Cisco 2017 Annual Cybersecurity Report

Executive Summary

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. 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.

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.

Download the *Cisco 2017 Annual Cybersecurity Report*
www.cisco.com/go/acr2017

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 January 2017