MS-ISAC Cyber Monthly Update
September 2019 Edition • Information current as of October 11, 2019

State, Local, Tribal, Territorial (SLTT) Government and Federal Awareness

TLP: WHITE The Cybersecurity and Infrastructure Security Agency (CISA) released four new CISA Insights products. These documents are informed by U.S. intelligence and real-world events and provide a description of the threat, lessons learned, recommendations, and additional relevant resources. The individual products are accessible via the following links:

- Mitigate DNS Infrastructure Tampering
- Remediate Vulnerabilities for Internet-Accessible Systems
- Secure High Value Assets
- Enhance Email and Web Security

Analyst Note: The first CISA Insights product, released on August 21, 2019, covered the ransomware outbreak topic. SLTT government entities are encouraged to read these products and implement any relevant recommendations.

---

TLP: WHITE On September 20, 2019, Microsoft announced two additions to its Defending Democracy Program. First, Microsoft is offering free security updates through the end of 2020 for Windows 7 operating systems installed on federally certified voting systems. Microsoft planned to stop providing free security updates for Windows 7 in January 2020, only offering updates for a fee until January 2023 as enterprises transition to newer systems. Additionally, the U.S. Election Assistance Commission says it will not de-certify voting systems using Windows 7 in an acknowledgement of the challenges keeping these systems up-to-date compared to newer systems, such as Windows 10. The second addition from Microsoft's Defending Democracy Program involves election offices using Microsoft Azure. Microsoft announced they are identifying and engaging election offices using Azure and providing them with guidance and technical assistance on how to use the most advanced security features they have to offer.

Analyst Note: The MS-ISAC recommends implementing a patch management program to keep systems up-to-date. SLTT government entities are encouraged to review the CIS End-of-Support (EOS) list and to audit their systems for out-of-date or EOS software requiring remediation. As systems approach end-of-life, SLTT government entities should review their system lifecycle to determine the need for continued support or replacement. This review should include engaging vendors to establish their expected level of support for systems after underlying hardware and software enters EOS. Even though Microsoft is specifically extending service support to voting systems operating on Windows 7, these updates are a temporary solution and will cease shortly after the election. Election officials should work now to identify systems or updates using newer
operating systems to replace Windows 7 instances shortly after the 2020 General Election concludes.

---

**TLP: WHITE** On September 25, 2019, CISA updated their National Emergency Communications Plan (NECP). Per CISA, “The NECP is the nation’s strategic plan to strengthen and enhance emergency communications capabilities. The NECP navigates the complex mission of maintaining and improving emergency communications capabilities for emergency responders and serves as the Nation’s roadmap to ensuring emergency communications interoperability at all levels of government.” Goal 6 of the NECP aims to strengthen the cybersecurity posture of the emergency communications ecosystem by:

- Developing and maintaining cybersecurity risk management
- Mitigating cybersecurity vulnerabilities
- Determining public safety-specific, standards-based cyber hygiene minimums and fund ongoing risk management.

**Malware, TTPs, and Cyber Threat Actors**

**TLP: WHITE** FireEye, a cybersecurity vendor, published a white paper on best practices for defending against ransomware attacks, “Ransomware Protection and Containment Strategies: Practical Guidance for Endpoint Protection, Hardening and Containment.” In the document overview, FireEye states that, “The purpose of this document is to provide practical endpoint security controls and enforcement measures which can limit the capability for a ransomware or malware variant to impact a large scope of systems within an environment. If there is an active outbreak, depending upon the propagation method that the variant is leveraging, implementing many of the recommendations within this document can potentially disrupt and contain the event.” The document is broken down into sections for “endpoint hardening” and “credential exposure and usage hardening.” The white paper includes instructions for implementing the recommendations, such as those for endpoint segmentation.

**Analyst Note:** The MS-ISAC recommends members read this white paper and other relevant ransomware best practices guides to supplement their current ransomware prevention and mitigation strategies. For an overview on ransomware, including recommendations, please visit the recently updated MS-ISAC Ransomware Security Primer.

