NEWS RELEASE

Cisco 2017 Midyear Cybersecurity Report Predicts New "Destruction of Service" Attacks, Scale and Impact of Threats Grows

2017-07-20

Key Industries Need To Improve Security Posture as Information Technology and Operational Technology Converge; Cisco Drives Down Time-To-Detection to 3.5 Hours

CASABLANCA, MOROCCO -- (Marketwired) -- 07/20/17 -- Cisco (NASDAQ: CSCO) -- The Cisco® 2017 Midyear Cybersecurity Report (MCR) uncovers the rapid evolution of threats and the increasing magnitude of attacks, leading researchers to forecast potential 'destruction of service' (DeOS) attacks which could eliminate organizations' backups and safety nets, required to restore systems and data after an attack. With the advent of the Internet of Things, key industries are bringing more operations online, increasing their attack surface and the potential scale and impact of these attacks.

Recent attacks such as WannaCry and Nyetya show the rapid spread and wide impact of attacks that look like ransomware, but are actually much more destructive. These foreshadow what Cisco is calling Destruction of Service attacks, which can be severely more damaging than traditional attacks, leaving businesses with no way to recover. The Internet of Things continues to offer new opportunities for these attackers, 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 attack that could potentially disrupt the Internet itself.

The good news for businesses is that 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 decrease in TTD is essential to limiting the impact of an attack and speeding recovery efforts to limit business disruptions.

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 the way adversaries are tailoring their delivery, obfuscation and evasion techniques.

Specifically, Cisco saw these adversaries increasingly requiring the victim to take action to activate a threat, such as clicking on a link or opening a file; developing fileless malware that resides completely in memory and is harder to detect or investigate as it is wiped out when a device restarts, and 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 many 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 continue to persist and bring risks to the enterprise. Cisco research sampled 300 companies over a four month period and found that 3 prevalent spyware families infected 20% 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 any criminal regardless of skillset, to carry out these attacks. Ransomware has been grabbing headlines for months and reportedly brought in more than $1 billion in 2016, but this may be mis-directing some organizations, who face an even greater, under-reported threat. Business email compromise, a social engineering attack in which an email designed to trick organizations into transferring money to the attacker, is becoming a highly lucrative threat vector. Between October 2013 and December 2016, $5.3 billion was stolen via BEC between according to The Internet Crime Complaint Center.

Unique Industries Face Common Challenges
As criminals continue to increase the sophistication and intensity of their attacks, businesses across a variety of industries are challenged with keeping up with even some of the foundational cybersecurity requirements. As Information Technology and Operational Technology converge in the Internet of Things, organizations are struggling with visibility and complexity. As part of its Security Capabilities Benchmark Study, Cisco surveyed close to 3000 security leaders across 13 countries and found that across industries, security teams are increasingly overwhelmed by the volume of attacks they are fighting, which leads many to become more reactive, in their protection efforts.

- No more than 2/3 of organizations are investigating security alerts, and in certain industries (such as healthcare and transportation), this number is closer to 50%
- Even in the most responsive industries, (such as finance and healthcare) businesses are mitigating less than 50% 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% of organizations, although some industries (such as transportation) are less responsive, falling just above 80%

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 --*** 32 percent said they'd lost revenue due to attacks in the past year with about one-fourth losing customers or business opportunities.
- ***Manufacturing --*** 40 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 --*** 37 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, organiztions 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 on to ensure complete understanding of risks, rewards and budgetary constraints
- Examine employee security training with role-based training vs. 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 set of security technology partners were invited to share data from which we could 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 our 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 industries 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 organziations' security efforts. Its 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.

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.

Cisco Public Information.

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

Media Contact:

Sonwabise Sebata
PR and Communications Lead: Africa
Cisco
+27 11 267 1000

Source: Cisco Systems South Africa (Pty) Ltd