Modern attacks and malware

Everything starts with an email and web

Dragan Novakovic
Cisco Systems
New Cyber Threat Reality

- Your environment will get breached
- You’ll most likely be infected via email
- Hackers will likely command and control your environment via web
Cisco Email Security Solutions
Email is still the #1 threat vector
Phishing leaves businesses on the line

- Phishing
- Spoofing
- Ransomware

Messages contain attachments and URL’s

- 94% of phish mail has malicious attachments\(^1\)
- 30% of phishing messages are opened\(^1\)

Socially engendered messages are well crafted and specific

Credential “hooks” give criminals access to your systems

Loss incurred due to phishing attacks in a year by US companies\(^2\)

\(^{1}\)2016 Cisco Annual Security Report
\(^{2}\)2016 Verizon Data Breach Report, Kerbs on Security

$500M

\(\text{Loss incurred due to phishing attacks in a year by US companies}^{2}\)
Spoofing rates are on the rise

Forged addresses fool recipients
Threat actors extensively research targets
Money and sensitive information are targeted

Spoofing
Phishing
Ransomware

2015 2016

270% increase

$2.3B

In losses from spoofing 2013 - 2015

FBI Warns of Dramatic Increase in Business email scams, 2016
Ransomware attacks are holding companies hostage.

- **Phishing**
- **Spoofing**
- **Ransomware**

Malware encrypts critical files, locking you out of your own system, and extortion demands are made.

Ransomware represents the biggest jump in occurrences of crimeware. 

9,515 users are paying ransoms per month.

Cost to consumers and companies of a single campaign: $60M.
Cisco Email Security

Before
- Email Reputation
- Mail Flow Policies
- Acceptance Controls
- Anti-Spam Anti-Virus

During
- AMP
  - File Reputation
  - ThreatGrid
- Graymail Management
- Safe Unsubscribe

After
- AMP
  - File Sandboxing & Retrospection
- WIT
  - Tracking User click Activity (Anti-Phish)

Outbound Email
- Inbound Email
- Outbound Liability

Outbound Liability
- Mail Flow Policies
- Anti-Spam and Anti-Virus
- Data Loss Protection
- Encryption

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Gain security backed by the most advanced threat intelligence

- 100 TB Of Data Received Daily
- 1.5 MILLION Daily Malware Samples
- 600 BILLION Daily Email Messages
- 16 BILLION Daily Web Requests
- MILLIONS Of Telemetry Agents
- 4 Global Data Centers
- Over 100 Threat Intelligence Partners
- 250+ Full Time Threat Intel Researchers

Global scanning 30 years building the world’s networks
Detect threats embedded in email content

Optimize detection with machine and human intelligence

Stop more than 99% of Spam

Keep good emails flowing with a < 1 in 1M false-positive rate
Guard against malicious attachments

Track email behavior with over 560 indicators
Quickly neutralize threats with Zero Hour Malware Protection
Continuously track files with retrospective security

Anti virus  File reputation  Advanced sandboxing  Retrospective alerting  Auto remediation for Office 365  Virus outbreak filters

Advanced Malware Protection (AMP)
Reduce the hassle of compliance

Protect intellectual property
• DLP prevents confidential information from leaving your network
• Ensure compliance with industry and government regulations
• RSA and Digital Guardian partnership

Enable users to do business
Encryption ensures your email is confidential with complete control as the sender
• Send confidential mail
• Read receipts
• Recall ability
• Secure reply and forwarding
• ZIX or CRES or S/MIME or TLS
Move to the cloud with confidence

Maintain peak performance with capacity assurance

- Ensure performance with continuous monitoring of system health
- Count on the stability and relatability of a strong tier one infrastructure
- Add capacity easily as message volumes increase

Avoid downtime with 99.999 availability

- Enjoy the highest levels of service availability with dedicated cloud infrastructure
- Receive dedicated IPs and storage
- Prevent shared-fate with compute instances
Expand with security that grows with you

Grow in the cloud
- Increase dedicated instances up to 50% of the originally sized environment at no cost

Expand geographically
- Utilize Cisco’s data center footprint as you grow into new regions

Gain full admin access
- Maintain full admin level access to your appliances at all times
- Easily orchestrate changes or access reports
Optimize security resources to focus on business outcomes

Keep consistent policy as you shift to cloud email

Reduce investigations and response times

Identify trends with scheduled and ad-hoc reporting
AsyncOS 10.0 – Feature rich release

- Forged Email Detection
- AMP Private Cloud
- Improved AMP Reporting
- Language Detection & Filter Actions
- SAML Authentication
- Malware Auto-Remediation for Office 365 Customers
- URL Logging & Message Tracking

Cisco Email Security
AsyncOS 10.0
Think Before You Click

Final version of the report

Joseph Tribbiani <joseph.tribbiani@nagts.org>
Tuesday, November 8, 2016 at 12:59 PM
To: Dragan Novakovic (dnovakov)

: Report02_FINAL.doc (15.9 KB) Preview

Dear Dragan,

Alisha Calderon asked me to send you the attached document, which contains the final version of the report.
Please let me know if you have any trouble with the file, and please let Alisha know if you have any questions about the contents of the report.

Kind regards,

Joseph Gibson
Program Mgr, Operations
This is an approved phishing test delivered by the Cisco Information Security team.

