CPA
Practice Advisor

destructive ransomware of 2017, followed closely by WannaCry and Locky. The data surveyed includes all devices running windows operating systems that were infected with ransomware ...

Oct. 31, 2017

Ransomware is increasingly threatening accounting firms and businesses, so much so that it seems businesses and pretty much anyone with a computer is under threat of attack. There are so many threats, however, it can be hard to know which ones pose the highest threat, and what a regular person can do about it. Webroot, a

NotPetya, WannaCry Take Top Spots

Two of the most destructive strains of ransomware ever seen exploded in 2017.

- NotPetya is crowned No. 1 because it was engineered to do damage to a country's infrastructure.
- NotPetya's code leveraged EternalBlue, the same exploit WannaCry used a month earlier. But NotPetya wasn't designed to extort money from its victims like most ransomware. It was created to destroy everything in its path.
- WannaCry takes second place on the list because it took the world by storm when it infected hundreds of thousands of users across the globe.

NotPetya and WannaCry attacked in 2017, but other ransomware on the list made their first appearances in 2016. These attacks either carried into 2017 or returned aggressively.

Nastiest Ransomware – The Top 10

1. **NotPetya**—Starting as a fake Ukrainian tax software update, NotPetya infected hundreds of thousands of computers in more than 100 countries within just a few days. This ransomware is a variant of an older attack dubbed Petya, except this time the attack uses the same exploit behind WannaCry.
2. **WannaCry**—As the first strain of ransomware to take the world by storm, WannaCry was also the first to use EternalBlue, which exploits a vulnerability in Microsoft's Server Message Block (SMB) protocol.
3. **Locky**—2016's most popular ransomware is alive and well in 2017. New variants of Locky, called Diablo and Lukitus, surfaced this year, using the same phishing email attack vector to initiate their exploits.
4. **CrySis**—The king of Remote Desktop Protocol (RDP) compromise started last year in Australia and New Zealand. RDP is one of the most common ways to deploy

ransomware because cybercriminals can compromise administrators and

7. **Spora**—To distribute this ransomware, cybercriminals hack legitimate websites to add JavaScript code. Then, a pop-up alert prompts users to update their Chrome internet browsers to continue viewing the webpage. Once users follow the “Chrome Font Pack” download instructions, they become infected.
8. **Cerber**—One of the multiple attack vectors Cerber utilizes is called RaaS (ransomware-as-a-service). Through this “service,” cybercriminals package up ransomware and then give other criminals the tools to distribute how they see fit.
9. **Cryptomix**—This ransomware is one of the few that does not have a type of payment portal available on the dark web. Instead, users have to wait for the cybercriminals to email them instructions to pay a hefty amount in Bitcoin.
0. **Jigsaw**—Another carryover from 2016, Jigsaw embeds an image of the clown from the “Saw” movies into a spam email. Once a user clicks, the ransomware not only encrypts files, but it also deletes files if a user takes too long to make the ransom payment of $150.

What Managed Service Providers (MSPs) and small- to medium-sized businesses can do to protect devices from ransomware:

- **Purchase and deploy a top-rated security solution.** Look for cybersecurity solutions that provide protection from multiple attack vectors, without affecting user experience by slowing devices during scans.
- **Keep your security software up to date.** Firmware and patches are how vendors push out important security updates. Keep both devices and operating systems up-to-date and create a process for patch management.
- **Backup and store sensitive data.** Generally, ransomware only has the means to encrypt files stored locally on a user’s system. Backup data to a hard, offline location. In the case of equipment failure or ransomware, you can access your backup and get back to business as usual.
- **Implement a strong password naming convention.** A strong password policy limits the likelihood of Remote Desktop Protocol (RDP) breaches.

What home users can do to protect computers from ransomware:

Key Quotes:

Aaron Sherrill, Senior Analyst, 451 Research
"Our research shows that ransomware is a top pain point for businesses due to its infectious nature and ability to spread quickly throughout entire systems. Ransomware does not have a bias and often times small- to medium-sized businesses are the most vulnerable due to their lack of resources. SMBs need to be proactive by consulting an MSP or MSSP on how to deploy a solution that will protect their business from these malicious threats."

David Dufour, Vice President of Engineering and Cybersecurity, Webroot
"This past year was unlike anything we've ever seen. Attacks such as NotPetya and WannaCry were hijacking computers worldwide and spreading new infections through tried-and-true methods. This list is further evidence that cybercriminals will continue to exploit the same vulnerabilities in increasingly malicious ways. Although headlines have helped educate users on the devastating effects of ransomware, businesses and consumers need to follow basic cybersecurity standards to protect themselves."

Additional resources:

- **Video:** Top 10 Nastiest Ransomware
- **Blog & Infographic:** Top 10 Nastiest Ransomware
- **Web Page:** How to Protect Your Business From Ransomware
- **Web Page:** How to Protect Yourself From Ransomware

Digital Currency • Firm Management • Security

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy