Cyber Threats and Federally-funded Cyber Resources

Eugene Kipniss
State, Local, Tribal, or Territorial Government Entity

CIS SecureSuite

MS-ISAC
Multi-State Information Sharing & Analysis Center

Elections Infrastructure
ISAC
Why SLTT Governments?

Criminals look for data... and governments have a lot of it!
In 2018, both the state and local peer groups reported a decrease in overall maturity (-1% for the state peer group and -4% for the local peer group). This is a reversal of the trend that was reported in 2016 and 2017, where the state and local peer groups reported an increase in overall maturity (3% and 10% respectfully).

Local governments continue to report lower overall maturity scores (3.44) than their state counterparts (4.70).

Tribal governments continue to report lower overall maturity scores (3.33) than both their state and local counterparts.

In 2018 the tribal peer group reported a 48% increase in overall maturity.

State, local and tribal peer groups continue to report overall scores that fall below the recommended minimum maturity level (5).

In 2018, 88% of the 33 sub-sector peer groups reported scores below the recommended minimum maturity level. The following sub-sector peer groups met the minimum maturity:

- Associations
- State Finance/Revenue
- State Information Technology
- State Museum

All peer groups continue to identify the same top five security concerns over the past four years:

- Lack of sufficient funding*
- Increasing sophistication of threats
- Lack of documented processes
- Emerging technologies
- Inadequate availability of cybersecurity professionals

* In 2018, we saw a shift in the order the top five security concerns were ranked. Lack of sufficient funding became the number one security concern.

In 2018, Supply Chain was added to the Identify function of the NIST Cybersecurity Framework and NCSR question set. The state and local peer groups scored lowest in the supply chain category within the identify function.
<table>
<thead>
<tr>
<th>January 2018</th>
<th>February 2018</th>
<th>March 2018</th>
<th>April 2018</th>
<th>May 2018</th>
<th>June 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kovter</td>
<td>Kovter</td>
<td>Kovter</td>
<td>Kovter</td>
<td>Kovter</td>
<td>WannaCry</td>
</tr>
<tr>
<td>WannaCry</td>
<td>WannaCry</td>
<td>Emotet</td>
<td>ZeuS</td>
<td>ZeuS</td>
<td>Emotet</td>
</tr>
<tr>
<td>Emotet</td>
<td>Emotet</td>
<td>ZeuS</td>
<td>Emotet</td>
<td>NanoCore</td>
<td>Kovter</td>
</tr>
<tr>
<td>ZeuS</td>
<td>ZeuS</td>
<td>Redyms</td>
<td>CoinMiner</td>
<td>Redyms</td>
<td>ZeuS</td>
</tr>
<tr>
<td>CoinMiner</td>
<td>NanoCore</td>
<td>TinyLoader</td>
<td>NanoCore</td>
<td>Mirai</td>
<td>Mirai</td>
</tr>
<tr>
<td>Gh0st</td>
<td>CoinMiner</td>
<td>CoinMiner</td>
<td>Xtrat</td>
<td>CoinMiner</td>
<td>Cerber</td>
</tr>
<tr>
<td>NanoCore</td>
<td>Gh0st</td>
<td>NanoCore</td>
<td>Redyms</td>
<td>WannaCry</td>
<td>NanoCore</td>
</tr>
<tr>
<td>Ursnif</td>
<td>Qarallex</td>
<td>Gh0st</td>
<td>WannaCry</td>
<td>Emotet</td>
<td>CoinMiner</td>
</tr>
<tr>
<td>Mirai</td>
<td>Latentbot</td>
<td>WannaCry</td>
<td>Mirai</td>
<td>Gh0st</td>
<td>Gh0st</td>
</tr>
<tr>
<td>Redyms</td>
<td>Mirai</td>
<td>Cerber</td>
<td>Gh0st</td>
<td>Latentbot</td>
<td>Xtrat</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>July 2018</th>
<th>February 2018</th>
<th>September 2018</th>
<th>October 2018</th>
<th>November 2018</th>
<th>December 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emotet</td>
<td>Kovter</td>
<td>Emotet</td>
<td>Emotet</td>
<td>WannaCry</td>
<td>WannaCry</td>
</tr>
<tr>
<td>Kovter</td>
<td>Emotet</td>
<td>WannaCry</td>
<td>Kooter</td>
<td>Emotet</td>
<td>ZeuS</td>
</tr>
<tr>
<td>ZeuS</td>
<td>ZeuS</td>
<td>Kovter</td>
<td>ZeuS</td>
<td>ZeuS</td>
<td>Emotet</td>
</tr>
<tr>
<td>NanoCore</td>
<td>CoinMiner</td>
<td>ZeuS</td>
<td>WannaCry</td>
<td>Kovter</td>
<td>Kovter</td>
</tr>
<tr>
<td>Cerber</td>
<td>WannaCry</td>
<td>CoinMiner</td>
<td>NanoCore</td>
<td>CoinMiner</td>
<td>Qakbot</td>
</tr>
<tr>
<td>Gh0st</td>
<td>NanoCore</td>
<td>NanoCore</td>
<td>Gh0st</td>
<td>Mirai</td>
<td>Samsam</td>
</tr>
<tr>
<td>CoinMiner</td>
<td>Mirai</td>
<td>Gh0st</td>
<td>CoinMiner</td>
<td>NanoCore</td>
<td>Gh0st</td>
</tr>
<tr>
<td>Trickbot</td>
<td>Gh0st</td>
<td>Mirai</td>
<td>Mirai</td>
<td>Gh0st</td>
<td>Mirai</td>
</tr>
<tr>
<td>WannaCry</td>
<td>Cerber</td>
<td>Trickbot</td>
<td>Ursnif</td>
<td>Smoke Loader</td>
<td>Brambul</td>
</tr>
<tr>
<td>Xtrat</td>
<td>Ursnif</td>
<td>AZORult</td>
<td>Smoke Loader</td>
<td>Ursnif</td>
<td>CoinMiner</td>
</tr>
</tbody>
</table>
Top 10 Malware - Initiation Vectors

