-located at your preferred datacenter.

Successful exploitation of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

MS-ISAC® Multi-State Information Sharing & Analysis Center® Cyber Threat Intelligence

MS-ISAC Cyber Alert

Subtitle

February 2021
TLP: LEVEL

Summary

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

- Lorem ipsum dolor sit amet, consectetur adipiscing elit;
- Sed do eiusmod tempor incididunt ut labore et dolore magna aliqua;
- Ut enim ad minim veniam;
- Quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat; and
- Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Analysis

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Indicators of Compromise

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

IPs

x.x.x[.]x – Confirmed C2

Domains

domain[.]com

Hashes

2d75cc1bf8e57872781f9cd04a529256

Monthly Newsletters

Keep cybersecurity at the forefront of your workforces' minds!

- Written for the end-user
- Template Format
- Re-brand & re-distribute as your own

Monthly Cybersecurity Tips Newsletter

October 2022 VOLUME 17, ISSUE 10 • 2022

Protect Your Identity This Cybersecurity Awareness Month

From the desk of Karen Sorady, VP for MS-ISAC Member Engagement

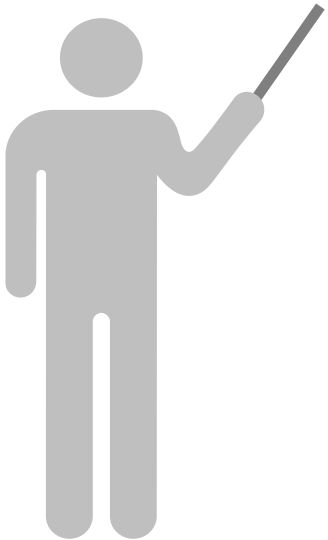
When you log on to a website, make an online payment, send an email, use a social network, post online, or even send a text, you're adding to your online identity. In today's world, it is unavoidable. The good news is there are ways you can protect yourself.

When logging on to a website, look at the address bar on the browser. If you see a padlock icon on the left-hand side of the address, the site is using encryption and verification. Clicking on the padlock shows the site's security certificate. Using only these types of sites ensures you are safely sharing

ISAC Working Groups and Communities

- **Business Resiliency**
- **Metrics**
- **K-12**
- **Leadership Mentoring**
- **Education & Awareness**

Cybersecurity Awareness Month



How Can You Participate?

- Create a Public Awareness Campaign
- Visit: www.cisecurity.org/ms-isac/ms-isac-toolkit

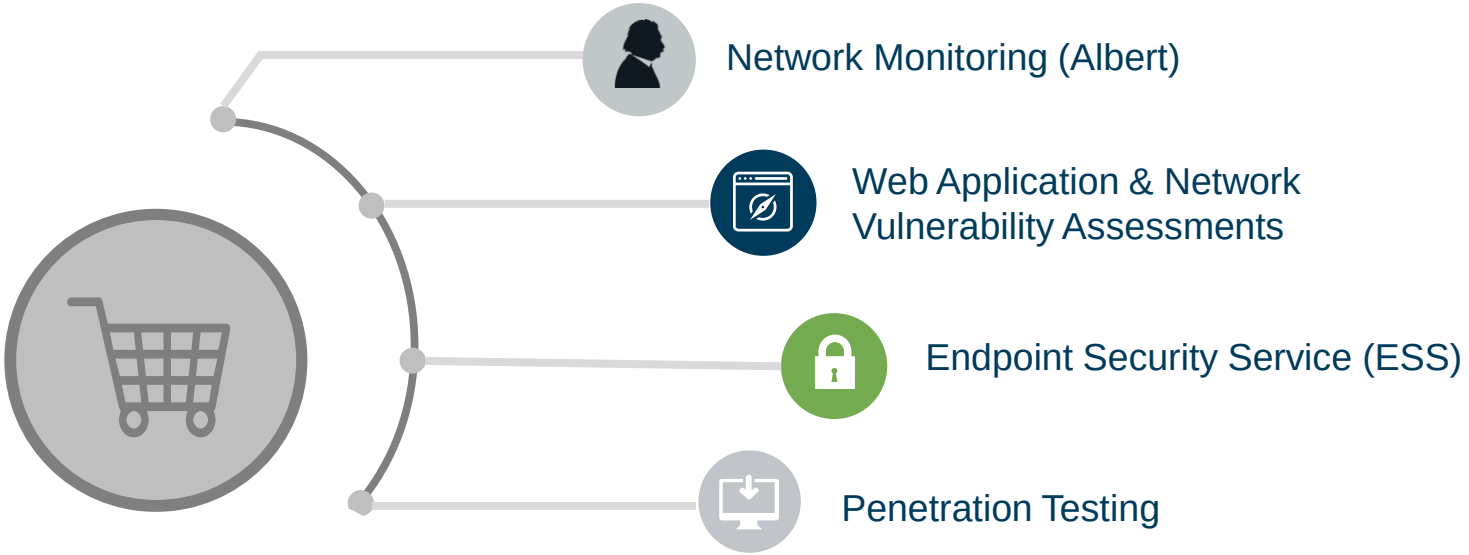
MS-ISAC Toolkit Resources

- Make it Official
- Train Your Staff
- Train the End-User
- Become More Mature
- Bring Security Home
- Best of the Web Contest

For More Information

- Contact: info@cisecurity.org

Fee Based Services



ANY QUESTIONS?

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Elections Infrastructure ISAC®

Thank You!

Security Operations Center
24/7/365
1-866-787-4722
soc@cisecurity.org

Kyle Bryans
Regional Engagement Manager
CISA Regions 4&6
Kyle.Bryans@cisecurity.org
518-880-0747