Malware, Malicious Domains, and More: How Cybercriminals Attack SLTT Organizations

Cybercriminals continue to target U.S. State, Local, Tribal, and Territorial (SLTT) government organizations at an alarming rate. Attackers often target SLTT organizations because they know their security teams need to run complex networks, as well as deal with numerous third-party systems and services. Many SLTT cybersecurity teams are also struggling with reduced security budgets and a well-documented shortage of skilled cybersecurity and networking professionals to fill open positions. COVID-19, and the subsequent increase in remote working by government employees and online accessibility requests for government resources by citizens, has only added to their security challenges.

Cybercriminals' SLTT Playbook

One of cybercriminals' favorite attack vectors against SLTT organizations is malware. Malware is malicious software designed to perform malicious actions on a device. It can be introduced to a system in various forms such as emails or malicious websites. Various types of malware have distinct capabilities dependent on their intended purpose, such as disclosing confidential information, altering data in a system, providing remote access to a system, issuing commands to a system, or destroying files or systems.

While malware comes in many flavors, the most prolific type used against SLTT organizations is ransomware. Ransomware is a type of malware that blocks access to a system, device, or file until a ransom is paid. Ransomware does this by encrypting files on the endpoint, threatening to erase files, or blocking system access. It can be particularly harmful when ransomware attacks affect hospitals, emergency call centers, and other critical infrastructure. The 2020 Verizon Data Breach Investigations Report (DBIR) found that ransomware disproportionately affects the public sector (over 60% of malware incidents vs. 27% of malware in all sectors). Additionally, incidents observed by the Multi-State Information Sharing and Analysis Center (MS-ISAC) showed a 153% increase in SLTT ransomware attacks from January 2018 to December 2019. In 2019, there were more than 100 publicly disclosed ransomware attacks against SLTT organizations – including an attack on the City of Baltimore's IT systems that locked out thousands of computers and disrupted nearly every city service. This attack is estimated to have cost the city as much as $18 million.

Other common types of malware affecting SLTT organizations include:

- **Trojans** are malware that appears to be a legitimate application or software that can be installed. Trojans can provide a backdoor to an attacker and subsequently full access to the device, allowing the attacker to steal banking and sensitive information, or download additional malware. Findings from the 2020 Verizon DBIR show that trojan variants were involved in over 50% of malware incidents in the public sector.
- **Downloaders or Droppers** are malware, which in addition to their own malicious actions, allow for other, often more dangerous, malware to infiltrate the infected system. Data collected by the 2020 Verizon DBIR shows that nearly 25% of public sector incidents involved a downloader or dropper.
- **Spyware** is malware that records keystrokes, listens in via computer microphones, accesses webcams, or takes screenshots and sends the information to a malicious actor. This type of malware may give actors access to usernames, passwords, any other sensitive information entered using the keyboard or visible on the monitor, and potentially information viewable through the webcam. Keyloggers, which mainly record keystrokes, are the most common type of spyware and ZeuS, the most famous keylogger, has been on the MS-ISAC's Top 10 Malware list for several years.
- **Click Fraud** is malware that generates fake automatic clicks to ad-laden websites. These ads create revenue when clicked on. The more clicks, the more revenue that is generated. Kovter, one of the more prolific versions of click fraud, has been on the MS-ISAC's Top 10 Malware list for the past few years.

Protecting Your Organization from Malware

Malware most commonly finds its way into SLTT organizations through either malspam, unsolicited emails that either direct users to malicious websites or trick users into downloading or opening malware, or malvertisements, malware introduced through malicious advertisements. The common thread between these vectors and the various types of malware they can introduce to your organization's IT systems is that they almost always involve either users or the malicious software they unintentionally download connecting to malicious web domains.

To help SLTT organizations protect themselves against these common types of cyber-attacks, the Center of Internet Security (CIS) is partnering through the MS-ISAC and Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) with the U.S. Department of Homeland Security (DHS) Cybersecurity Infrastructure Security Agency (CISA) and Akamai to offer its new Malicious Domain Blocking and Reporting (MDBR) service at **no cost** to U.S. SLTT government members of the MS- and EI-ISACs. The service allows SLTT security teams to quickly add an additional layer of cybersecurity protection against their systems connecting to malicious web domains and to enhance their existing network defenses.

For organizations not eligible to join the MS- or EI-ISAC, similar protection can be obtained through Quad9. Quad9 is a **no-cost**, recursive, anycast DNS platform that provides end users robust security protections, high-performance, and privacy. Quad9 was developed by the Global Cyber Alliance (GCA), an international nonprofit organization founded by a partnership of law enforcement and research organizations focused on combating systemic cyber risk in real, measurable ways (CIS is a founding organization of GCA).

About Malicious Domain Blocking and Reporting (MDBR)

The MDBR service is only available to members of the MS- and EI-ISAC. For those who are not eligible for membership, please see the section below on Quad9 for a similar service available to the General Public.

MDBR proactively blocks network traffic from an organization to known harmful web domains, helping protect IT systems against cybersecurity threats and limit infections related to known malware, ransomware, phishing, and other cyber threats. This capability can block the vast majority of ransomware infections just by preventing the initial outreach to a ransomware delivery domain. In just the first five weeks of service, the MDBR service blocked 10 million malicious requests from more than 300 SLTT entities.

Once an organization points its domain name system (DNS) requests to Akamai's DNS server IP addresses, every DNS lookup will be compared against a list of known or suspected malicious domains. Attempts to access known malicious domains, such as those associated with malware, phishing, or ransomware, are blocked and logged.

Akamai provides all logged data to the MS- and EI-ISACs' Security Operations Center (SOC), including both successful and blocked DNS requests. The SOC uses this data to perform detailed analysis and reporting for the betterment of the SLTT community, as well as regular organization-specific reporting and intelligence services. If necessary, remediation assistance is provided for each SLTT organization that implements the service.

Any U.S. SLTT government entity that is a member of the MS- or EI-ISAC can sign up for MDBR. They are able to take advantage of this additional layer of cybersecurity protection at absolutely **no cost**, courtesy of funding support provided by CISA.

To learn more about MDBR and sign up your organization for the service, please visit https://www.cisecurity.org/ms-isac/services/mdbr/.

About Quad9

Quad9 blocks against known malicious domains, preventing your organization's computers and IoT devices from connecting to malware or phishing sites. Whenever a Quad9 user clicks on a website link or types an address into their web browser, Quad9 checks the site against a list of domains compiled from over 18 different threat intelligence partners. Each threat intelligence partner supplies a list of malicious domains that are based on heuristics examining factors such as scanned malware discovery, network IDS past behaviors, visual object recognition, optical character recognition (OCR), structure and

linkage to other sites, as well as individual reports of suspicious or malicious behavior. Based on the results, Quad9 resolves or denies the lookup attempt, preventing connections to malicious sites when there is a match. Quad9 routes your organization's DNS queries through a secure network of servers around the globe.

Unlike MDBR, please note that Quad9 does not provide a reporting or support component and will limit its actions solely to the blocking of malicious domains around phishing, malware, and exploit kit domains. However, setup is very simple, as no signup or registration is required, and most importantly, it serves as a very resourceful **no-cost** blocking service available to any organization or individual.

For more information, please visit https://www.quad9.net.

MS-ISAC
Multi-State Information Sharing & Analysis Center

STOP | THINK CONNECT™

Acknowledgement: This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number, (19PDMSI00002).