NEWS RELEASE

Cisco 2016 Midyear Cybersecurity Report Predicts Next Generation of Ransomware; New Tactics Emerging to Maximize Profit

2016-07-26

Closing Attackers' "Window of Opportunity" Is Top Priority for Organizations; Cisco Leads Industry in Reducing Time to Detection With New 13-Hour Low
SAN JOSE, CA -- (Marketwired) -- 07/26/16 -- The Cisco® (NASDAQ: CSCO) 2016 Midyear Cybersecurity Report (MCR) finds that organizations are unprepared for future strains of more sophisticated ransomware. Fragile infrastructure, poor network hygiene, and slow detection rates are providing ample time and air cover for adversaries to operate. According to the report's findings, the struggle to constrain the operational space of attackers is the biggest challenge facing businesses and threatens the underlying foundation required for digital transformation. Other key findings in the MCR include adversaries expanding their focus to server-side attacks, evolving attack methods and increasing use of encryption to mask activity.

So far in 2016, ransomware has become the most profitable malware type in history. Cisco expects to see this trend continue with even more destructive ransomware that can spread by itself and hold entire networks, and therefore companies, hostage. New modular strains of ransomware will be able to quickly switch tactics to maximize efficiency. For example, future ransomware attacks will evade detection by being able to limit CPU usage and refrain from command-and-control actions. These new ransomware strains will spread faster and self-replicate within organizations before coordinating ransom activities.

Visibility across the network and endpoints remains a primary challenge. On average, organizations take up to 200 days to identify new threats. Cisco's median time to detection (TTD) continues to outpace the industry, hitting a new low of approximately 13 hours to detect previously unknown compromises for the six months ending in April 2016. This result is down from 17.5 hours for the period ending in October 2015. Faster time to detection of threats is critical to constrain attackers' operational space and minimize damage from intrusions. This figure is based on opt-in security telemetry gathered from Cisco security products deployed worldwide.

As attackers innovate, many defenders continue to struggle with maintaining the security of their devices and systems. Unsupported and unpatched systems create additional opportunities for attackers to easily gain access, remain undetected, and maximize damage and profits. The Cisco 2016 Midyear Cybersecurity Report shows that this challenge persists on a global scale. While organizations in critical industries such as healthcare have experienced a significant uptick in attacks over the past several months, the report's findings indicate that all vertical markets and global regions are being targeted. Clubs and organizations, charities and non-governmental organization (NGOs), and electronics businesses have all experienced an increase in attacks in the first half of 2016. On the world stage, geopolitical concerns include regulatory complexity and contradictory cybersecurity policies by country. The need to control or access data may limit and conflict with international commerce in a sophisticated threat landscape.

Attackers Operating Unconstrained

For attackers, more time to operate undetected results in more profits. In the first half of 2016, Cisco reports, attacker profits have skyrocketed due to the following:

Expanding Focus: Attackers are broadening their focus from client-side to server-side exploits, avoiding detection and maximizing potential damage and profits.

- Adobe Flash vulnerabilities continue to be one of the top targets for malvertising and exploit kits. In the popular Nuclear exploit kit, Flash accounted for 80 percent of successful exploit attempts.
- Cisco also saw a new trend in ransomware attacks exploiting server vulnerabilities -- specifically within JBoss servers -- of which, 10 percent of Internet-connected JBoss servers worldwide were found to be compromised. Many of the JBoss vulnerabilities used to compromise these systems were identified five years ago, meaning that basic patching and vendor updates could have easily prevented such attacks.

Evolving Attack Methods: During the first half of 2016, adversaries continued to evolve their attack methods to capitalize on defenders' lack of visibility.

- Windows Binary exploits rose to become the top web attack method over the last six months. This method provides a strong foothold into network infrastructures and makes these attacks harder to identify and remove.
- During this same timeframe, social engineering via Facebook scams dropped to second from the top spot in 2015.

