



# Cisco Email Security

Industry-Leading Protection  
Across the Attack Continuum

Manfred Zhu  
TAC Engineer

Jun 2015



# The Way We Use Email Is Changing

## Making It More Difficult To Protect Your Network



Mobile



Coffee shop



Corporate



Home



Airport

# The Reality

## Organizations Are Under Attack



of large companies  
targeted by malicious traffic

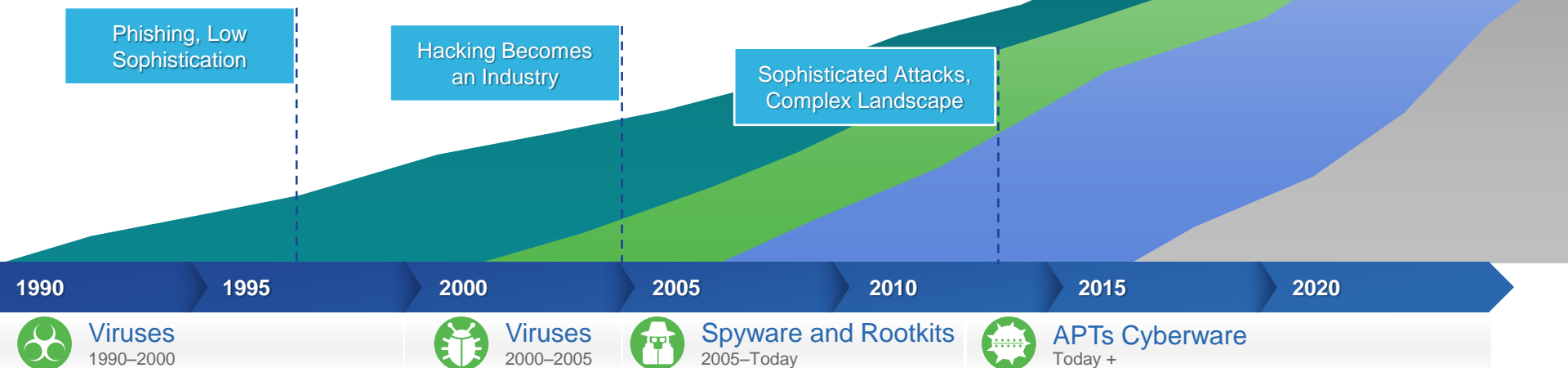
95%



of organizations interacted  
with websites hosting malware

100%

- Cybercrime is lucrative, barrier to entry is low
- Hackers are smarter and have the resources to compromise your organization
- Malware is more sophisticated
- Organizations face tens of thousands of new malware samples per hour



# High-Availability Email Protection with Cisco Email Security Appliance

## Featured Benefits

- Threat-focus
- High Performance
- Continuous innovation



[www.cisco.com/go/esa](http://www.cisco.com/go/esa)

# Cisco Email Security Benefits

## Threat-focus



- Layered defense built-into single appliance
- Multiple anti-spam engines, Email and Web Reputation, Multiple AV-Scanners, and Outbreak Filters
- Exceptional threat identification infrastructure using Cisco's Talos Research Group
- Zero-day and blended threat protection
- Advanced Malware Protection

