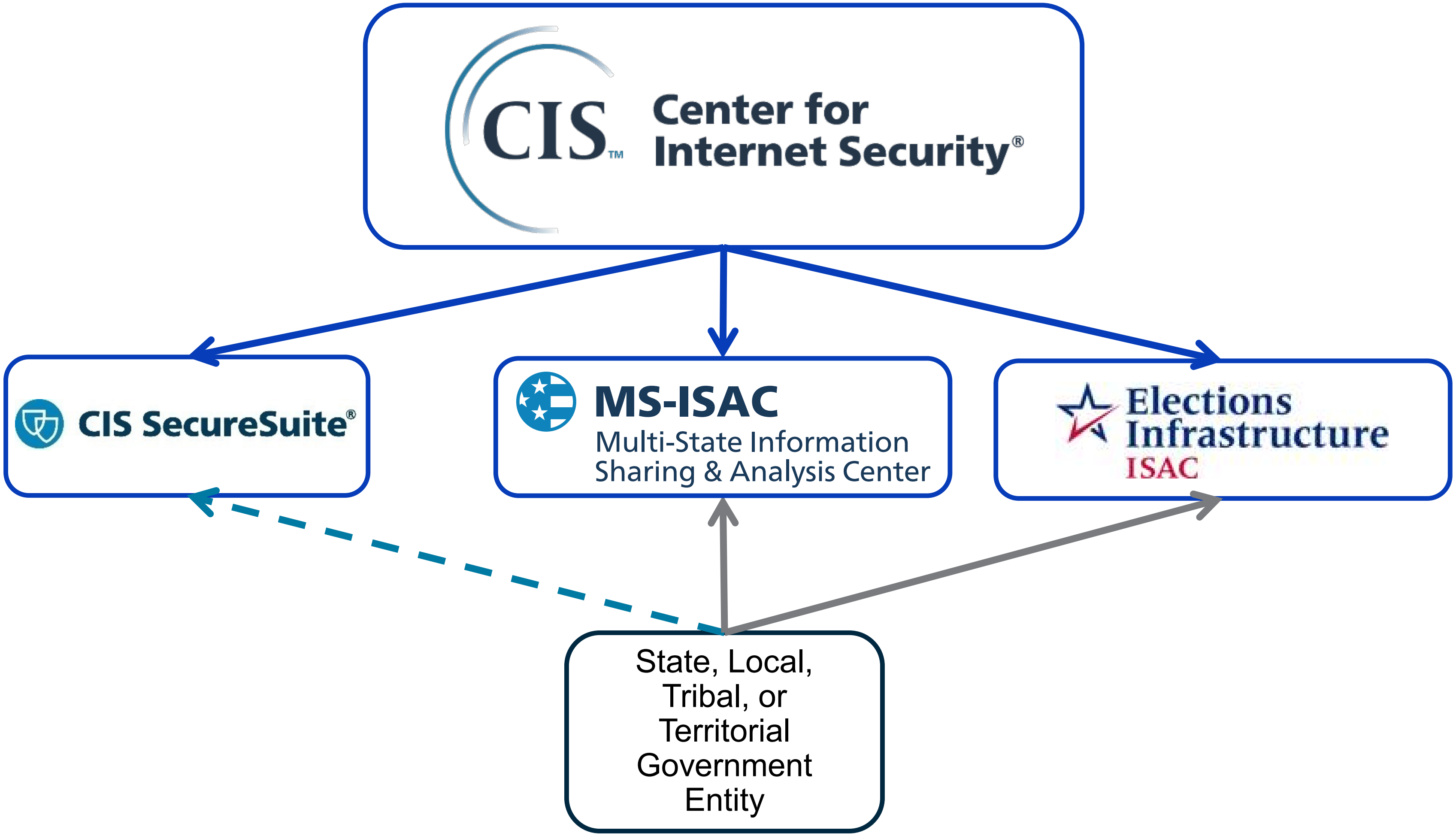
CIS™ Center for Internet Security®

MS-ISAC Multi-State Information Sharing & Analysis Center

Cyber Threats and Federally-funded Cyber Resources

Eugene Kipniss

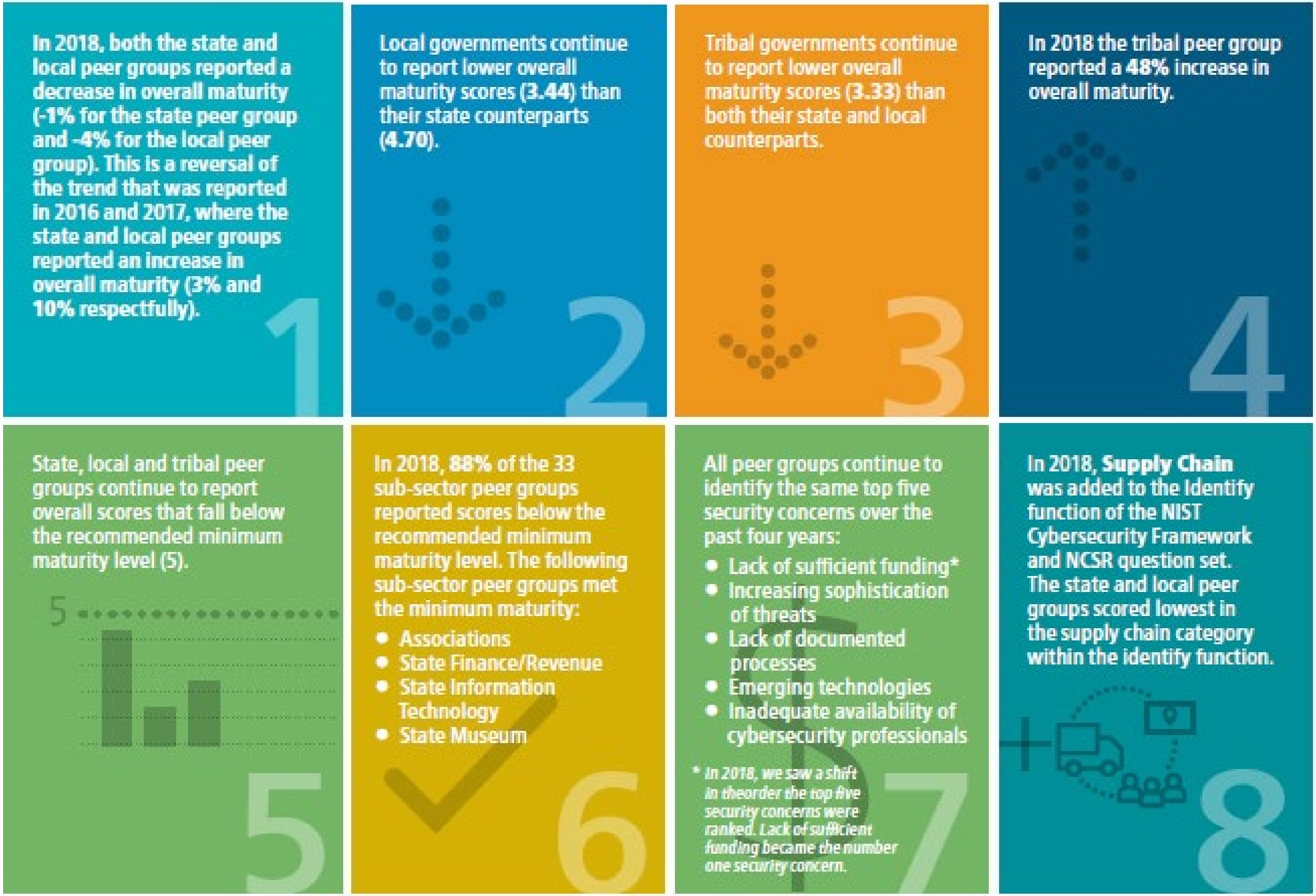

CIS Center for Internet Security®
CIS SecureSuite®
MS-ISAC Multi-State Information Sharing & Analysis Center
Elections Infrastructure ISAC
State, Local, Tribal, or Territorial Government Entity

Why SLTT Governments?

Criminals look for data…

and governments have a lot of it!

2018 NCSR Findings Preview



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 theorder the top five security concerns were ranked. Lack of sufficient funding became the number one security concern.*

