BEST PRACTICES GUIDE

Protect Against a Perfect Storm of Cyber Threats

Symantec™

"It's not a matter of if you will be attacked—it's when."

There's good reason that's an increasingly common battle cry among cyber security professionals: Fresh digital security threats continually emerge from new and unexpected sources. Just consider the sudden spread of viruses like WannaCry and Petya/NotPetya, the expansion of ransomware threats, the growth in coinmining and cryptojacking attacks, and the success of malicious living off the land (LOTL) attacks such as PowerShell intrusions.

Cyber criminals adapt to your defenses by designing new malware variants to evade network and endpoint security. The 2018 Symantec Internet Security Threat Report (ISTR) documents the enormous number of malware variants—nearly two million—we detect daily.

The ISTR report also shows:

- Ransomware attacks increased 40 percent and ransomware variants increased 46 percent year over year.
- Cryptojacking attacks increased 8,000+ percent year over year.
- One in 13 URLs analyzed at the gateway was malicious. In 2016, it was 1 in 20; that's a 50+ percent increase.

In the face of these challenges, unfortunately, many organizations report they are not equipped to fend off a targeted attack: 63 percent admit they are unprepared for zero-day threats[1] and a majority say they can't find enough trained personnel to fill cyber security/information security positions.[2]

It all adds up to a perfect threat storm: Too few trained IT security personnel using disjointed and incomplete security products and processes to protect complex environments against sophisticated and ever-evolving threats.

To help you fight back, we've compiled this list of best practices for several of the advanced threat vectors we're tracking.

Minimize exposure to ransomware—and, if compromised, respond correctly

Ransomware attacks, such as WannaCry and Petya, in which data is encrypted until a ransom is paid, are trending upward. As noted in the 2018 ISTR, although the number of ransomware families has decreased year over year, the number of ransomware variants has increased by 46 percent. This indicates criminal groups may be innovating less but they remain very productive.

Cyber criminals aren't only interested in making money: Targeted attack groups are using cyber methods to raise foreign currency or to cover for other types of attacks.

Multilayered security minimizes the chance of infection. Adopt a three-stage strategy to protect against malware.

Prevent—Preventing infection should be the core of your strategy. Email and exploit kits are among the most common infection vectors for ransomware, but new generations of self-propagating ransomware exploit vulnerabilities and spread across networks using stolen credentials.

Contain—If an infection has successfully breached your defenses, it is critical you limit its spread. See our recommendations, below.

Respond—Develop and test your incident response program, learn from the attacks, and apply those learnings to improve your defenses.

[1] *Betanews: Mid-market enterprises are too confident of their cyber security*
[2] *ISACA State of Cybersecurity 2018*

Already infected?

Take these steps for a speedy recovery:

Identify the primary infection point to contain further spread

Determine who was behind the threat, what they were after, why they targeted you, and how they executed the attack. It's critical you understand the threat holistically, as ransomware could be one tactic in a larger, advanced campaign.

Consider that paying the ransom does not always work

Attackers may not send a decryption key; the decryption process could damage files if it's poorly implemented; and attackers may make a larger ransom demand after receiving the initial payment.

Analyze the malware to determine how data was encrypted and create a data recovery plan

Incident responders may be able to recover data easily as malware writers often make implementation mistakes. A skilled malware analyst can reverse engineer ransomware to identify such weaknesses.

Follow these best practices to avoid a ransomware attack:

- **Back up important data**—This is a key method for combating ransomware infections. However, there have been cases of ransomware encrypting backups, so backups are only one element of a robust security strategy.
- **Advise users to immediately delete any suspicious emails**—Especially those containing links or attachments.
- **Avoid enabling macros in Microsoft Office**—Advise users to be wary of Microsoft Office attachments that prompt them to enable macros. While macros can be used for legitimate purposes, such as automating tasks, attackers often use malicious macros to deliver malware through Office documents. Microsoft mitigates this infection vector by disabling Office macros by default. Attackers may use social engineering to convince users to enable macros to run.
- **Perform a full network scan to identify all infected computers**—Then isolate compromised computers from the network until they have been fully cleaned and restored.