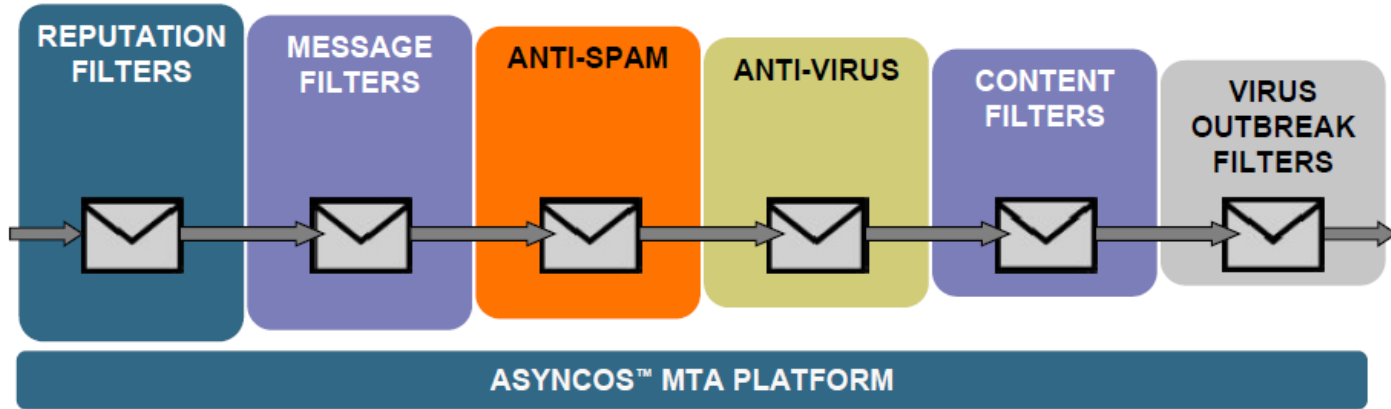


“ With Cisco, a substantial reduction in total cost of ownership and the new features to battle viruses and spam [are] a reality. ”

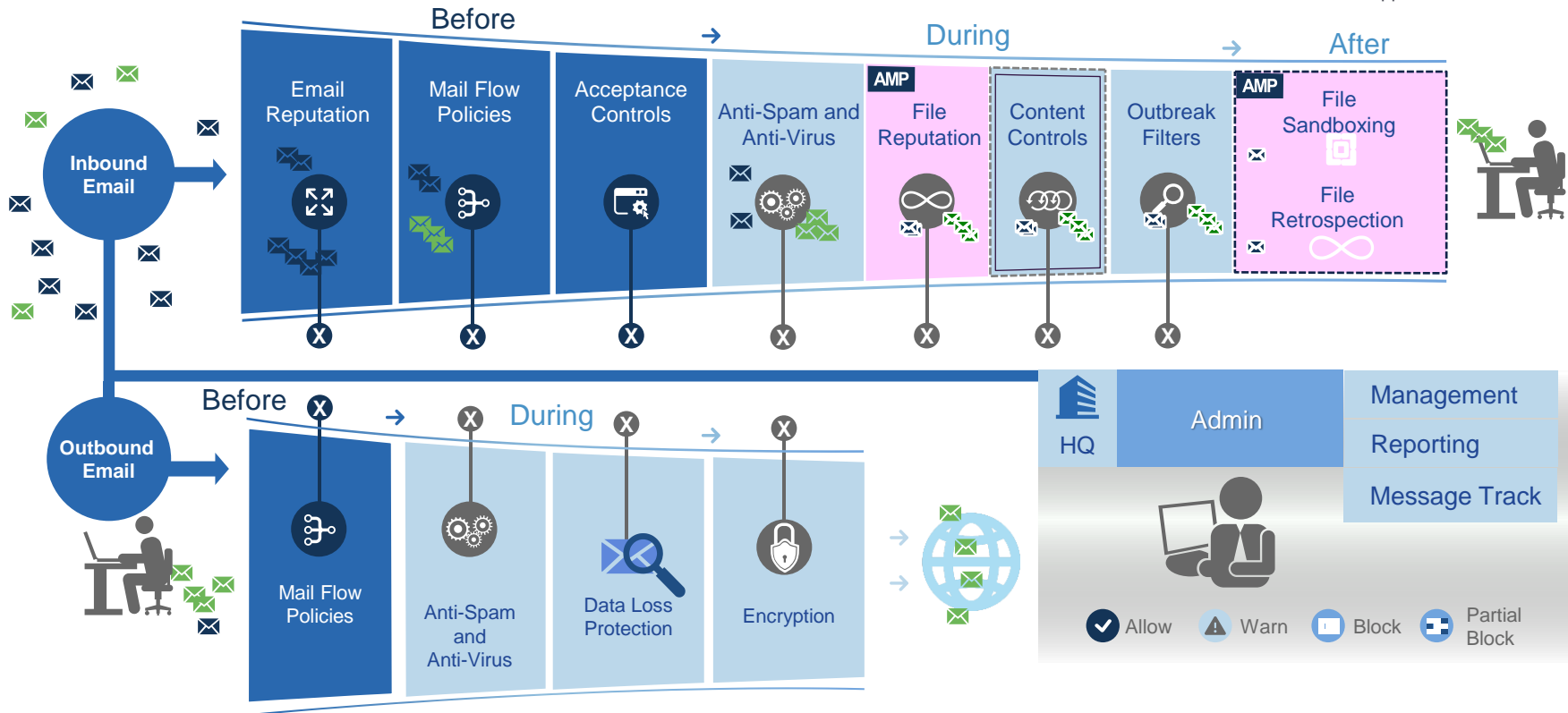
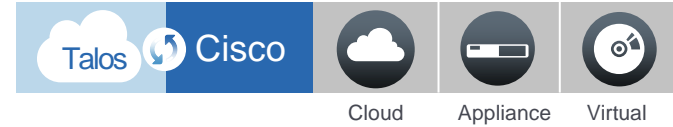
Kenichi Tabata  
Komatsu. Ltd. Japan