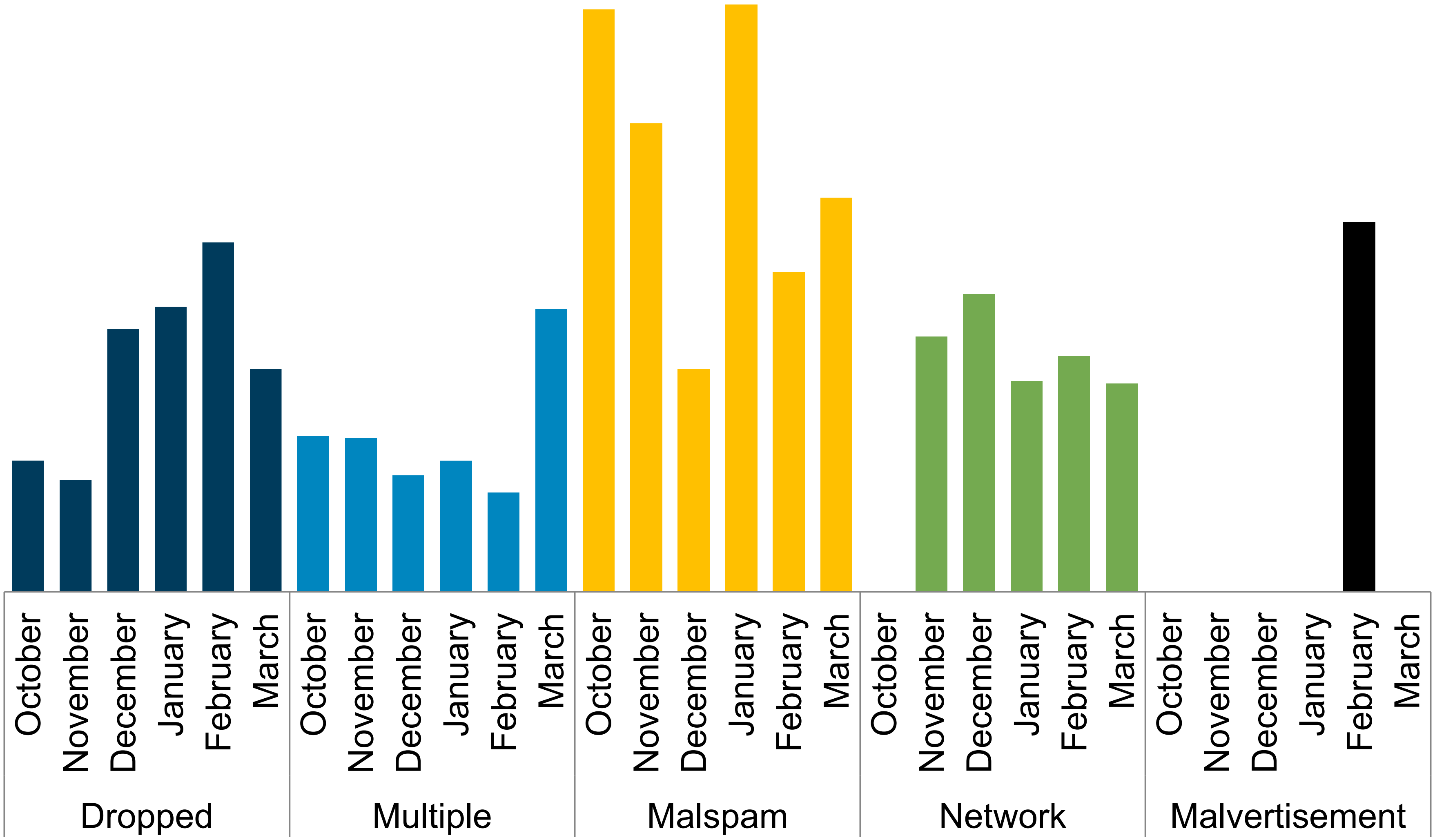
In 2018, **Supply Chain** was added to the Identify function of the NIST Cybersecurity Framework and NCSR question set. The state and local peer groups scored lowest in the supply chain category within the identify function.

Top 10 Malware 2018

January 2018	February 2018	March 2018	April 2018	May 2018	June 2018
Kovter	Kovter	Kovter	Kovter	Kovter	WannaCry
WannaCry	WannaCry	Emotet	ZeuS	ZeuS	Emotet
Emotet	Emotet	ZeuS	Emotet	NanoCore	Kovter
ZeuS	ZeuS	Redyms	CoinMiner	Redyms	ZeuS
CoinMiner	NanoCore	TinyLoader	NanoCore	Mirai	Mirai
Gh0st	CoinMiner	CoinMiner	Xtrat	CoinMiner	Cerber
NanoCore	Gh0st	NanoCore	Redyms	WannaCry	NanoCore
Ursnif	Qarallex	Gh0st	WannaCry	Emotet	CoinMiner
Mirai	Latentbot	WannaCry	Mirai	Gh0st	Gh0st
Redyms	Mirai	Cerber	Gh0st	Latentbot	Xtrat

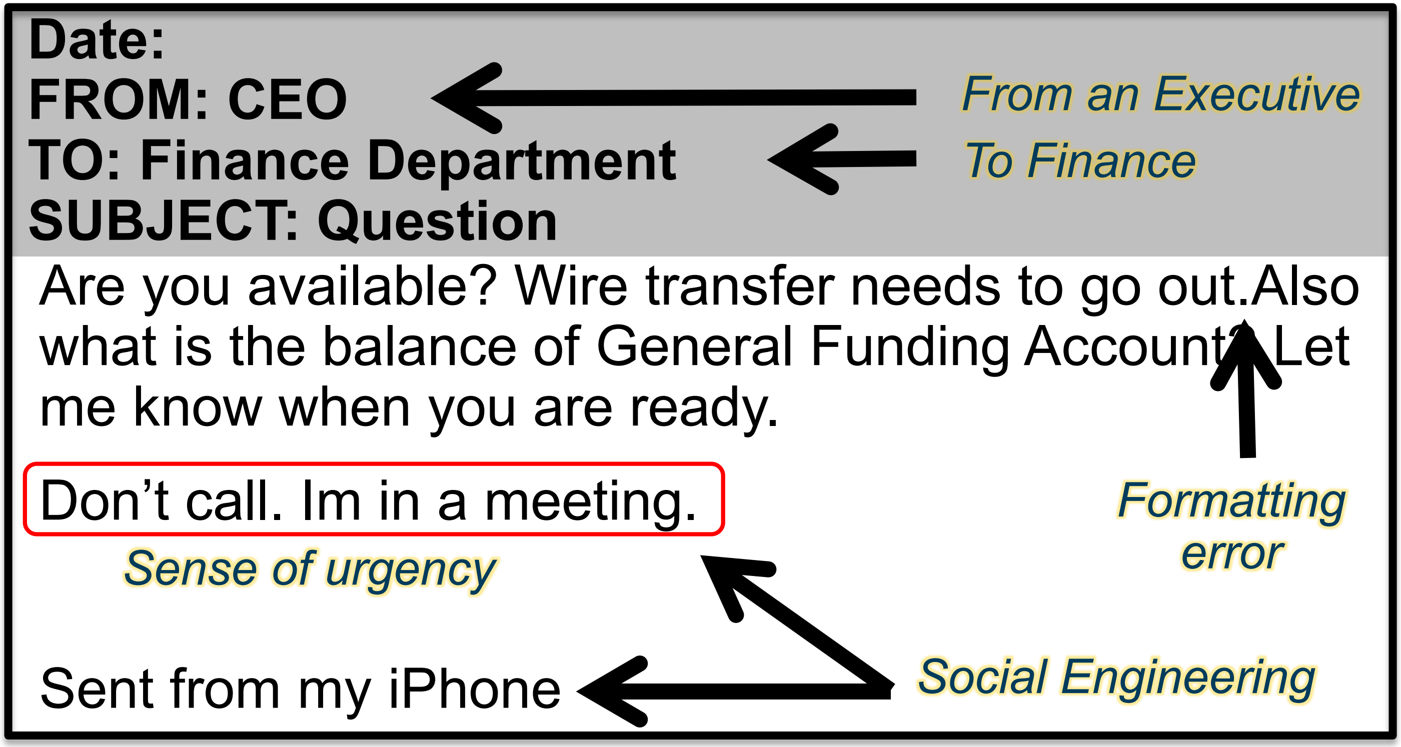
July 2018	February 2018	September 2018	October 2018	November 2018	December 2018
Emotet	Kovter	Emotet	Emotet	WannaCry	WannaCry
Kovter	Emotet	WannaCry	Kovter	Emotet	ZeuS
ZeuS	ZeuS	Kovter	ZeuS	ZeuS	Emotet
NanoCore	CoinMiner	ZeuS	WannaCry	Kovter	Kovter
Cerber	WannaCry	CoinMiner	NanoCore	CoinMiner	Qakbot
Gh0st	NanoCore	NanoCore	Gh0st	Mirai	Samsam
CoinMiner	Mirai	Gh0st	CoinMiner	NanoCore	Gh0st
Trickbot	Gh0st	Mirai	Mirai	Gh0st	Mirai
WannaCry	Cerber	Trickbot	Ursnif	Smoke Loader	Brambul
Xtrat	Ursnif	AZORult	Smoke Loader	Ursnif	CoinMiner

Top 10 Malware - Initiation Vectors



TLP: WHITE

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. Im in a meeting.

Sent from my iPhone

From an Executive

To Finance

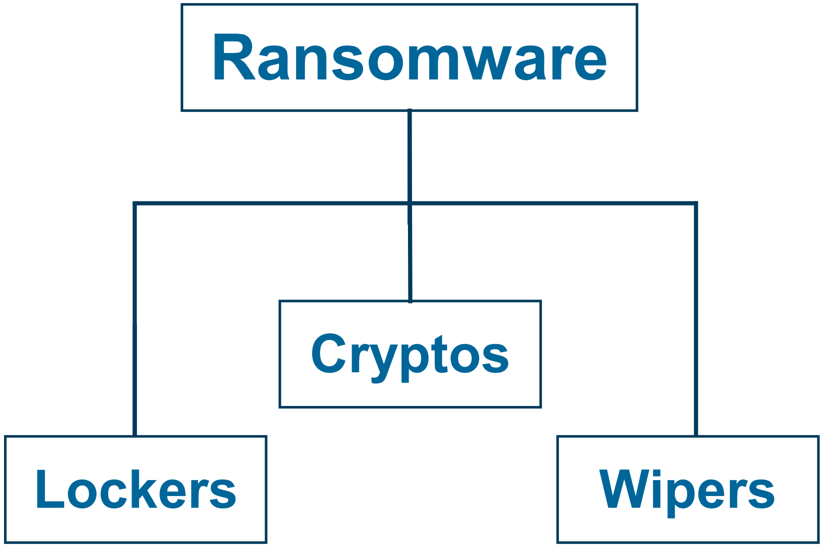
Formatting error

Sense of urgency

Social Engineering

Ransomware

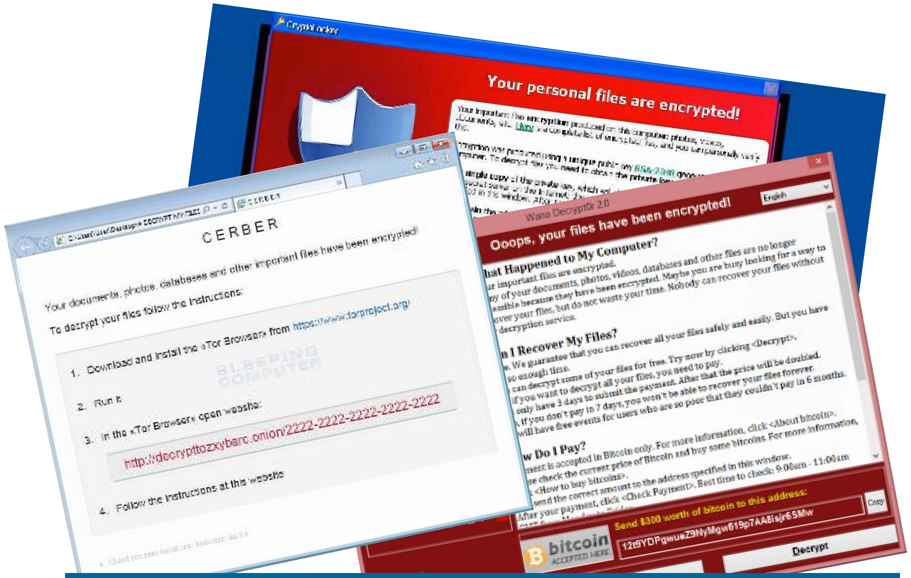
malware that blocks access to a system, device, or file until a ransom is paid; commonly demand that the victim pays $200 - $1,000 in bitcoins, gift cards, etc.