---

**TLP: WHITE** On September 10, 2019, the U.S. Department of Justice announced the arrest of 281 people associated with Business Email Compromise (BEC) schemes. According to the Department of Justice, “BEC, also known as ‘cyber-enabled financial fraud,’ is a sophisticated scam often targeting employees with access to company finances and businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments.” The arrests and seizures were the end result of Operation reWired, which was a four-month long coordinated law enforcement effort conducted by multiple U.S. federal departments. The operation concluded with arrests in the U.S. and across the globe, including individuals from Turkey, Ghana, France, Italy, Japan, Kenya, Malaysia, the United Kingdom, and Nigeria. The U.S. Department of Justice announcement includes BEC statistics from the FBI’s Internet Crime Complaint Center (IC3) showing that, in 2018, BEC and its variants accounted for nearly $1.3 billion in losses.

---

**TLP: GREEN**

Limited disclosure, restricted to the community. Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. TLP: GREEN information may not be released outside of the community. [https://www.us-cert.gov/tlp](https://www.us-cert.gov/tlp)
**TLP: GREEN**

**Analyst Note:** State, local, tribal, and territorial (SLTT) governments are frequently targeted by BEC scams that attempt to deceive victims into sending money, personally identifiable information (PII), or material goods, or modifying direct deposit information. The emails often originate from spoofed, compromised, or fraudulent email accounts and if fulfilled may result in significant financial loss or data exposure. For more information on BEC, please visit the MS-ISAC Security Primer.

---

**TLP: WHITE** Multiple cybersecurity publications are reporting that the Emotet malware is back in operation after a four month disappearance. Some of the recent campaigns are targeting victim’s email inboxes to hijack legitimate email conversations in an effort to further propagate the malware. This tactic allows the cyber threat actors (CTA) to more easily evade email filters. Additionally, it increases the likelihood that recipients will download the malware because they recognize the ongoing email chain. After vanishing in early June 2019, recently observed malspam emails are delivering Emotet with language templates designed for distribution across Europe and the United States.

**Analyst Note:** Over the past few weeks, the MS-ISAC began receiving suspicious email submissions from SLTT government entities that included links or attachments for the Emotet payload. Additionally, over the same time period, MS-ISAC Albert sensors started firing on signatures related to Emotet activity. It is likely that this activity will continue to increase in the near-future.

Emotet is among the most costly and destructive malware affecting SLTT governments. Its highly infectious nature makes it difficult to combat and costs SLTT government up to $1 million per incident due to its worm-like features, resulting in rapid, network-wide infections. Emotet is an advanced, modular infostealer that primarily functions as a downloader or dropper of banking trojans. Emotet is disseminated through malspam, emails containing malicious attachments or links, using branding familiar to the recipient, including the MS-ISAC name.

Please visit the MS-ISAC Emotet Security Primer for more information.

**Data Breaches**

**TLP: WHITE** On September 19, 2019, researchers at Greenbone Networks, a German company, reported that confidential patient data is freely accessible on the internet. Their research shows that, “Of the 2,300 archive systems worldwide that were analyzed, 590 of them have been identified as accessible on the internet; together they contain over 24 million data records from patients from across 52 countries. There are more than 737 million images linked to this patient data, around 400 million of which are accessible or can be easily downloaded from the internet. In addition, there are 39 systems that allow access to patient data via an unencrypted HTTP Web Viewer, without any protection.”

**Analyst Note:** An important cybersecurity best practice is to ensure that sensitive data is not publicly available on the internet. It is equally important to mitigate known vulnerabilities, which could lead to unauthorized access. This highlights the importance of asset/software inventory and continuous vulnerability scanning.

