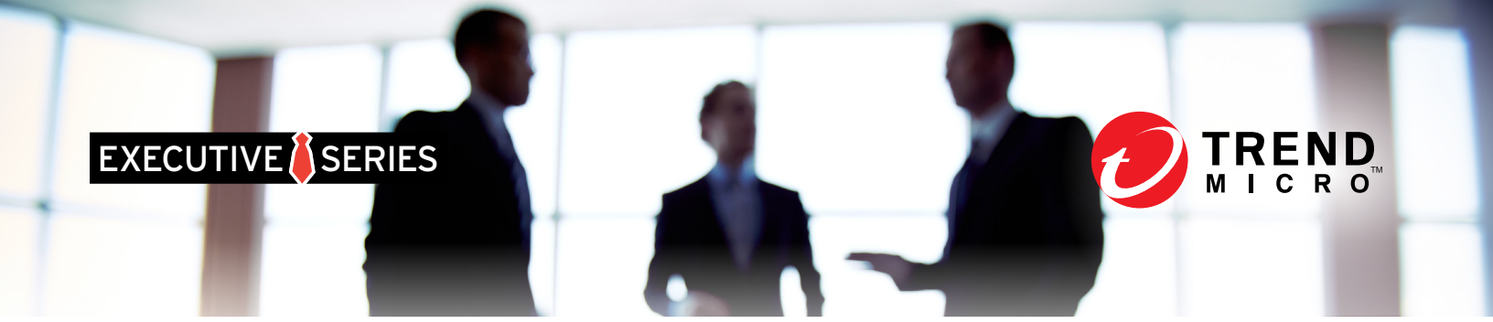


Ransomware as a Service

Cybercrime-as-a-Service Series

Cybercrime as a service (CaaS) is an important trend in Deep Web forums because it puts cybercriminal tools and services in the hands of a wider range of threat actors—even the nontechnical, such that anyone can become a cybercriminal with minimal investment. At the same time, cybercriminals are now seeing the advantages of expanding their targets from home users to larger enterprise networks. This is a matter that IT administrators need to be ready for.

Ransomware as a Service

Ransomware[1] use one of the more chilling widespread cybercrime models today. Victims get ransomware through the Internet and once installed, they hold victims' documents hostage in exchange for money.

The fear factor works. In 2015, CryptoWall operators raked in US$325 million from individuals and businesses worldwide through this modus operandi. Several ransomware families continue to do so today.

> Hollywood Presbyterian paid **US$17,000** to decrypt files encrypted by Locky.

Once exclusively a home user problem, ransomware's social engineering tactics and technical capabilities have since evolved to dip into enterprise networks as well. We confirmed this through the increase in focus of crypto-ransomware on office-related documents such as database files, web pages, SQL files, and other file types not typically found on home computers.

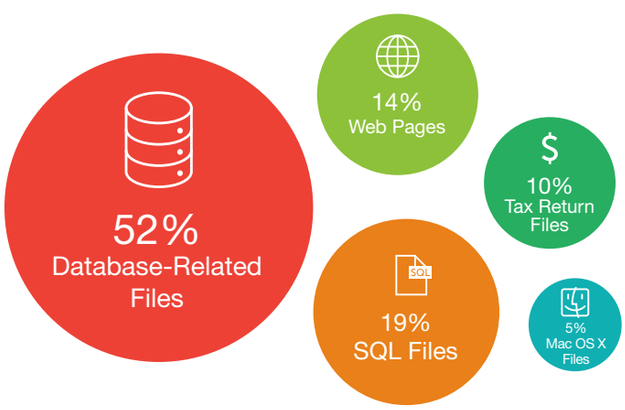


Figure 1. An increasing number of crypto-ransomware families have been seen encrypting file types typically seen in enterprise networks.

In an expected but disturbing turn, ransomware are now being sold in Deep Web forums as a service (ransomware as a service [RaaS]), meaning anyone, even with basic technical know-how, can launch his own ransomware campaign.

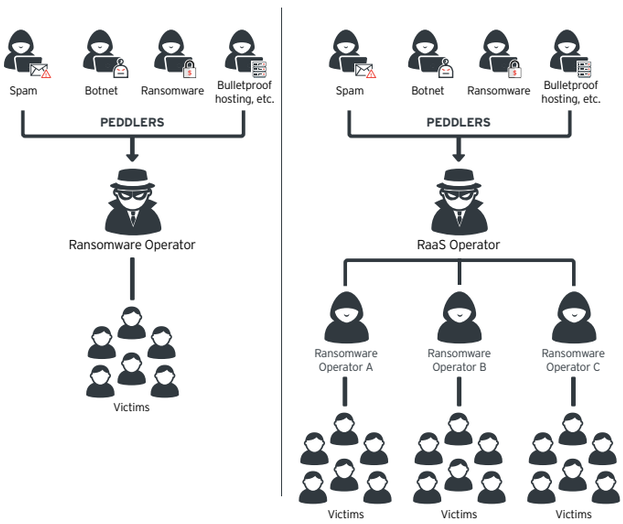


Figure 2. In RaaS, the operator gets a cut from each victim's payment, resulting in more potential profit than from the traditional ransomware business model.

