The MS-ISAC

A free cybersecurity resource for State, Local, Tribal, and Territorial Governments

Benjamin Spear
Sr. Intelligence Analyst

Eugene Kipniss
Program Specialist

NATIONAL CYBER SECURITY AWARENESS MONTH




Hackers take aim at prison locks and other
Detective's stolen laptop puts thousands at risk of identity theft
By Tracy Vedder | Published: Jun 24, 2013 at 8:25 PM PDT | Last Updated: Jun 25, 2013 at 10:59 AM PDT
Coach suspends entire team
alls, Montana TV station
Operation Last Resort: "Anonymous" retaliation for Swartz death
3.5 million
dates
By KELLEY SHANNON
Warn Medical Device Makers, Hospita
Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating
Capital One, Disney, Others
by Dennis Fisher
Share
Like
45
18 Comments
June 24, 2011
Hacked Me
By MARC LACEY and RICH

Multi-State Information Sharing and Analysis Center



The U.S. Department of Homeland Security has designated the MS-ISAC as its key cybersecurity resource for cyber threat prevention, protection, response and recovery for all U.S. State, Local, Tribal and Territorial (SLTT) governments.

Who We Serve

MS-ISAC Members include:

- All 56 US States and Territories
- All 78 federally recognized fusion centers
- More than 1,000 local governments and tribal nations

State, Local, Tribal, and Territorial

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

Fusion Centers



WHY GOVERNMENT?



Criminals look for data.....

And governments have a lot of it!

AFFECTED ENTITIES



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@msisac.org

Levels of Access

Public Information

Fee Based Services



Any SLTT

Full MS-ISAC Membership

Public Information

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

MS-ISAC Advisories

This message was sent with High importance.

From: MS-ISAC Advisory
Sent: Thu 10/15/2015 10:19 A
To: Thomas Duffy
Cc:
Subject: MS-ISAC CYBER SECURITY ADVISORY - Multiple Vulnerabilities in Adobe Flash Player Could Allow for Remote Code Execution (APSB15-25) - TLP: WHITE

TLP: WHITE
MS-ISAC CYBER SECURITY ADVISORY

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 (APSB15-25)

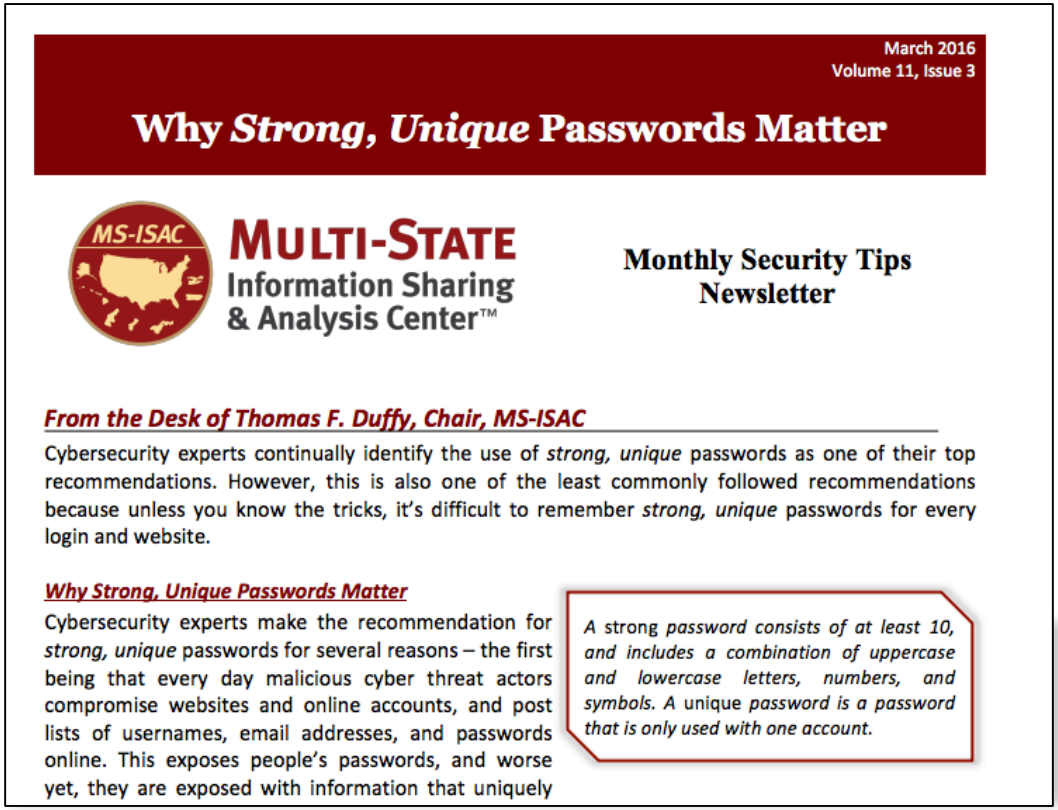
OVERVIEW:
Multiple vulnerabilities in Adobe Flash Player could allow remote code execution. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. Successful exploitation could result in an attacker compromising data security, potentially allowing access to confidential data, compromising processing resources in a user's computer, or remote code execution. Failed exploit attempts will likely cause denial-of-service conditions.