SLTT government entities can leverage the MS-ISAC’s Vulnerability Management Program (VMP) to receive monthly reports on any outdated software that could pose a threat to assets. In

**TLP: GREEN**

Limited disclosure, restricted to the community. Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. TLP: GREEN information may not be released outside of the community. https://www.us-cert.gov/tlp
order to alert members of outdated software, the MS-ISAC collects server type and version (IIS, Apache, Nginx, etc.), web programming language and version (PHP, ASP, etc.), and content management system and version (WordPress, Joomla, Drupal, etc.). The MS-ISAC Services Guide provides a full list of resources available to SLTTs.

Nation-States

TLP: WHITE The RAND Corporation, an American global policy think tank, released a free e-book on international cyber coercion, “Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace.” The authors report that nation-states like Russia and North Korea appear to be more likely to have used cyber operations as a coercive tool than China and Iran. Despite their low probability of success, the authors still anticipate that nation-states will continue to use these methods in the future. The RAND Corporation listed the following key findings:

- Cyber operations intended to coerce are a small subset of overall cyber operations globally.
- Espionage remains the predominant purpose of states’ cyber operations.
- Russian cyber operations appear to have had some coercive intent in Ukraine and Montenegro.
- Chinese cyber operations show a continued focus on espionage, but potentially with some coercive intent as a secondary objective.
- Iranian cyber operations appear more focused on retaliating against regional neighbors and the West, rather than serving a direct coercive purpose.
- North Korea has routinely engaged in coercive acts in the physical world and sees cyber operations as another means to coerce others.
- The assessment of these cases indicates how the threat, threat actor, and the desired change in behavior is often unclear and ambiguous, though this ambiguity does not appear to prevent countries from pursuing these coercive campaigns.

The authors also recommend that the United States and its partners need to develop a better understanding of cyber coercion, including ways to deter and respond to it.

***

TLP: WHITE On September 23, 2019, the U.S. Department of State released a “Joint Statement on Advancing Responsible State Behavior in Cyberspace,” which was affirmed by 26 other countries. Their statement recognizes that, “State and non-state actors are using cyberspace increasingly as a platform for irresponsible behavior from which to target critical infrastructure and our citizens, undermine democracies and international institutions and organizations, and undercut fair competition in our global economy by stealing ideas when they cannot create them.” The statement reiterates the importance for the framework on responsible state behavior in cyberspace, which was affirmed by all members of the United Nations General Assembly in 2010, 2013, and 2015. Additionally, these countries commit to further developing an international rules-based order, helping others build their cybersecurity capacities, and to hold states accountable for bad behavior in cyberspace.

General Awareness

TLP: WHITE On September 26, 2019, DEF CON released the report from the DEF CON 27 Voting Village. The report, “Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure,” reviewed the results of participants attempting to access the provided election equipment including direct-recording electronic voting machines, electronic poll books, optical

TLP: GREEN

Limited disclosure, restricted to the community. Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. TLP: GREEN information may not be released outside of the community. https://www.us-cert.gov/tlp
scanners, and for the first time, ballot marking devices and hybrid systems. According to the report, this year’s participants were able to replicate previously published methods as well as find new ways to compromise the available direct recording electronic machines, which could lead to altering of stored vote tallies, the ballots displayed to voters, or the internal software that controls the voting machines. The findings underscored how all segments of a system in terms of hardware, software, and firmware may have vulnerabilities to evaluate and mitigate. There were no significant updates from the vulnerabilities identified in the August reporting of this year’s Voting Village, which included the use of default credentials, exploitation of removable media, administrative access, and potential remote exploitation. As with previous reports, the researchers detailed concerns on the election supply chain and the lack of best practices, such as using voting equipment with paper record trails and risk-limiting audits to offset potential tampering attempts. They also provided security recommendations for state and local election officials and mutual next steps for the U.S. Congress and election offices.

