Cisco
2017 Annual Cybersecurity Report

cisco

Table of Contents

Executive Summary

As the attack surface increases, defenders must focus on their most important goal: reducing their adversaries' operational space.

Adversaries have more tools at their disposal than ever before. They also have a keen sense of when to use each one for maximum effect. The explosive growth of mobile endpoints and online traffic works in their favor. They have more space in which to operate and more choices of targets and approaches.

Defenders can use an array of strategies to meet the challenges of an expanding threat landscape. They can purchase best-of-breed solutions that work separately to provide information and protection. And they can compete for personnel in a market where talent is in short supply and budgets are tight.

Stopping all attacks may not be possible. But you can minimize both the risk and the impact of threats by constraining your adversaries' operational space and, thus, their ability to compromise assets. One measure you can take is simplifying your collection of security tools into an interconnected and integrated security architecture.

Integrated security tools working together in an automated architecture can streamline the process of detecting and mitigating threats. You will then have time to address more complex and persistent issues. Many organizations use at least a half dozen solutions from just as many vendors (page 53). In many cases, their security teams can investigate only half the security alerts they receive on a given day.

The Cisco 2017 Annual Cybersecurity Report presents research, insights, and perspectives from Cisco Security Research. We highlight the relentless push-and-pull dynamic between adversaries trying to gain more time to operate and defenders working to close the windows of opportunity that attackers try to exploit. We examine data compiled by Cisco threat researchers and other experts. Our research and insights are intended to help organizations respond effectively to today's rapidly evolving and sophisticated threats.

This report is divided into the following sections:

Attacker Behavior

In this section, we examine how attackers reconnoiter vulnerable networks and deliver malware. We explain how tools such as email, third-party cloud applications, and adware are weaponized. And we describe the methods that cybercriminals employ during the installation phase of an attack. This section also introduces our "time to evolve" (TTE) research, which shows how adversaries keep their tactics fresh and evade detection. We also give an update on our efforts to reduce our average median time to detection (TTD). In addition, we present the latest research from Cisco on malware risk for various industries and geographic regions.

Defender Behavior

We offer updates on vulnerabilities in this section. One focus is on the emerging weaknesses in middleware libraries that present opportunities for adversaries to use the same tools across many applications, reducing the time and cost needed to compromise users. We also share Cisco's research on patching trends. We note the benefit of presenting users with a regular cadence of updates to encourage the adoption of safer versions of common web browsers and productivity solutions.

Cisco 2017 Security Capabilities Benchmark Study

This section covers the results of our third Security Capabilities Benchmark study, which focuses on security professionals' perceptions of the state of security in their organizations. This year, security professionals seem confident in the tools they have on hand, but they are uncertain about whether these resources can help them reduce the operational space of adversaries. The study also shows that public security breaches are having a measurable impact on opportunities, revenue, and customers. At the same time, breaches are driving technology and process improvements in organizations. For more in-depth analysis around the state of security in organizations, go to page 49.

Industry

In this section, we explain the importance of ensuring value chain security. We examine the potential harm of governments stockpiling information about zero-day exploits and vulnerabilities in vendors' products. In addition, we discuss the use of rapid encryption as a solution for protecting data in high-speed environments. Finally, we outline the challenges of organizational security as global Internet traffic, and the potential attack surface, grow.

Conclusion

In the conclusion, we suggest that defenders adapt their security practices so they can better meet typical security challenges along the attack chain and reduce adversaries' operational space. This section also offers specific guidance on establishing an integrated and simplified approach to security: one that will connect executive leadership, policy, protocols, and tools to prevent, detect, and mitigate threats.

