Cyber Security Resources

2018 NCSL Summit

Paul Hoffman
Program Manager Stakeholder Engagement
There are only two types of companies: those that have been hacked, and those that will be.

- Robert S. Mueller III, Former Director of the FBI

In Hacking, A.P. Twitter Feed Sends False Report of Explosions

April 23, 2014
The Internet
Why SLTT Governments?

Criminals look for data... and governments have a lot of it!
Cyber Threat Actors

- Nation-states
- Terrorists
- Cybercriminals
- Hacktivists
- Insiders
The MS-ISAC has been designated by DHS as the key resource for cyber threat prevention, protection, response and recovery for the nation’s state, local, tribal, and territorial governments

https://www.cisecurity.org/ms-isac/
Members include:

- 50 State Governments
- 79 DHS-Recognized Fusion Centers
- 6 Territorial Governments
- 53 Tribal Governments
- More than 3300 local governments

State, Local, Tribal, and Territorial

Cities, counties, towns, airports, public education, police departments, ports, transit associations, and more
Members include:

- 50 State Elections Offices
- 3 Territorial Elections Offices
- 5 Public Elections Associations
- Over 800 Local Elections Offices
About MS-ISAC Membership

Free and Voluntary
No Mandated Information Sharing
One Membership Document Required

Benefits:
• Access to information, intelligence, products, resources, and webcasts
• Insider access to federal information
• Training and resource discounts
• DHS HSIN Portal access
• Cybersecurity exercise participation
• Malicious Code Access Program (MCAP) access

To join or get more information:
www.cisecurity.org/ms-isac/
24x7 Security Operations Center

Central location to report any cybersecurity incidents

• **Support:**
  – Network Monitoring Services
  – Research and Analysis
  – Incident Response

• **Analysis:**
  – Threats & Trends
  – Vulnerabilities
  – Attacks & TTPs
  – Cyber Threat Actor Activity

• **Reporting:**
  – Cyber Alerts & Advisories
  – IP & Domain Monitoring
  – Automated Indicator Sharing
  – Strategic Intelligence

To report an incident or request assistance:
  **Phone:** 1-866-787-4722
  **Email:** soc@msisac.org
Intelligence Sources

- 24x7 monitoring
- Analysis of more than 2 trillion logs/month
- Integration with federal agencies via the NCCIC
- Trusted private companies
- Constant contact with all ISACs

Information Sharing and Analysis Centers
CERT

Computer Emergency Response Team

- Incident Response
- Malware Analysis
- Computer & Network Forensics
- Log Analysis

To report an incident or request assistance:

Phone: 1-866-787-4722
Email: soc@msisac.org
to join or get more information:

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

1-866-787-4722
SOC@cisecurity.org

Paul Hoffman
MS-ISAC Program Manager
518-880-0768
Paul.hoffman@cisecurity.org
Who do I call?

Security Operations Center (SOC)
SOC@cisecurity.org - 1-866-787-4722
31 Tech Valley Dr., East Greenbush, NY 12061-4134
www.cisecurity.org

to join or get more information:
https://learn.cisecurity.org/ms-isac-registration
VMP
Vulnerability Management Program

Notifies members on a monthly basis about any outdated software that could pose a threat to assets.

Analysis & review categories

Not Vulnerable
• System’s patch level is current for vulnerabilities

Vulnerable
• System is not up-to-date
• Provides CVE score and links to the CVE

soc@msisac.org
Port Profiler

• MS-ISAC will connect to 12 common ports on public IPs provided for our monitoring program.
  – Services: FTP, SSH, HTTP(S), SMB, RDP, VNC, SQL, and MongoDB
  – 21, 22, 23, 25, 80, 139, 443, 445, 1433, 8080, 3306, 3389, 5432, 5900, 27017

• Services are identified by reading the banner information once we connect.
  – We seek predetermined keywords in the banner information that then allows us to tag hosts or services that need a second look for if they need to be public facing.
• Quarterly notifications

• Contact vmp.dl@ciscosity.org to:
  • Opt out of this service
  • Provide feedback on the Port Profiler

• Contact soc@ciscosity.org if:
  • You wish to add IP addresses
  • To verify “VMP Notification” contacts