**Analyst Note:** Similar to the Voting Village in previous years, extended physical access to the machines was a major factor in the successful compromise of election equipment. Many of the reported vulnerabilities can be mitigated using best practices, such as a voter verified paper audit trails, physical security measures, and common cybersecurity measures. For access to relevant best practices, please reference the CIS’ (Center for Internet Security’s) [*A Handbook for Elections Infrastructure Security*](https://www.us-cert.gov/tip).

---

**TLP: WHITE** On September 5, 2019, IBM Security announced the results of a survey gauging taxpayers views on municipal ransomware attacks. IBM Security sponsored the study, which was conducted by Morning Consult and based on the responses of 2,200 US citizens. Some of the key findings include:

- 75% of respondents expressed concern about the threat to personal data and nearly 80% feared the impact on cities
- Close to 60% of U.S. citizens are against their local governments using tax dollars to pay ransoms
- More than 60% of respondents would prefer their city to deal with the larger recovery costs rather than use tax dollars to pay ransom in a ransomware attack
- Just under half of responding citizens believe protecting cities from ransomware is the federal government’s job, above state and local decision makers - and nearly 90% of U.S. citizens are in favor of increasing federal funding to improve cybersecurity in cities

---

**TLP: WHITE** On September 18, 2019, the MITRE Corporation updated their “Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Errors (CWE Top 25).” The MITRE Corporation describes the CWE Top 25 as “a demonstrative list of the most widespread and critical weaknesses that can lead to vulnerabilities in software."

**Analyst Note:** The MITRE Corporation is also well-known for the creation of the MITRE ATT&CK™ Framework, which enumerates a CTA’s tactics, techniques, and procedures (TTPs). SLTT government entities can use this framework to map out likely attack scenarios and to better understand how these attacks should be mitigated.
Appendix A

MS-ISAC Speaking Engagements

Below is the list of October and November 2019 speaking engagements where MS-ISAC staff will be in attendance:

- October 21-23: IIPS Fall Conference 2019 (Charlotte, NC); Jamie Ward
- October 24-26: Nebraska County Election Officials’ October Training (Kearny, NE); Kateri Gill
- October 30: FEMA Regional Workshop Series (Bossier City, LA); Stacey Wright
- November 7: 4th Annual Security and Risk Management Symposium (Pittsburgh, PA); Stacey Wright
- November 12-15: CETPA Annual Conference (Anaheim, CA); Greta Noble & Brendan Montagne
- November 14: Delaware Cyber Security Advisory Council (Delaware); Stacey Wright
Appendix B

New Papers
TLP: GREEN Papers recently disseminated by MS-ISAC and EI-ISAC
- MS-ISAC Cyber Alert, "Widespread Sextortion Hoax Scam Affecting SLTT Governments" (TLP: GREEN) September 11, 2019
- EI-ISAC Cybersecurity Spotlight, "Hardware, Software, and Firmware" (TLP: WHITE) September 13, 2019
- MS-ISAC Cyber Alert, "Emotet Resume Malspam Campaign Using MS-ISAC Branding" (TLP: GREEN) September 20, 2019
- MS-ISAC Intel Advisory, "DNS-Over-HTTPS (DOH) Adoption in Process" (TLP: WHITE) September 23, 2019

TLP: GREEN MS-ISAC disseminated papers from other sources
- FBI FLASH, “Increased Number of Emotet Command and Control IP Addresses Identified” (TLP: WHITE) September 9, 2019
- United States Secret Service Information Only Alert, “Inventory/Invoice Fraud and BEC” (TLP: GREEN) September 9, 2019
- FBI Public Service Announcement, “Business Email Compromise: The $26 Billion Scam” (TLP: WHITE) September 10, 2019
- Canadian Centre for Cyber Security Cyber FLASH, “TFlower Ransomware Campaign” (TLP: GREEN) September 23, 2019

Recipients are encouraged to further disseminate this newsletter to their membership.

TLP: WHITE The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation’s state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance is available at 866-787-4722, SOC@cisecurity.org. The MS-ISAC is interested in your comments - an anonymous feedback survey is available.