



# Information Sharing Resources for Municipal Utilities

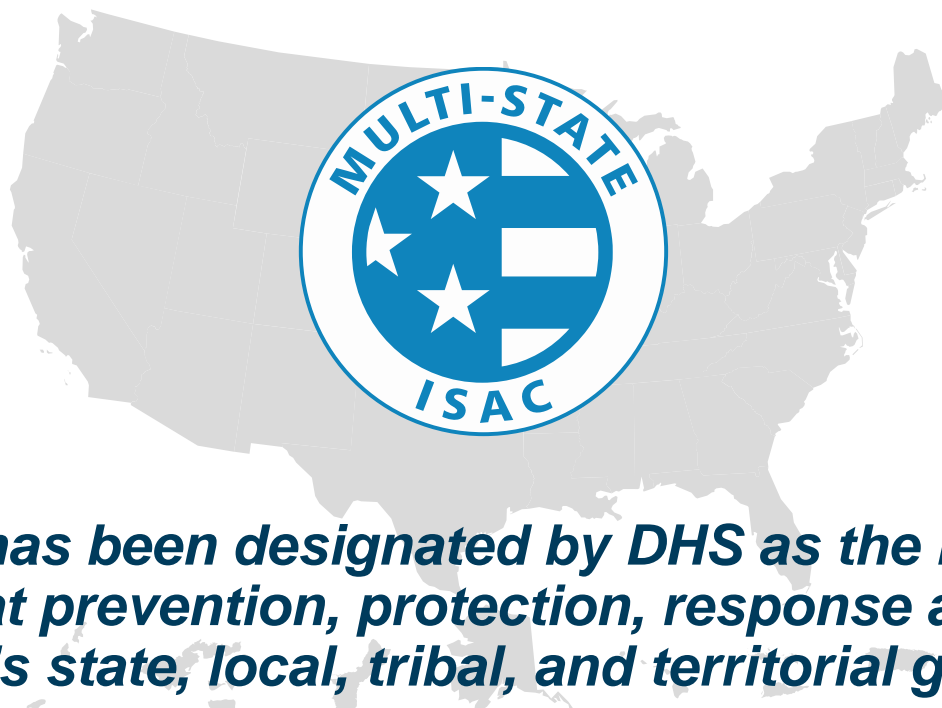
**Kyle Bryans**  
**Program Specialist**  
**MS-ISAC**



---

## Multi-State Information Sharing and Analysis Center

---



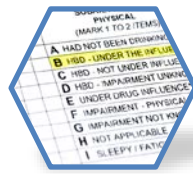
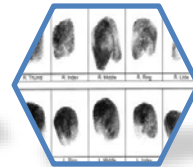
*The MS-ISAC has been designated by DHS as the key resource for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal, and territorial governments*