Major Findings

- Three leading exploit kits—Angler, Nuclear, and Neutrino—abruptly disappeared from the landscape in 2016, leaving room for smaller players and new entrants to make their mark.
- According to the Cisco 2017 Security Capabilities Benchmark Study, most companies use more than five security vendors and more than five security products in their environment. Fifty-five percent of the security professionals use at least six vendors; 45 percent use anywhere from one to five vendors; and 65 percent use six or more products.
- The top constraints to adopting advanced security products and solutions, according to the benchmark study, are budget (cited by 35 percent of the respondents), product compatibility (28 percent), certification (25 percent), and talent (25 percent).
- The Cisco 2017 Security Capabilities Benchmark Study found that, due to various constraints, organizations can investigate only 56 percent of the security alerts they receive on a given day. Half of the investigated alerts (28 percent) are deemed legitimate; less than half (46 percent) of legitimate alerts are remediated. In addition, 44 percent of security operations managers see more than 5000 security alerts per day.
- Twenty-seven percent of connected third-party cloud applications introduced by employees into enterprise environments in 2016 posed a high security risk. Open authentication (OAuth) connections touch the corporate infrastructure and can communicate freely with corporate cloud and software-as-a-service (SaaS) platforms after users grant access.
- An investigation by Cisco that included 130 organizations across verticals found that 75 percent of those companies are affected by adware infections. Adversaries can potentially use these infections to facilitate other malware attacks.
- Increasingly, the operators behind malvertising campaigns are using brokers (also referred to as “gates”). Brokers enable them to move with greater speed, maintain their operational space, and evade detection. These intermediary links allow adversaries to switch quickly from one malicious server to another without changing the initial redirection.
- Spam accounts for nearly two-thirds (65 percent) of total email volume, and our research suggests that global spam volume is growing due to large and thriving spam-sending botnets. According to Cisco threat researchers, about 8 percent to 10 percent of the global spam observed in 2016 could be classified as malicious. In addition, the percentage of spam with malicious email attachments is increasing, and adversaries appear to be experimenting with a wide range of file types to help their campaigns succeed.
- According to the Security Capabilities Benchmark Study, organizations that have not yet suffered a security breach may believe their networks are safe. This confidence is probably misplaced, considering that 49 percent of the security professionals surveyed said their organizations have had to manage public scrutiny following a security breach.

- The Cisco 2017 Security Capabilities Benchmark Study also found that nearly a quarter of the organizations that have suffered an attack lost business opportunities. Four in 10 said those losses are substantial. One in five organizations lost customers due to an attack, and nearly 30 percent lost revenue.
- When breaches occur, operations and finance were the functions most likely to be affected (36 percent and 30 percent, respectively), followed by brand reputation and customer retention (both at 26 percent), according to respondents to the benchmark study.
- Network outages that are caused by security breaches can often have a long-lasting impact. According to the benchmark study, 45 percent of the outages lasted from 1 to 8 hours; 15 percent lasted 9 to 16 hours, and 11 percent lasted 17 to 24 hours. Forty-one percent (see page 55) of these outages affected between 11 percent and 30 percent of systems.
- Vulnerabilities in middleware—software that serves as a bridge or connector between platforms or applications—are becoming more apparent, raising concerns that middleware is becoming a popular threat vector. Many enterprises rely on middleware, so the threat could affect every industry. During the course of a Cisco® project, our threat researchers discovered that a majority of new vulnerabilities examined were attributable to the use of middleware.
- The cadence of software updates can affect user behavior when it comes to installing patches and upgrades. According to our researchers, regular and predictable update schedules result in users upgrading their software sooner, reducing the time during which adversaries can take advantage of vulnerabilities.
- The 2017 Security Capabilities Benchmark Study found that most organizations rely on third-party vendors for at least 20 percent of their security, and those who rely most heavily on these resources are most likely to expand their use in the future.

Introduction

Introduction

Adversaries have a vast and varied portfolio of techniques for gaining access to organizational resources and for attaining unconstrained time to operate. Their strategies cover all the basics and include:

- Taking advantage of lapses in patching and updating
- Luring users into socially engineered traps
- Injecting malware into supposedly legitimate online content such as advertising

They have many other capabilities, as well, from exploiting middleware vulnerabilities to dropping malicious spam. And once they've achieved their goals, they can quickly and quietly shut down their operations.

Adversaries work nonstop to evolve their threats, move with even more speed, and find ways to widen their operational space. The explosive growth in Internet traffic—driven largely by faster mobile speeds and the proliferation of online devices—works in their favor by helping to expand the attack surface. As that happens, the stakes grow higher for enterprises. The Cisco 2017 Security Capabilities Benchmark Study found that more than one-third of organizations that have been subject to an attack lost 20 percent of revenue or more. Forty-nine percent of the respondents said their business had faced public scrutiny due to a security breach.

How many enterprises can suffer such damage to their bottom line and remain healthy? Defenders must focus their resources on reducing their adversaries' operational space. Attackers will then find it extremely difficult to gain access to valuable enterprise resources and to conduct their activities without being detected.

