NEWS RELEASE

Cisco 2017 Midyear Cybersecurity Report predicts new "Destruction of Service" attacks; scale and impact of threats grow

2017-07-20

Key industries need to improve security posture as information technology and operational technology converge

SAN JOSE, CA -- (Marketwired) -- 07/20/17 -- The Cisco® (NASDAQ: CSCO) 2017 Midyear Cybersecurity Report (MCR) uncovers the rapid evolution of threats and the increasing magnitude of attacks, and forecasts potential "destruction of service" (DeOS) attacks. These could eliminate organizations' backups and safety nets, required to restore systems and data after an attack. Also, with the advent of the Internet of Things (IoT), key industries are bringing more operations online, increasing attack surfaces and the potential scale and impact of these threats.

Recent cyber incidents such as WannaCry and Nyetya show the rapid spread and wide impact of attacks that look like traditional ransomware, but are much more destructive. These events foreshadow what Cisco is calling destruction of service attacks, which can be far more damaging, leaving businesses with no way to recover.

The Internet of Things continues to offer new opportunities for cybercriminals, and its security weaknesses, ripe for exploitation, will play a central role in enabling these campaigns with escalating impact. Recent IoT botnet activity already suggests that some attackers may be laying the foundation for a wide-reaching, high-impact cyber-threat event that could potentially disrupt the Internet itself.

Measuring effectiveness of security practices in the face of these attacks is critical. Cisco tracks progress in reducing "time to detection" (TTD), the window of time between a compromise and the detection of a threat. Faster time to detection is critical to constrain attackers' operational space and minimize damage from intrusions. Since November 2015, Cisco decreased its median time-to-detection (TTD) from just over 39 hours to about 3.5 hours for the period from November 2016 to May 2017. This figure is based on opt-in telemetry gathered from Cisco security products deployed worldwide.

Threat Landscape: What's Hot and What's Not
Cisco security researchers watched the evolution of malware during the first half of 2017 and identified shifts in how adversaries are tailoring their delivery, obfuscation and evasion techniques. Specifically, Cisco saw they increasingly require victims to activate threats by clicking on links or opening files. They are developing fileless malware that lives in memory and is harder to detect or investigate as it is wiped out when a device restarts. Finally adversaries are relying on anonymized and decentralized infrastructure, such as a Tor proxy service, to obscure command and control activities.

While Cisco has seen a striking decline in exploit kits, other traditional attacks are seeing a resurgence:

- Spam volumes are significantly increasing, as adversaries turn to other tried-and-true methods, like email, to distribute malware and generate revenue. Cisco threat researchers anticipate that the volume of spam with malicious attachments will continue to rise while the exploit kit landscape remains in flux.
- Spyware and adware, often dismissed by security professionals as more nuisance than harm, are forms of malware that persist and bring risks to the enterprise. Cisco research sampled 300 companies over a four-month period and found that three prevalent spyware families infected 20 percent of the sample. In a corporate environment, spyware can steal user and company information, weaken the security posture of devices and increase malware infections.
- Evolutions in ransomware, such as the growth of Ransomware-as-a-Service, make it easier for criminals, regardless of skill set, to carry out these attacks. Ransomware has been grabbing headlines and reportedly brought in more than $1 billion in 2016, but this may be misdirecting some organizations, who face an even greater, underreported threat. Business email compromise (BEC), a social engineering attack in which an email is designed to trick organizations into transferring money to attackers, is becoming highly lucrative. Between October 2013 and December 2016, $5.3 billion was stolen via BEC, according to the Internet Crime Complaint Center.

Unique Industries Face Common Challenges
As criminals continue to increase the sophistication and intensity of attacks, businesses across industries are challenged to keep up with even foundational cybersecurity requirements. As Information Technology and Operational Technology converge in the Internet of Things, organizations struggle with visibility and complexity. As part of its Security Capabilities Benchmark Study, Cisco surveyed close to 3,000 security leaders across 13 countries and found that across industries, security teams are increasingly overwhelmed by the volume of attacks. This leads many to become more reactive in their protection efforts.

- No more than two-thirds of organizations are investigating security alerts. In certain industries (such as healthcare and transportation), this number is closer to 50 percent.
- Even in the most responsive industries (such as finance and healthcare), businesses are mitigating less than 50 percent of attacks they know are legitimate.
- Breaches are a wake-up call. Across most industries, breaches drove at least modest security improvements in at least 90 percent of organizations. Some industries (such as transportation) are less responsive, falling just above 80 percent.