• Source IP address: 52.14.79.150
A web-based service, which allows members to submit files and IOCs for analysis in a controlled and non-public fashion

Submit:
- Executables
- DLLs
- Documents
- Quarantine files
- Archives
- Domains

Analyze:
- Domains
- IP addresses
- URLs
- Hashes
- IOCs

https://www.cisecurity.org/ms-isac/services/
Notifications for IP Ranges & Domains

**IP Notifications**
- IPs connecting to sinkholed C2s
- Compromised IPs
- Indicators of compromise from MS-ISAC network monitoring

**Domain Notifications**
- Notifications on compromised user credentials, open source, and third party information
- Vulnerability Management Program (VMP)

Send domains, IP ranges, and contact info to: soc@msisac.org

Any SLTT Government   TLP: WHITE
Weekly Malware IPs and Domains

Automated Threat Indicator Sharing via Anomali

Attached to this email is a list of IP addresses and domains associated with the MS-ISAC.

Recipients may only share TLP: GREEN information with peers and partner organizations within their sector or country.

This list is produced from data collected by the MS-ISAC. Currently, this data is being collected across a number of States and Localities.

The spreadsheet contains four tabs with the following information:

1. Malware IP Data

   IP Address – This is either the IP address that is attacking a system or the IP address malware on an infected system is coming from.

   Counts – This is the number of alerts generated for malicious traffic to or from the IP address.

   Country, Region, City – Location of the potentially malicious IP address.

To gain an Anomali account contact:

VMP@cisecurity.org
Anomali

Machine-to-Machine indicator transfer

Two free Threatstream accounts

To gain an account contact: indicator.sharing@cisecurity.org
CIS SecureSuite Membership

- CIS-CAT Pro Assessor
  - 80+ CIS Benchmarks
- CIS-CAT Pro Dashboard
  - Controls View
  - System Tagging
  - Exception Reporting
- CIS Controls Library
- CIS Technical Support

- CIS WorkBench
- Distribute SecureSuite Resources
- Remediation Content
  - GPOs, Linux Scripts
- CIS Benchmarks, w/ artifacts
  - Word, Excel, OVAL, XML, etc.

https://www.cisecurity.org/cis-securesuite/
MS-ISAC Cyber Alerts

TO: All MS-ISAC Members, Fusion Centers, and Intel Partners

DATE: January 12, 2017

SUBJECT: Increase in SLTT Government Owned WebLogic Server Compromises

The MS-ISAC has observed an increase in exploitation of CVE-2017-10271 against state, local, tribal, and territorial (SLTT) government Oracle WebLogic servers, which results in complete compromise of the server by the cyber threat actor. Currently, the MS-ISAC is identifying exploitation for the purposes of monetization through Monero miners and is aware of open source reporting indicating the use of other cryptocurrency miners. However, the nature of the exploit does not prohibit other uses and it is important to note that PeopleSoft software is often run on WebLogic servers.

Depending on privileges assigned to the WebLogic webservers, cyber threat actors could use the initial compromise to gain a foothold in an organization’s PeopleSoft server environment. PeopleSoft is a software suite widely used to handle a range of tasks from human resources to financial planning. These servers may contain employees’ sensitive personally identifiable information (PII), electronic personal health information (ePHI), and financial information that will be exposed in the event of a compromise.

CVE-2017-10271 bypasses a security feature built into WebLogic servers, which was patched in the October 2017 Oracle Quarterly Update. Systems running WebLogic versions prior to 12.2.1.2.171017, 12.2.1.1.171017, 12.1.3.0.171017, 10.3.6.0.171017 are vulnerable.

Cryptocurrency miners are malware trojans that use a compromised system’s resources in order to generate revenue for an actor. This use causes the computer to run slower, which can lead to stuttering or freezing during intense resource use. It also causes the CPU to run at above average temperatures for extended periods of time, which could shorten the life of the CPU.