# Cisco Email Security

A Reminder Of Those Good Old Days...

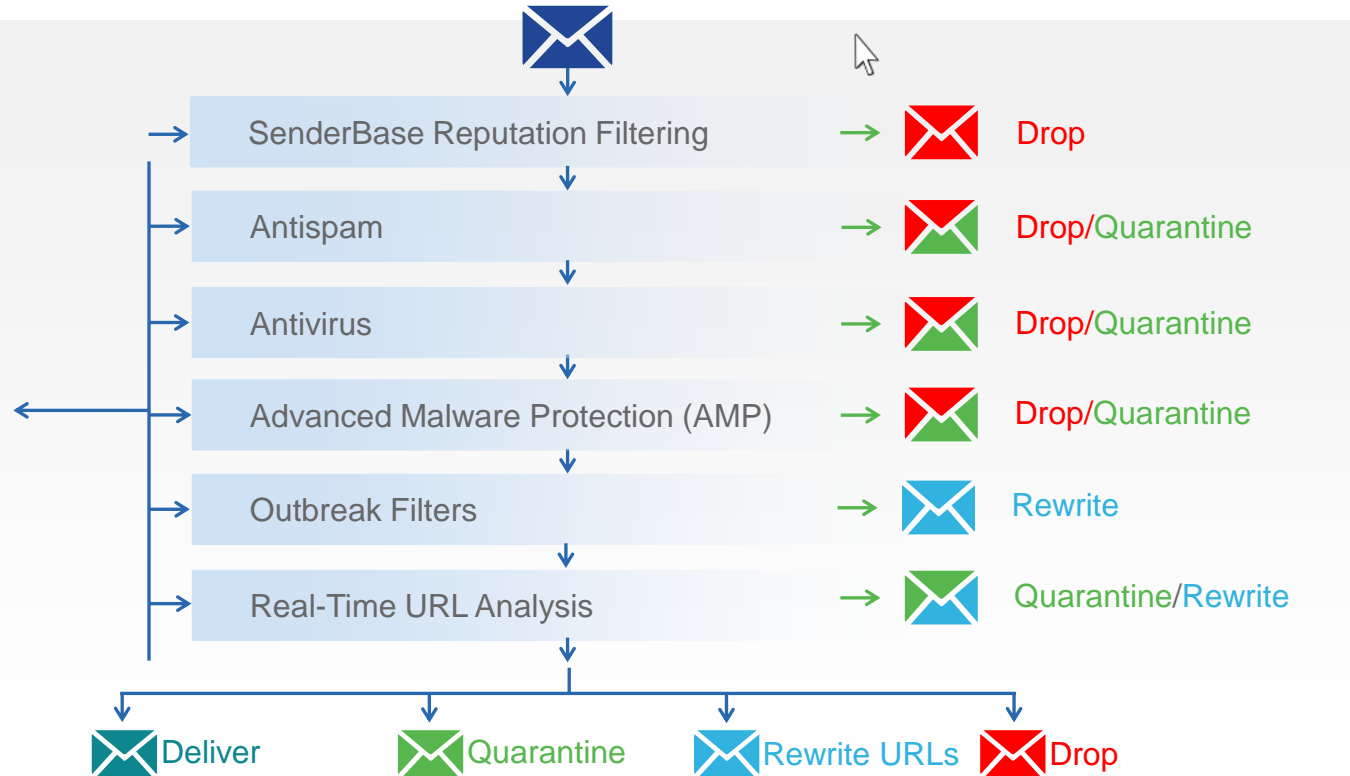


# Cisco Email Security



# Cisco Email Security Threat Defense

## Complete Inbound Protection







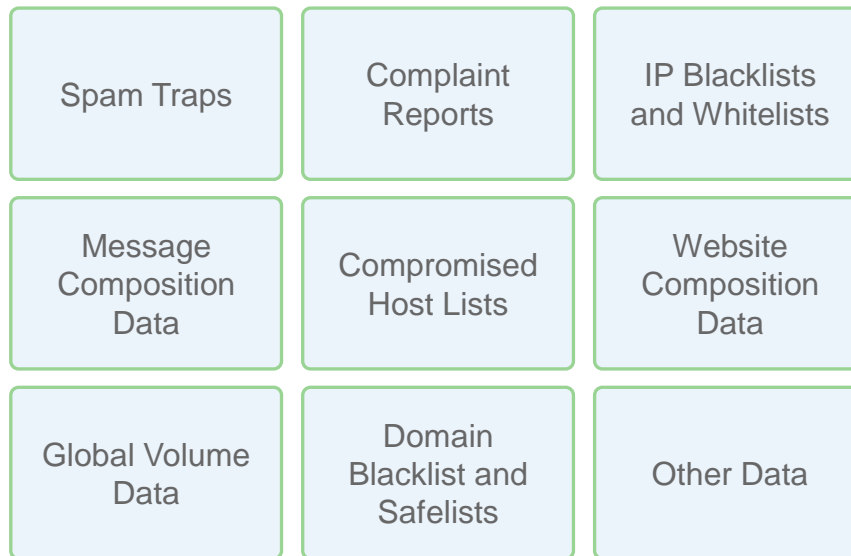
# Cisco Email Reputation Database

## Threat Intelligence

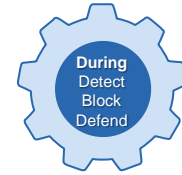
- Over 1.6 million global devices
- Historical library of 40,000 threats
- 35% of global email traffic seen per day
- 13 billion+ worldwide web requests seen per day
- 200+ parameters tracked

## Benefits

- 360-degree dynamic threat visibility