- Dropped
- Multiple
- Malspam
- Network
- Maladvertisement
BEC: CEO Compromise Example

Date:
FROM: CEO
TO: Finance Department
SUBJECT: Question

Are you available? Wire transfer needs to go out. Also what is the balance of General Funding Account? Let me know when you are ready.

Don’t call. I’m in a meeting.

Sent from my iPhone

From an Executive
To Finance

Sense of urgency
Formatting error
Social Engineering
Ransomware

malware that blocks access to a system, device, or file until a ransom is paid; commonly demand that the victim pays $200 - $1,000 in bitcoins, gift cards, etc.

1. Lockers – blocks access to files or the system
2. Cryptos – encrypts files
3. Wipers – erases files; no recovery
Emotet

- Emotet is the single most destructive piece of malware currently affecting state, local, tribal, and territorial (SLTT) governments in the U.S.
- Highly infectious due to worm-like capabilities
- Infostealer
- Modular
- Business continuity disaster
- Potential data breach
TrickBot

• Modular banking trojan that targets user financial information and acts as a dropper for other malware.
  – Man-in-the-browser attacks
  – Continuously releasing new modules/versions
  – Malspam campaigns or dropped
  – Some modules abuse SMB Protocol for lateral movement

https://www.cisecurity.org/white-papers/security-primer-trickbot/
Cryptocurrency Miners

Malware:
• CoinMiner – TOP 10
• Coinhive
• WannaMine
• Dark Test
• BrowseAloud

Infection Vectors:
• Malspam
• EternalBlue
• Exploit Kits
• Worms
• Tech Support Scam
• Plugins

• Masquerading as Windows/system files, Fake AV, apps
• Fileless malware
• Infecting: Windows, Mac, smartphones, smartTVs, SCADA systems
Insider Crypto-mining

New York City Government Punishes Employee For Mining Bitcoin at Work

Harvard Student Uses 14,000-Core Supercomputer to Mine Dogecoin

Florida State Employee Arrested for Allegedly Mining Crypto at Work

Federal Reserve Employee Mines Bitcoin Using the Fed’s Server

PSA: Don't mine cryptocurrency on government computers
Theft of Currency and Wallets

SIM Swapping/Jacking

Joel Ortiz and the $5 Million SIM heist

- Attacker does recon of social media etc.
- Next they contact the mobile carrier
- Socially engineer a SIM re-issue or change
- Reset email accounts using phone verification
- Intercept all communication – including 2FA!
Hoax Extortion Schemes

SAMPLE EMAIL TEXT

Subject: <username> - <password>

I'm aware, <password>, is your pass word. You do not know me and you are most likely wondering why you are getting this e-mail, correct?