Ransomware

Cryptos

Lockers

Wipers



Your personal files are encrypted!

CERBER

Your documents, photos, databases and other important files have been encrypted!

To decrypt your files follow the instructions:

1. Download and install the «Tor Browser» from https://www.torproject.org/
2. Run it
3. In the «Tor Browser» open website:

   http://decrypttozxybarc.onion/2222-2222-2222-2222-2222
4. Follow the instructions at this website

Ooops, your files have been encrypted!

hat Happened to My Computer?

ur important files are encrypted.

ny of your documents, photos, videos, databases and other files are no longer
essible because they have been encrypted. Maybe you are busy looking for a way to
over your files, but do not waste your time. Nobody can recover your files without
decryption service.

n I Recover My Files?

e. We guarantee that you can recover all your files safely and easily. But you have
so enough time.
can decrypt some of your files for free. Try now by clicking <Decrypt>.
if you want to decrypt all your files, you need to pay.
only have 3 days to submit the payment. After that the price will be doubled.
, if you don't pay in 7 days, you won't be able to recover your files forever.
will have free events for users who are so poor that they couldn't pay in 6 months.

w Do I Pay?

ment is accepted in Bitcoin only. For more information, click <About bitcoin>.
se check the current price of Bitcoin and buy some bitcoins. For more information,
: <How to buy bitcoins>.
send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Extortion

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

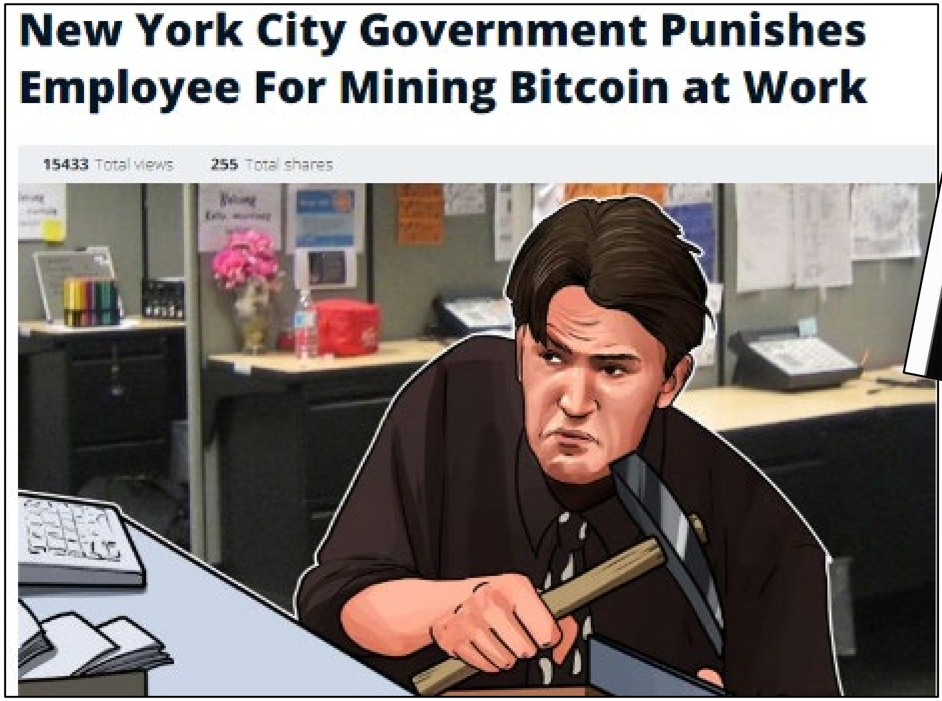
Infection Vectors:

- 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

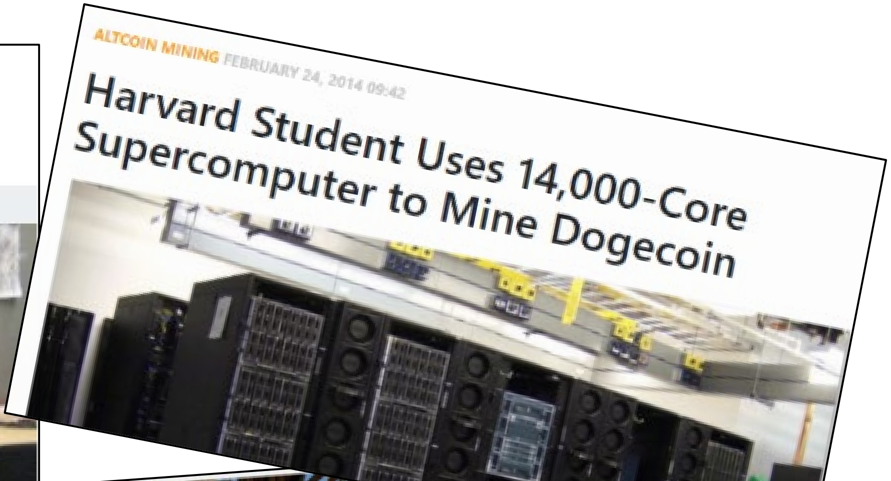
TLP: WHITE

Insider Crypto-mining



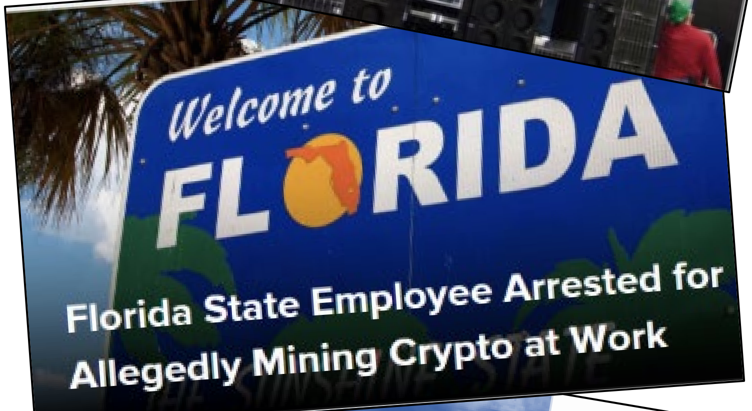
New York City Government Punishes Employee For Mining Bitcoin at Work

15433 Total views 255 Total shares

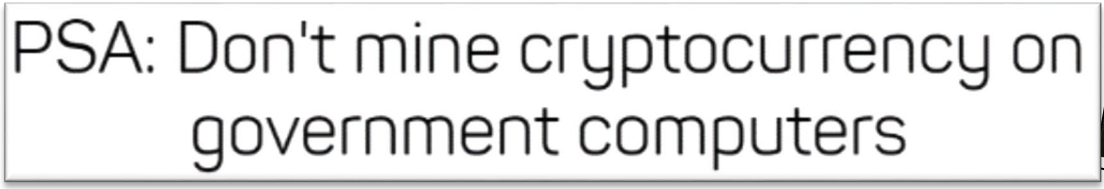


ALTCOIN MINING FEBRUARY 24, 2014 09:42

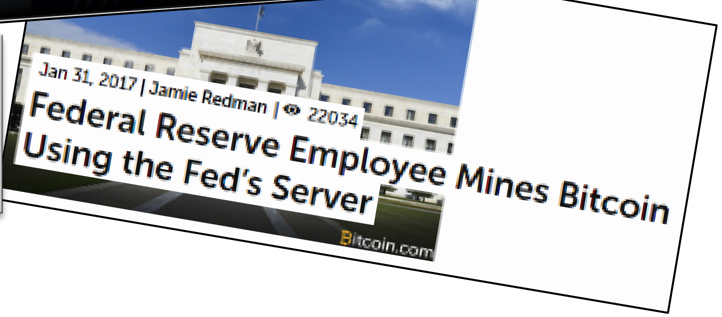
Harvard Student Uses 14,000-Core Supercomputer to Mine Dogecoin



Florida State Employee Arrested for Allegedly Mining Crypto at Work



PSA: Don't mine cryptocurrency on government computers



Jan 31, 2017 | Jamie Redman | 22034

Federal Reserve Employee Mines Bitcoin Using the Fed's Server

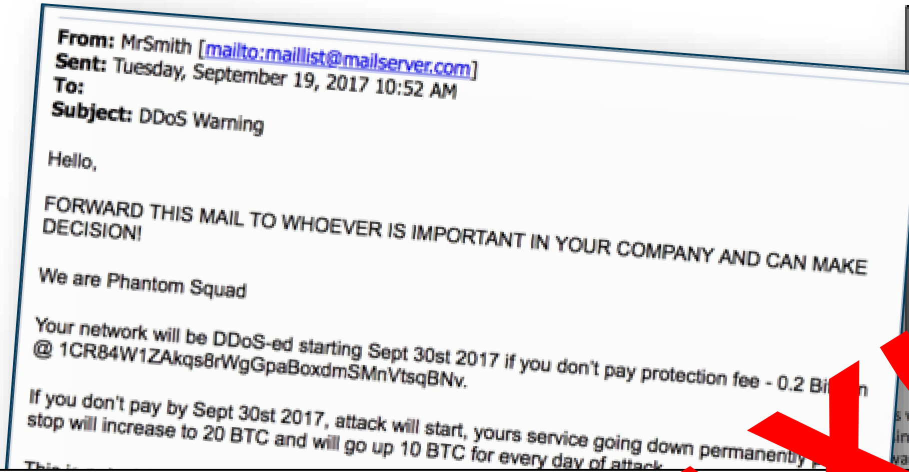
TLP: WHITE

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



From: MrSmith [mailto:maillist@mailserver.com]
Sent: Tuesday, September 19, 2017 10:52 AM
To:
Subject: DDoS Warning