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 is being used in limited, targeted attacks.

Monthly Newsletter

Distributed in template form to allow for re-branding and redistribution by <u>your</u> agency



March 2016
Volume 11, Issue 3

Why *Strong, Unique* Passwords Matter

MS-ISAC
MULTI-STATE Information Sharing & Analysis Center™

Monthly Security Tips Newsletter

From the Desk of Thomas F. Duffy, Chair, MS-ISAC

Cybersecurity experts continually identify the use of *strong, unique* passwords as one of their top recommendations. However, this is also one of the least commonly followed recommendations because unless you know the tricks, it's difficult to remember *strong, unique* passwords for every login and website.

Why Strong, Unique Passwords Matter

Cybersecurity experts make the recommendation for *strong, unique* passwords for several reasons – the first being that every day malicious cyber threat actors compromise websites and online accounts, and post lists of usernames, email addresses, and passwords online. This exposes people's passwords, and worse yet, they are exposed with information that uniquely

A strong password consists of at least 10, and includes a combination of uppercase and lowercase letters, numbers, and symbols. A unique password is a password that is only used with one account.

National Webcasts

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

- Prioritize Your NIST CSF Implementation with the CIS Critical Security Controls (June)
- Internet of Things (April)
- 2016 Predictions from the MS-ISAC (February)
- Cybersecurity Year in Review and 2016 Preview (December 2015)
- National Cybersecurity Awareness Month: Tips for Staying Safe Online (October 2015)

