# 2018 SLTT Government Outlook

January 2018

MS-ISAC®

Multi-State Information Sharing & Analysis Center®

*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 2018 SLTT Government Outlook

The Multi-State Information Sharing and Analysis Center (MS-ISAC) expects financial gain will remain the most prevalent cybercrime motivation and that the majority of cyber incidents affecting state, local, tribal, and territorial (SLTT) governments will continue to be opportunistic in nature. As with past years we believe the sophistication of malware, cyber threat actors, and tactics, techniques, and procedures (TTPs) will continue to increase.

Risk will continue to expand beyond traditional network boundaries, with apps, the Internet of Things (IOT), social media, smart cities, cloud computing, mobile devices, point of sale (PoS) systems, cryptocurrencies, supply chains, and third parties playing an increasingly large role in SLTT governments' cybersecurity. New ways SLTT governments engage citizens and gather information, such as the use of social media reporting, apps for citizen reporting, drones, body cams, and smart parking meters, will challenge how SLTT government CISOs perform their jobs.

There will be greater recognition of SLTT governments' role in the nation's cybersecurity efforts. With this, cybersecurity will most likely become increasingly important among SLTT government executives, including executives in roles that have not traditionally focused on cybersecurity, such as Secretaries of State. SLTT government executives will almost certainly respond to the increased microscope on SLTT cybersecurity by further prioritizing strategic cybersecurity plans, workforce initiatives, and security centers, while federal entities will likely seek to acknowledge the greater SLTT government role through more inclusive language and outreach.

The MS-ISAC is convinced that the 2018 cybersecurity workforce demand will continue to outstrip the available workforce, further enforcing an employment gap that will stress SLTT government functions and encourage a shift toward outsourcing and third-party providers. This gap will, in particular, endanger SLTT government cybersecurity efforts, as SLTT governments face challenges in matching private sector salaries and providing flexible work environments. Compounding this issue will be considerations as to the most important knowledge, skills, and abilities of new hires. This will be evidenced through the need for cybersecurity management staff to communicate to executives in business terms rather than technical terms and a focus on hiring entry-level employees with soft, people-oriented skills and a passion for the work, under the argument that cybersecurity can be taught to the right employee.

As SLTT government cybersecurity efforts gain maturity, the focus on mitigation efforts will move past basic hygiene programs to more detailed efforts, resulting in more effective governance. For many SLTT governments this will include implementation of the Domain Message Authentication Reporting and Conformance (DMARC) email authentication, policy, and reporting protocol, as well as developing forward leaning policies regarding potential future incidents, and information and response sharing strategies.

## *TACTICS, TECHNIQUES, and PROCEDURES*

### Top 10 Malware list stabilizing

We believe the volatility of the monthly Top 10 Malware identified by the MS-ISAC will further stabilize with a small number of malware variants, most likely Kovter, Emotet, and a cryptocurrency miner, will dominate the list during the first half of the year. Kovter is currently the leading click fraud malware and is a staple of the MS-ISAC's monthly Top 10 Malware list. It is probable that Kovter will linger as malware with a significant impact on the SLTT government domain during the first half of 2018 and potentially longer, unless a takedown or vast shift in malware occurs. Emotet is highly likely

to remain a consistent threat with peaks and lulls driven by varying campaigns. SLTT governments experiencing Emotet infections will need to remain wary for related issues, including the creation of email server rules that could indicate a network compromise and potential data breach issue.

Cryptocurrency malware, driven by the current high cryptocurrency prices, will almost certainly remain a significant threat as actors seek to compromise systems in order to mine the currency of choice. Based on 2017 trends, we are confident that this activity will result in the compromise of both desktop machines and servers, and miners will continue as a major type of malware as long as cryptocurrency prices remain high enough for the activity to have a large profit margin.

We believe it is possible that malware authors will sustain and potentially increase the use of spreader implementations, such as those that operate over Server Message Block (SMB), or use tools, such as PowerShell or mimikatz. Chances are good that additional spreader implementations that operate by scraping email clients will also remain prevalent.

### Malspam, malvertising, and RDP as initiation vectors

Cyber threat actors are highly likely to continue using malspam and, secondarily, malvertising as the primary initiation vectors during the first half of 2018 and possibly longer. The current growth in malware-as-a-service suggests that initiation vectors may shift during 2018 due to new cyber threat actors buying into different tactics for delivery for known malware variants. If the infection vectors do shift, it will likely trigger a large change in the monthly Top 10 Malware list. Attacks via Remote Desktop Protocol (RDP), while rare, are likely to continue in 2018. In some cases, these compromises are currently and will likely continue to be used as a final effort to monetize platforms no longer useful in other criminal activity.

### Well-crafted social engineering

We are almost certain that cybercrime will continue to develop in sophistication. Cyber threat actors, using a combination or research and social engineering, and understanding the value of better targeting, will continue to develop more accurate phishing emails, scams, and tailored lures as these activities result in better returns. The MS-ISAC understands this approach as a combination of opportunistic and strategic targeting, where an agency is targeted strategically but individual users are targeted opportunistically, as was demonstrated with multiple agency-wide campaigns in 2017. 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.

### Increased use of extortion

A variety of extortion threats and attacks will continue to gain ground in 2018, posing an ongoing risk to SLTT governments. High-availability SLTT government networks and devices will remain a target for extortion attempts originating from strategic ransomware infections. Unlike traditional ransomware, these incidents will escalate into targeted extortion attempts with high-dollar payment demands. Other extortion attempts, including hoaxes and DDoS attacks, are likely to continue as actors seek higher payouts from more targeted approaches.