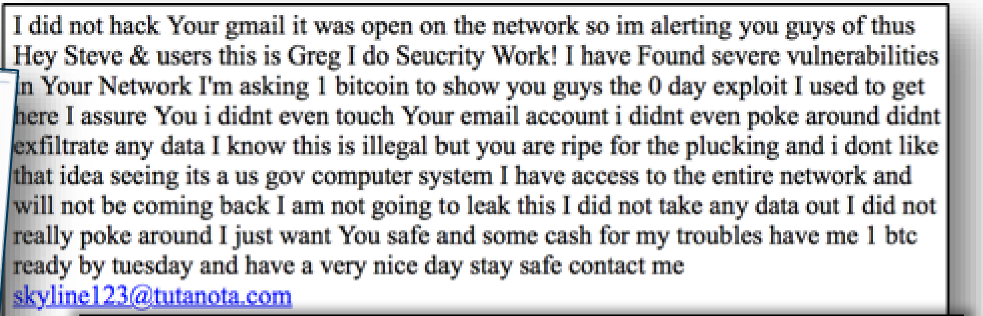
Hello,

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Phantom Squad

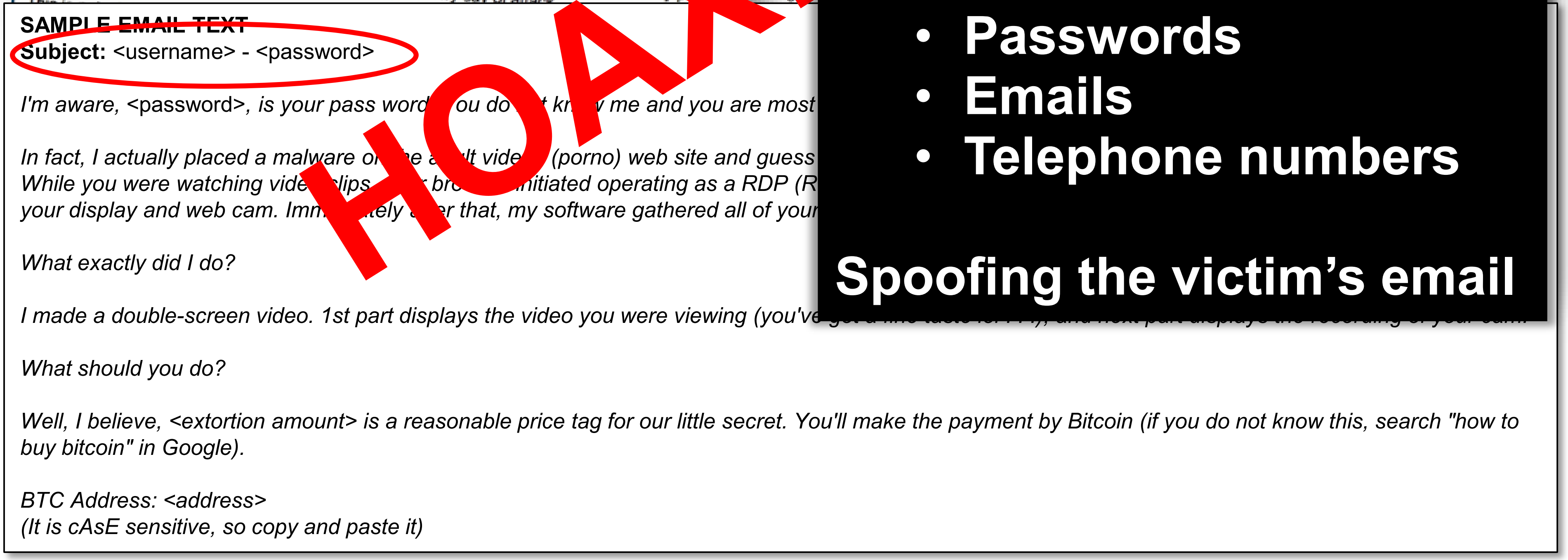
Your network will be DDoS-ed starting Sept 30st 2017 if you don't pay protection fee - 0.2 Bi n @ 1CR84W1ZAkqs8rWgGpaBoxdmSMnVtsqBNv.

If you don't pay by Sept 30st 2017, attack will start, yours service going down permanently stop will increase to 20 BTC and will go up 10 BTC for every day of attack.



I did not hack Your gmail it was open on the network so im alerting you guys of thus Hey Steve & users this is Greg I do Seucrity Work! I have Found severe vulnerabilities in Your Network I'm asking 1 bitcoin to show you guys the 0 day exploit I used to get here I assure You i didnt even touch Your email account i didnt even poke around didnt exfiltrate any data I know this is illegal but you are ripe for the plucking and i dont like that idea seeing its a us gov computer system I have access to the entire network and will not be coming back I am not going to leak this I did not take any data out I did not really poke around I just want You safe and some cash for my troubles have me 1 btc ready by tuesday and have a very nice day stay safe contact me skyline123@tutanota.com

HOAX!



SAMPLE EMAIL TEXT
Subject: <username> - <password>

I'm aware, <password>, is your pass word. You do not know me and you are most

In fact, I actually placed a malware on the adult video (porno) web site and guess
While you were watching video clips, your browser initiated operating as a RDP (R
your display and web cam. Immediately after that, my software gathered all of your

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 for [illegible]), 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).

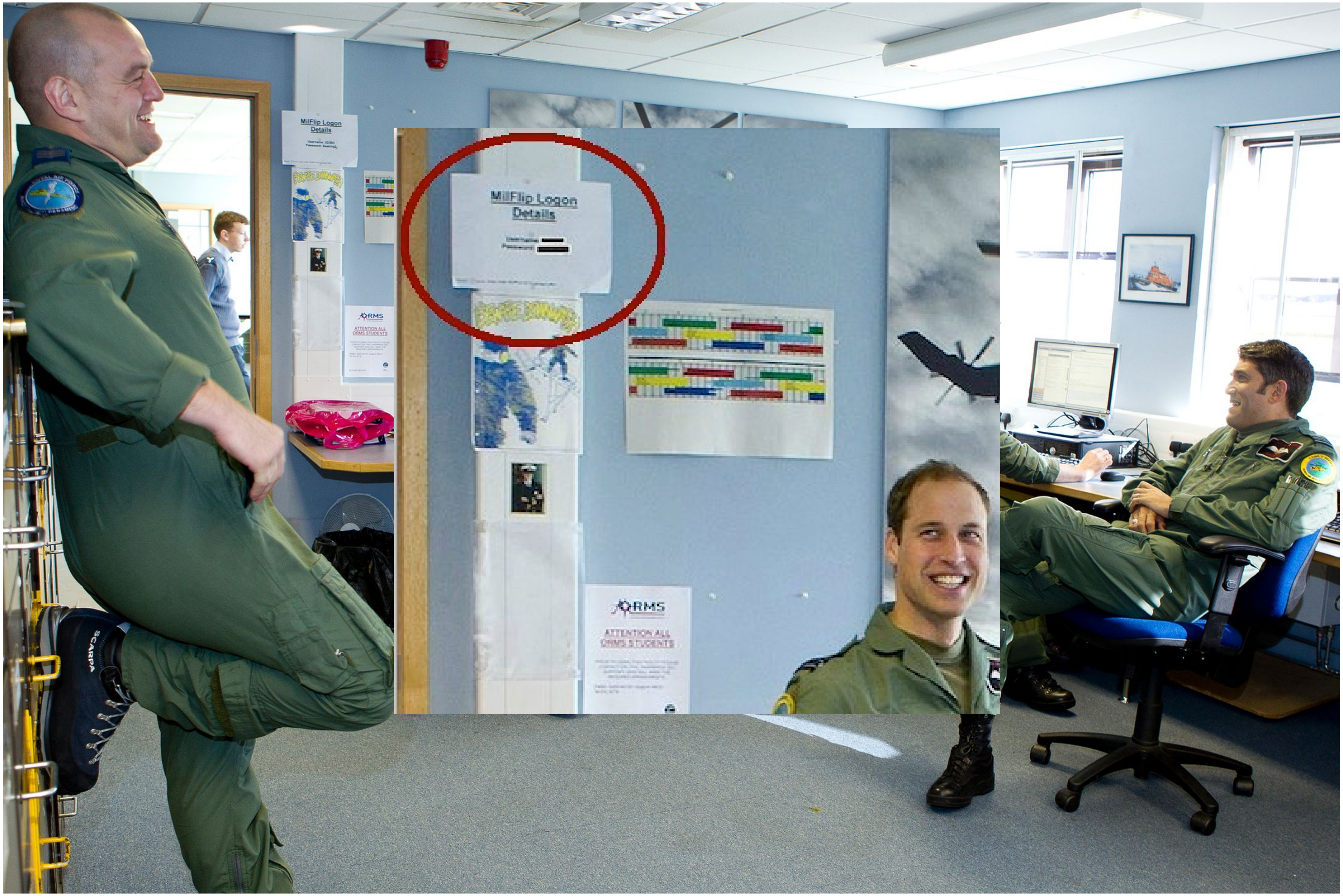
BTC Address: <address>
(It is cAsE sensitive, so copy and paste it)

Emails can include user's:
- **Names**
- **Passwords**
- **Emails**
- **Telephone numbers**