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

Any SLTT Government

MS-ISAC

Multi-State Information Sharing & Analysis Center™

VULNERABLE SOFTWARE



Vulnerabilities

Content Management Systems

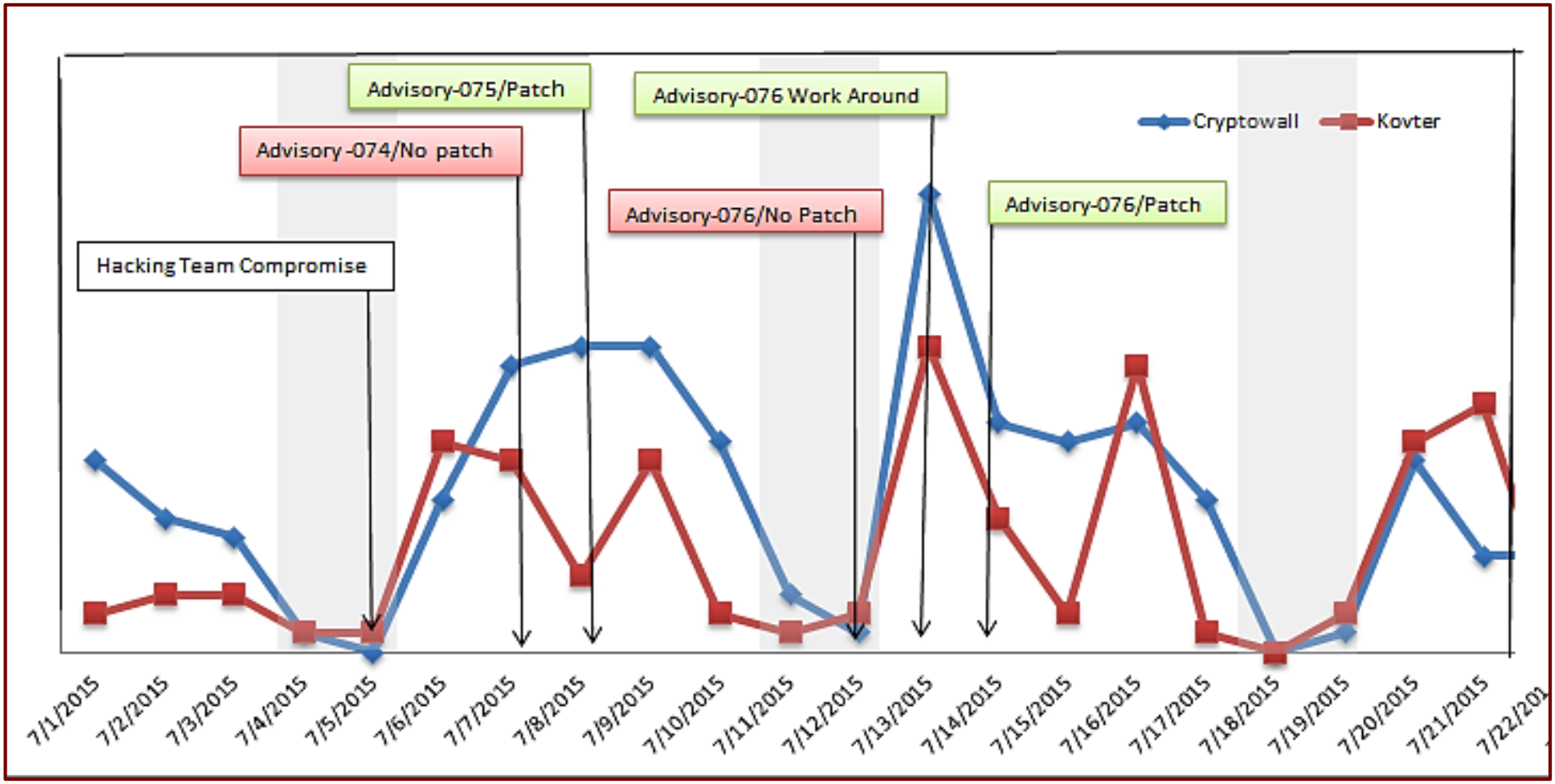
Plug In's



Server

Web Programming Language

Information Sharing



Vulnerability Management Program

What Data Are We Collecting?

- 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

Computer Emergency Response Team (CERT)

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

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

What is an "Incident"?

As defined by NIST:
A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Examples:

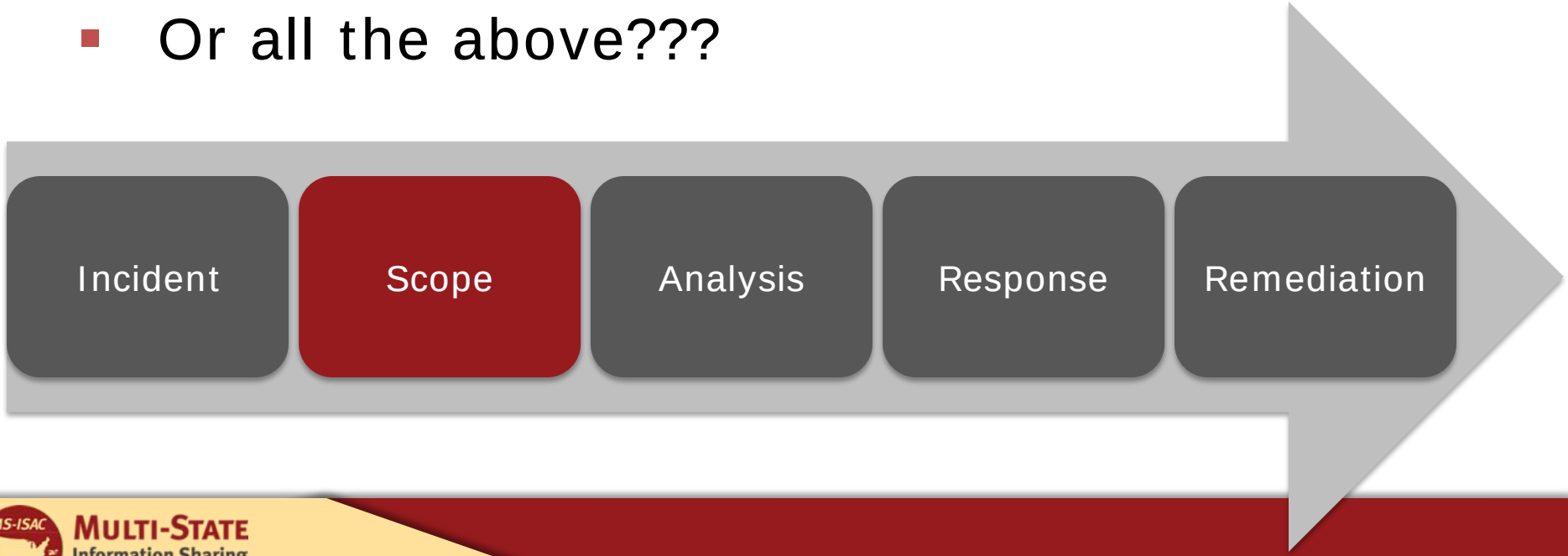
- Phishing
- Network Intrusion
- DDoS
- Ransomware



Determining the Scope

What is being affected?

- Workstation
- Server
- Network Segment
- Perimeter
- Or all the above???



