Advanced Attacks: What They Are and Why You Should Care

Overview

Advanced attacks are an issue for everyone. Sophisticated attackers are not just going after nation states. They're not just going after infrastructure. They're going after every industry, and they're going after you, as well. Highly stealthy and persistent, these attackers create ingenious techniques to hide themselves while compromising your defenses and critical data. What do you have that's worth stealing? Your valuable data, such as customer information. Sophisticated attackers place you at risk of financial loss, reputation damage, and more for their gain. Think about how many customers you'd lose if your competitors learned exactly how you bid against them.

It's no longer just about the threats. The stakes are higher now because the attacks are getting more complex and advanced. Attackers use advanced tools to get inside more networks faster than most businesses can launch a defense. And once they've invaded your networks, they can remain hidden for years—stealing business and customer data undetected. Anything of value to you is a worthwhile target for them.

We have to get better because the attackers are getting better. One clear sign is the professional attitude attackers have adopted. Their tactics have evolved. Cybercrime organizations now name themselves, and develop logos to brand themselves. They operate out of call centers. They're documenting their code. They even take weekends and holidays off. They can steal important data and cripple a business, and every organization of every size is at risk.[1] This is what it means to be an advanced attacker. It's what we call professionalization—and we're all up against it. We all need to step up our game.

The purpose of this brief is to help you understand advanced attacks, the tactics professional attackers use to deploy threats, and how Symantec can help you protect against them.

Symantec™

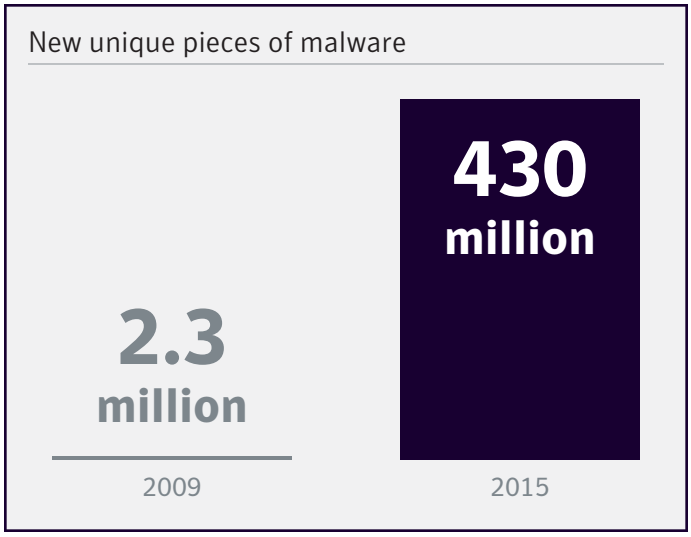
1 – Dridex:Tidal waves of spam pushing dangerous financial Trojan, O'Brien

How Are Advanced Attacks and Threats Evolving?

Advanced attacks and the threats they deliver are coming faster and with more complexity than ever. To help put this in perspective, Symantec discovered more than 2.3 million unique pieces of malware in 2009. In 2015, that number increased to 430 million. That's over 1.1 million new pieces of malware per day.[2]

In addition, attackers are using more complicated techniques to deliver malware. They have software that can create variants—taking a single piece of malware and making it look different to avoid detection; some can create a new variant every 15 seconds.[3] Other attackers use multiple drops for the data they steal, to cover their tracks and avoid detection. Once inside your infrastructure, attackers use special tools and, in some cases, your own software, to stay hidden and traverse the network, from endpoint systems to servers. Once they have their prize, they transfer your data to remote command-and-control servers—to sell or use themselves, for profit.

