CUSTOMER

January 2014

Executive Corner

John N. Stewart, SVP and Chief Security Officer of Global Government and Corporate Security at Cisco

Cisco Annual Security Report Documents Unprecedented Growth of Advanced Attacks and Malicious Traffic

Threats Take Advantage of Expanding Attack Surface with New Techniques

The Cisco 2014 Annual Security Report released last week, reveals that threats designed to take advantage of users' trust in systems, applications, and personal networks have reached startling levels. According to the report, a worldwide shortage of nearly a million skilled security professionals is hampering the ability of organizations to monitor and secure networks, while overall vulnerabilities and threats reached their highest levels since 2000.

Some of this year's top findings:

- **Overall vulnerabilities and threats reached their highest level** since tracking began in May 2000. As of October 2013, cumulative annual alert totals increased 14 percent year-over-year from 2012.
- **The report indicates a shortage of more than a million security professionals** across the globe in 2014. The sophistication of the technology and tactics used by online criminals—and their nonstop attempts to breach networks and steal data—have outpaced the ability of IT and security professionals to address these threats. Most organizations have neither the people nor the systems to continuously monitor extended networks and detect infiltrations, and then apply protection, in a timely and effective manner.
- **One hundred percent of a sample of 30 of the world's largest multinational company networks generated visitor traffic to websites that host malware.** Ninety-six percent of the reviewed networks communicated traffic to hijacked servers. Similarly, 92 percent transmitted traffic to webpages without content, which typically host malicious activity.

Read the press release.

Cisco at RSA Conference 2014, Moscone Center, San Francisco
Intelligent Cybersecurity for the Real World

February 24-28, 2014

The RSA Conference is the most comprehensive forum in information security for enterprise and technical professionals. We invite you to save the dates and participate in a variety of Cisco and Sourcefire activities, and learn how our products, solutions, and services help protect against threats across the attack continuum: before, during and after an attack.

Learn more or obtain a code to be our guest at the show by visiting our RSA Conference event site

Cisco Security Virtual Experience

For those just visiting the show, free expo-only passes are available for Cisco employees, partners, and customers with the registration pass code: SC4CXSCO. The deadline to register is Friday, February 21. Log in at https://ae.rsaconference.com/US14/portal/login.ww

Customer Story of the Month

Voice of the Customer: Navaho

The European services provider Navaho serves small and medium-sized enterprises, with Cisco helping it to bring the cloud to healthcare. Navaho uses the Cisco® Email Security Appliance, noting that Cisco ESA offers one of the best false-alarm ratios in the industry, helping to assure customers that they will receive only legitimate emails. The Cisco Web Security Appliance is also is offered, with Cloud Web Security scheduled to be offered in the future. Find the **Navaho** case study here.

Subscribe Now

Refer a Colleague to our Cisco Security Connections Newsletter

Get security trends, product updates, and solutions emailed to you monthly.

Subscribe Now

Social Media

Quick Links

Security Products and Solutions

Ask the Experts

Security Updates

Forrester Total Economic Impact Analysis for Cisco Identity Services Engine

Cisco Identity Services Engine (ISE) is a security policy management and control platform. It automates and simplifies access control and security compliance for wired, wireless, and VPN connectivity. Understand the business value of Cisco ISE: The Forrester analysis reveals a strong ROI.

Product Updates

New Cisco Secure Data Center Solution Design Guides

The Cisco Secure Data Center for the Enterprise portfolio of solutions provides design and implementation guidance for businesses that need the best protection available to address today's advanced security threats. The first-look design guide for Cisco Single Site Clustering with the Cisco TrustSec® solution connects key technologies, products, and associated architectures to bring application awareness to the data center fabric and network services. It provides:

- Simplified operations
- Increased high availability
- Enhanced security throughout the fabric
- Flexible scalability

Read the Cisco Secure Data Center for Enterprise and the Cisco Cyber Threat Defense for the Data Center Solution guides.

End-of-Life Announcement for Cisco ASA 7.2 Software

The Cisco ASA 5500 Series Adaptive Security Appliance Software Release 7.2 end-of-life announcement has been posted on Cisco.com.

See details

Cisco Cyber Threat Defense 1.1.1 (New Release)

New features of the Cisco Cyber Threat Defense Solution include:

- Integration with Cisco ISE 1.2
  - Syslog integration
  - Identity and device table verified to 210,000 active sessions
  - Up to 2000 authentications per second
- Enhanced support for Cisco ASA 8.4(5) and 9.1(2) NetFlow Secure Event Logging
- Cisco Catalyst® 3850 NetFlow validation
- Application-layer distributed denial of service (DDoS) detection
- User interface enhancements for identity attribution

See release notes.