Analysis of available data

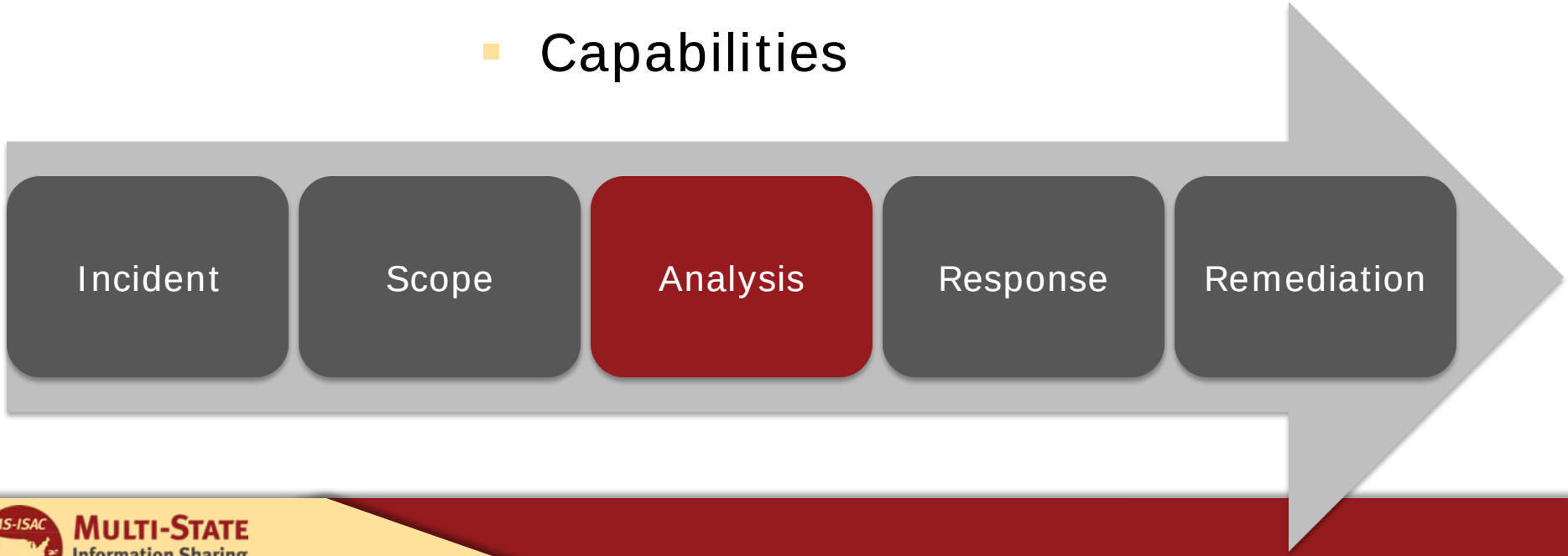
What do we have?

- Logs
- Files
- Emails

What do we know?

- Scope
- Indicators

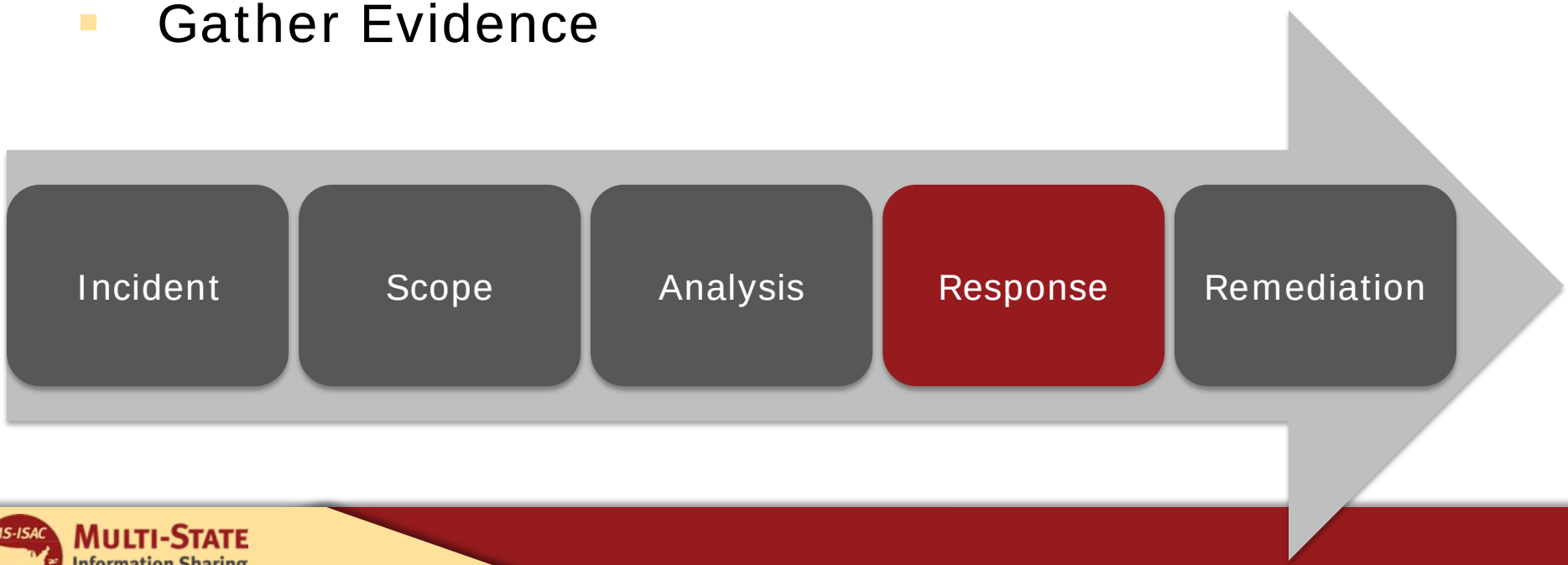
- **What do we do?**
- Resources
- Capabilities



Responding to the Incident

Dependent on the scope

- Deployment
- Remote
- How critical is it?
- Mitigate or Monitor
- Gather Evidence



Remediation

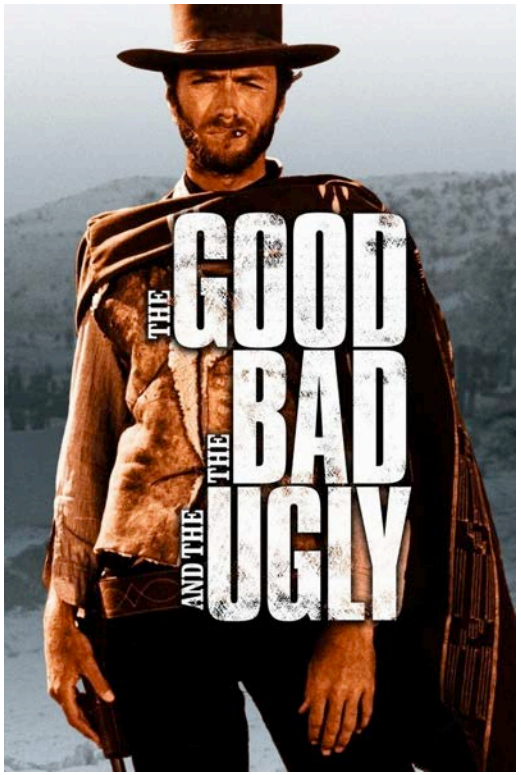
Dependent on the Evidence

- Isolation
- Re-image, reconfigure or creation



After Action Review

- Who, What, Why, Where and How it Happened
- The Good, The Bad, and The Ugly
- Incident Response Plan
- Training
- Documentation



MS-ISAC Membership

MULTI-STATE
Information Sharing
& Analysis Center™

Benefits of Membership

- Access to information, intelligence, products, resources, and webcasts
- Insider access to federal information
- Training and resource discounts
- CIS Security Benchmarks discounts
- US-CERT Portal access
- Cybersecurity exercise participation
- Malicious Code Analysis Platform (MCAP) access

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

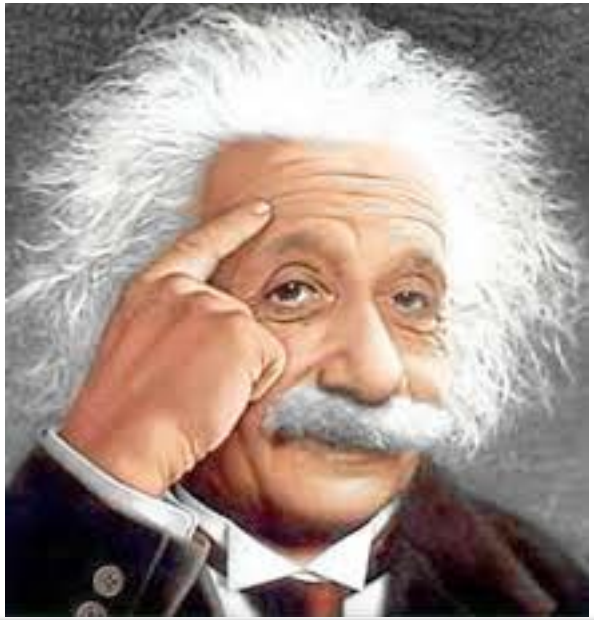
Domain Monitoring

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

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

Network Monitoring (Albert)