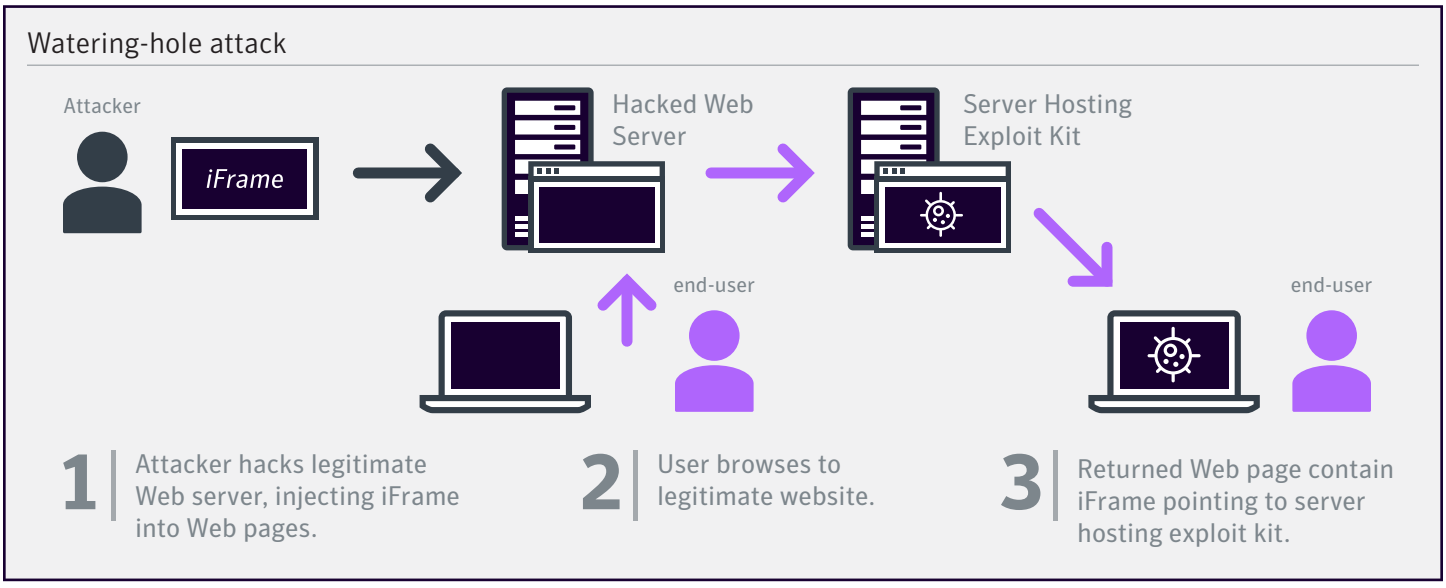
This is why you need multiple layers of protection with technologies working together to secure your organization. Threats aren't just annoyances anymore. Advanced attacks can cripple the business. And it's not just happening to the big names we see in the newspaper. It's happening to businesses everywhere.



Targeted attacks

All businesses are potentially vulnerable to targeted attacks, and spear-phishing and watering-hole attacks are the favored avenues.

Spear phishing targets individuals within a specific organization using email that appears to be from a legitimate source. A spear-phishing attack entices the victim to click on a link or download a file, which infects the user's system and spreads to infect other user. Symantec reported a concerning increase in the number and sophistication of phishing attempts targeting specific departments within organizations.[4]



2 – Symantec 2016 Internet Security Threat Report

3 – New Cerber Ransomware Variants Morph Every 15 Seconds, Cimpanu

4 – Symantec 2016 Internet Security Threat Report

In a watering-hole attack, the attacker profiles victims and the websites they frequent. When attackers find a vulnerable website, they inject it with code. This code redirects the victim to a separate site controlled by the attacker, which hosts the exploit code for the vulnerability. In short, the compromised website "waits" to infect the profiled victim with a zero-day exploit—just like a lion waiting at the watering hole.

Unfortunately, as organizations adopt new technologies, the attack surface expands. With businesses turning more to cloud technology and the prevalence of IoT devices, we expect to see targeted attacks exploiting vulnerabilities in these systems within the next year or two.[5]

Zero-day vulnerabilities

A zero-day vulnerability is an undisclosed window into an application that can be exploited by a criminal to get malware onto your machines. It's like a stranger finding a key to your front door. When hackers discover and exploit a security weakness before a fix becomes available, it's called a "zero-day" vulnerability (meaning that developers have zero days to fix the problem before it's exploited).

The number of zero-day vulnerabilities discovered in 2015 more than doubled from the year before, with an average of one new zero-day vulnerability found each week.[6] Vulnerabilities can appear in almost any type of software, but the most attractive to targeted attackers is software that's widely used, such as Internet Explorer and Adobe Flash Player. Once discovered, the zero days are quickly added to cybercriminal toolkits and exploited. At this point, millions will be attacked and hundreds of thousands infected if a patch isn't available, or if people haven't moved quickly enough to apply the patch.

Hackers who discover vulnerabilities will sell the zero-day exploit to other hackers and organizations. In short, these zero-day exploits are sold as weaponized code. And it's big business. According to an article published on Forbes.com, zero-day exploits can sell from $5,000 to $250,000, depending on how widely used the target software is, as well as how difficult it was to find the zero-day exploit.[7]

Zero-day vulnerabilities have always been a problem, but as the market thrives, these exploits gain value, and we're seeing a lot more of them. They're coming faster, and our exposure to them is much greater. Vulnerabilities that leave you susceptible to zero-day attacks can be disastrous for your business.

Ransomware

There are two main forms of ransomware in circulation today. Locker ransomware (computer locker) denies access to the computer or device by locking the screen, and Crypto ransomware (data locker) prevents access to files or data through encryption. The strategy of both is to use phishing schemes or web browser vulnerabilities to invade your system, deny access to your files, and only offer to return what is rightfully yours if a ransom is paid.

Ransomware is changing. No longer merely a consumer threat, we expect to see more targeted ransomware attacks on businesses in the future. Currently, 99 percent of all ransomware is simply random—throwing out a net and trying to get as many people as possible. With cybercriminals hitting millions of users worldwide, if even a small percentage of victims pay the ransom, it could make the scheme worthwhile.

Typically, ransomware fails in the business environment because businesses back up their files. They simply restore their files and everyone goes along their way. The chances for attackers to be successful, in the past, were pretty slim.

However, recently there have been some high-profile incidents where businesses were infected with ransomware and paid thousands of dollars to get their files back. These companies had a few users who clicked on a link in a spam phishing email and suddenly had their files encrypted. The companies panicked and paid the ransom to get their files back.

That's like blood in the water. When attackers see companies paying ransoms, they realize organizations aren't doing a good job of backing up files, and will increase their efforts accordingly. Now, cyber gangs are trying to figure out how to destroy existing protection against ransomware in the enterprise—backups. As long as they're successful in their attacks, they'll make money, and other gangs will start to follow them. For your business, a successful ransomware attack could mean a loss of worker productivity and worse because your critical files are locked up and held for ransom.

5 – Symantec 2016 Internet Security Threat Report

6 – Symantec 2016 Internet Security Threat Report

7 – Guide to Zero-Day Exploits, Park, 2015

Advanced persistent threats

In addition to common attack methods, advanced persistent threats (APTs) often use highly customized tools and intrusion techniques, developed specifically for the campaign. APTs often launch multiple threats simultaneously to breach their targets and ensure ongoing access to targeted systems. Sometimes, a "sacrificial" threat is included to trick the target into thinking the attack has been successfully repelled.

APT attacks occur over long periods of time; the attackers move slowly and quietly to avoid detection. In contrast to the "smash and grab" tactics of many targeted attacks launched by more typical cybercriminals, the goal of the APT is to stay undetected by moving "low and slow" with continuous monitoring and interaction until the attackers achieve their defined objectives.

With the growing number of attack vectors, systems, and targets available to attackers, a single approach to security can no longer keep data safe; you need to use multiple protection techniques. Moreover, you need to quickly respond to threats that hit your endpoints and proactively defend against malicious attacks.

Symantec™ Intelligent Endpoint Solution

Knowing the attacks you're up against is only the first step to securing your organization. To combat the professionalism of advanced attackers, you need to up your game. In this section, we'll introduce how Symantec helps you:

- Block as many threats as possible upfront before they infect your endpoint.
- Rapidly detect anomalies across all control points and remediate all detected instances of threats if they ever slip past.
- Remediate the most elusive threats detected in your IT environment, with just one click.
- Preempt future attacks with automated risk assessments and strategic planning to improve your security posture.
- Stop data breaches from lost or stolen endpoints.

Block advanced threats before they infect your endpoint

Blocking advanced threats before they infect your endpoint is the key to keeping your endpoints secure. Symantec™ Endpoint Protection blocks zero days and unknown threats with 99.99 percent accuracy.

The Intrusion Prevention System (IPS) feature in Symantec Endpoint Protection is the first layer of defense against zero-day exploits and web-based attacks at the network level. Our reputation-based protection and behavior monitoring features also provide crucial defense against ransomware and unknown threats. The reputation analysis feature can accurately identify suspicious files with less than a 0.01 percent false-positive rate, leveraging Symantec's global threat intelligence. The behavior monitoring feature uses an advanced machine-learning algorithm to watch what programs are doing on your computer and to stop suspicious file from executing in real-time.

Symantec neutralizes advanced threats before endpoint infection, using a multilayered approach of defense and advanced machine learning that's constantly trained and fine-tuned by Symantec's threat experts. Traditional machine learning relies solely on a single dimension of classifiers to detect new attack artifacts, like malicious files or URLs. However, Symantec uses a multi-dimensional machine learning approach to analyze interactions between users, software files, and websites across the internet. This provides more proactive protection and produces far fewer false-positives.

Detect anomalies across all control points

Highly-customized tools and intrusion techniques are involved in targeted attacks and advanced persistent threats. The tactics are designed for a long-term attack campaign. Symantec™ Advanced Threat Protection is the most effective solution of its kind[8] to uncover threats across endpoint, network, and email. When threats are detected, an event alert helps you identify high-risk users and actively infected systems, who is downloading malware or suspicious files, the origins of the attack, which assets have been impacted, and the spread across all control points.

Symantec uses a cloud-based sandboxing and payload detonation service to arrest suspicious files. The service combines Symantec's advanced machine learning and real-time global threat intelligence. It covers the most popular file types used in targeted attacks and executes them in a virtual environment—or if necessary, a "bare metal" environment—to uncover "virtual machine-aware" threats. Since advanced threats may exhibit different behaviors in different environments, it's crucial to have both physical and virtual sandboxing awareness.

In addition, Symantec Advanced Threat Protection helps you cut through the noise of thousands of unknowns and focus on threats that matter most, typically bubbling up the most suspicious one to two percent. It provides a full body of evidence on the attack with the unique Synapse™ correlation technology. You can also investigate attacks and search for attack artifacts—by file hash, registry key, or the source IP address and URL—across your entire infrastructure.

8 – Enterprise Anti-Virus Protection, Oct-Dec 2015, Dennis Technology Labs

Remediate the most stealthy threats with one click

Once you detect threats in your IT environment, you can quickly remediate them. Symantec Advanced Threat Protection can rapidly restore normal operations after targeted attacks, and contain and remediate all detected instances of threats in minutes. Our Endpoint Detection and Response (EDR) technology provides all attack data in one place—including files used in a particular attack, originating email addresses, and IP addresses where employees downloaded the file. You can remediate any of these artifacts with just a click. Rapid detection and remediation decreases your exposure to potential risks and controls damage from spreading attacks.

Since Symantec Advanced Threat Protection is integrated with Symantec Endpoint Protection, you can quickly see whether Symantec Endpoint Protection has successfully protected against the threat, which means a drastic reduction of incidents and alerts for you. You can prevent, detect, and remediate threats without deploying a new endpoint agent.

Preempt future attacks with automated risk assessments and strategic planning

Symantec can better prepare you before you're the victim of an attack. Symantec™ Risk Insight provides a comprehensive view of your internal risk posture and extended enterprise, including your customers, benchmarked against peers in your industry. An executive dashboard helps you quantify the effectiveness of your security program, track improvements over time, and justify future investments. In addition, its granular drill-down capabilities and advanced analytics helps you to pinpoint specific weaknesses such as high-risk users and endpoints, suspicious applications, and unpatched vulnerabilities.

Symantec Risk Insight answers questions such as, "Is my web security sufficient across all regions?" "Do certain individuals pose a higher insider risk?" "Are my customers posing a high risk to my organization?" Integrated with Symantec Endpoint Protection, Symantec Risk Insight provides the deep visibility and rich insights you need to make important security decisions, without requiring additional agents, software, or hardware provisioning. It streamlines complex manual assessments with an automated cloud-based service, making risk assessment a much simpler process. With Symantec Risk Insight, you can preempt advanced threats more effectively.

Stop breaches from lost or stolen endpoints

Symantec Intelligent Endpoint solution not only stops cyber threats, but also stops "physical threats" of endpoints. If your devices are physically lost or stolen, endpoint encryption is essential. It's the best way to protect the data on laptops, desktops and removable media when an endpoint goes missing, because even if it's lost, the data remains safe.

Symantec™ Endpoint Encryption uses a pre-boot passphrase to protect a machine and prevent it from booting-up until the correct passphrase is entered. Without the passphrase, the information on the device remains scrambled and prevents outsiders from accessing data. With an intuitive central management platform, Symantec helps administrators prove a device was encrypted should it go missing.

Summary

Advanced attacks are coming faster and they're more complex than ever. Common cybercriminals have adopted professional behaviors, and they're intent on getting what they're after. All businesses of every size and in every industry are at risk. Blocking is not enough to stay ahead of advanced attacks. You can't rely on antivirus or any single protection technique because it's too easy for attackers to crash it.

The most effective defense against advanced attackers is a layered defense—a solution that blocks the majority of threats before infection; rapidly detects and remediates if malware slips past; and provides an automated risk assessment to help you understand your risk posture and deflect critical attacks to your organization.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

Symantec Corporation World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934

www.symantec.com

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.

07/16 xxxxxxxx