Look out for cryptojacking

Cryptojacking, in which cyber criminals secretly run coinminers on user devices, is one of the largest and fastest-growing attack types we track. Cryptojacking bogs down CPUs, slowing device operations, overheating batteries, consuming more energy, reducing productivity, and, sometimes, rendering devices unusable.

Subvert coinmining with the following tactics:

- **Advise users to be careful with emails from unfamiliar sources**—Especially if the emails contain attachments the users haven't solicited; such emails may contain file-based coinmining malware.
- **Train users to be wary of clicking on ads for unfamiliar websites, and when downloading apps to their phone**—Mobile phones can be used for mining cryptocurrency too. Use the same caution when downloading browser extensions.
- **Train users to monitor battery usage on their devices**—If they notice a suspicious spike in battery usage, scan the device for file-based miners. If you don't find any, take note of the websites that were open when the spike occurred.
- **Train users to install the latest patches** on their devices, use strong passwords, and enable two-factor authentication.
- **Educate users about the signs that indicate their computer may have a coinminer**—Instruct them to inform IT immediately, especially if their device is on the company network.
- **Ensure your router—and all IoT devices**—are fully patched, and the firmware is updated.
- **Monitor network logs (IPS logs, DNS logs, firewall logs) for suspicious outgoing connections to mining-related IP addresses**—Block these addresses at the corporate firewall, and consider suspicious any computer that continues to access those addresses.
- **Lock down Remote Desktop Protocol (RDP) access** and frequently replace all user passwords, especially for users with admin access.
- **Run a recent release of PowerShell (5 or higher)** and configure it to log detailed activity.
- **Secure your computers' built-in Windows Management Instrumentation (WMI)**—Attackers, including those seeking to mine coins, increasingly abuse this technology. Consider creating Group Policy Objects (GPO) or firewall rules to prevent unauthorized remote WMI actions, and look at controlling access by user accounts.

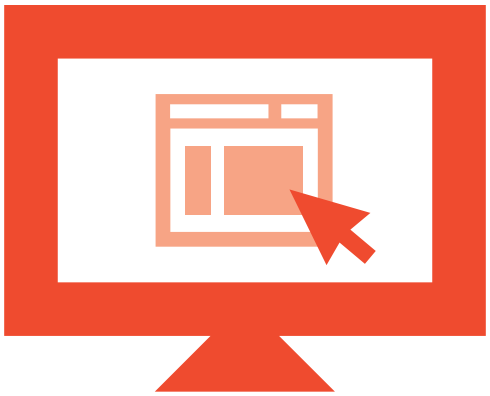
> “The growth in coin mining in the final months of 2017 was immense. Overall coin-mining activity increased by 34,000 percent over the course of the year; while file-based detections of coinminers on endpoint machines increased by 8,500 percent.”
>
> — Internet Security Threat Report – Vol. 23

Prevent living off the land (LOTL)/fileless attacks

Hackers use trusted, off-the-shelf, already installed system tools to infiltrate networks. Because these tools are pervasive and used by system administrators for legitimate work, you cannot completely block access to these programs or easily distinguish between approved and malicious behaviors. The result: Attackers hide in plain sight.

To avoid fileless attacks, follow these best practices:

- Monitor the usage of dual-use tools inside your network.
- Use application whitelisting where applicable.
- Continually update security software, operating systems, and applications.
- Enable advanced account security features, such as two-factor authentication and login notification, if available.



- Train users to:
  - Exercise caution with unsolicited, unexpected, or suspicious emails.
  - Be wary of attachments that prompt them to enable macros.
  - Use strong passwords for all their accounts.
  - Always log out of session when done.
  - If using untrusted Wi-Fi networks, avoid activities such as using apps that transmit sensitive information or logging into online accounts.
  - Download mobile apps only from official app stores; third-party app stores are more likely to contain malware.

Conclusion

Cyber crime is big business. There is likely no single activity that will carry your entire security program. You have to institute multiple, overlapping, and mutually supportive defensive systems to guard against single point failures in specific technologies or protection methods. This includes implementing endpoint, email, and web gateway protection technologies as well as firewalls and vulnerability assessment solutions. Stay informed and apply system patches and updates to ensure your security system takes advantage of the latest protection capabilities.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com, subscribe to our blogs, or connect with us on Facebook, Twitter, and LinkedIn.

Symantec™

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

19C206371_GDE_ADV-Threats-Best-Practices_EN