Cisco 2017
Midyear Cybersecurity Report

Executive Summary

For nearly a decade, Cisco has published comprehensive cybersecurity reports that are designed to keep security teams and the businesses they support apprised of cyber threats and vulnerabilities—and informed about steps they can take to improve security and cyber-resiliency. In these reports, we strive to alert defenders to the increasing sophistication of threats and the techniques that adversaries use to compromise users, steal information, and create disruption.

With this latest report, however, we find we must raise our warning flag even higher. Our security experts are becoming increasingly concerned about the accelerating pace of change—and yes, sophistication—in the global cyber threat landscape. That is not to say defenders are not improving their ability to detect threats and prevent attacks, or to help users and organizations avoid or recover more quickly from them. But we see two dynamics undermining their hard-won successes, hindering further progress, and helping to usher in a new era of cyber risks and threats:

The escalating impact of security breaches

Revenue generation is still the top objective of most threat actors. However, some adversaries now have the ability—and often now, it seems, the inclination—to lock systems and destroy data as part of their attack process. Our researchers see this more sinister activity as a precursor to a new and devastating type of attack that is likely to emerge in the near future: destruction of service (DeOS).

Within the past year, we have also observed adversaries employing Internet of Things (IoT) devices in DDOS attacks. Botnet activity in the IoT space suggests some operators may be focused on laying the foundation for a wide-reaching, high-impact attack that could potentially disrupt the Internet itself.

The pace and scale of technology

Our threat researchers have been monitoring for years how mobility, cloud computing, and other technology advancements and trends are stretching and eroding the security perimeter that enterprises must defend. What they can see even more clearly today, however, is how malicious actors are taking advantage of that ever-expanding attack surface. The breadth and depth of recent ransomware attacks alone demonstrate how adept advesaries are at exploiting security gaps and vulnerabilities across devices and networks for maximum impact.

Lack of visibility into dynamic IT environments, the risks presented by “shadow IT,” the constant barrage of security alerts, and the complexity of the IT security environment are just some reasons resource-strapped security teams struggle to stay on top of today’s evasive and increasingly potent cyber threats.

What we cover in this report

The *Cisco 2017 Midyear Cybersecurity Report* explores the above dynamics through the discussion of:

Adversary tactics

We examine select methods threat actors are using to compromise users and infiltrate systems. It is important for defenders to understand changes in adversaries' tactics so that they can, in turn, adapt their security practices and educate users. Topics covered in this report include new developments in malware, trends in web attack methods and spam, the risks of potentially unwanted applications (PUAs) like spyware, business email compromise (BEC), the changing economics of malicious hacking, and medical device compromise. Our threat researchers also offer analysis of how—and how quickly—some adversaries are evolving their tools and techniques, and deliver an update on Cisco's efforts to reduce our Time to Detection (TTD) of threats.

Vulnerabilities

In this report, we also provide an overview of vulnerabilities and other exposures that can leave organizations and users susceptible to compromise or attack. Weak security practices, such as not moving swiftly to patch known vulnerabilities, not limiting privileged access to cloud systems, and leaving infrastructure and endpoints unmanaged, are discussed. Also in focus: why the expanding IoT and the convergence of IT and operational technology (OT) create even more risk for organizations and their users, as well as for consumers, and what defenders should do now to address these risks before they are impossible to manage.

Opportunities for defenders

The *Cisco 2017 Midyear Cybersecurity Report* presents additional findings from Cisco's latest Security Capabilities Benchmark Study. We offer in-depth analysis of the key security concerns of eight industry verticals: service providers, public sector, retail, manufacturing, utilities, healthcare, transportation, and finance. Industry experts from Cisco offer recommendations on how these businesses can improve their security posture, including using services to bridge knowledge and talent gaps, reducing complexity in their IT environment, and embracing automation.

The concluding section of the report includes a call to action for security leaders to seize the opportunity to engage senior executives and boards of directors in discussions about cybersecurity risks and budgets—and offers suggestions for how to start that conversation.

Major findings

- Business email compromise (BEC) has become a highly lucrative threat vector for attackers. According to the Internet Crime Complaint Center (IC3), US$5.3 billion was stolen due to BEC fraud between October 2013 and December 2016. In comparison, ransomware exploits took in US$1 billion in 2016.
- Spyware that masquerades as potentially unwanted applications (PUAs) is a form of malware—and a risk that many organizations underestimate or dismiss completely. However, spyware can steal user and company information, weaken the security posture of devices, and increase malware infections. Spyware infections are also rampant. Cisco threat researchers studied three select spyware families and found that they were present in 20 percent of the 300 companies in the sample.
- The Internet of Things (IoT) holds great promise for business collaboration and innovation. But as it grows, so too does security risk. Lack of visibility is one problem: Defenders are simply not aware of what IoT devices are connected to their network. They need to move quickly to address this and other hurdles to IoT security. Threat actors are already exploiting security weaknesses in IoT devices. The devices serve as strongholds for adversaries, and allow them to move laterally across networks quietly and with relative ease.
- Cisco has been tracking our median time to detection (TTD) since November 2015. Since that time, the overall trend has been downward—from just over 39 hours at the start of our research to about 3.5 hours for the period from November 2016 to May 2017.

US$5.3 billion

was stolen due to BEC fraud between October 2013 and December 2016

- Cisco has been observing an overall increase in spam volume since mid-2016, which seems to coincide with a significant decline in exploit kit activity during the same period. Adversaries who had relied heavily on exploit kits to deliver ransomware are turning to spam emails, including those containing macro-laden malicious documents that can defeat many sandboxing technologies because they require user interaction to infect systems and deliver payloads.
- Supply chain attacks offer adversaries a way to spread malware to many organizations through a single compromised site. In an attack studied by RSA, a Cisco partner, a software vendor's download webpage was compromised, allowing the infection to spread to any organization that downloaded the software from this vendor.
- The dramatic increase in cyber attack frequency, complexity, and size over the past year suggests that the economics of hacking have turned a corner, according to Radware, a Cisco partner. Radware notes that the modern hacking community is benefitting from quick and easy access to a range of useful and low-cost resources.

Revenue generation is still the top objective of most threat actors. However, some adversaries now have the ability to lock systems and destroy data as part of their attack process.

- When it comes to enterprise security, cloud is the ignored dimension: Open authorization (OAuth) risk and poor management of single privileged user accounts create security gaps that adversaries can easily exploit. Malicious hackers have already moved to the cloud and are working relentlessly to breach corporate cloud environments, according to Cisco threat researchers.
- In the exploit kit landscape, activity has declined dramatically and innovation has stagnated since Angler and other leading players have disappeared or changed their business model. This situation is likely temporary, given previous patterns in this market. But other factors, such as the greater difficulty of exploiting vulnerabilities in files built with Adobe Flash technology, may be slowing the resurgence.
- DevOps services that have been deployed improperly or left open intentionally for convenient access by legitimate users pose a significant risk to organizations, according to research by Rapid7, a Cisco partner. In fact, many of these instances have already been ransomed.
- A ThreatConnect analysis of colocated domains used by adversaries connected to the Fancy Bear cyberespionage group showed the value of studying bad actors' IP infrastructure tactics. By studying this infrastructure, defenders gain a larger list of domains, IP addresses, and email addresses to proactively block.
- In late 2016, Cisco threat researchers discovered and reported three remote code-execution vulnerabilities in Memcached servers. A scan of the Internet a few months later revealed that 79 percent of the nearly 110,000 exposed Memcached servers previously identified were still vulnerable to the three vulnerabilities because they had not been patched.

Download the Cisco 2017 Midyear Cybersecurity Report at cisco.com/go/mcr2017.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Published July 2017