TLP: WHITE

Image Credit: iStockphoto/Thinkstock

2017 SLTT Government Outlook

January 2017

Multi-State Information Sharing and Analysis Center
31 Tech Valley Drive, East Greenbush, NY 12061 • 518-266-3460 • info@cisecurity.org,
www.cisecurity.org

TLP: WHITE

MS-ISAC 2017 SLTT Government Outlook

The Multi-State Information Sharing and Analysis Center (MS-ISAC) expects that the majority of cyber incidents affecting state, local, tribal, and territorial (SLTT) governments will continue to be opportunistic in nature. We also believe the sophistication of routine malware, cyber threat actors,[1] and their tactics, techniques, and procedures (TTPs) will continue to increase.

TACTICS, TECHNIQUES, and PROCEDURES

Well-Crafted Social Engineering

The MS-ISAC expects cyber threat actors using a combination of research and social engineering will produce more accurate phishing emails and tailored lures, with fewer obvious mistakes. The current trend of compromising login credentials in order to send phishing emails from the compromised email accounts is also highly likely to continue and is a good case example of well-crafted social engineering in opportunistic targeting.

In 2016 there were numerous Business Email Compromise (BEC) scams, which affected industry as a whole, as well as the SLTT government community, and we believe these scams will continue in 2017. We are confident that the targeting of SLTT governments was opportunistic, although the cyber threat actors conducted research in order to craft more tailored lures. As with 2016, it is highly likely that SLTT governments, including schools and universities, will mostly encounter two of the variants - the wire transfer/purchase order variant and the W-2/personally identifiable information (PII) request variant.

Malware

We are almost certain that the increasing sophistication of cybercrime TTPs identified in 2016 will continue in 2017. This is likely to result in new hybrid malware variants, more detailed scams and social engineering ruses, and more sophisticated delivery mechanisms. As with past years, we expect that financially-motivated cyber threat activity will remain the most prevalent type of activity during 2017, with most malware and attacks motivated by this purpose. Based on the last half of 2016, we believe that ransomware, downloaders, and banking Trojans will be the most common types of malware posing a threat to SLTT governments during the first half of 2017.

Extortion

In 2016 cyber extortion became a common TTP, and we believe that it will remain a prominent threat in 2017, with expanding capabilities. We have high confidence that crypto-ransomware variants, in particular, will remain among the top type malware for SLTT government entities for the majority of the year. Cyber threat actors will almost certainly continue to develop hybrid ransomware variants, including additional TTPs and merging ransomware with other types of scams, frauds, and malware, to create hybrid attacks. We believe that other extortion TTPs will also continue to increase in popularity and threaten/result in data exposure, DDoS attacks, and other malicious activity.

DDoS

We expect that distributed denial of service (DDoS) attacks targeting SLTT governments will continue to be a common TTP. It is highly probable that

[1] A cyber threat actor is a participant *(person, group, or organization)* in an action or process that is characterized by malice or hostile action *(intending harm)* towards an environment of computers, information technology, or virtual reality.

motivations will range from unknown causes to causes as specific as preventing a school exam, or in response to an incident involving a perceived injustice or the alleged use of excessive force by a law enforcement official. We are virtually certain that many DDoS attacks against SLTT governments in 2017 will continue as lower bandwidth attacks, compared to the record bandwidth attacks reported by some sectors. Despite this, it is critical to note that these attacks are still likely to cause outages for most targeted SLTT government websites and networks. Additionally, we confidently assess that cyber threat actors are highly likely to continue using unsecured Internet of Things (IoT) device botnets to conduct DDoS attacks and that it is possible that the IoT botnets will target or tangentially impact SLTT government networks. It is equally as likely that SLTT government owned devices will be compromised and included in the botnets, resulting in SLTT governments participating in DDoS attacks against other entities.

Based on historical trends, we believe the chances are good that a few K-12 schools will specifically be targeted by DDoS attacks around the time of school exams, with the intent of disrupting the exams.

Destructive Attacks

In 2016 our assessment was that there was a slight chance that purely destructive cyber attacks, currently occurring outside of the SLTT government sector and could unintentionally affect SLTT government entities. This assessment has not changed for 2017.

TARGETED DATA and SYSTEMS

Internet of Things & Critical Infrastructure

IoT will almost certainly play a defining role in the 2017 cyber threat landscape. In addition to DDoS attacks, we have moderate to high confidence that all of the news media and cybersecurity interest in IoT devices will drive the development of new TTPs or modification of existing TTPs to use and target IoT devices. There is a slight chance that the focus on IoT will result in a derivative focus on IoT devices in critical infrastructure. If this occurs, we have moderate confidence of an increased threat to SLTT government owned critical infrastructure.

We are convinced that SLTT government end-users are currently and will continue to bring IoT devices into their workplaces for personal and professional use. As a result, SLTT governments will need to contend with the related wireless connectivity, data sharing, and security concerns related to personal use devices. Approved SLTT government-owned IoT devices, such as drones and body worn cameras, as well as the push for smart cities and pervasive WiFi access, will create a greater burden on information technology departments as they seek to inventory these devices, incorporate them into the network, and ensure cybersecurity remains a priority.

