Symantec

INTERNET SECURITY THREAT REPORT

Executive Summary

2019 Internet Security Threat Report

ISTR

Volume 24

Executive Summary

Formjacking. Targeted attacks. Living off the land. Coming for your business.

Like flies to honey, miscreants swarm to the latest exploits that promise quick bucks with minimal effort. Ransomware and cryptojacking had their day; now it's formjacking's turn.

In the Symantec Internet Security Threat Report, Volume 24, we share the latest insights into global threat activity, cyber criminal trends, and attacker motivations.

The report analyzes data from Symantec's Global Intelligence Network, the largest civilian threat intelligence network in the world, which records events from 123 million attack sensors worldwide, blocks 142 million threats daily, and monitors threat activities in more than 157 countries.

{FORMJACKING}

Cyber criminals get rich quick with formjacking

Formjacking attacks are simple and lucrative: cyber criminals load malicious code onto retailers' websites to steal shoppers' credit card details, with 4,800+ unique websites compromised on average every month.

Both well-known (Ticketmaster and British Airways) and small-medium businesses were attacked, conservatively yielding tens of millions of dollars to bad actors last year.

All it takes is 10 stolen credit cards per compromised website to result in a yield of up to $2.2M per month, as each card fetches up to $45 in underground selling forums. With more than 380,000 credit cards stolen, the British Airways attack alone may have netted criminals more than $17 million.

RANSOMWARE

CRYPTOJACKING

Down, but not out

Ransomware and cryptojacking were go-to moneymakers for cyber criminals. But 2018 brought diminishing returns, resulting in lower activity.

For the first time since 2013, ransomware declined, down 20 percent overall, but up 12 percent for enterprises.

With a 90 percent plunge in the value of cryptocurrencies, cryptojacking fell 52 percent in 2018. Still, cryptojacking remains popular due to a low barrier of entry and minimal overhead; Symantec blocked four times as many cryptojacking attacks in 2018 compared to the previous year.

TARGETED ATTACKS

Targeted attackers have an appetite for destruction

Supply chain and Living-off-the-Land (LotL) attacks are now a cyber crime mainstay: supply chain attacks ballooned by 78 percent in 2018.

Living-off-the-land techniques allow attackers to hide inside legitimate processes. For example, the use of malicious PowerShell scripts increased by 1,000 percent last year.

Symantec blocks 115,000 malicious PowerShell scripts each month, but this number accounts for less than one percent of overall PowerShell usage. A sledgehammer approach toward blocking all PowerShell activity would disrupt business, further illustrating why LotL techniques have become the preferred tactic for many targeted attack groups, allowing them to fly under the radar.

MORE AMBITIOUS AND STEALTHIER

Attackers also increased their use of tried-and-true methods like spear phishing to infiltrate organizations. While intelligence gathering remains their primary motive, some groups also focus on destruction. Nearly one in ten targeted attack groups now use malware to destroy and disrupt business operations, a 25 percent increase from the previous year.

One stark example is Shamoon, which notably re-emerged after a two-year absence, deploying wiping malware to delete files on computers of targeted organizations in the Middle East.

Cloud challenges: If it's in the cloud, security's on you

A single misconfigured cloud workload or storage instance could cost an organization millions or cause a compliance nightmare. In 2018, more than 70 million records were stolen or leaked from poorly configured S3 buckets. Off-the-shelf tools on the web allow attackers to identify misconfigured cloud resources.

Hardware chip vulnerabilities, including Meltdown, Spectre, and Foreshadow allow intruders to access companies' protected memory spaces on cloud services hosted on the same physical server. Successful exploitation provides access to memory locations that are normally forbidden.

This is particularly problematic for cloud services because while cloud instances have their own virtual processors, they share pools of memory—meaning that a successful attack on a single physical system could result in data being leaked from several cloud instances.

IoT

Your favorite IoT device is an attacker's best friend

Although routers and connected cameras make up 90 percent of infected devices, almost every IoT device is vulnerable, from smart light bulbs to voice assistants.

Targeted attack groups increasingly focus on IoT as a soft entry point, where they can destroy or wipe a device, steal credentials and data, and intercept SCADA communications.

And industrial IT shaped up as a potential cyber warfare battleground, with threat groups such as Thrip and Triton vested in compromising operational and industrial control systems.

ELECTION INTERFERENCE 2018

Did your social media feed sway an election?

With all eyes on the 2018 US Midterms, thankfully, no major disruptions landed. But social media continued as a hyperactive battlefield.

Malicious domains mimicking legitimate political websites were discovered and shut down, while Russia-linked accounts used third parties to purchase social media ads for them.

Social media companies took a more active role in combatting election interference. Facebook set up a war room to tackle election interference; Twitter removed over 10,000 bots posting messages encouraging people not to vote.

Get the details. Download the Symantec 2019 Internet Security Threat Report (ISTR)
https://go.symantec.com/ISTR

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 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