Important findings per industry include:

- ***Public Sector -*** Of threats investigated, 32 percent are identified as legitimate threats, but only 47 percent of those legitimate threats are eventually remediated.
- ***Retail -*** Thirty-two percent said they'd lost revenue due to attacks in the past year with about one-fourth losing customers or business opportunities.
- ***Manufacturing -*** Forty percent of the manufacturing security professionals said they do not have a formal security strategy, nor do they follow standardized information security policy practices

such as ISO 27001 or NIST 800-53.
- ***Utilities -*** Security professionals said targeted attacks (42 percent) and advanced persistent threats, or APTs (40 percent), were the most critical security risks to their organizations.
- ***Healthcare -*** Thirty-seven percent of the healthcare organizations said that targeted attacks are high-security risks to their organizations.

Cisco's Advice for Organizations
To combat today's increasingly sophisticated attackers, organizations must take a proactive stance in their protection efforts. Cisco Security advises:

- Keeping infrastructure and applications up to date, so that attackers can't exploit publicly known weaknesses.
- Battle complexity through an integrated defense. Limit siloed investments.
- Engage executive leadership early to ensure complete understanding of risks, rewards and budgetary constraints.
- Establish clear metrics. Use them to validate and improve security practices.
- Examine employee security training with role-based training versus one-size-fits-all.
- Balance defense with an active response. Don't "set and forget" security controls or processes.

For the 2017 MCR, a diverse group of 10 security technology partners were invited to share data from which to jointly draw threat landscape conclusions. Partners that contributed to the report include Anomali, Flashpoint, Lumeta, Qualys, Radware, Rapid7, RSA, SAINT Corporation, ThreatConnect and TrapX. Cisco's security technology partner ecosystem is a key component of the company's vision to bring security that is simple, open and automated to customers.

Supporting Quotes
"As recent incidents like WannaCry and Nyetya illustrate, our adversaries are becoming more and more creative in how they architect their attacks. While the majority of organizations took steps to improve security following a breach, businesses across industry's are in a constant race against the attackers. Security effectiveness starts with closing the obvious gaps and making security a business priority."
- Steve Martino, Vice President and Chief Information Security Officer, Cisco

"Complexity continues to hinder many organizations' security efforts. It's obvious that the years of investing in point products that can't integrate is creating huge opportunities for attackers who can easily identify overlooked vulnerabilities or gaps in security efforts. To effectively reduce Time to Detection and limit the impact of an attack, the industry must move to a more integrated, architectural approach that increases visibility and manageability, empowering security teams to close gaps."
- David Ulevitch, Senior Vice President and General Manager, Security Business Group, Cisco

About the Report
The Cisco 2017 Midyear Cybersecurity Report examines the latest threat intelligence gathered by Cisco Collective Security Intelligence. The report provides data-driven industry insights and cybersecurity trends from the first half of the year, along with actionable recommendations to improve security posture. It is based on data from a vast footprint, amounting to a daily ingest of over 40 billion points of telemetry. Cisco researchers translate intelligence into real-time protections for our products and service offerings that are immediately delivered globally to Cisco customers.

Supporting Resources
Cisco Executive Security Video with Steve Martino: Cisco 2017 Midyear Cybersecurity Report
Cisco 2017 Midyear Cybersecurity Report
Cisco Blogs: Threats with Escalating Impact: Announcing the Cisco 2017 Midyear Cybersecurity Report
Cisco 2017 Midyear Cybersecurity Report Graphics
Follow Cisco on Twitter @CiscoSecurity

Like Cisco Security on Facebook

About Cisco
Cisco (NASDAQ: CSCO) is the worldwide technology leader that has been making the Internet work since 1984. Our people, products, and partners help society securely connect and seize tomorrow's digital opportunity today. Discover more at newsroom.cisco.com and follow us on Twitter at @Cisco.

RSS Feed for Cisco: http://newsroom.cisco.com/rss-feeds

Embedded Video Available

Press Relations
Ella Nevill
617-951-6622
elnevill@cisco.com

Analyst Relations
Jenna Duston
408-424 7210
jeabeyta@cisco.com

Investor Relations
Marty Palka
408-526 6635
mpalka@cisco.com

Source: Cisco