Data Reuse

The chances are good that the threat from data reuse will continue to escalate in 2017. This threat is mostly derived from publicly shared data dumps containing login credentials, which end-users have used for both work and personal accounts.

TARGETED SECTORS

Universities

We have high confidence that universities will remain a common target in 2017. Common malware meant for financial gain will be the most likely threat, although attempts to compromise login credentials, gain access to PII and/or sensitive research, or for use as a launching point in other attacks are all possible.

Supply Chain

The MS-ISAC does not believe that the SLTT government supply chain, which includes both products and third-party provided services, is being specifically targeted. However, we do believe that the supply chain continues to be a point of weakness and that supply chain compromises will almost certainly affect SLTT governments. SLTT governments should have a heightened interest in the cybersecurity of third parties, as a result of the various third party compromises that affected SLTT governments in 2016 and the open source reporting of backdoors and other vulnerabilities in common software and devices.

Industrial Control Systems

The 2017 threat against Industrial Control Systems (ICS) remains a wildcard, especially with the current interest in IoT. Exploits exist to target ICS, and tools, such as SHODAN and Censys, make identifying Internet-facing systems extremely easy, while at the same time security researchers publicly discuss ICS vulnerabilities and malicious actors show interest in ICS honeypots. However, these factors have existed together for the last several years with only a few major attacks occurring.

High-Availability Entities

We believe there is a slight chance high-availability industries or services, such as the critical functionality in healthcare and transit that requires 100% uptime, will be strategically targeted as cyber threat actors take advantage of the availability requirements.

Healthcare

It is likely that the healthcare sector will remain a popular target for cybercriminals in 2017. Beyond the common TTP's experienced by all SLTT sectors, the MS-ISAC is confident that the strict regulation on protected health information and the recently expanded definition of what constitutes a "data breach," will impact how health organizations respond to intrusions in the coming year.

CYBER THREAT ACTORS

Cybercriminals & Hacktivists

The pattern of singular cyber threat actors, primarily cybercriminals and hacktivists, appearing and conducting a multitude of limited-duration campaigns against SLTT governments will continue to occur into 2017, creating prominent, but unpredictable spikes in activity. We have high confidence that DDoS attacks and doxing will continue to be two of the most prolific TTPs. It is possible that hacktivists will also continue to target associations and other SLTT government-affiliated entities, during campaigns targeting SLTT governments.

The attention seeking motivation is highly likely to remain a common motivation among cybercriminals who take credit for their activities. While we do not believe the sale of compromised SLTT government data will pose a significant threat to SLTT government entities in 2017, we do believe that a few cybercriminals will attempt to compromise and sell SLTT government data for financial gain. In addition, we believe the trend of falsified claims, especially cyber threat actor claims of exfiltrating data that is already publicly available and/or providing falsified data, will continue.

Traditional Criminals

The MS-ISAC believes that there is a growing movement by traditional criminals to include cyber TTPs either to commit or obscure crime. This trend is highly likely to continue in 2017, and eventually diminish the differences between cybercriminals and traditional criminals.

DEVELOPING ISSUES

Authentication

We have moderate confidence that there will be changes to the traditional password recommendations, possibly with a shift toward multi-factor authentication instead of passwords or a change in password complexity requirements. It's probable that there will be increasing pressure to implement multi-factor authentication for logins in 2017. With these changes, we have low to moderate confidence that there will be increasing interest in the safety and exploitation of biometric security.

IPv6

IPv6 adoption is current at approximately 26% of the United States-based Internet,[2] and we are virtually certain the adoption rates will continue to increase in 2017. While unlikely to significantly affect SLTT governments in 2017, we recommend that SLTT governments monitor the continuing transition to IPv6, disable IPv6 on IPv4 networked devices where it is enabled by default, and consider developing their own transition plans.

Workforce

The MS-ISAC is convinced that the 2017 cybersecurity workforce demand will continue to outstrip the available workforce, creating an employment gap that will stress on SLTT government functions. This gap will, in particular, endanger SLTT government cybersecurity efforts, as SLTT governments face challenges in matching private sector salaries and providing the flexible work environments that new college graduates prefer.

WHAT WE MEAN WHEN WE SAY: An Explanation of Estimative Language

We use phrases such as "we judge," "we assess," and "we expect," as well as probabilistic terms such as "we believe" and "we are almost certain," to convey analytical assessments and judgements. These assessments and judgments are generally based on historical trends and collected information, which can be incomplete or fragmentary.

Description of Probability or Confidence	***Synonyms***
Highly Likely	Highly probable; We are convinced; Virtually certain; Almost certain; High confidence; High likelihood; Odds/chances are overwhelming.
Likely	Probable; We believe; Chances are good; High-moderate confidence; Greater than 60% likelihood.
Even Chance	Chances are slightly greater/less than even; Chances are about even; Moderate confidence; Possible.
Unlikely	Probably not; Not likely; Improbable; We believe…not; Low confidence; Possible but not likely; We doubt/doubtful.
Highly Unlikely	Highly improbable; Nearly impossible; Only a/some slight chance; Highly doubtful; Almost certainly not; Virtually impossible.

[2] Based on Akamai data on January 10, 2017 available at https://www.stateoftheinternet.com/trends-visualizations-ipv6-adoption-ipv4-exhaustion-global-heat-map-network-country-growth-data.html.