### Status Quo for DDoS

We expect that distributed denial of service (DDoS) attacks targeting SLTT governments will continue to be a common TTP, although we are not confident assessing duration or variant. That being stated, we believe that approximately half of all DDoS attacks against SLTT governments will be motivated by personal grievances against the targeted government. This leads us to believe

that DDoS attacks will likely remain a more significant threat to local governments rather than state governments. In addition, large-scale attacks on non-SLTT governments are likely to produce reciprocal effects experienced by SLTT governments. We are virtually certain that many DDoS attacks against SLTT governments in 2018 will continue as lower bandwidth attacks, compared to the record bandwidth attacks reported by some sectors. It is equally as likely that SLTT government owned devices will be compromised and included in botnets, resulting in SLTT governments participating in DDoS attacks against other entities.

Data Breaches a serious threat

Data breaches will continue to pose a serious threat to SLTT government networks and data. It is highly probable that SLTT government susceptibility to data breaches will be exacerbated by vulnerabilities in third-party systems used to store SLTT government data, outsource functionality, and provide services to constituents. We think this is likely to result in at least one 2018 data breach that affects multiple SLTT governments due to the tendency of vendors to provide similar services to multiple governments. Additionally, it is highly likely the W-2 variant of the Business Email Compromise (BEC) scam will return in 2018, with especially prominent effects on local governments and K-12 school districts between February and April.

Data Reuse

The data reuse threat, especially the threat posed by passwords reused across multiple login locations, will continue to escalate in 2018.

### *TARGETED DATA, SYSTEMS, and SECTORS*

Mid-Term Elections will refocus attention

The 2018 mid-term elections will re-focus attention on the security of election systems. Following the high visibility of purported incidents in 2016 and continued activity reports from 2017, the MS-ISAC expects similar efforts in 2018 to impact perception and reduce confidence in the electoral system. There is a chance that cybercriminal, hacktivist, or nation-state actors may attempt to conduct targeted compromises of election systems. However, reported election-related activity will likely include cyber threat actor and news media misunderstandings, such as the intentional or accidental propagation of falsified claims that involve the release of publicly available data that is portrayed as a legitimate compromise. Individuals are also likely to have additional motivations including gaining notoriety or identifying vulnerabilities to improve election system security.

Internet of Things a major discussion point

IoT will almost certainly continue to be a major discussion point in 2018 as SLTT government end-users continue to bring IoT devices into their workplaces for personal and professional use and executives seek further information on the topic. As a result, SLTT governments will need to contend with the related wireless connectivity, data sharing, and security concerns. SLTT government-owned IoT, devices, such as smart parking meters, point of sale terminals, drones, body worn cameras, and smart city technology will increase the cybersecurity burden, which will need to be addressed by policy and technology prior to implementation.

Industrial Control Systems is a wildcard

As with previous years, the 2018 threat against Industrial Control Systems (ICS) remains a wildcard. Known vulnerabilities commonly exist in ICS systems, with exploitation facilitated by tools that make identifying Internet-facing systems easy. However, these factors have existed together for the last several years with only a few major attacks occurring, reducing our confidence in the threat to this sector.

Supply Chains a point of weakness

We find it unlikely that the SLTT government supply chain is being strategically targeted. However, we do believe that the supply chain continues to be a point of weakness that will almost certainly affect SLTT governments in 2018. In addition, supply chain issues will be a point of contention in 2018 as SLTT governments struggle to reconcile federal recommendations with industry views.

University threat continuing

We have high confidence that universities will remain one of the most impacted sectors in 2018, with phishing emails as the primary initiation vector. As with other sectors, opportunistic infections of common malware meant for financial gain will remain the most likely threat. However, website defacements and attempts to gain access to sensitive research are highly likely to remain more common within this sector than other sectors.

Healthcare is a popular target

It is likely that the healthcare sector will remain a popular target for cybercriminals in 2018. Beyond the common TTP's experienced by all SLTT sectors, the MS-ISAC believes it is likely a series of strategic attacks will target individual agencies within the sector. We think it is likely these attacks will involve ransomware and extortion attempts, and potentially include other types of targeting.

***CYBER THREAT ACTORS***

Cybercriminals & Hacktivists

Financial gain will remain the driving motivator for the majority of attacks and malware, with cyber threat actors increasing maturity displayed through new skills and more efficient activities. One area of growth will be in profit maximization with some actors choosing to increase profits per attack while decreasing the number of attempted attacks through more carefully orchestrated schemes, higher levels of planning, and a greater attention to detail. We believe there is also a slight chance that opportunistic actors will develop one or more strategic targeting methods, resulting in the opportunistic identification of potential victims followed by a strategic compromise attempt. These actions, along with the more strategic social engineering approaches previously discussed, will amount to a slight, although significant, move away from wholesale opportunistic targeting.

The pattern of singular cyber threat actors, primarily cybercriminals and hacktivists, appearing and conducting limited-duration campaigns involving multiple TTPs or SLTT governments will almost certainly continue in 2018. As cybercriminal and hacktivist activity is largely unpredictable, we are uncertain as to when peaks and valleys will occur throughout the year. The attention seeking motivation is highly likely to remain common among cybercriminals who take credit for their activities. In addition, we believe the trend of falsified claims, made for the purpose of gaining notoriety for compromising a perceived high value target, will continue with cyber threat actors posting manipulated images and open source data.

Traditional Criminals

The MS-ISAC believes that criminals are frequently incorporating cyber TTPs and tools in their criminal activity, either because the cyber component simplifies the activity, expands the actor's reach, obscures the actor's identity, or results in a decreased chance of and penalty when caught. In addition, some criminals may commit physical crimes for digital purposes, such as the physical theft of cryptocurrency wallet keys. This trend is highly likely to continue, diminishing the differences between cybercriminals and traditional criminals.

***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. |