# EXECUTIVE BRIEF: HOLDING FEDERAL GOVERNMENT AGENCIES FOR RANSOM

**Ransomware in the headlines, common vulnerabilities and best-practice defenses**

## Abstract

Ransomware attacks on federal government agencies are on the rise. Coordinated attacks are hitting agencies. Cybercriminals continue to find government agencies a lucrative target for ransomware, and geopolitical cyberwarfare is a growing concern. However, there are known steps you can take to help prevent being a victim.

### Introduction

Recent ransomware attacks on government have become all the more pertinent in light of geopolitical tensions. Government services have been locked up, and critical government operations face risk.

### A Disturbing Trend

According to the Mid-Year Update to the 2020 SonicWall Cyber Threat Report ransomware continues to grow — and is growing at an increasing clip, due to its low barrier of entry, ease of use and anonymous payouts. By mid-year 2019, global ransomware was up 15%. This year, it's up 20%. Within this 20% lies a great deal of variation, however. Ransomware in the U.K. has fallen by 6% year over year, to 5.9 million, and in other places it's dropped by nearly half. In North America, ransomware is up 105% — including a 109% increase in the United States, where it rose to 80 million.

Such attacks on secured federal facilities are made all-the-more timely by recent state-actor breaches, such as the January 2020 breach of the U.S. Federal Depository Library Program's website by the "Iran Cyber Security Group Hackers."

### Case in Point: Ryuk attack on MTSA facility

In December 2019, the United States Coast Guard issued a bulletin confirming a ransomware intrusion at a Maritime Transportation Security Act (MTSA) regulated facility. As reported in a SiliconANGLE article, the attack involved the Ryuk ransomware and is believed to have entered the network of the base via a phishing email. The base and its port operations were disrupted for over 30 hours as a result of the attack.

### Analysis: Common Threads

"The U.S. Coast Guard's announcement that a computer virus forced a maritime base offline," says SonicWall CEO Bill Conner, "is the latest in a growing trend of specialized ransomware attacks.... While global ransomware volume was down 10% through November 2019, cybercriminals are being more targeted than ever before, focusing on lucrative and defined targets over massive volume."

Conner adds, "It is too easy to demand and receive ransom payment without the risks associated with traditional data exfiltration. Until organizations are serious about ransomware protection, these types of wide-reaching ransomware attacks will, unfortunately, continue. As we've witnessed, ransomware attacks are highly disruptive."

Ransomware no longer infects a singular device but multiple devices with the intent to infect the entire network. First made famous with the WannaCry attack, ransomware authors now try to leverage vulnerabilities like SMB in Windows to spread to other drives. Not all computers are up to date and this leaves an opportunity to not only infect that device but to also infect others.

Some government agencies may be rich in data and poor in security, which makes them a target. Agencies that worked to digitize older records without proper backups in place may be at risk of losing this data or having to go back and digitize them again. Organizations must continually keep everything backed up with those backups off the network, whether it is on LTO tape or in the cloud.

Most ransomware attacks come unsolicited in email. They may come in attachments with subject lines such as:

- Here is my resume
- This is an unpaid invoice
- Here is the invoice for your flight/ package etc. (in hopes people will be shocked into thinking their credit card info was stolen).

They also use malicious URLs. These will look like real URLs but lead to other places like www.[yourname].com. Common ones are:

- Your card has been charged, please review
- Is this you in this video?
- Your package has arrived

### Be Prepared with Best Practices

The US Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) recommends the following precautions to protect users against the threat of ransomware:

- Update software and operating systems with the latest patches; outdated applications and operating systems are the target of most attacks
- Never click on links or open attachments in unsolicited emails
- Back up data on a regular basis; keep it on a separate device and store it offline
- Follow safe practices when browsing the Internet

CISA also recommends that organizations employ the following best practices:

- Restrict users' permissions to install and run software applications and apply the principle of "least privilege" to all systems and services; restricting these privileges may prevent malware from running or limit its capability to spread through a network
- Use application whitelisting to allow only approved programs to run on a network
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email to prevent email spoofing
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users
- Configure firewalls to block access to known malicious IP addresses

In addition, SonicWall suggests the following best practice steps:

- Educate users on cyber security best practices
- Use a next-generation firewall to eliminate known threats
- Implement sandboxing on those firewalls to identify unknown threats
- Deploy endpoint security with advanced AI to stop attacks before they happen on the endpoint
- Avoid paying ransom; doing so only adds to the problem by encouraging more attacks

## Conclusion

Unfortunately, with differing approaches on responding to ransomware demand being driven by budget and resources, cybercriminals have found government to be a lucrative target for ransomware attacks. While these ransomware attacks are widespread, there are commonalities to consider. It is critical to be prepared by implementing known best practices and the latest ransomware countermeasures.

**Learn more.** Read our Solution Brief: 7 Best Practices for Fighting Ransomware.

Except as set forth in the terms and conditions specified in the license agreement for this product, SonicWall and/or its affiliates assume no liability whatsoever and disclaims any express, implied or statutory warranty relating to its products including, but not limited to, the implied warranty of merchantability, fitness for a particular purpose, or non-infringement. In no event shall SonicWall and/or its affiliates be liable for any direct, indirect, consequential, punitive, special or incidental damages (including, without limitation, damages for loss of profits, business interruption or loss of information) arising out of the use or inability to use this document, even if SonicWall and/or its affiliates have been advised of the possibility of such damages.

SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

## About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.
www.sonicwall.com