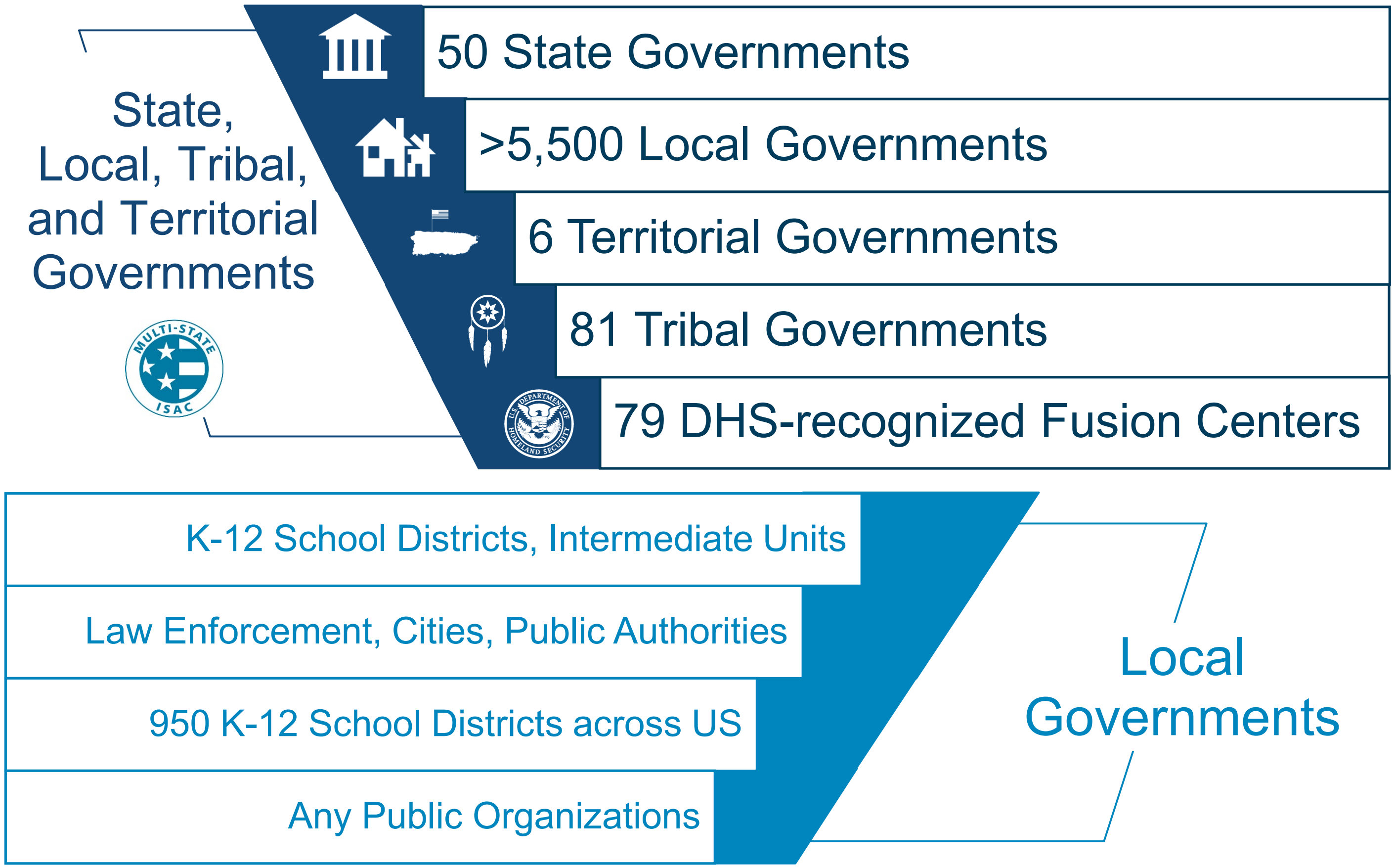
Spoofing the victim's email

Employee Mistakes

Why care? - Employee Mistakes



Who We Serve



State, Local, Tribal, and Territorial Governments

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

Local Governments

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

How to access MS-ISAC resources

- **Register for the MS-ISAC's services here:**

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

TLP: WHITE

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

TLP: WHITE

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

TLP: WHITE

Vulnerability Management Program

Web Profiler

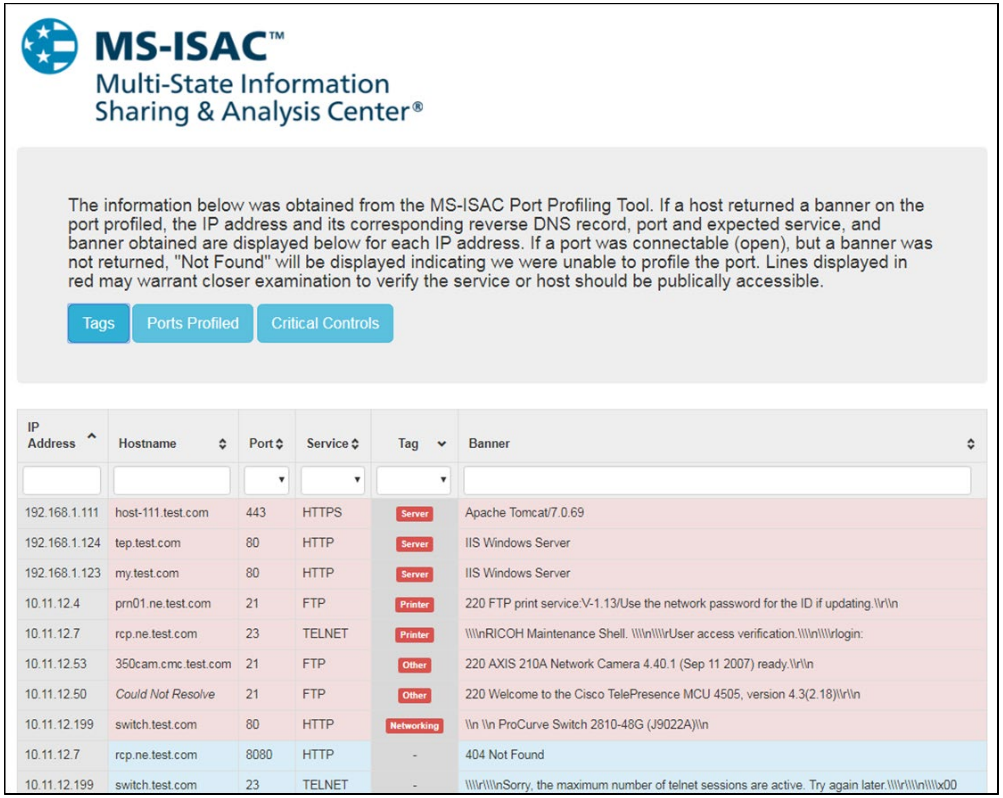
- ✓Server type and version (IIS, Apache, etc.)
- ✓Web programming language and version (PHP, ASP, etc.)
- ✓Content Management System and version (WordPress, Joomla, Drupal, etc.)

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

Port Profiler

- **Quarterly notifications**
- **Contact vmp.dl@cisecurity.org to:**
  - Opt out of this service
  - Provide feedback on the Port Profiler
- **Contact soc@cisecurity.org if:**
  - You wish to add IP addresses
  - To verify "VMP Notification" contacts
- **Source IP address: 52.14.79.150**



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

The information below was obtained from the MS-ISAC Port Profiling Tool. If a host returned a banner on the port profiled, the IP address and its corresponding reverse DNS record, port and expected service, and banner obtained are displayed below for each IP address. If a port was connectable (open), but a banner was not returned, "Not Found" will be displayed indicating we were unable to profile the port. Lines displayed in red may warrant closer examination to verify the service or host should be publically accessible.

IP Address	Hostname	Port	Service	Tag	Banner
192.168.1.111	host-111.test.com	443	HTTPS	Server	Apache Tomcat/7.0.69
192.168.1.124	tep.test.com	80	HTTP	Server	IIS Windows Server
192.168.1.123	my.test.com	80	HTTP	Server	IIS Windows Server
10.11.12.4	prn01.ne.test.com	21	FTP	Printer	220 FTP print service:V-1.13/Use the network password for the ID if updating.\\r\\n
10.11.12.7	rcp.ne.test.com	23	TELNET	Printer	\\\\nRICOH Maintenance Shell. \\\\n\\\\rUser access verification.\\\\n\\\\rlogin:
10.11.12.53	350cam.cmc.test.com	21	FTP	Other	220 AXIS 210A Network Camera 4.40.1 (Sep 11 2007) ready.\\r\\n
10.11.12.50	*Could Not Resolve*	21	FTP	Other	220 Welcome to the Cisco TelePresence MCU 4505, version 4.3(2.18)\\r\\n
10.11.12.199	switch.test.com	80	HTTP	Networking	\\n \\n ProCurve Switch 2810-48G (J9022A)\\n
10.11.12.7	rcp.ne.test.com	8080	HTTP	-	404 Not Found
10.11.12.199	switch.test.com	23	TELNET	-	\\\\r\\\\nSorry, the maximum number of telnet sessions are active. Try again later.\\\\r\\\\n\\\\x00

Malicious Code Analysis Platform

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

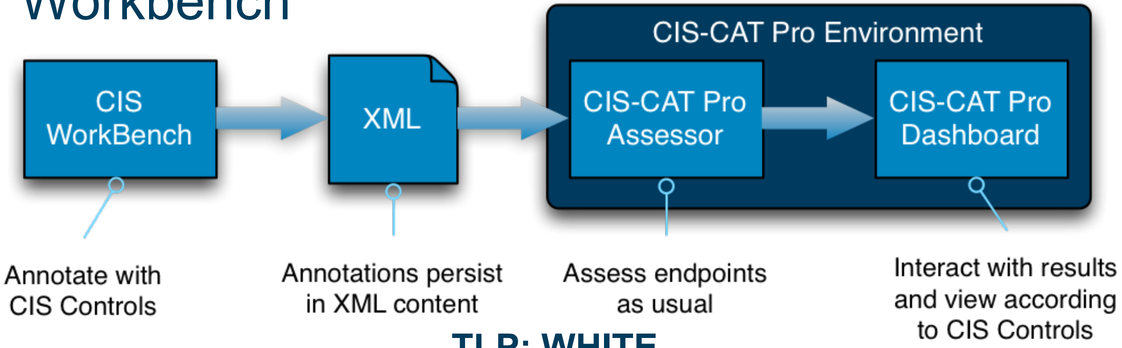
- Executables
- DLLs
- Documents
- Quarantine files
- Archives