- Understanding of vulnerabilities and exploit technologies
- Visibility into highest threat vehicles
- Latest attack trends and techniques



# www.senderbase.org



## SenderBase

The world's largest Email and Web traffic monitoring network

Search IP, domain or a

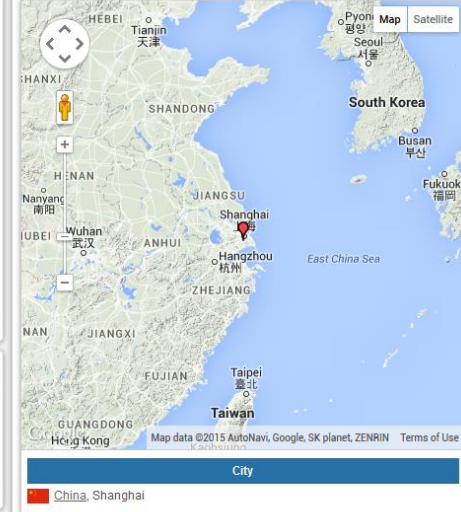
### Email Overview



### Details

IP Address	223.166.86.41	
Fwd/Rev DNS Match	?	
Email Reputation	Poor	
Web Reputation	Neutral	
	Last Day	Last Month
Email Volume	0.0	0.0
Volume Change	0%	
Hostname		
Domain	?	
Network Owner	CHINA UNICOM Shanghai network	

