MONTHLY
Cyber Security
Newsletter

Security Tips

Mississippi Department of
Information Technology Services

Security Services Division

September 2020

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

From the desk of Michael Aliperti, MS-ISAC Chair

INSIDE TOPIC:

- Protecting Your Organization from Malware

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 involve 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.

Organizations can reduce the risk associated with malware by following the security practices below:

- **Install and maintain antivirus software**. Antivirus software recognizes malware and protects your computer against it. Installing antivirus software from a reputable vendor is an important step in preventing and detecting infections. Always visit vendor sites directly rather than clicking on advertisements or email links. Because attackers are continually creating new viruses and other forms of malicious code, it is important to keep your antivirus software up-to-date.
- **Use caution with links and attachments**. Take appropriate precautions when using email and web browsers to reduce the risk of an infection. Be wary of unsolicited email attachments and use caution when clicking on email links, even if they seem to come from people you know. (See Using Caution with Email Attachments for more information.)

- **Block pop-up advertisements**. Pop-up blockers disable windows that could potentially contain malicious code. Most browsers have a free feature that can be enabled to block pop-up advertisements.
- **Use an account with limited permissions**. When navigating the web, it's a good security practice to use an account with limited permissions. If you do become infected, restricted permissions keep the malicious code from spreading and escalating to an administrative account.
- **Disable external media AutoRun and AutoPlay features**. Disabling AutoRun and AutoPlay features prevents external media infected with malicious code from automatically running on your computer.
- **Change your passwords**. If you believe your computer is infected, change your passwords. This includes any passwords for websites that may have been cached in your web browser. Create and use strong passwords, making them difficult for attackers to guess. (See Choosing and Protecting Passwords and Supplementing Passwords for more information.)
- **Keep software updated**. Install software patches on your computer so attackers do not take advantage of known vulnerabilities. Consider enabling automatic updates, when available. (See Understanding Patches and Software Updates for more information.)
- **Back up data**. Regularly back up your documents, photos, and important email messages to the cloud or to an external hard drive. In the event of an infection, your information will not be lost.
- **Install or enable a firewall**. Firewalls can prevent some types of infection by blocking malicious traffic before it enters your computer. Some operating systems include a firewall; if the operating system you are using includes one, enable it. (See Understanding Firewalls for Home and Small Office Use for more information.)
- **Use anti-spyware tools**. Spyware is a common virus source, but you can minimize infections by using a program that identifies and removes spyware. Most antivirus software includes an anti-spyware option; ensure you enable it.
- **Monitor accounts**. Look for any unauthorized use of, or unusual activity on, your accounts—especially banking accounts. If you identify unauthorized or unusual activity, contact your account provider immediately.
- **Avoid using public Wi-Fi**. Unsecured public Wi-Fi may allow an attacker to intercept your device's network traffic and gain access to your personal information.

Visit the Mississippi Department of Information Technology Services (ITS) for more infomation on malware, cybercrime, and more.

Provided By

MS-ISAC
Multi-State Information

STOP | THINK
CONNECT™