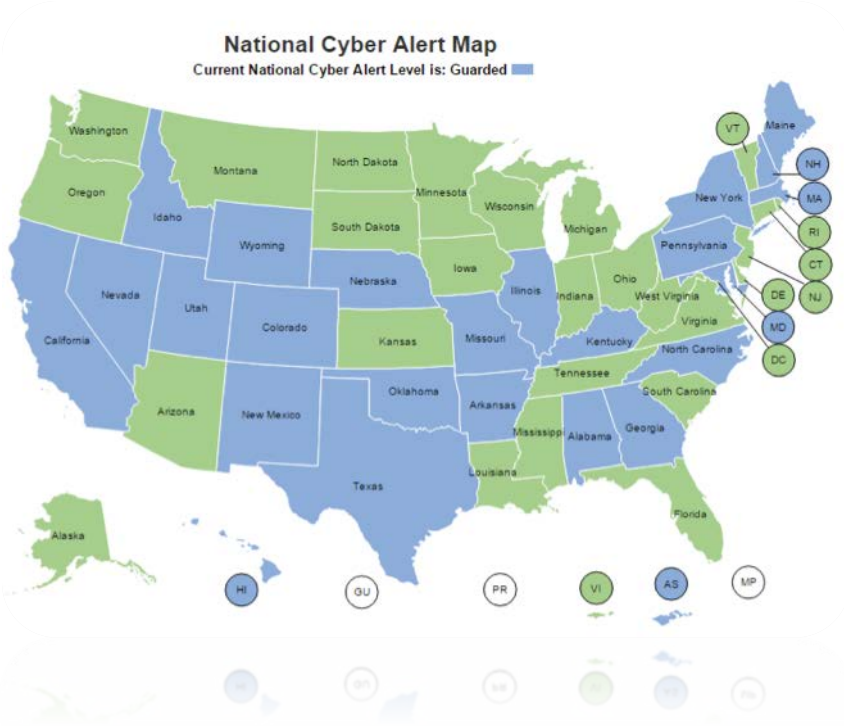
- SLTT focus – Funded for States and Territories
- 24x7x365 research, analysis, and support
- Signatures unique to SLTT governments
- Integration of research on specific attacks and actors, including nation-state actors (APT)
- Real-time information sharing with FSLTT partners
- Experienced cybersecurity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



HSIN Access

Access to:

- MS-ISAC Cyber Alert Map
- Archived webcasts & products
- Cyber Table Top Exercises
- Guides and templates
- Message Boards



Cyber Threat Intelligence

24x7 Assistance



- Cyber Threat Actor information
- TTP trends and patterns
- Answers to technical questions
- IOCs
- Incident response and assistance
- Statistics
- Joint Papers
- Pointers to other resources and introductions to other agencies

Intelligence Sources

- 24 x 7 x 365 Monitoring
- Analysis of ~600 billion logs/month
- Integration with federal agencies via the NCCIC, NCIJTF and private companies
- Research into vulnerabilities, exploits, TTPs, patterns, and trends
- Constant contact with all ISACs



Information Sharing and Analysis Centers

Multi-State	Electric Sector	Public Transit	Aviation	Legal Services	Real Estate Sector
Defense Industrial Base	Downstream Natural Gas	ICS	Supply Chain	Water Sector	Maritime
Health	Oil and Gas	Research and Education	Emergency Management and Response		Nuclear Sector
Surface Transportation	Information Technology	Automotive	Financial Services		Communications

