NEWS RELEASE

Cisco Launches New Advanced Malware Protection Capabilities and Incident Response Services, Giving Customers Powerful Tools for Faster Time to Detection and Resolution

2015-04-07

New Threat Intelligence, Dynamic Malware Analysis and Retrospective Security Capabilities for Protecting Across the Attack Continuum
SAN JOSE, CA -- (Marketwired) -- 04/07/15 -- Cisco (NASDAQ: CSCO) today unveiled a host of new capabilities and services that give security professionals extensive intelligence and analysis on potential compromises and solutions to protect against, respond to and recover from attacks.

Cisco announces the addition of AMP Threat Grid to the Cisco® Advanced Malware Protection (AMP) portfolio, which integrates innovation acquired through last year's acquisition of ThreatGRID. This integration provides the latest malware threat intelligence and dynamic malware analysis capabilities, both on-premise and in the cloud, that strengthen Cisco AMP's continuous analysis and zero-day detection capabilities. In addition, Cisco is introducing Incident Response Services that equip organizations with teams of information security experts that utilize threat intelligence and best practices for readiness and response from network to endpoint to cloud.

As dynamic as the modern threat landscape is, there are some constants; adversaries are committed to continually refining and developing new techniques that can evade detection and hide malicious activity. This is evident by the 250 percent increase in malvertising attacks as cited in the Cisco 2015 Annual Security Report. Additionally, the report continues to show that enterprises are in a persistent state of infection, showing that 100 percent of networks analyzed had traffic going to websites hosting malware.

AMP Everywhere
New threat intelligence, dynamic malware analysis and retrospective security capabilities for Cisco AMP enhance protection across the attack continuum. These capabilities, which now include the integration

of AMP Threat Grid, are deployable across the extended network including endpoints, mobile devices and virtual systems, as well as Cisco Web and email security appliances.

New Dynamic Malware Analysis and Threat Intelligence

- ***AMP Threat Grid provides*** dynamic malware analytics and threat intelligence. These advanced capabilities are provided as a standalone cloud service or via new UCS based on premise appliances. AMP Threat Grid analytics engines provide security teams with breach detection against advanced malware, allowing them to quickly scope and recover from a breach by providing context-rich, actionable threat intelligence.

- ***Vulnerability visibility and prioritization:*** AMP for Endpoints brings additional visibility to the extended network by providing a list of hosts that contain vulnerable software, a list of the vulnerable software on each host, and the hosts most likely to be compromised. Powered by Cisco threat intelligence and security analytics, AMP identifies vulnerable software being targeted by malware and the potential exploit, and provides customers with a prioritized list of hosts to patch.

Enhanced Retrospective Security Capabilities
Unique to Cisco AMP, the solution continuously records and analyzes file activity at and after initial inspection. If a file exhibits malicious behavior after the fact, retrospective security rolls back the tape to see the origin of a potential threat and the behavior it exhibited, and provides built-in response capabilities to contain and eliminate the threat.

- ***Endpoint Indicators of Compromise (IoCs):*** Security teams can now perform deeper levels of investigation on lesser known advanced threats specific to applications in their environment by directly submitting Endpoint IoCs to Cisco AMP.

- ***Low Prevalence:*** Further empowering security teams to quickly scope and understand targeted attacks, AMP for Endpoints can now display files that have been executed across the organization ordered from lowest to highest number of instances. Customers also have the ability to submit identified low prevalent files for dynamic malware analysis for even greater visibility and context, either manually or automatically by policy. This set of capabilities can help surface previously undetected and targeted threats that were only seen by a small number of users.

Cisco Security Incident Response Services: Threat Protection Expertly Applied
There is a widening gap between the availability of expert security practitioners and the industry's needs, as companies lack both funding and manpower to adequately protect assets and infrastructure. Chief Information Security Officers are increasingly looking to external experts for security guidance.

Utilizing threat intelligence from the Cisco Talos Security Intelligence and Research Group, AMP and the expertise of the Cisco Security Solutions (CSS) team, the Incident Response Services group works with organizations to identify the source of infection, where it entered the environment, and what data was compromised. By utilizing Cisco security products like AMP, the incident response team is able to find the source -- patient zero -- and identify malware movement throughout the environment, allowing organizations to minimize the cost and overall impact of any breach, as well as identify methods to reduce future risk. The Incident Response Services supports businesses in two areas:

- ***Cyber Attack Response:*** Every event is unique and Cisco Security Incident Response methodology provides expedience and allows for flexibility to continuously adjust to the dynamic threat landscape. Whether it's an insider threat, distributed denial of service, advanced malware at the

endpoints or customer data breach, the team guides an organization through identification, isolation and resolution using Assessment, Analysis and Data Mining; Forensic Image Analysis; Infected System Dynamic Instrumentation; Malware Reverse Engineering and Exploit Analysis and Re-Implementation.

- ***Cybersecurity Readiness:*** As businesses fall victim to increasingly targeted cyber-attacks and data breaches, they need external expertise to assess and promote security best practices as well as to protect corporate data and prepare for the inevitable data breach incident. Cisco Incident Response offerings span infrastructure breach preparedness assessments, security operations readiness assessment and breach communications assessments among others.

Supporting Quotes
Roland Cloutier, Global Chief Security Officer, ADP
"The integration of AMP Threat Grid into our environment provides our existing security, risk, and privacy business protection technologies with automated and integrated threat intelligence, enhancing their effectiveness and enriching our overall cyber defense posture. This advanced threat picture enables our Critical Incident Response Centers to more rapidly analyze and mitigate potential malware," says Roland Cloutier, Global Chief Security Officer at ADP.

Marty Roesch, Vice President, Chief Architect, Cisco Security Business Group
"Every day organizations are faced with advanced threats that infiltrate and persist in company environments for months before they are discovered. We believe that the most effective way to address these real-world challenges is continuous threat protection against these attacks. Further enhancements like advanced correlation of indicators of compromise, vulnerability mapping and expanded retrospective security further differentiate Cisco AMP and strengthen security teams' responses before, during and after an attack."

James Mobley, Vice President, Cisco Security Solutions Group
"Attacks are occurring at an alarming rate. Unfortunately, many enterprises do not have cybersecurity professionals with the necessary expertise and skills to prepare for and mitigate these attacks. The Cisco Incident Response Services team works with businesses to address these challenges, taking an intelligence-driven approach to security, so that security blind spots can be reduced and network visibility improved. Armed with this insight, Cisco can significantly minimize the impact of a breach via proven readiness and response services."

Supporting Resources
RSA Conference - AMP Threat Grid Demo - Booth N3801
AMP Everywhere Product Information
Cisco Security Solutions for Incident Response
Poseidon - Incident Response Case Study
Cisco 2015 Annual Security Report
Cisco Security Webcast

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.

other company.

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

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