You just opened an attachment in a test phishing e-mail. If this was not a test, your action may have exposed Cisco to risk of malware or data compromise. The following signs should have alerted you that this was a phishing email:

- Unknown Sender - unexpected external message, sender does not match name at bottom of e-mail
- Unexpected attachment - unsolicited e-mails with attachments are a common sign of phishing

This phishing sample is based on a real phishing e-mail used to deliver the Locky ransomware and JSDropper malware.

The good news is this - it was just a test. Please visit our Phishing Awareness site, http://phishing.cisco.com, to validate this test, learn about the various types of phishing attacks, and understand how to handle them.

Please send questions or comments about this training program to infosec-phishing-feedback@cisco.com.

What is ransomware?

Ransomware is a type of malicious code that, if executed on your system, usually through an attachment or link, will lock your system, encrypt the hard drive, and demand a payment in return for the key to unlock your files. You can protect yourself through the following steps:

1. Do not open unexpected attachments from unknown senders. Exercise caution.
2. Make sure your work and home computers are protected by antivirus software.
3. Enable pop-up blockers.
4. Backup your systems regularly

Some phishing attacks simply need you to click a link in order to launch an exploit against your web browser, infecting your computer with viruses and malware.

We have seen successful phishing attempts against CEOs of Fortune 500 companies, security professionals, IT administrators, customer service representatives, and accountants alike.

Every user will be targeted at some point.
With Cisco email security, you can...

Reduce exposure with advanced threat protection

Support growth with availability and assurance

Achieve agility through operational efficiency
Cisco Web Security Solutions
Cisco Web Security Protects the Web Vector While Supporting Your Business

- Comprehensive Defense
- Advanced Threat Protection
- Superior Flexibility

Cisco Web Security Appliance (WSA)
Cisco Cloud Web Security (CWS)
It Starts with Usage Control and Active Defense

- **Web Filtering**: Block over 50 million known malicious sites
- **Web Reputation**: Restrict access to sites based on assigned reputation score
- **Dynamic Content Analysis**: Categorize webpage content and block sites automatically
- **Outbreak Intelligence**: Identify unknown malware and zero-hour outbreaks in real time
- **Application Visibility and Control**: Regulate access to website components and apps
- **DLP Integration**: Prevent confidential information from leaving your network
- **Time and Bandwidth Quotas**: Set controls for users in terms of time on social media sites as well as bandwidth usage
- **Roaming User Protection**: Protect users while away from the corporate network

Available only on WSA/WSAv
Available only on CWS
Extending Protection Beyond the Network

Key Benefits

- Save network bandwidth
- Improve user experience
- Defend against malware
- Protect your investment

Diagram:
- WSA
- HQ
- Remote Sites
- WAN
- VPN
- Mobile User
- CWS Browser
- WWW
- Roaming User

Text:
- Protect your investment
And Extending User Identity and Context

ISE Integration

- Acquires important context and identity from the network
- Monitors and provides visibility into unauthorized access
- Provides differentiated access to the network
- Cisco TrustSec® provides segmentation throughout the network
- Cisco Web Security Appliance provides web security and policy enforcement

Available only on WSA
Cisco Web Security Combats Evolving Threats

Cisco Advanced Malware Protection (AMP)

File Reputation
Increase the accuracy of threat detection by examining every aspect of a file

File Sandboxing
Determine the malicious intent of a file before it enters the network

File Retrospection
Identify a breach faster by tracking a file’s disposition over time
Updating Security to Meet Tomorrow’s Challenges

Security Intelligence and Research Group

- Get industry-specific threat intelligence tailored to your business
- Catch advanced threats endpoints miss with Cisco’s reverse engineers and threat analysts
- Stay protected against the latest threats with regular updates pushed automatically

Talos

Threat Intelligence

Research Response

Industry-leading research

600+ Researchers

Multi-tiered defense

Web
Network
Endpoint
Virtual
Cloud
Email
Identifying Unnamed Threats and Breaches

Continuous Capabilities with Cisco® Cognitive Threat Analytics (CTA)

- **Anomaly Detection**: Detect infections faster by automatically scanning for symptoms of an attack.
- **Behavioral Analysis**: Identify unknown breaches by analyzing a user’s behavior over time.
- **Machine Learning**: Automatically learn and adapt to threats with big-data algorithms.
With Unified Reporting and Policy Management

Unified Reporting

Roaming User

HQ

Web Security Reporting Application

Unified Policies

Roaming User

HQ

Cloud Web Security Graphical User Interface
And Work with Your Existing Environment

CWS Traffic Redirectors

WSA Models

Physical Appliance
- Perfect for small business branches: WSA-S190
- Perfect for mid-size offices: WSA-S390
- Perfect for large enterprises: WSA-S690

Virtual Appliance (WSAv)
Respond instantly to traffic spikes and eliminate capacity planning by never shipping or installing a physical appliance

*GRE over IPsec

Perfect for mid-size offices:
WSA-S390

Perfect for small business branches:
WSA-S190

Perfect for large enterprises:
WSA-S690

*GRE over IPsec

© 2015 Cisco and/or its affiliates. All rights reserved.
Only Cisco Offers Web Security with Advanced Threat Protection

- Comprehensive Defense
- Advanced Threat Protection
- Superior Flexibility
Thank you