### Location Data



### Blacklists

bl.spamcop.net	Not Listed
cbl.abuseat.org	Not Listed
pbl.spamhaus.org	Listed
sbl.spamhaus.org	Not Listed

### IP Addresses

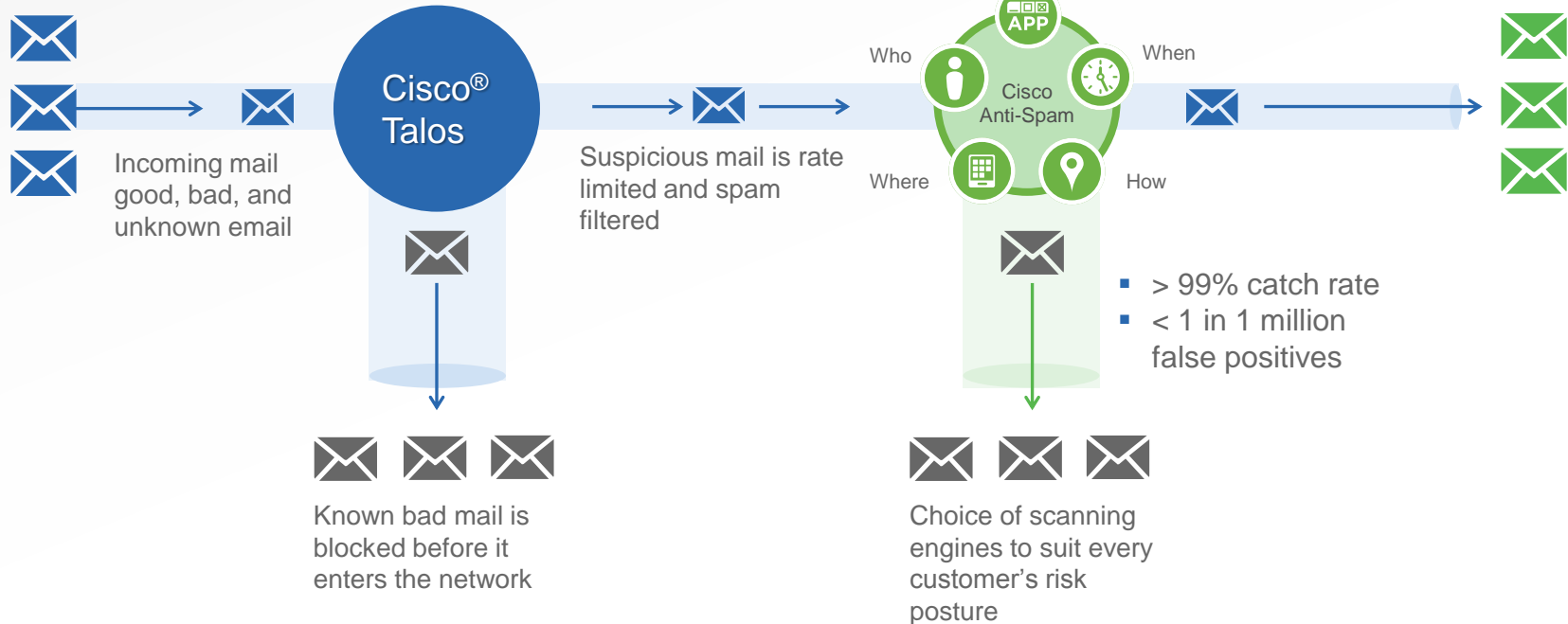
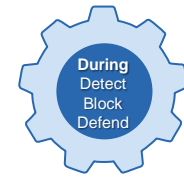
Whois

Email Volume History

Top IP addresses used to send emails in 223.166.86.41 /24

No IP addresses found.