<https://www.cisecurity.org/ms-isac/>



# Why SLTT Governments?

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





# Why care? - Employee Mistakes

---







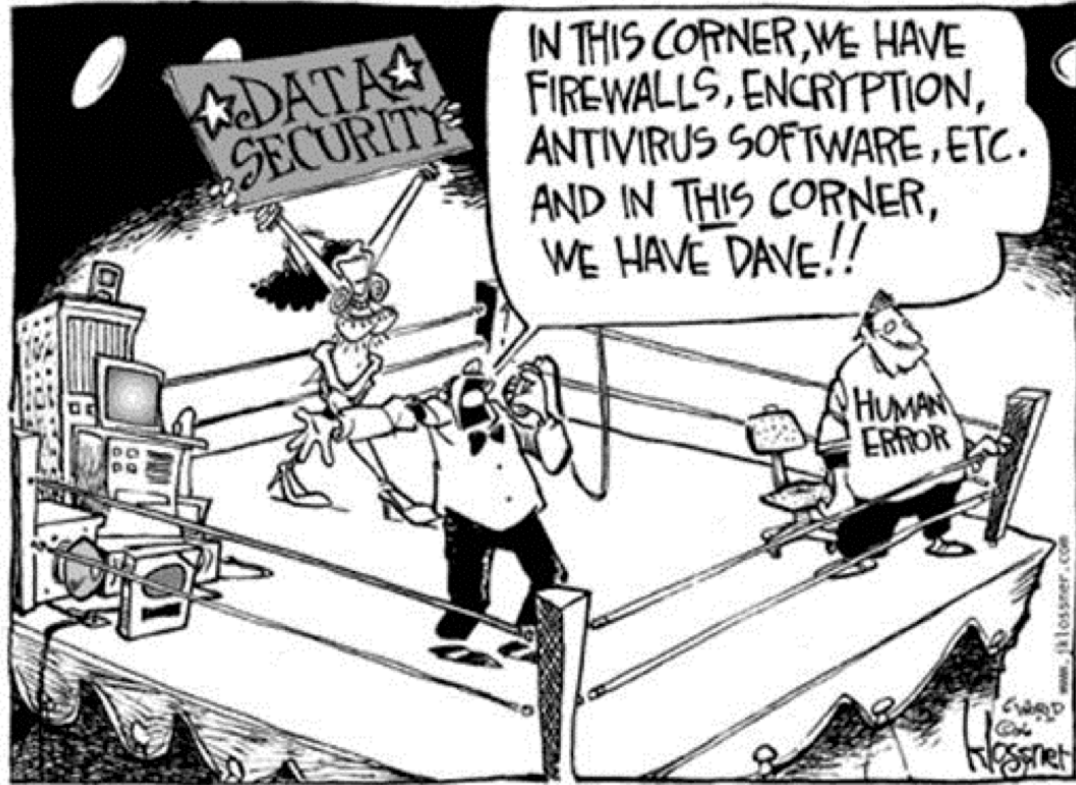
# Why care? - Employee Mistakes



TLP: GREEN



# Why care? – Employee Mistakes





# 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](mailto:soc@cisecurity.org)



# Network Monitoring (Albert)

---

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



**Albert**  
CIS Network Monitoring





# 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)

Send domains, IP ranges,  
and contact info to:  
**[soc@cisecurity.org](mailto: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](mailto:soc@cisecurity.org)



# CIS SecureSuite

 **CIS SecureSuite<sup>®</sup>**  
Membership

 **CIS WorkBench**  
| CIS Community Website & Access Member Resources |

 **CIS Controls<sup>™</sup>**  
| Secure Organization |

 **CIS Benchmarks<sup>™</sup>**  
| Secure Platforms |

 **CIS-CAT Pro**  
| Assess, Remediate, & Maintain |



Improve cybersecurity posture  
with resources included in  
CIS SecureSuite Membership.

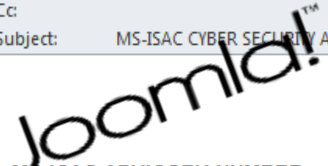
*Start Secure. Stay Secure.<sup>®</sup>*



# MS-ISAC Advisories



This message was sent with High importance.  
 From: MS-ISAC Advisory  
 To: Thomas Duffy  
 Cc:  
 Subject: MS-ISAC CYBER SECURITY ADVISORY - Multiple Vulnerabilities in Adobe Flash Player Could Allow for Remote Code Execution



MS-ISAC ADVISORY NUMBER:  
 2015-119 - UPDATED

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. An attacker could gain access to confidential data, compromising processing resources in a user's computer, or remotely execute code on the user's computer.

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-2015-7645 critical vulnerability was used to compromise a user's computer.

TLP: WHITE  
 MS-ISAC CYBER SECURITY ADVISORY



chrome

**2017 MS-ISAC Cybersecurity Advisories**

**March 2017**

- #2017-028 » Thursday, March 16, 2017  
[Multiple Vulnerabilities in Drupal Could Allow for Remote Code Execution](#)
- #2017-027 » Tuesday, March 14, 2017  
[Multiple Vulnerabilities in Microsoft Office Could Allow for Remote Code Execution \(MS17-014\)](#)
- #2017-026 » Tuesday, March 14, 2017  
[Multiple Vulnerabilities in Microsoft Office Could Allow for Remote Code Execution \(MS17-014\)](#)
- #2017-025 » Tuesday, March 14, 2017  
[Multiple Vulnerabilities in Microsoft Graphics Component Could Allow for Remote Code Execution \(MS17-013\)](#)
- #2017-024 » Tuesday, March 14, 2017  
[Multiple Vulnerabilities in Microsoft Uniscribe Could Allow for Remote Code Execution \(MS17-011\)](#)
- #2017-023 » Tuesday, March 14, 2017  
[A Vulnerability in Microsoft Windows SMB Server Could Allow for Remote Code Execution \(MS17-010\)](#)
- #2017-022 » Tuesday, March 14, 2017  
[Cumulative Security Update for Microsoft Edge \(MS17-007\)](#)
- #2017-021 » Tuesday, March 14, 2017  
[Cumulative Security Update for Internet Explorer \(MS17-006\)](#)
- #2017-019 » Friday, March 10, 2017  
[Multiple Vulnerabilities in Adobe Flash Player Could Allow for Code Execution \(APSB17-07\)](#)
- #2017-018 » Thursday, March 09, 2017  
[Vulnerability in Apache Struts Could Allow for Remote Code Execution](#)
- #2017-017 » Wednesday, March 08, 2017  
[Multiple Vulnerabilities in Mozilla Firefox Could Allow for Arbitrary Code Execution](#)
- #2017-016 » Monday, March 06, 2017  
[Multiple Vulnerabilities in Google Android OS Could Allow for Remote Code Execution](#)