To gain an account contact:

mcap@cisecurity.org

SecureSuite

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

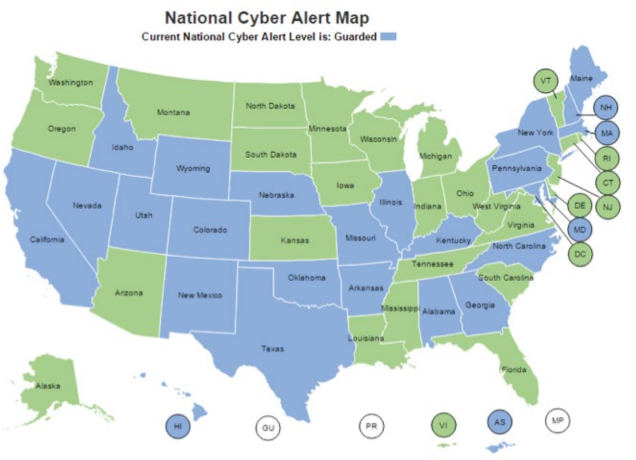

CIS-CAT Pro Environment
CIS WorkBench
XML
CIS-CAT Pro Assessor
CIS-CAT Pro Dashboard
Annotate with CIS Controls
Annotations persist in XML content
Assess endpoints as usual
Interact with results and view according to CIS Controls

TLP: WHITE

HSIN Community of Interest

Access to:

- MS-ISAC Cyber Alert Map
- Archived webcasts & products
- Cyber table top exercises
- Guides and templates
- Message boards



National Cyber Alert Map

Current National Cyber Alert Level is: Guarded

HSIN

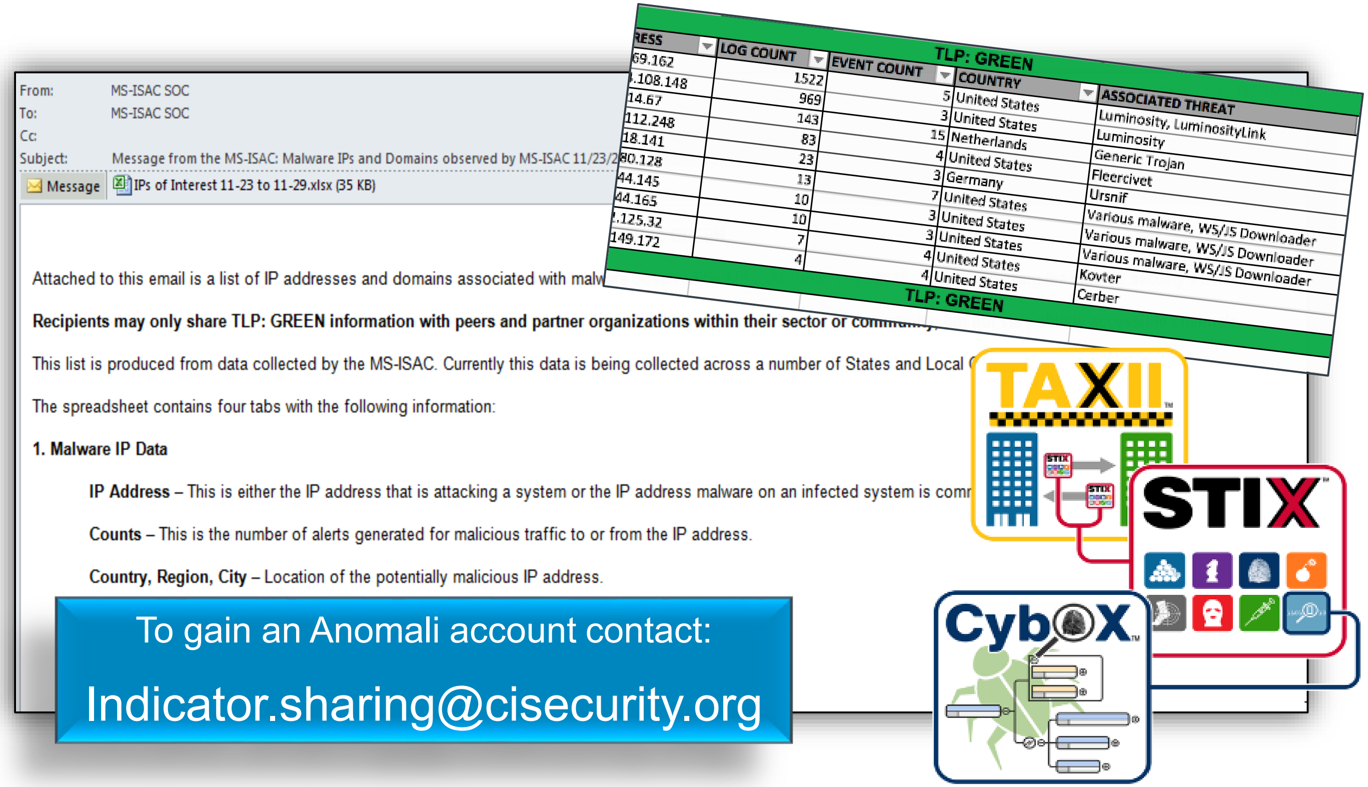
HOMELAND SECURITY INFORMATION NETWORK

The Trusted DHS Information Sharing Environment

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 11/23/2

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 malw

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 Local

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 comr

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.

TLP: GREEN

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

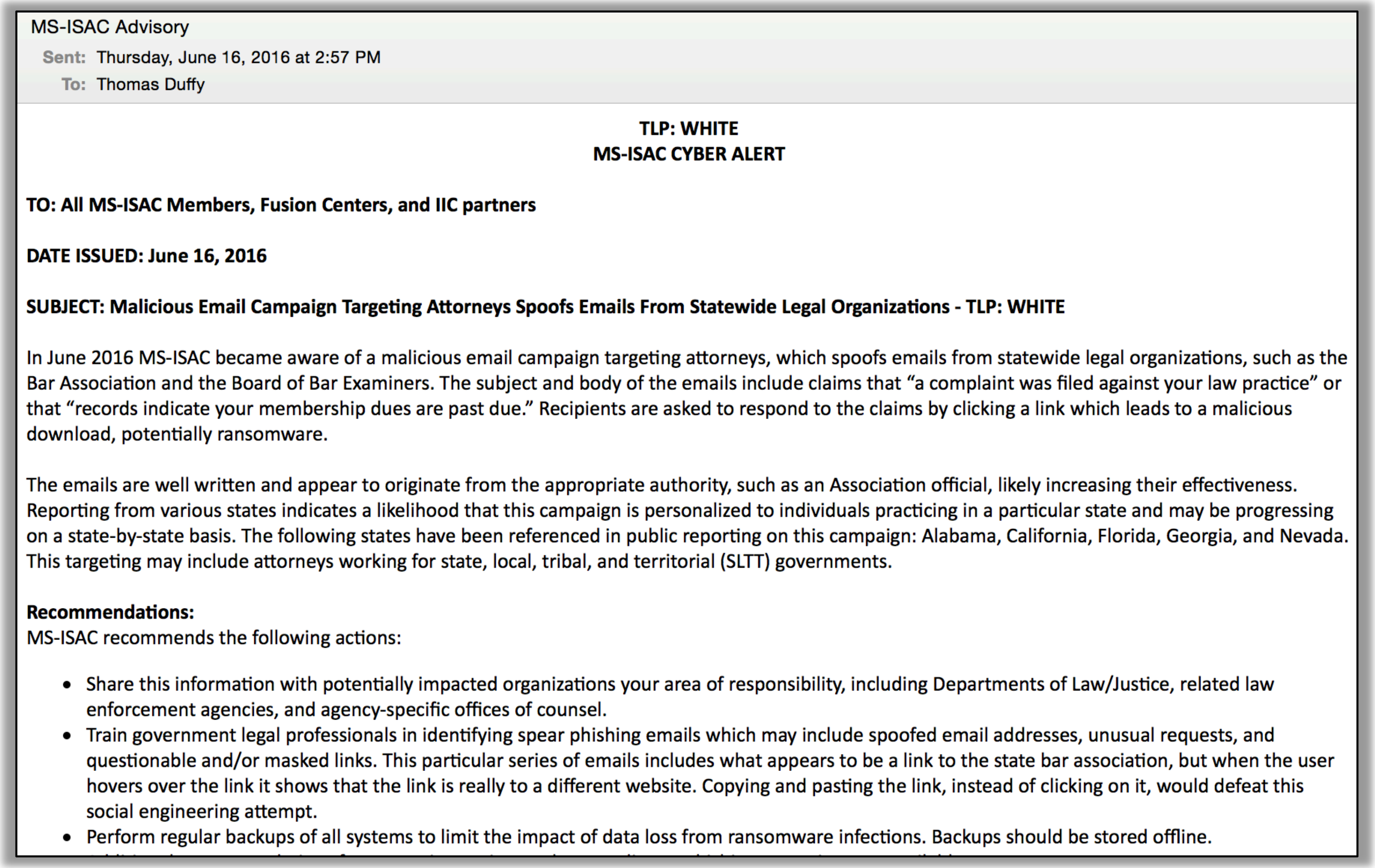
TLP: GREEN

To gain an Anomali account contact:

Indicator.sharing@cisecurity.org

TLP: WHITE

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

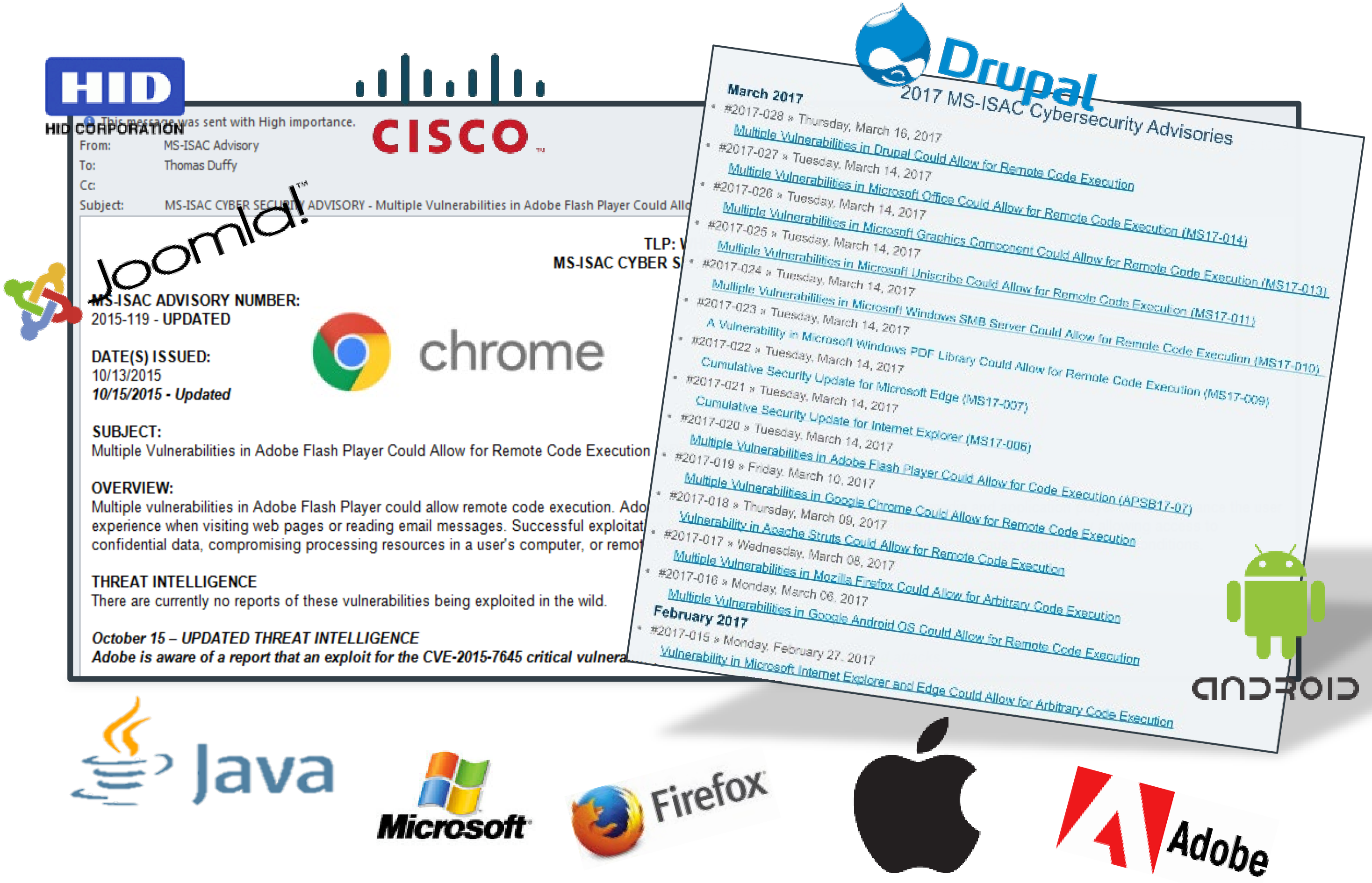
In June 2016 MS-ISAC became aware of a malicious email campaign targeting attorneys, which spoofs emails from statewide legal organizations, such as the Bar Association and the Board of Bar Examiners. The subject and body of the emails include claims that “a complaint was filed against your law practice” 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.

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 Allo

TLP: W
MS-ISAC CYBER S

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. Ado
experience when visiting web pages or reading email messages. Successful exploitat
confidential data, compromising processing resources in a user's computer, or remot

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 vulnera

2017 MS-ISAC Cybersecurity Advisories

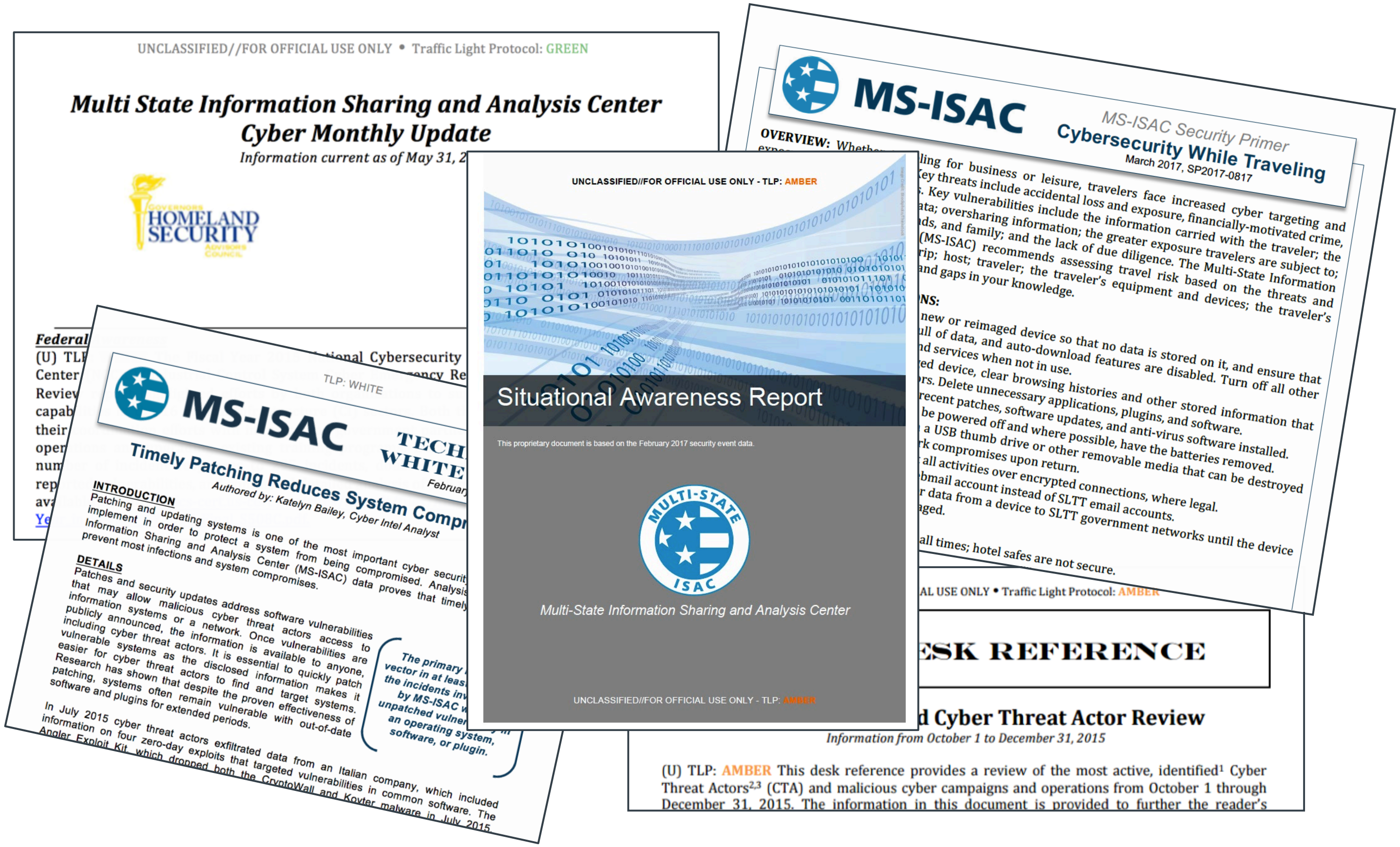
March 2017

- #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 Graphics Component Could Allow for Remote Code Execution (MS17-013)
- #2017-025 » Tuesday, March 14, 2017
  Multiple Vulnerabilities in Microsoft Uniscribe Could Allow for Remote Code Execution (MS17-011)
- #2017-024 » Tuesday, March 14, 2017
  Multiple Vulnerabilities in Microsoft Windows SMB Server Could Allow for Remote Code Execution (MS17-010)
- #2017-023 » Tuesday, March 14, 2017
  A Vulnerability in Microsoft Windows PDF Library Could Allow for Remote Code Execution (MS17-009)
- #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)
- #2017-020 » Tuesday, March 14, 2017
  Multiple Vulnerabilities in Adobe Flash Player Could Allow for Code Execution (APSB17-07)
- #2017-019 » Friday, March 10, 2017
  Multiple Vulnerabilities in Google Chrome Could Allow for Remote Code Execution
- #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

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, 2

Federal
(U) TL... Center... Review... capab... their... oper... num... rep... ava... Ye...
...onal Cybersecurity ...ency Re...

MS-ISAC TLP: WHITE
TECH... WHITE...
Februar...

Timely Patching Reduces System Compr...

Authored by: Katelyn Bailey, Cyber Intel Analyst

INTRODUCTION
Patching and updating systems is one of the most important cyber securit... implement in order to protect a system from being compromised. Analysis... Information Sharing and Analysis Center (MS-ISAC) data proves that timely... 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 leas... the incidents inv... by MS-ISAC w... unpatched vulner... 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: Wheth... expo... ...ling for business or leisure, travelers face increased cyber targeting and ...Key threats include accidental loss and exposure, financially-motivated crime, ...s. Key vulnerabilities include the information carried with the traveler; the ...ata; oversharing information; the greater exposure travelers are subject to; ...nds, and family; and the lack of due diligence. The Multi-State Information ...(MS-ISAC) recommends assessing travel risk based on the threats and ...rip; host; traveler; the traveler's equipment and devices; the traveler's ...and gaps in your knowledge.

...NS:
...new or reimaged device so that no data is stored on it, and ensure that ...ull of data, and auto-download features are disabled. Turn off all other ...nd services when not in use.
...ed device, clear browsing histories and other stored information that ...rs. Delete unnecessary applications, plugins, and software.
...recent patches, software updates, and anti-virus software installed.
...be powered off and where possible, have the batteries removed.
...a USB thumb drive or other removable media that can be destroyed ...rk compromises upon return.
...all activities over encrypted connections, where legal.
...bmail account instead of SLTT email accounts.
...r data from a device to SLTT government networks until the device ...aged.
...all times; hotel safes are not secure.