In fact, I actually placed a malware on the adult video (porno) web site and guess what, you visited this site to experience fun (you know what I mean).

While you were watching video clips, your browser initiated operating as a RDP (Remote Desktop) that has a key logger which provided me accessibility to your display and web cam. Immediately after that, my software gathered all of your contacts from your Messenger, Facebook, and email.

What exactly did I do?

I made a double-screen video. 1st part displays the video you were viewing (you’ve got a fine taste lol . . .), and next part displays the recording of your cam.

What should you do?

Well, I believe, <extortion amount> is a reasonable price tag for our little secret. You’ll make the payment by Bitcoin (if you do not know this, search "how to buy bitcoin" in Google).

BTC Address: <address>
(It is case sensitive, so copy and paste it)

Emails can include user’s:
- Names
- Passwords
- Emails
- Telephone numbers

Spoofing the victim’s email
Employee Mistakes
Why care? - Employee Mistakes
Who We Serve

- 50 State Governments
- >5,500 Local Governments
- 6 Territorial Governments
- 81 Tribal Governments
- 79 DHS-recognized Fusion Centers

K-12 School Districts, Intermediate Units
Law Enforcement, Cities, Public Authorities
950 K-12 School Districts across US
Any Public Organizations

Local Governments
How to access MS-ISAC resources

- Register for the MS-ISAC’s services here: [https://learn.cisecurity.org/ms-isac-registration](https://learn.cisecurity.org/ms-isac-registration)

- The MS-ISAC Stakeholder Engagement team will provide you with next steps:
  - Register your HSIN account
  - Submit public IPs, domains, and subdomains
  - Register for an MCAP account
  - Add additional staff to your account
24 x 7 Security Operations Center

Central location to report any cybersecurity incident

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

• **Analysis and Monitoring:**
  – Threats
  – Vulnerabilities
  – Attacks

• **Reporting:**
  – Cyber Alerts & Advisories
  – Web Defacements
  – Account Compromises
  – Hacktivist Notifications

To report an incident or request assistance:

**Phone:** 1-866-787-4722  
**Email:** soc@cisecurity.org
Computer Emergency Response Team

- Incident Response (includes on-site assistance)
- Network & Web Application Vulnerability Assessments
- Malware Analysis
- Computer & Network Forensics
- Log Analysis
- Statistical Data Analysis

To report an incident or request assistance:

Phone: 1-866-787-4722
Email: soc@cisecurity.org
Monitoring of IP Range & Domain Space

**IP Monitoring**
- IPs connecting to malicious C&Cs
- Compromised IPs
- Indicators of compromise from the MS-ISAC network monitoring (Albert)
- Notifications from Spamhaus

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

Send domains, IP ranges, and contact info to: soc@cisecurity.org
Vulnerability Management Program

Web Profiler

- Server type and version (IIS, Apache, etc.)
- Web programming language and version (PHP, ASP, etc.)
- Content Management System and version (WordPress, Joomla, Drupal, etc.)

Email notifications are sent with 2 attachments containing information on out-of-date and up-to-date systems:

- Out-of-Date systems should be patched/updated and could potentially have a vulnerability associated with it
- Up-to-Date systems have the most current patches
Vulnerability Management Program

Port Profiler

- 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
Malicious Code Analysis Platform

A web based service that enables members to submit and analyze suspicious files in a controlled and non-public fashion

- Executables
- DLLs
- Documents
- Quarantine files
- Archives

To gain an account contact: mcap@cisecurity.org
SecureSuite

- **Workbench**
  - Platform for creating and maintaining resources
  - [https://workbench.cisecurity.org](https://workbench.cisecurity.org)

- **Controls**
  - Prioritized set of actions to protect your organization and data from known cyber attack vectors

- **Benchmarks**
  - Well-defined, un-biased, consensus-based industry best practices

- **CIS-CAT Pro**
  - Configuration and Vulnerability Assessment Tool
  - Assessor and Dashboard can be downloaded from Workbench
HSIN Community of Interest

Access to:

• MS-ISAC Cyber Alert Map
• Archived webcasts & products
• Cyber table top exercises
• Guides and templates
• Message boards
Weekly Malware IPs and Domains

Automated Threat Indicator Sharing via Anomali

To gain an Anomali account contact:
Indicator.sharing@cisecurity.org
TO: All MS-ISAC Members, Fusion Centers, and IIC partners

DATE ISSUED: June 16, 2016

SUBJECT: Malicious Email Campaign Targeting Attorneys Spoofs Emails From Statewide Legal Organizations - TLP: WHITE

In June 2016 MS-ISAC became aware of a malicious email campaign targeting attorneys, which spoofs emails from statewide legal organizations, such as the Bar Association and the Board of Bar Examiners. The subject and body of the emails include claims that “a complaint was filed against your law practice” or that “records indicate your membership dues are past due.” Recipients are asked to respond to the claims by clicking a link which leads to a malicious download, potentially ransomware.

The emails are well written and appear to originate from the appropriate authority, such as an Association official, likely increasing their effectiveness. Reporting from various states indicates a likelihood that this campaign is personalized to individuals practicing in a particular state and may be progressing on a state-by-state basis. The following states have been referenced in public reporting on this campaign: Alabama, California, Florida, Georgia, and Nevada. This targeting may include attorneys working for state, local, tribal, and territorial (SLTT) governments.

Recommendations:
MS-ISAC recommends the following actions:

• Share this information with potentially impacted organizations your area of responsibility, including Departments of Law/Justice, related law enforcement agencies, and agency-specific offices of counsel.
• Train government legal professionals in identifying spear phishing emails which may include spoofed email addresses, unusual requests, and questionable and/or masked links. This particular series of emails includes what appears to be a link to the state bar association, but when the user hovers over the link it shows that the link is really to a different website. Copying and pasting the link, instead of clicking on it, would defeat this social engineering attempt.
• Perform regular backups of all systems to limit the impact of data loss from ransomware infections. Backups should be stored offline.
MS-ISAC Advisories

**DATE(S) ISSUED:**
10/13/2015
10/15/2015 - Updated

**SUBJECT:**
Multiple Vulnerabilities in Adobe Flash Player Could Allow for Remote Code Execution

**OVERVIEW:**
Multiple vulnerabilities in Adobe Flash Player could allow remote code execution. Add experience when visiting web pages or reading email messages. Successful exploitation of this vulnerability could allow an attacker to compromise an affected system.

**THREAT INTELLIGENCE:**
There are currently no reports of these vulnerabilities being exploited in the wild.

October 15 - UPDATED THREAT INTELLIGENCE
Adobe is aware of a report that an exploit for the CVE-2015-7644 critical vulnerability was reported to Adobe in early October 2015. The public release of a working exploit was reported on October 15, 2015.

**Note:** This advisory is part of the MS-ISAC Cybersecurity Advisories series.

**Additional Information:**
- **MS-ISAC Cybersecurity Advisories:**
  - [Link to MS-ISAC Cybersecurity Advisories]

**Contact:**
Thomas Duffy
Tel: 703-323-1700

**TLP:**
WHITE
Day in and day out, employees hear the same things from their IT staff about cybersecurity and safety. Though they may sound like a broken record, there are very important reasons and rationale behind these practices and advice. Keeping safe and secure while connected isn't just about how your system is set up - it is also very much about how you end up using it. Below, we discuss some common IT staff wisdom and provide some background information and the rationale as to why it definitely merits your attention.

**Make sure you lock your screen when you are away from your desk.**

Screen locking policies exist for a reason. Even if you are leaving for just a few minutes at a time, be sure to lock your screen. Though physical intruders are rare during daytime and in conventionally secured offices, intrusions do occasionally happen. Screen locks also thwart opportunistic insider attacks from other employees that may seek to obtain information or access information beyond what they should normally have. If you don't adhere to a screen locking policy, an attacker can simply walk up and start manipulating or stealing your...
FedVTE

Free Online Training Environment

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

www.fedvte.usalearning.gov
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
MS-ISAC 24x7 Security Operations Center
1-866-787-4722
SOC@cisecurity.org

info@msisac.org

Eugene Kipniss
Program Manager
MS-ISAC
518.880.0716
Eugene.Kipniss@cisecurity.org