Indicators of Compromise (IOC):
- Files: watch-smartd, xlog-daemon, carbon, default, rcp_bh, watch-smartd1, infoed, xfsallocd, content, and localfile-
- MD5: faca70429c736cbf0caf2c3a4622078f
- SHA-1: f79a2ba735a988fa5f5998e1f3d39684727bdc4

Recommendations:
- Apply patch 12.2.1.3 provided by Oracle to vulnerable systems immediately after appropriate testing.
- If you believe that cryptocurrency mining may be occurring on your network, check for abnormally high resource use, and suspicious files and log entries. The SANS ISC feed contains IP addresses of known miner pools for correlation efforts.
From: MS-ISAC Advisory
To: Thomas Duffy
Cc: 
Subject: MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in DotNetNuke Could Allow for Remote Code Execution

MS-ISAC ADVISORY NUMBER:
2017-085

DATE(S) ISSUED:
09/19/2017

SUBJECT:
Multiple Vulnerabilities in DotNetNuke Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in DotNetNuke (DNN), which is a content management system. These vulnerabilities, if exploited, could allow malicious code to be uploaded. Successful exploitation of these vulnerabilities could allow an attacker to delete data; or create new accounts with full user rights. Users whose data could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There have been no reports of these vulnerabilities being exploited in the wild.
HSIN Community of Interest

Access to:
- MS-ISAC Cyber Alert Map
- Archived webcasts & products
- Table top exercises
- Guides and templates
- Sector specific message boards
Nationwide Cyber Security Review

NCSR

A voluntary self-assessment survey designed to evaluate cyber security management within SLTT governments

All states (and agencies within), local government jurisdictions (and departments within), tribal and territorial governments can participate.

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

TLP: WHITE
• Collaborative Purchasing
  – End-User Security Awareness Training
  – Advanced Technical Training Courses & Degree Programs
  – Consulting Services
  – Two-Factor Authentication
  – Cloud Access Security Management

• Over $40 million in savings for our members

• Learn more at www.cisecurity.org/services/cis-cybermarket or contact info@cisalliance.org
Education and Awareness Resources
Monthly Newsletter

Distributed in template form to allow for rebranding and redistribution by your agency

https://www.cisecurity.org/resources/newsletter/
National Webcasts

A collaborative effort between DHS and MS-ISAC to provide timely and relevant cybersecurity education and information

- Cybersecurity While Traveling (February 2017)
- Cybersecurity Year in Review and 2017 Preview (December 2016)
- National Cybersecurity Awareness Month – Be a Part of Something Big (October 2016)
- State and Local Roundtable – Effective Cyber Disruption Strategies (August 2016)
- Prioritize Your NIST CSF Implementation with the CIS Critical Security Controls (June 2016)

https://msisac.cisecurity.org/webcast/
FedVTE

Free Online Training Environment

- CompTIA A+, Network+, Security+
- CISSP Certification Prep
- Operating System Security

www.fedvte.usalearning.gov
Cybersecurity Awareness Toolkit

- Be careful of what you post!
- Beware of online predators!
- Watch out for phishing messages!
- Protect your devices!

2017 MS-ISAC Cybersecurity Calendar

New Jersey – Ashley, Grade 7
MS-ISAC Workgroups

Cyber Security Metrics
Business Continuity, Recovery and Cyber Exercise
Intel & Analysis
Mentoring Group
Education and Awareness

New Jersey – Ashley, Grade 7
2017 MS-ISAC Cybersecurity Calendar
Fee Based Services

https://www.cisecurity.org/ms-isac/services/
Fee Based Services

- Network monitoring (Albert)
- Web application vulnerability assessments
- Network vulnerability assessments
- Penetration testing
- Phishing engagements

For more info on any of these contact:
info@msisac.org
Network Monitoring (Albert)

• SLTT focus
• 24x7x365 research, analysis, and support
• Signatures unique to SLTT governments
• Integration of research on specific attacks and actors, including nation-state actors (APT)
• Real-time information sharing with FSLTT partners
• Experienced cybersecurity analysts who review each event minimizing the number of false-positive notifications
NCSAM Awareness Programs

• Governors’ proclamations
  – Seeking official displays of State level support for NCSAM

• Best of the Web Contest – State and Local
  – All States participate as a default
  – All Local, Tribal, Territorial, Authority etc. entities are welcome to compete