NEWS RELEASE

Cisco Midyear Security Report Reveals Sophisticated Cyberattacks Are Defining the Innovation Race Between Adversaries and Defenders

2015-07-28

Findings Underscore the Need for Retrospective Analysis to Reduce Time to Detection
SAN JOSE, CA -- (Marketwired) -- 07/28/15 -- The Cisco® (NASDAQ: CSCO) 2015 Midyear Security Report released today, which analyzes threat intelligence and cybersecurity trends, reveals the critical need for organizations to reduce time to detection (TTD) in order to remediate against sophisticated attacks by highly motivated threat actors. The Angler Exploit Kit represents the types of common threats that will challenge organizations as the digital economy and the Internet of Everything (IoE) create new attack vectors and monetization opportunities for adversaries.

The report shows that new risks associated with Flash, the evolution of ransomware, and the Dridex mutating malware campaign, reinforce the need for reduced time to detection. With the digitization of business and the IoE, malware and threats become even more pervasive, which shines a light on the security industry's estimates of 100 to 200 days for TTD. In contrast, the average TTD for Cisco Advanced Malware Protection (AMP), with its retrospective analysis of attacks that make it past existing defenses, is 46 hours.

The findings also underscore the need for businesses to deploy integrated solutions vs. point products, work with trustworthy vendors, and enlist security services providers for guidance and assessment. Further, geopolitical experts have declared that a global cyber governance framework is needed to sustain economic growth.

Watch the video of John Chambers, Cisco Chairman and John N. Stewart, Cisco SVP and Security & Trust Officer discuss the Top Insights from 2015 Cisco Midyear Security Report

Other key findings from the study include the following:

- ***Angler: Adversaries Darting in the Shadows -*** Angler is currently one of the most sophisticated and widely used exploit kits because of its innovative use of Flash, Java, Internet Explorer, and Silverlight vulnerabilities. It also excels at attempting to evade detection by employing domain shadowing, as one of its techniques, accounting for the lion's share of domain shadowing activity.

- ***Flash is Back -*** Exploits of Adobe Flash vulnerabilities, which are integrated into Angler and Nuclear exploit kits, are on the rise. This is due to lack of automated patching, as well as consumers who fail to update immediately.
    - In the first half of 2015, there has been a 66 percent increase in the number of Adobe Flash Player vulnerabilities reported by the Common Vulnerabilities and Exposure (CVE) system over all of 2014. At this rate, Flash is on pace to set an all-time record for the number of CVEs reported in 2015.

- ***The Evolution of Ransomware -*** Ransomware remains highly lucrative for hackers as they continue to release new variants. Ransomware operations have matured to the point that they are completely automated and carried out through the dark web. To conceal payment transactions from law enforcement, ransoms are paid in cryptocurrencies, such as bitcoin.

- ***Dridex: Campaigns on the Fly -*** The creators of these quickly mutating campaigns have a sophisticated understanding of evading security measures. As part of their evasion tactics, attackers rapidly change the emails' content, user agents, attachments, or referrers and launch new campaigns, forcing traditional antivirus systems to detect them anew.

A Call to Arms

The innovation race between adversaries and security vendors is accelerating, placing end users and organizations at increasing risk. Vendors must be vigilant in developing integrated security solutions that help organizations be proactive and align the right people, processes, and technology.

Integrated Threat Defense - Organizations face significant challenges with point product solutions and need to consider an integrated threat defense architecture that embeds security everywhere, and will enforce at any control point.

Services Fill the Gap - As the security industry addresses increased fragmentation, a dynamic threat landscape, and how to cope with a rising shortfall of skilled talent, businesses must invest in effective, sustainable and trusted security solutions and professional services.

Global Cyber Governance Framework - Global cyber governance is not prepared to handle the emerging threat landscape or geopolitical challenges. The question of boundaries -- how governments collect data about citizens and businesses and share among jurisdictions -- is a significant hurdle to achieving cohesive cyber governance as worldwide cooperation is limited. A collaborative, multi-stakeholder cyber governance framework is required to sustain business innovation and economic growth on a global stage.

Trustworthy Vendors - Organizations should demand that their technology vendors are transparent about and able to demonstrate the security they build into their products in order to be considered trustworthy**.** These organizations must carry this understanding across all aspects of product development starting with the supply chain and through the deployed life of their products. They must ask vendors to contractually back up their claims and demand better security.

Download a copy of the Cisco 2015 Midyear Security Report

Supporting Quotes

John N. Stewart, senior vice president, chief security and trust officer, Cisco

"Organizations cannot just accept that compromise is inevitable, even if it feels like it today. The technology industry must up the game and provide reliable and resilient products and services, and the security industry must provide vastly improved, yet meaningfully simplified, capabilities for detecting, preventing, and recovering from attacks. This is where we are leading. We are regularly told that business strategy and security strategy are the top two issues for our customers, and they want trusted partnerships with us. Trust is tightly linked to security, and transparency is key so industry-leading technology is only half the battle. We're committed to providing both: industry-defining security capabilities and trustworthy solutions across all product lines."

Jason Brvenik, principal engineer, Security Business Group, Cisco

"Hackers, being unencumbered, have the upper hand in agility, innovation and brazenness. We see this time and again, whether it is nation state actors, malware, exploit kits or ransomware. A purely preventive approach has proven ineffective, and we are simply too far down the road to accept a time to detection measured in hundreds of days. The question of 'what do you do when you are compromised' highlights the need for organizations to invest in integrated technologies that work in concert to reduce time to detection and remediation to a matter of hours; and then they should demand their vendors help them to reduce this metric to minutes."

Supporting Resources

John N. Stewart commentary on Cisco 2015 Midyear Security Report
MSR Infographic
Cisco Security Blog
Cisco Security products and solutions
Twitter @CiscoSecurity Facebook http://facebook.com/ciscosecurity

Embed: Top Insights from 2015 Cisco Midyear Security report: https://www.youtube.com/watch?v=DsfLmT9baTs

About Cisco

Cisco (NASDAQ: CSCO) is the worldwide leader in IT that helps companies transform the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected. For ongoing news, please go to http://thenetwork.cisco.com.

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

Embedded Video Available

Press Relations

Kelly Cytron
415-271-3638
kcytron@cisco.com

Analyst Relations

Trevor Bratton
949-823-1212
trbratto@cisco.com

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

Source: Cisco