**February 2017**

- #2017-015 » Monday, February 27, 2017  
[Vulnerability in Microsoft Internet Explorer and Edge Could Allow for Arbitrary Code Execution](#)



ANDROID



TLP: WHITE



# Weekly Malware IPs and Domains

## Automated Threat Indicator Sharing via Anomali

From: MS-ISAC SOC  
 To: MS-ISAC SOC  
 Cc:  
 Subject: Message from the MS-ISAC: Malware IPs and Domains observed by MS-ISAC 11/23/2011  
 Message | IPs of Interest 11-23 to 11-29.xlsx (35 KB)

IP ADDRESS	LOG COUNT	EVENT COUNT	COUNTRY	ASSOCIATED THREAT
69.162				
108.148	1522			
14.67	969		5 United States	Luminosity, LuminosityLink
112.248	143		3 United States	Luminosity
18.141	83		15 Netherlands	Generic Trojan
80.128	23		4 United States	Fleercivet
44.145	13		3 Germany	Ursnif
44.165	10		7 United States	Various malware, WS/JS Downloader
125.32	10		3 United States	Various malware, WS/JS Downloader
149.172	7		3 United States	Various malware, WS/JS Downloader
	4		4 United States	Kovter
			4 United States	Cerber

Attached to this email is a list of IP addresses and domains associated with malware.

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

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:

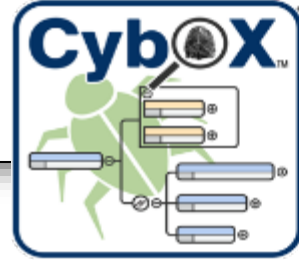
### 1. Malware IP Data

**IP Address** – This is either the IP address that is attacking a system or the IP address malware on an infected system is communicating with.

**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:  
[Indicator.sharing@cisecurity.org](mailto:Indicator.sharing@cisecurity.org)



TLP: WHITE





# MS-ISAC Intel Papers

UNCLASSIFIED//FOR OFFICIAL USE ONLY • Traffic Light Protocol: GREEN

## Multi State Information Sharing and Analysis Center Cyber Monthly Update

Information current as of May 31, 2017



Federal  
(U) TLP:  
Center  
Review  
capab  
their  
oper  
num  
rep  
av  
Ye

International Cybersecurity  
Agency Re  
TLP: WHITE



# MS-ISAC

## TECH WHITE February

### Timely Patching Reduces System Compromises

Authored by: Katelyn Bailey, Cyber Intel Analyst

#### INTRODUCTION

Patching and updating systems is one of the most important cyber security practices to implement in order to protect a system from being compromised. Analysis of information shared by the Multi-State Information Sharing and Analysis Center (MS-ISAC) data proves that timely patching can prevent most infections and system compromises.

#### DETAILS

Patches and security updates address software vulnerabilities that may allow malicious cyber threat actors access to information systems or a network. Once vulnerabilities are publicly announced, the information is available to anyone, including cyber threat actors. It is essential to quickly patch vulnerable systems as the disclosed information makes it easier for cyber threat actors to find and target systems. Research has shown that despite the proven effectiveness of patching, systems often remain vulnerable with out-of-date software and plugins for extended periods.

The primary vector in at least the incidents investigated by MS-ISAC was an unpatched vulnerability in an operating system, software, or plugin.

In July 2015 cyber threat actors exfiltrated data from an Italian company, which included information on four zero-day exploits that targeted vulnerabilities in common software. The Angler Exploit Kit, which dropped both the CryptoWall and Kovter malware in July 2015.

UNCLASSIFIED//FOR OFFICIAL USE ONLY - TLP: AMBER

## Situational Awareness Report

This proprietary document is based on the February 2017 security event data.