# Anti-Spam Defense in Depth



# Missed Spam Analysis

Sender Type	Nov 2013	Apr 2014
Other sender	53%	46%
Marketing sender	38%	37%
Snowshoe sender	7%	15%
Freemail sender	2%	2%



- Offer spam (Micro-category) = [Sell goods or services](#).
- Majority of Offer spam uses Snowshoe techniques
- Snowshoe spam – technique used by spammers to cover their tracks, go under the radar. Its objective is to defeat traditional Anti-Spam techniques.
- Short campaigns – morphs fast – constantly changing

## Anti-Sender Reputation

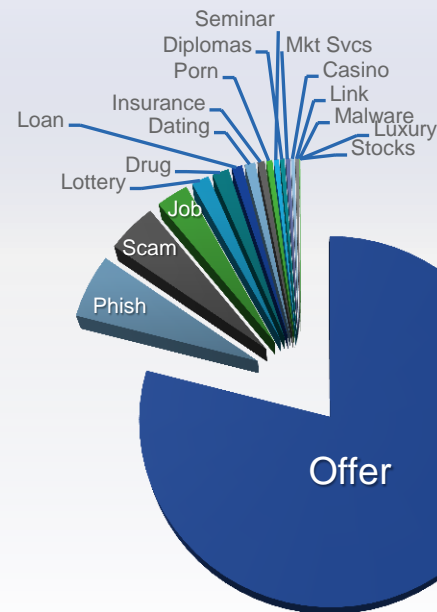
- Never use the same IP to send more than x amount of spam in more than y period of time.
- Never send the same spam from the same IP.

## Anti-Content Analysis

- Never use the same series of words
- Never reuse the same images
- Never use the same URL

- Not “new” techniques, however, usage has increased
- Fine line to balance catch rate and false positive

## Categories of Missed Spam (Customer submissions since Jan/14)



# What does a typical snowshoe campaign look like?

Received: from mta191fr.dim425.com ([5.135.21.191]) by [trap server]  
with ESMTP (betamax) id x; Tue, 20 May 2014 12:16:26 +0000  
To: [trap recipient]

## Query bl.spamcop.net - 5.135.21.191

5.135.21.191 = mta191fr.dim425.com

Lookup another:

[\(Help\)](#) [\(Trace IP\)](#) [\(SenderBase Lookup\)](#) [\(Report history\)](#)

5.135.21.191 not listed in bl.spamcop.net

**Rationale:** Spam score 0.00000: spam report ratio (0.00000) falls under threshold (0.00020)

[More details..](#)

1 different users have identified this as a spam source.

5.135.21.191	Qty		Most Recent	Oldest
<b>5.135.21/24 (Updated daily)</b>	<b>Total</b>	<b>Hosts</b>	<b>Most Recent</b>	<b>Oldest</b>
Sample traffic:	216	159	11 hours ago	39.4 days ago
Trap recipients:	15	15	7 hours ago	7.4 days ago
Spam reports:	9	8	7 hours ago	7.4 days ago

Other hosts in this block with spam reports:

[5.135.21.37 \(1\)](#) [5.135.21.121 \(1\)](#) [5.135.21.130 \(1\)](#) [5.135.21.133 \(1\)](#) [5.135.21.141 \(3\)](#) [5.135.21.145 \(1\)](#)  
[5.135.21.147 \(3\)](#) [5.135.21.151 \(1\)](#) [5.135.21.155 \(1\)](#) [5.135.21.156 \(1\)](#) [5.135.21.157 \(1\)](#) [5.135.21.159 \(1\)](#)  
[5.135.21.160 \(1\)](#) [5.135.21.174 \(1\)](#) [5.135.21.181 \(1\)](#) [5.135.21.202 \(1\)](#) [5.135.21.217 \(1\)](#) [5.135.21.232 \(1\)](#)  
[5.135.21.233 \(1\)](#) [5.135.21.236 \(1\)](#) [5.135.21.238 \(1\)](#)