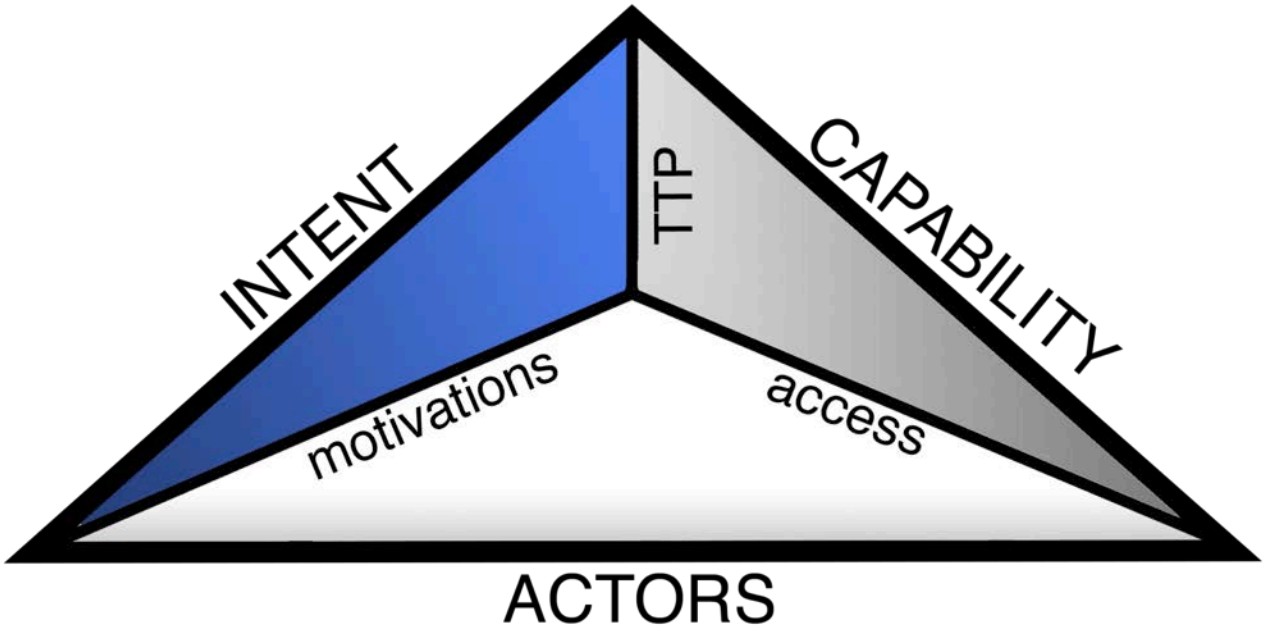
Intelligence Scope

Tactics, Techniques, and Procedures

Targeted Data and Systems

Cyber Threat Actors

Developing Issues



MS-ISAC Products

Cybersecurity Advisory:
short, timely, emails containing technical information regarding system patching and similar system maintenance activity

Purchasing Alliance:
Discounted purchasing buys

Incident Notifications:
via phone or email, as appropriate – domain & IP based

National Webcasts:
6 bi-monthly webcasts on national topics of interest

End User Newsletters:
Monthly newsletter to rebrand and distribute

Members Only

Cyber Alerts:
short, timely, emails containing information on a specific cyber incident or threat

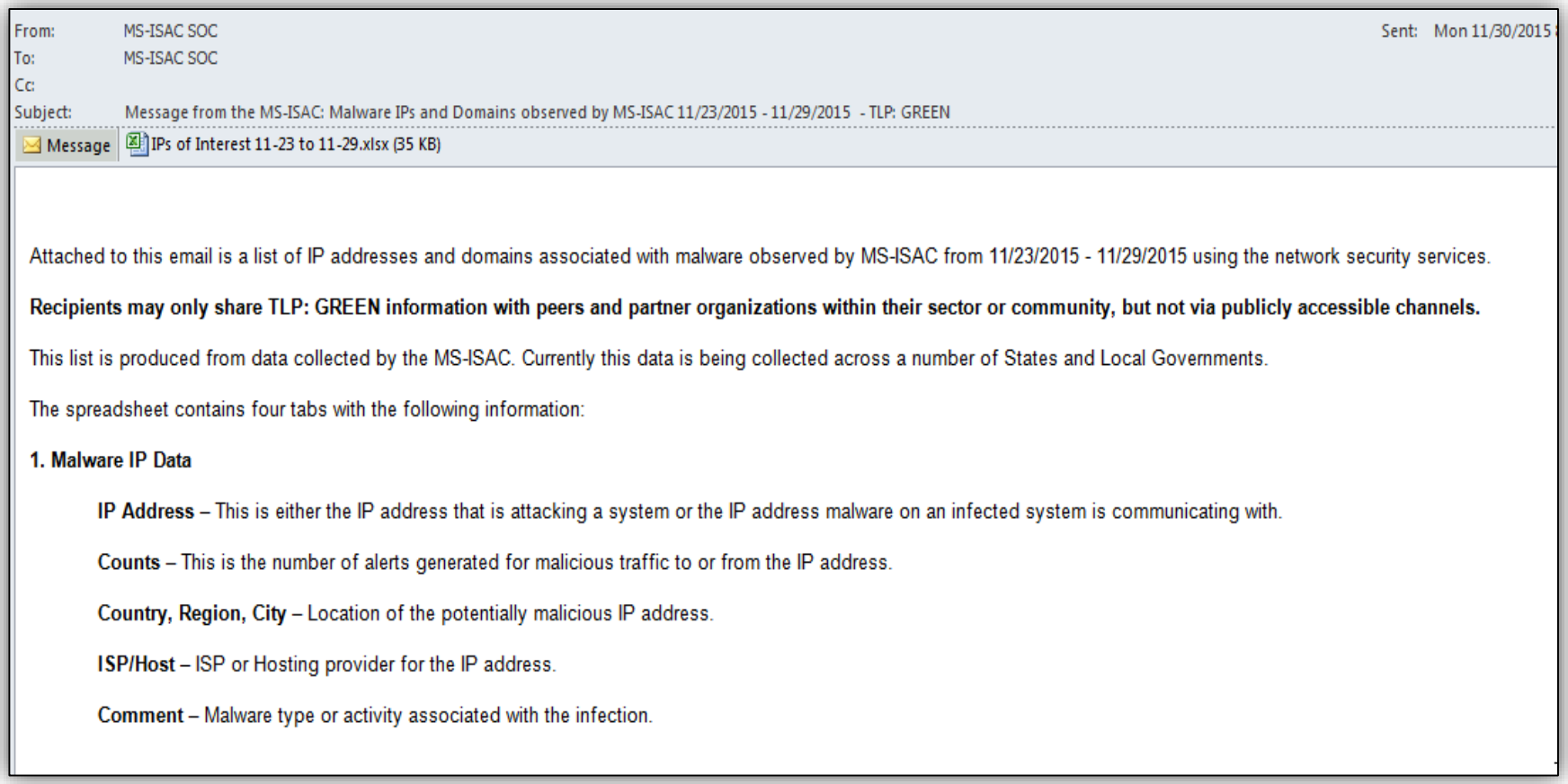
Intel Papers:
Intelligence-driven papers on TTPs, trends, patterns, and actors affecting SLTT governments

