Symantec™

Executive Summary

2018 Internet Security Threat Report

ISTR

Volume 23

Executive Summary

From the sudden spread of WannaCry and Petya/NotPetya, to the swift growth in coinminers, 2017 provided us with another reminder that digital security threats can come from new and unexpected sources. With each passing year, not only has the sheer volume of threats increased, but the threat landscape has become more diverse, with attackers working harder to discover new avenues of attack and cover their tracks while doing so.

Coin mining attacks explode

Cyber criminals who have been firmly focused on ransomware for revenue generation are now starting to explore other opportunities. During the past year, the astronomical rise in crypto currency values inspired many cyber criminals to shift to coin mining as an alternative revenue source. This coin mining gold rush resulted in an 8,500 percent increase in detections of coinminers on endpoint computers in 2017.

Malware

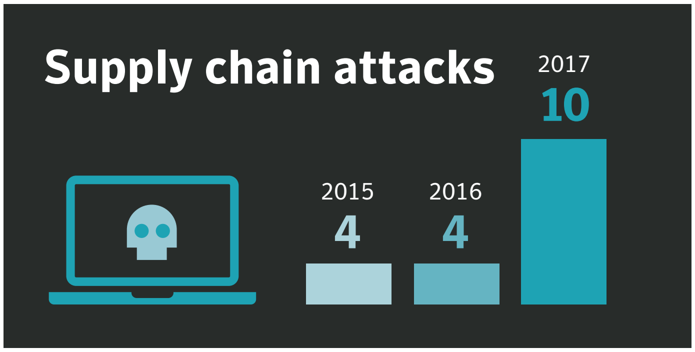
92% Increase in new downloader variants

80% Increase in new malware on macs

8,500% Increase in coinminer detections

With a low barrier of entry—only requiring a couple lines of code to operate—cyber criminals are using coinminers to steal computer processing power and cloud CPU usage from consumers and enterprises to mine crypto currency. While the immediate impact of coin mining is typically performance related—slowing down devices, overheating batteries, and in some cases, rendering devices unusable—there are broader implications, particularly for organizations. Corporate networks are at risk of shutdown from coinminers aggressively propagated across their environment. There may also be financial implications for organizations who find themselves billed for cloud CPU usage by coinminers.

As malicious coin mining evolves, IoT devices will continue to be ripe targets for exploitation. Symantec already found a 600 percent increase in overall IoT attacks in 2017, which means that cyber criminals could exploit the connected nature of these devices to mine en masse.



Spike in software supply chain attacks

Despite the EternalBlue exploit wreaking havoc in 2017, the reality is that vulnerabilities are becoming increasingly difficult for attackers to identify and exploit. In response to this, Symantec is now seeing an increase in attackers injecting malware implants into the supply chain to infiltrate unsuspecting organizations, with a 200 percent increase in these attacks—one every month of 2017 as compared to four attacks annually in years prior.

Hijacking software updates provides attackers with an entry point for compromising well-protected targets, or to target a specific region or sector. The Petya/NotPetya (Ransom.Petya) outbreak was the most notable example: After exploiting Ukrainian accounting software as the point of entry, Petya/NotPetya used a variety of methods, spreading across corporate networks to deploy the attackers' malicious payload.

Ransomware business experiences market correction

When viewed as a business, it's clear that ransomware profitability in 2016 led to a crowded market, with overpriced ransom demands. In 2017, the ransomware 'market' made a correction with fewer ransomware families and lower ransom demands—signaling that ransomware has become a commodity. Many cyber criminals may have shifted their focus to coin mining as an alternative to cash in while crypto currency values are high. Some online banking threats have also experienced a renaissance as established ransomware groups have attempted to diversify.

Last year, the average ransom demand dropped to $522, less than half the average of the year prior. And while the number of ransomware variants increased by 46 percent, indicating the established criminal groups are still quite productive, the number of ransomware families dropped, suggesting they are innovating less and may have shifted their focus to new, higher value targets.

Ransomware

5.4B WannaCry attacks blocked

46% Increase in new ransomware variants

Drop in zero days can't halt the rise in targeted attacks

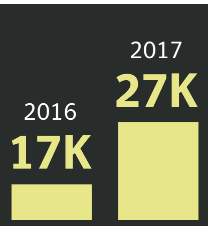
Symantec has found that overall targeted attack activity is up by 10 percent in 2017, motivated primarily by intelligence gathering (90 percent). However, a not-so-insignificant 10 per cent of attack groups engage in some form of disruptive activity.

The 'living off the land' trend continues with attack groups opting for tried-and-trusted means to infiltrate target organizations. Spearphishing is the number one infection vector, employed by 71 percent of organized groups in 2017. The use of zero days continues to fall out of favor. In fact, only 27 percent of the 140 targeted attack groups that Symantec tracks have been known to use zero-day vulnerabilities at any point in the past.

Mobile malware continues to surge

Threats in the mobile space continue to grow year-over-year. The number of new mobile malware variants increased by 54 percent in 2017, as compared to 2016. And last year, an average of 24,000 malicious mobile applications were blocked each day.

Mobile



54% Increase in mobile malware variants

24K Average number of malicious mobile apps blocked each day

While threats are on the increase, the problem is exacerbated by the continued use of older operating systems. In particular, on Android™, only 20 percent of devices are running the newest major version and only 2.3 percent are on the latest minor release.

Mobile users also face privacy risks from grayware, apps that aren't completely malicious but can be troublesome. Symantec found that 63 percent of grayware apps leak the device's phone number. With grayware increasing by 20 percent in 2017, this isn't a problem that's going away.

For the details, download the
Symantec 2018 Internet Security Threat Report (ISTR)
go.symantec.com/aa/istr

Symantec™

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.

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043
United Stated of America

+1 650 527–8000
+1 800 721–3934

For specific country offices and contact numbers, please visit our website. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec.com

ISTR