...AL USE ONLY • Traffic Light Protocol: AMBER

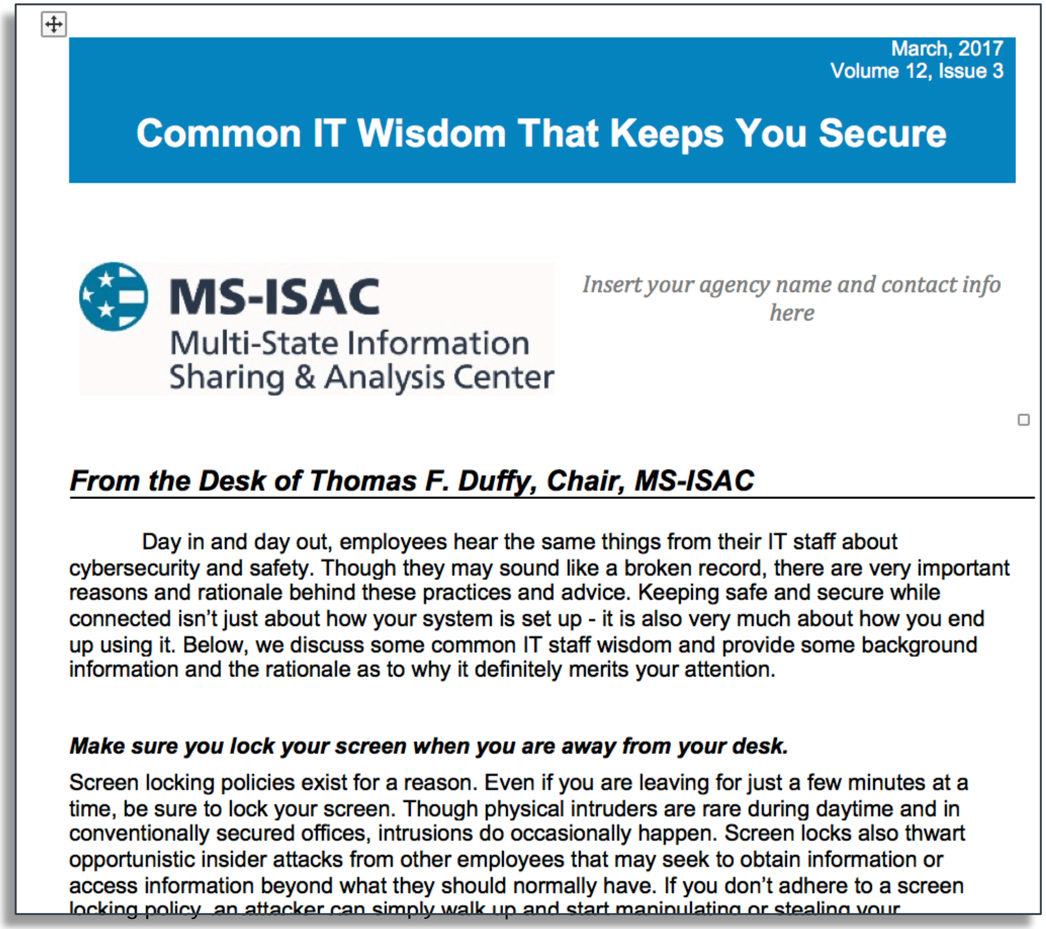
...ESK REFERENCE

...d 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[1] Cyber Threat Actors[2,3] (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

Monthly Newsletter

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



March, 2017
Volume 12, Issue 3

Common IT Wisdom That Keeps You Secure

MS-ISAC
Multi-State Information Sharing & Analysis Center

Insert your agency name and contact info here

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

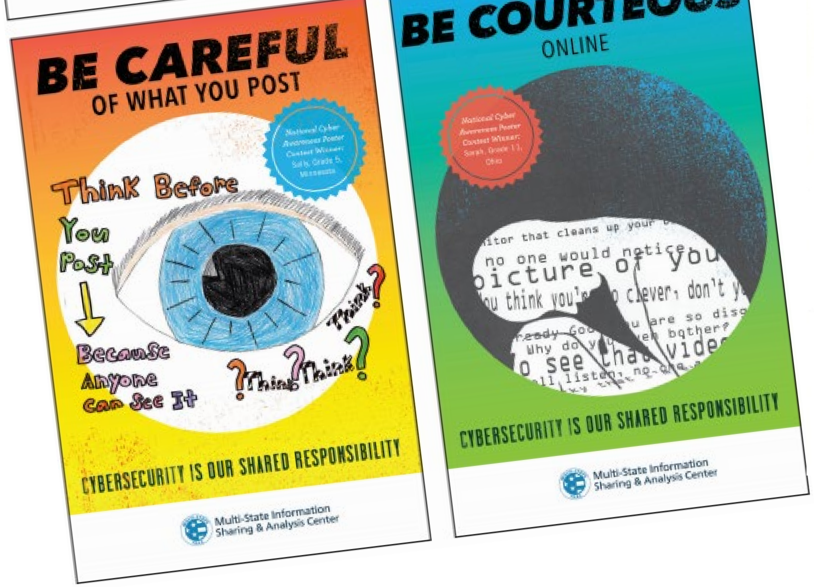
Day in and day out, employees hear the same things from their IT staff about cybersecurity and safety. Though they may sound like a broken record, there are very important reasons and rationale behind these practices and advice. Keeping safe and secure while connected isn't just about how your system 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.

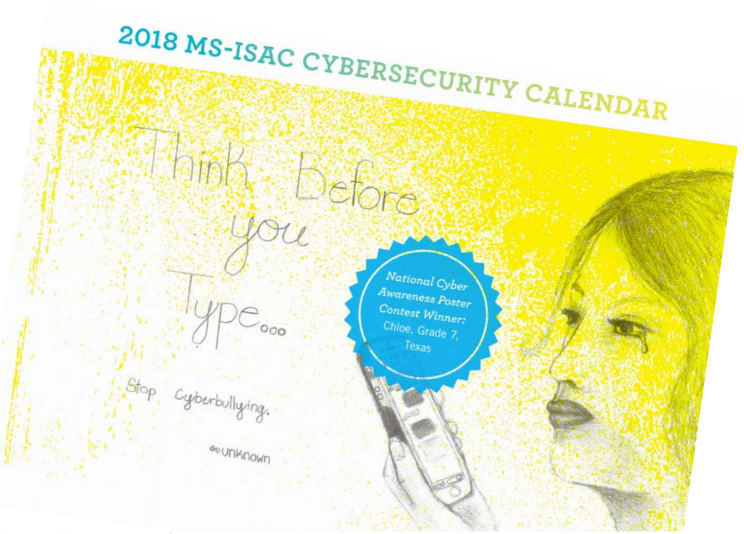
Make sure you lock your screen when you are away from your desk.

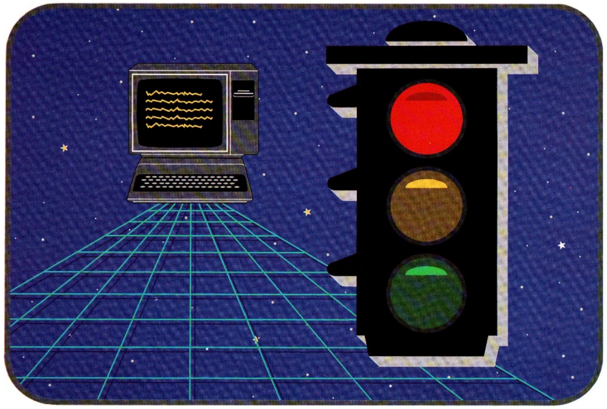
Screen locking policies exist for a reason. Even if you are leaving for just a few minutes at a time, be sure to lock your screen. Though physical intruders are rare during daytime and in conventionally secured offices, intrusions do occasionally happen. Screen locks also thwart opportunistic insider 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

Cybersecurity Awareness Toolkit

DON'T SHARE
PERSONAL INFORMATION ONLINE
National Cyber Awareness Poster Contest Winner: Faith, Grade 11, Virginia
CYBERSECURITY IS OUR SHARED RESPONSIBILITY
Multi-State Information Sharing & Analysis Center
ONLY VISIT
TRUSTED SITES
National Cyber Awareness Poster Contest Winner: Sergio, Grade 10, Virginia
CARD
CYBERSECURITY IS OUR SHARED RESPONSIBILITY
Multi-State Information Sharing & Analysis Center


BE CAREFUL
OF WHAT YOU POST
National Cyber Awareness Poster Contest Winner: Sally, Grade 5, Minnesota
Think Before You Post
Because Anyone Can See It
Think? Think? Think?
CYBERSECURITY IS OUR SHARED RESPONSIBILITY
Multi-State Information Sharing & Analysis Center
BE COURTEOUS
ONLINE
National Cyber Awareness Poster Contest Winner: Sarah, Grade 11, Ohio
no one would notice
picture of you
you think you're clever, don't y
why do you bother?
CYBERSECURITY IS OUR SHARED RESPONSIBILITY
Multi-State Information Sharing & Analysis Center


2018 MS-ISAC CYBERSECURITY CALENDAR
Think Before you Type...
Stop Cyberbullying.
unknown
National Cyber Awareness Poster Contest Winner: Chloe, Grade 7, Texas



Have you logged off your terminal?

© 1988 Vanguard Marketing Services 441 Howard Street Northborough, MA 01532 (617) 393-8347

FedVTE

Free Online Training Environment

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

www.fedvte.usalearning.gov

FedVTE
FEDERAL VIRTUAL TRAINING ENVIRONMENT
U.S. DEPARTMENT OF HOMELAND SECURITY
CYBER SECURITY

Request Account

Request an access email here.

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

TLP: WHITE

CIS™ Center for Internet Security®

MS-ISAC
Multi-State Information
Sharing & Analysis Center

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