Multi-State Information Sharing and Analysis Center

UNCLASSIFIED//FOR OFFICIAL USE ONLY - TLP: AMBER



# MS-ISAC

## MS-ISAC Security Primer Cybersecurity While Traveling

March 2017, SP2017-0817

OVERVIEW: Whether you are traveling for business or leisure, travelers face increased cyber targeting and key threats include accidental loss and exposure, financially-motivated crime, data; oversharing information; the information carried with the traveler; the traveler's family; and the lack of due diligence. The Multi-State Information Sharing and Analysis Center (MS-ISAC) recommends assessing travel risk based on the threats and gaps in your knowledge.

When traveling for business or leisure, travelers face increased cyber targeting and key threats include accidental loss and exposure, financially-motivated crime, data; oversharing information; the information carried with the traveler; the traveler's family; and the lack of due diligence. The Multi-State Information Sharing and Analysis Center (MS-ISAC) recommends assessing travel risk based on the threats and gaps in your knowledge.

#### TIPS:

- Use a new or reimaged device so that no data is stored on it, and ensure that all data, and auto-download features are disabled. Turn off all other services when not in use.
- Use a dedicated device, clear browsing histories and other stored information that is not necessary for the trip.
- Delete unnecessary applications, plugins, and software.
- Use recent patches, software updates, and anti-virus software installed.
- Power off and where possible, have the batteries removed.
- Use a USB thumb drive or other removable media that can be destroyed if compromised upon return.
- Use encrypted connections for all activities over encrypted connections, where legal.
- Use a Gmail account instead of SLTT email accounts.
- Do not store sensitive data from a device to SLTT government networks until the device is no longer needed.

Use a new or reimaged device so that no data is stored on it, and ensure that all data, and auto-download features are disabled. Turn off all other services when not in use.

UNCLASSIFIED//FOR OFFICIAL USE ONLY • Traffic Light Protocol: AMBER

## DESK REFERENCE

### Cyber Threat Actor Review

Information from October 1 to December 31, 2015

(U) TLP: AMBER This desk reference provides a review of the most active, identified<sup>1</sup> Cyber Threat Actors<sup>2,3</sup> (CTA) and malicious cyber campaigns and operations from October 1 through December 31, 2015. The information in this document is provided to further the reader's



# MS-ISAC Cyber Alerts

MS-ISAC Advisory

**Sent:** Thursday, June 16, 2016 at 2:57 PM

**To:** Thomas Duffy

**TLP: WHITE**  
**MS-ISAC CYBER ALERT**

**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:

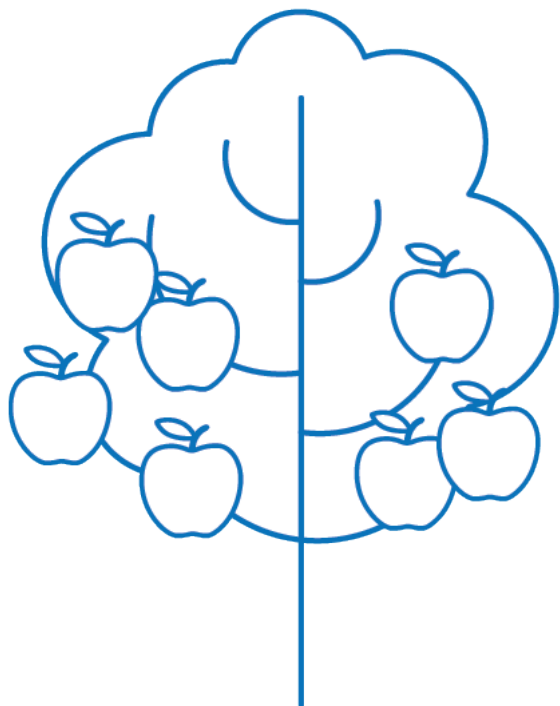
- Share this information with potentially impacted organizations your area of responsibility, including Departments of Law/Justice, related law enforcement agencies, and agency-specific offices of counsel.
- Train government legal professionals in identifying spear phishing emails which may include spoofed 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.

**TLP: WHITE**



# What Can You Do?

---



1. PATCH!
2. Use defensive software
3. Train users
4. Enforce passwords standards & 2FA
5. Have frequent, complete, off-line, off-site, and tested back-ups
6. Create a culture where it's OK to ask
7. Work with your ISAC Partners



## **MS-ISAC 24x7 Security Operations Center**

**1-866-787-4722**

**[SOC@cisecurity.org](mailto:SOC@cisecurity.org)**

**[info@msisac.org](mailto:info@msisac.org)**

**Kyle Bryans**

**Program Specialist**

**MS-ISAC**

**518.880.0747**

**[Kyle.Bryans@cisecurity.org](mailto:Kyle.Bryans@cisecurity.org)**