Cisco 2018 Annual Cybersecurity Report

# EXECUTIVE SUMMARY

What if defenders could see the future? If they knew an attack was coming, they could stop it—or at least, mitigate its impact and ensure what they need to protect most is safe. The fact is, defenders can see what's on the horizon. Many clues are out there—and obvious.

Adversaries and nation-state actors already have the expertise and tools necessary to take down critical infrastructure and systems and cripple entire regions. But when news surfaces about disruptive and destructive cyber attacks—such as those in Ukraine, for example, or elsewhere in the world—some security professionals might initially think, "Our company's market/region/technology environment wasn't a target, so, we're probably not at risk."

However, by dismissing what seem like distant campaigns, or allowing the chaos of daily skirmishes with attackers to consume their attention, defenders fail to recognize the speed and scale at which adversaries are amassing and refining their cyber weaponry.

For years, Cisco has been warning defenders about escalating cybercriminal activity around the globe. In this, our latest annual cybersecurity report, we present data and analysis from Cisco threat researchers and several of our technology partners about attacker behavior observed over the past 12 to 18 months. Many of the topics examined in the report align with three general themes:

## Adversaries are taking malware to unprecedented levels of sophistication and impact

The evolution of malware was one of the most significant developments in the attack landscape in 2017. The advent of network-based ransomware cryptoworms eliminates the need for the human element in launching ransomware campaigns. And for some adversaries, the prize isn't ransom, but obliteration of systems and data, as Nyetya—wiper malware masquerading as ransomware—proved. Self-propagating malware is dangerous and has the potential to take down the Internet, according to Cisco threat researchers.

## Adversaries are becoming more adept at evasion—and weaponizing cloud services and other technology used for legitimate purposes

In addition to developing threats that can elude increasingly sophisticated sandboxing environments, malicious actors are widening their embrace of encryption to evade detection. Encryption is meant to enhance security, but it also provides malicious actors with a powerful tool to conceal command-and-control (C2) activity, affording them more time to operate and inflict damage.

Cybercriminals are also adopting C2 channels that rely on legitimate Internet services like Google, Dropbox, and GitHub. The practice makes malware traffic almost impossible to identify.

Also, many attackers are now launching multiple campaigns from a single domain to get the best return on their investments. They are also reusing infrastructure resources, such as registrant email addresses, autonomous system numbers (ASNs), and nameservers.

## Adversaries are exploiting undefended gaps in security, many of which stem from the expanding Internet of Things (IoT) and use of cloud services

Defenders are deploying IoT devices at a rapid pace but often pay scant attention to the security of these systems. Unpatched and unmonitored IoT devices present attackers with opportunities to infiltrate networks. Organizations with IoT devices susceptible to attack also seem unmotivated to speed remediation, research suggests. Worse, these organizations probably have many more vulnerable IoT devices in their IT environments that they don't even know about.

Meanwhile, IoT botnets are expanding along with the IoT and becoming more mature and automated. As they grow, attackers are using them to launch more advanced distributed-denial-of-service (DDoS) attacks.

Attackers are also taking advantage of the fact that security teams are having difficulty defending both IoT and cloud environments. One reason is the lack of clarity around who exactly is responsible for protecting those environments.

## Recommendations for defenders

When adversaries inevitably strike their organizations, will defenders be prepared, and how quickly can they recover? Findings from the **Cisco 2018 Security Capabilities Benchmark Study**—which offers insights on security practices from more than 3600 respondents across 26 countries—show that defenders have a lot of challenges to overcome.

Even so, defenders will find that making strategic security improvements and adhering to common best practices can reduce exposure to emerging risks, slow attackers' progress, and provide more visibility into the threat landscape. They should consider:

- Implementing first-line-of-defense tools that can scale, like cloud security platforms.
- Confirming that they adhere to corporate policies and practices for application, system, and appliance patching.
- Employing network segmentation to help reduce outbreak exposures.
- Adopting next-generation endpoint process monitoring tools.
- Accessing timely, accurate threat intelligence data and processes that allow for that data to be incorporated into security monitoring and eventing.
- Performing deeper and more advanced analytics.
- Reviewing and practicing security response procedures.
- Backing up data often and testing restoration procedures—processes that are critical in a world of fast-moving, network-based ransomware worms and destructive cyber weapons.
- Reviewing third-party efficacy testing of security technologies to help reduce the risk of supply chain attacks.
- Conducting security scanning of microservice, cloud service, and application administration systems.
- Reviewing security systems and exploring the use of SSL analytics—and, if possible, SSL decryption—as soon as possible

Defenders should also consider adopting advanced security technologies that include machine learning and artificial intelligence capabilities. With malware hiding its communication inside of encrypted web traffic, and rogue insiders sending sensitive data through corporate cloud systems, security teams need effective tools to prevent or detect the use of encryption for concealing malicious activity.

Download the *Cisco 2018 Annual Cybersecurity Report*: **cisco.com/go/acr2018**

**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 February 2018