- Low IP complaint rate
- Spread out spam load
- Not listed in RBL

# What does a typical snowshoe campaign look like?

**Date:** Fri Aug 15 07:42:39 2014  
**From:** Gayle %%EOF <[REDACTED]>  
**To:** <[REDACTED]>  
**Subject:** invoice 2727917.pdf  
**Attachments:** invoice\_2727917.pdf (application/pdf) [13.5928 KB]

**Unfiltered**

ASCII [us-ascii]

- From header varies
- Misspelling “invoice” in subject
- Attachment name varies
- Very sample content
- Malicious PDF attachment

This email contains an invoice file attachment

# Anti-Snowshoe - CASE 3.4.1-001

## Steps to Take in Battling Spam

“Maintain leadership in anti-spam efficacy through ever-changing threat landscape to protect our customers and keep ahead of the competition”

- Sensor footprint expansion for early awareness of snowshoe campaigns
- Increase automation and auto-classification of emails for faster response
- Better defense against Snowshoe spam through enhanced Contextual analysis





Antivirus

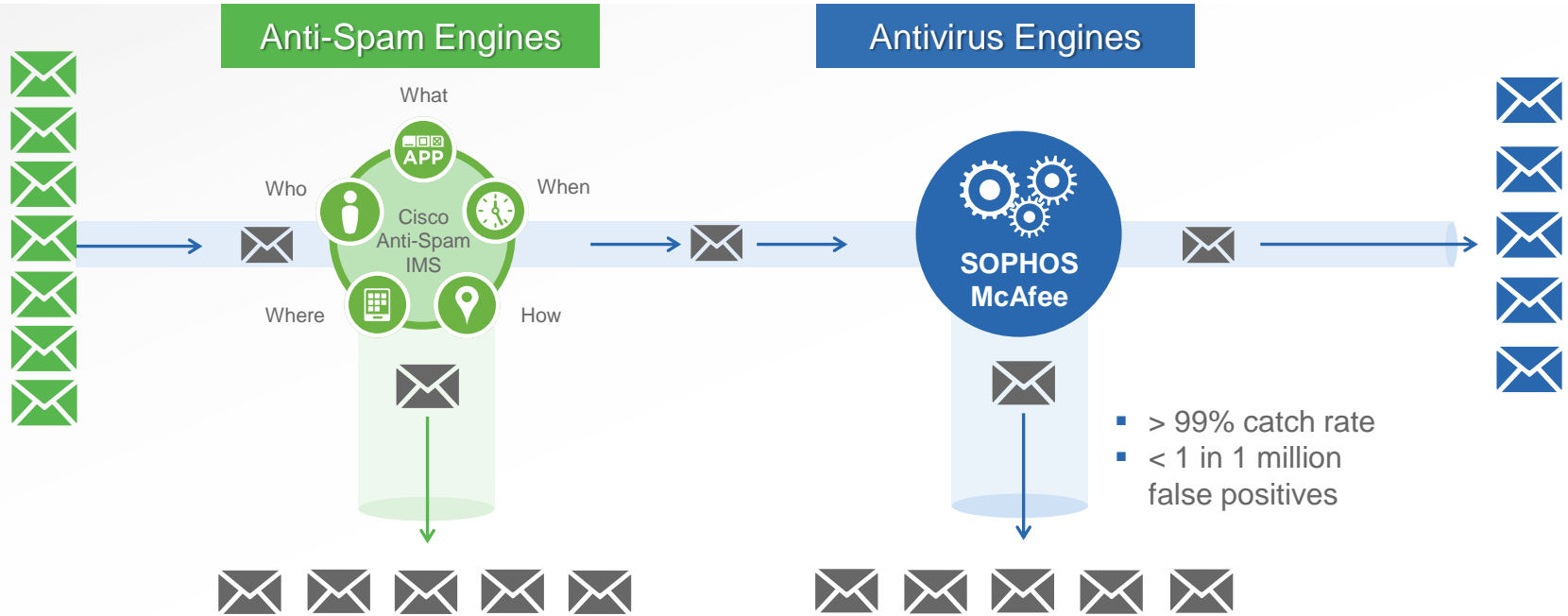
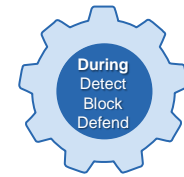
&