Covering Tracks: Contributing to defenders' visibility challenges, adversaries are increasing their use of encryption as a method of masking various components of their operations.

- Cisco saw an increased use of cryptocurrency, Transport Layer Security and Tor, which enables anonymous communication across the web.
- Significantly, HTTPS-encrypted malware used in malvertising campaigns increased by 300 percent from December 2015 through March 2016. Encrypted malware further enables adversaries to conceal their web activity and expand their time to operate.

Defenders Struggle to Reduce Vulnerabilities, Close Gaps

In the face of sophisticated attacks, limited resources and aging infrastructure, defenders are struggling to keep pace with their adversaries. Data suggests defenders are less likely to address adequate network hygiene, such as patching, the more critical the technology is to business operations. For example:

- In the browser space, Google Chrome, which employs auto-updates, has 75 to 80 percent of users using the newest version of the browser, or one version behind.

- When we shift from looking at browsers to software, Java sees slow migrations with one-third of the systems examined running Java SE 6, which is being phased out by Oracle (the current version is SE 10).
- In Microsoft Office 2013, version 15x, 10 percent or less of the population of a major version are using the newest service pack version.

In addition, Cisco found that much of their infrastructure was unsupported or operating with known vulnerabilities. This problem is systemic across vendors and endpoints. Specifically, Cisco researchers examined 103,121 Cisco devices connected to the Internet and found that:

- Each device on average was running 28 known vulnerabilities.
- Devices were actively running known vulnerabilities for an average of 5.64 years.
- More than 9 percent have known vulnerabilities older than 10 years.

In comparison, Cisco also looked across software infrastructure at a sample of over 3 million installations. The majority were Apache and OpenSSH with an average number of 16 known vulnerabilities, running for an average of 5.05 years.

Browser updates are the lightest-weight updates for endpoints, while enterprise applications and server-side infrastructure are harder to update and can cause business continuity problems. In essence, the more critical an application is to business operations, the less likely it is to be addressed frequently, creating gaps and opportunities for attackers.

Cisco Advises Simple Steps to Protect Business Environments

Cisco's Talos researchers have observed that organizations that take just a few simple yet significant steps can greatly enhance the security of their operations, including:

- ***Improve network hygiene***, by monitoring the network; deploying patches and upgrades on time; segmenting the network; implementing defenses at the edge, including email and web security, Next-Generation Firewalls and Next-Generation IPS.
- ***Integrate defenses***, by leveraging an architectural approach to security versus deploying niche products.
- ***Measure time to detection,*** insist on fastest time available to uncover threats then mitigate against them immediately. Make metrics part of organizational security policy going forward.
- ***Protect your users everywhere they are*** and wherever they work, not just the systems they interact with and when they are on the corporate network.
- ***Back up critical data,*** and routinely test their effectiveness while confirming that back-ups are not susceptible to compromise.

Supporting Quote

"As organizations capitalize on new business models presented by digital transformation, security is the critical foundation. Attackers are going undetected and expanding their time to operate. To close the attackers' windows of opportunity, customers will require more visbility into their networks and must improve activities, like patching and retiring aging infrastructure lacking in advanced security capabilities.

"As attackers continue to monetize their strikes and create highly profitable business models, Cisco is working with our customers to help them match and exceed their attackers' level of sophistication, visbility and control."
-- Marty Roesch, Vice President and Chief Architect, Security Business Group, Cisco

About the Report

The Cisco 2016 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 Video with David Goeckeler, Steve Martino: Cisco 2016 Midyear Cybersecurity Report
Cisco 2016 Midyear Cybersecurity Report
Cisco Blog: Time is of the Essence: Announcing the Cisco 2016 Midyear Cybersecurity Report
Cisco Infographic
Cisco 2016 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
Trevor Bratton
949-823-1212
trbratto@cisco.com

Investor Relations
Suresh Bashkaran Nair
408-853-2014
surbhask@cisco.com

Source: Cisco