Send questions to cyber-pm@cisco.com

Collateral and Resources

A Cisco Guide to Defending Against Distributed Denial of Service Attacks

This white paper provides a number of tools that can be part of a toolkit to help identify and mitigate potential DDoS attacks on a customer's network.

Read the white paper

Cisco Next-Generation Firewall (YouTube Video)

See how the Cisco ASA 5500-X Series Next-Generation Firewalls combine the enhanced visibility and control of a next-generation firewall with the protection of a stateful inspection firewall. Learn how to quickly deploy a full-service business network that is ready for next-generation threats.

View introductory video (3:44 min)

Updated Security Documentation

Cisco ASA 5500-X Next-Generation Firewall Data Sheet
Cisco ASA 5500-X Next-Generation Firewall Services FAQ
Cisco ASA 5500-X Next-Generation Firewall At-a-Glance
Cisco Prime Security Manager Data Sheet
Cisco Prime Security Manager FAQ

Latest Secure Mobility VODs

Secure Mobility in State and Local Government (2:23 min)
Secure Mobility in Higher Education (2:20 min)
Secure Mobility in K-12 Education (2:43 min)

Cisco on Cisco
End-to-End Security Policy Control

The Cisco Identity Services Engine is an integral part of end-to-end policy control and security compliance. Cisco IT validates rigorous identity and policy enforcement in its own wired and wireless networks.

Read article.

Case Studies

Managing Different Devices and Network Access Policy Safely

One of Europe's largest Cisco ISE deployments enables Kela to secure flexible working practices and simplify IT management.

Read the case study
View a one-slide summary
See the social media version promoted through SlideShare

New Security Video Case Study: Bucks County Intermediate Unit 22

The video case study for Bucks County Intermediate Unit 22 in Pennsylvania (Americas) is now available on Cisco.com. The organization supports technology services initiatives for 13 school districts, three public career and technical centers, and private schools. The IT team takes advantage of the power of Cisco ISE and Cisco AnyConnect® to manage increasing network demands and to provide users with highly secure network access and a trusted bring-your-own-device (BYOD) experience. Cisco TrustSec technology is in its future to better segment users, strengthening its security posture. Results include wired and wireless user authentication that is consolidated from separate district systems into a single source; highly secure access and an enhanced experience for all users regardless of device, supporting the BYOD policy; and a reduction in help desk tickets by 50 percent.

View the case study (4:50 min)

New Cloud Success Story in France

This case study includes several Cisco Content Security products. The Security team worked with the Enterprise Networks team on this project for Navaho, a French cloud computing provider. This customer uses the Cisco Web Security Appliance and Email Security Appliance and plans to use Cisco Cloud Web Security.

Read the case study.

Trinity University has deployed Cisco ISE to support its BYOD policy, along with Cisco ASA Next-Generation Firewalls and Cisco Web Security Appliance.

Read the case study.

Webinars and Training

An Ecosystem for Enhanced Network Security

The Cisco Identity Services Engine has changed the network security landscape. By combining Cisco ISE policy capabilities with security technologies from industry-leading partners, networks can more rapidly adapt to the changing world of mobility, BYOD, and persistent threats. Join us for a series of live webinars that showcase how Cisco and these partners are working to deliver unrivaled security solutions. Register now.

January 15: Replay AirWatch and mobile device management
January 29: Splunk and security information and event management

Recent Secure Access Webinars

How to See the Malware That Is Operating on Your Network
Cisco and MobileIron Enable Secure Use of Personal Mobile Devices

How to See the Malware That Is Operating Inside Your Network

Hear the value of integrating Cisco Secure Access technology with the Cisco ISE and Cisco TrustSec solutions combined with SIEM (security information and event management) from Lancope to accelerate the time to identify and remediate potential insider threats on your network or in your data center.

View Webinar Replay

News and Blogs

2014: A Look Ahead

John Stewart, senior vice president and chief security officer at Cisco, takes a look ahead at security trends in this recent post. "We've seen more and increasingly virulent attacks, continued 'innovation' by adversaries, and a minor revival of distributed denial of services (DDOS) actions perpetrated by hacktivists and other socio-politically motived actors."

Read the blog.
View the video (4:02 min)

Sourcefire in Our Data Center – the First Inline Production Deployment at Cisco

Blog post by John Stewart
More information on Sourcefire

Secure Access blog posts

Beware: Insider Threats Getting Worse
Education Embraces the Mobility Excitement
Access Control with Cisco TrustSec: Moving from "IP Addresses" to "Roles and Attributes"

Contact Us

Back to Top