Threat Information:
Information on malicious domains, IPs, and current threat events

Cybersecurity Toolkit:
Items to promote cybersecurity awareness in your organization

Hot Topics Webcasts:
Monthly guest speakers on areas of interest to MS-ISAC members

Weekly Malware IPs and Domains



From: MS-ISAC SOC
To: MS-ISAC SOC
Cc:
Subject: Message from the MS-ISAC: Malware IPs and Domains observed by MS-ISAC 11/23/2015 - 11/29/2015 - TLP: GREEN
Sent: Mon 11/30/2015

Message | IPs of Interest 11-23 to 11-29.xlsx (35 KB)

Attached to this email is a list of IP addresses and domains associated with malware observed by MS-ISAC from 11/23/2015 - 11/29/2015 using the network security services.

Recipients may only share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

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

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.

ISP/Host – ISP or Hosting provider for the IP address.

Comment – Malware type or activity associated with the infection.

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.

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:
soc@msisac.org

SOLTRA EDGE

Machine-to-Machine indicator transfer



To gain an account contact:
Scott.Parish@cisecurity.org

Fee Based Services

- Network Monitoring (Albert)
- Managed Security Services (MSS)
- Web application vulnerability assessments
- Network vulnerability assessments
- Penetration testing
- Phishing engagements
- Security assessments

For more info on any of these contact:
info@msisac.org

MS-ISAC Annual Meeting



2016 Location…

San Antonio, TX!



MS-ISAC

MULTI-STATE
Information Sharing
& Analysis Center™

WRAPPING IT UP

What Can You Do?

Low Hanging Fruit!



1. PATCH!
2. Use defensive software
3. Back-up
4. Train users
5. Enforce strong, complex, unique passwords

Critical Security Controls

1. Identify authorized and unauthorized devices
2. Inventory authorized and unauthorized software
3. Secure configurations for hardware and software
4. Continuous vulnerability assessment and remediation
5. Controlled use of admin privileges

Identify Malicious Activity



- Antivirus
- Firewalls
- IDS/IPS
- Logs (90 days!)
- Places to Look
  - Pastebin, Ghostbin, Zerobin
  - Twitter
  - Facebook
  - Google
  - SHODAN
- Things to Look For:
  - Announcements
  - Hashtags
  - Doxings

Share Information

- **Be prepared**
  - Learn from others' best practices
  - Gather intel to help you be proactive
- **Be willing to ask for help**
  - Identify other resources to augment what you are doing
- **Be a part of the solution**
  - Take part in information sharing

Who do I call?



Security Operations Center (SOC)

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

31 Tech Valley Dr., East Greenbush, NY 12061-4134

www.cisecurity.org

To join or get more information:

https://msisac.cisecurity.org/members/register

QUESTIONS?


I HAVE CONCERNS ABOUT THIS CYBERSECURITY CANDIDATE.
HE'S AVAILABLE.
ANYTHING IN PARTICULAR?
·few·
klosshet

MS-ISAC Contact Numbers

Benjamin Spear
Ben.spear@cisecurity.org

Eugene Kipniss
Eugene.kipniss@cisecurity.org

Security Operations Center

24/7 Phone Number

1-866-787-4722

soc@msisac.org

MS-ISAC HQ

Front Desk

518-266-3460

info@msisac.org