Figure 3. We saw several cybercriminal underground forum posts advertising RaaS, some even offering a full lifetime license for only US$39.

This trend further pushed ransomware into the mainstream. Based on our monitoring, ransomware families already hit a 172% increase in the first half of 2016 alone[2], compared to the whole 2015.

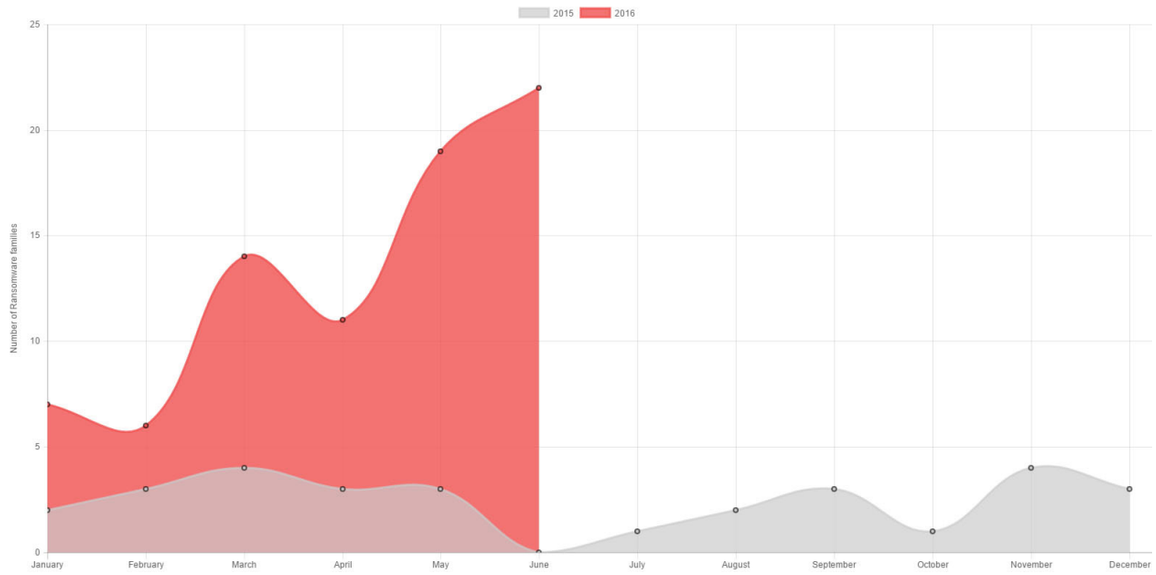


Figure 4. In the first six months of 2016 alone, we saw 79 new ransomware families.

What It Means for Enterprises

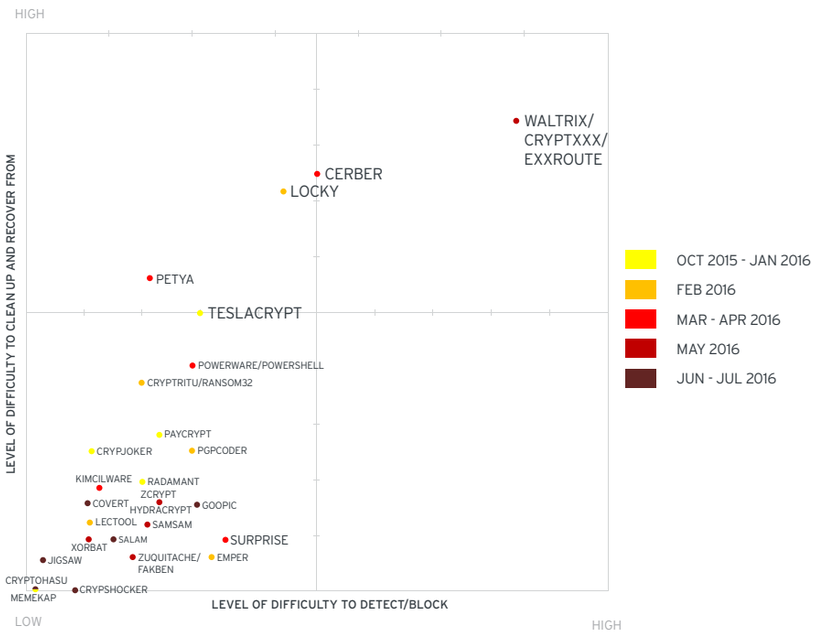
This means, now more than ever, that any file in digital form is at risk, whether it's a top-secret formula for a pharmaceutical company; a list of high-profile contacts for a sales company; or a normal system file that is mission-critical to a hospital, a nuclear plant, or an Industrial Control System (ICS) operation. Ransomware can affect a company's bottom line, either directly or indirectly, as manifested in:

- Lost sales
- Payment, delivery, or transaction delays
- Unfulfilled orders
- Business process disruption
- Productivity losses
- Legal fines
- Regulatory penalties
- Damage to the company's brand and reputation

The danger is not expected to stop anytime soon. Ransomware continue to grow in complexity, devising new ways to evade detection and impede cleanup and recovery. Our analysis of recent ransomware families affecting enterprises show an uptick in technical modifications that make it more challenging for security vendors to detect and clean up after ransomware binaries.

Should enterprises pay the ransom?

Kansas Heart Hospital paid the hackers, but the hackers did not restore full access to its files. Instead, they demanded a second payment.



WALTRIX/CryptXXX uses a cocktail of evasion-and-arrival techniques like using the Angler Exploit Kit, legitimate services, and fast-changing binaries, among others.

Other recent arrival methods include:

- SURPRISE arrives via Remote Desktop Control software
- PETYA arrives as a job application to HR with a link to a "resume"

Other recent ransomware behaviors observed:

- CRYPSAM/Samsam and KIMCILWARE exploit vulnerable Web servers
- PETYA overwrites the Master Boot Record, causing BSoD
- CERBER disables Windows Startup Repair

Figure 5. Detection and cleanup matrix for ransomware known to target enterprises

Ransomware Solutions

Network defenders are expected to employ best practices against ransomware, including multilayered protection, data backup[3] and recovery strategies, access control, timely patching, and employee education, without compromising business productivity.

Trend Micro understands the value of analyzing the entire ransomware attack chain—from entry points such as malicious URLs and spam and the use of exploits and various evasion techniques to the ransomware's phone-home communication back to operators—and strengthening the ability to block ransomware before they execute on systems.

Furthermore, as network defenders scale up to protect hundreds to thousands of endpoints, the different layers of protection must be able to "talk to each other," forming a connected threat defense strategy. All layers must have access to threat intelligence, security updates, and protection afforded by security technologies like:

- Advanced anti-malware (beyond blacklisting)
- Antispam at the Web and messaging gateways
- Web reputation
- Application control (whitelisting)
- Content filtering
- Vulnerability shielding
- Mobile app reputation
- Intrusion prevention
- Host-based firewall protection

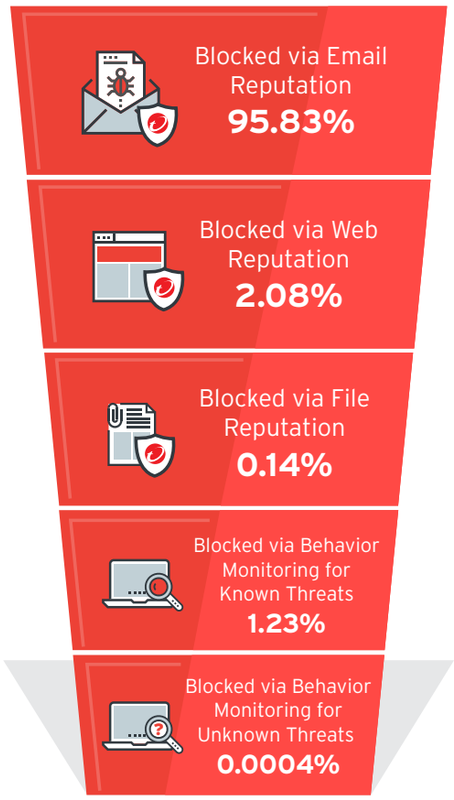


Figure 6. Typical distribution of ransomware detection by vector-specific security technology

A majority of today's threats can be detected by the aforementioned techniques working together, but ransomware are guaranteed to evolve, so enterprises must finally be able to catch zero-day and "unknown" threats through behavior and integrity monitoring as well as sandboxing.

References:

[1] http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-101-what-it-is-and-how-it-works

[2] http://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/the-reign-of-ransomware

[3] http://blog.trendmicro.com/trendlabs-security-intelligence/world-backup-day-the-3-2-1-rule/