Automation is essential to achieving this goal. It helps you understand what normal activity is in the network environment, so you can focus scarce resources on investigating and resolving true threats. Simplifying security operations also helps you become more effective at eliminating adversaries' unconstrained operational space. However, the benchmark study shows that most organizations are using more than five solutions from more than five vendors (page 53).

Such a complex web of technology, and the overwhelming number of security alerts, is a recipe for less, not more, protection. Adding more security talent can help, of course. With more experts on board, the logic goes, the better the organization's ability to manage technology and deliver better outcomes. However, scarce security talent and limited security budgets make hiring sprees unlikely. Instead, most organizations must make do with the talent they have. They rely on outsourced talent to add muscle to their security teams while also conserving budget.

The real answer to meeting these challenges, as we explain later in this report, is to operationalize people, processes, and technology in an integrated manner. To operationalize security is to truly understand what the enterprise needs to protect, as well as what measures should be used to protect those vital assets.

The Cisco 2017 Annual Cybersecurity Report presents our latest security industry advances designed to help organizations and users defend against attacks. We also look at the techniques and strategies that adversaries use to break through those defenses. The report also highlights major findings from the Cisco 2017 Security Capabilities Benchmark Study, which examines the security posture of enterprises and their perceptions of their preparedness to defend against attacks.

The Expansion of the Attack Surface

The Expansion of the Attack Surface

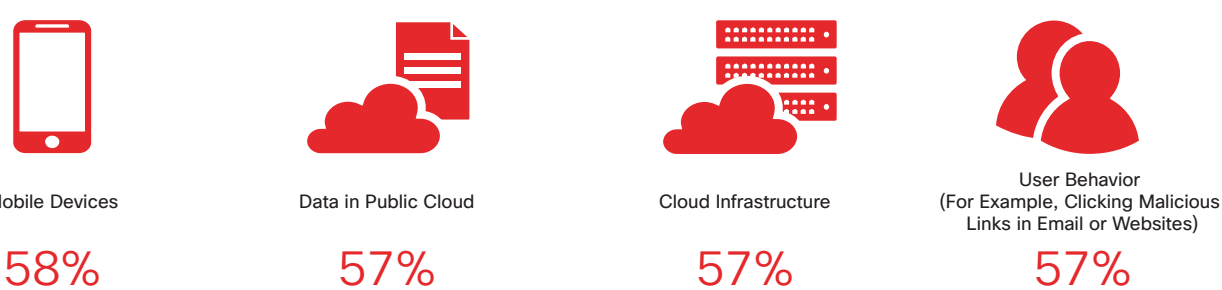
Mobile devices. Public cloud. Cloud infrastructure. User behavior. Security professionals who participated in Cisco's third annual Security Capabilities Benchmark Study cited all those elements as top sources of concern when they think about their organization's risk of exposure to a cyber attack (**Figure 1**). This is understandable: The proliferation of mobile devices creates more endpoints to protect. The cloud is expanding the security perimeter. And users are, and always will be, a weak link in the security chain.

As businesses embrace digitization—and the Internet of Everything (IoE)[1] begins to take shape—defenders will have even more to worry about. The attack surface will only expand, giving adversaries more space to operate.

For more than a decade, the Cisco® Visual Networking Index (VNI) has provided global IP traffic forecasts and analyzed the dynamic factors that facilitate network growth. Consider these statistics from the most recent report, *The Zettabyte Era—Trends and Analysis*:[2]

- Annual global IP traffic will pass the zettabyte (ZB) threshold by the end of 2016 and reach 2.3 ZB per year by 2020. (A zettabyte is 1000 exabytes, or 1 billion terabytes.) That represents a threefold increase in global IP traffic in the next 5 years.
- Traffic from wireless and mobile devices will account for two-thirds (66 percent) of total IP traffic by 2020. Wired devices will account for only 34 percent.
- From 2015 to 2020, average broadband speeds will nearly double.
- By 2020, 82 percent of all consumer Internet traffic globally will be IP video traffic, up from 70 percent in 2015.

Figure 1 Security Professionals' Biggest Sources of Concern Related to Cyber Attacks



Percentage of Security Professionals Who Find the Categories Very or Extremely Challenging

Source: Cisco 2017 Security Capabilities Benchmark Study

Download the 2017 graphics at: **www.cisco.com/go/acr2017graphics**

[1] "Internet of Everything FAQ," Cisco: http://ioeassessment.cisco.com/learn/ioe-faq.
[2] *The Zettabyte Era—Trends and Analysis*, Cisco VNI, 2016: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html.