Advanced Malware Protection





# Antivirus Defense in Depth



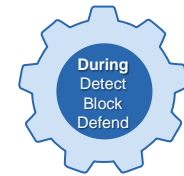
- > 99% catch rate
- < 1 in 1 million false positives

## Choice of Antivirus Engines

- Sophos
- McAfee

# Antivirus Defense in Depth

www.virustotal.com



🔄 Your file is being analysed.

SHA256: 238aa84035808e228c2cb781f226aa603bec09ebc48cc4aa07e9d28788170

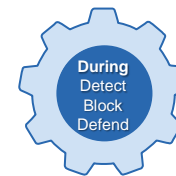
File name: invoice9313758.zip

Detection ratio: 42 / 53

Analysis | Additional information | Comments | Votes

Antivirus	Result	Update
ALYac	Trojan.Cutwall.Aj	20150619
AVG	FakeAlert	20150619
AVware	Win32.Malware/Drop	20150619
Ad-Aware	Trojan.Upatre.AC	20150619
Agnitum	Trojan.DL.Upatre!	20150618
Antiy-AVL	Trojan[Downloader]/Win32.Upatre	20150618
Arcabit	Trojan.Upatre.AC	20150619
Avast	Win32.Malware-gen	20150619
Axira	TR/Crypt.Xpack.166937	20150618
Baidu-International	Trojan.Win32.Upatre.vlv	20150618
BitDefender	Trojan.Upatre.AC	20150619
CAT-QuickHeal	Trojan/Dwindr.Upatre.MUE.A5	20150618

# Advanced Malware Detection on Email



发件人: Sales <martinadetey@kksecurity.com> 发送时间: 2015/5/14  
收件人: Recipients  
抄送:  
主题: Re: Outstanding Payment  
附件: COPIES98762.rar

Dear Sir/Madam,  
Pls find attached Outstanding list with payment  
Kindly do the needful ASAP  
Zhou

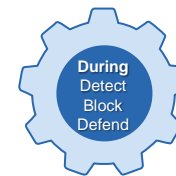
发件人: Accounts <roland-schacke@t-online.de> 发送时间: 2015/5/19  
收件人: Accounts  
抄送:  
主题: Re: Revised invoice  
附件: SWIFT- MT103.rar

Dear Sir/Madam,  
Pls find attached revised invoice w  
Kindly confirm the same ASAP  
Brian  
Finance Manager

发件人: Zhou <BSchram383@t-online.de> 发送时间: 2015/5/15  
收件人: Accounts  
抄送:  
主题: Re: Payment copy  
附件: Details983642.rar ATT00001.bin

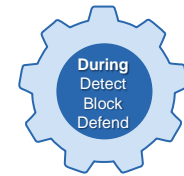
Payment copy  
Thanks  
Zhou

# Advanced Malware Detection on Email



AVScan	✔	20150619
AVScan2	✔	20150619
AVScan3	✔	20150619
AVScan4	✔	20150619
AVScan5	✔	20150618
AVScan6	✔	20150618
AVScan7	✔	20150618
AVScan8	✔	20150619
AVScan9	✔	20150618
AVScan10	✔	20150618
AVScan11	✔	20150619
AVScan12	✔	20150618
AVScan13	✔	20150619
AVScan14	✔	20150619
AVScan15	✔	20150619
AVScan16	✔	20150619
AVScan17	✔	20150619
AVScan18	✔	20150618
AVScan19	⊙	20150618
AVScan20	✔	20150619
AVScan21	⊙	20150618

# Cisco AMP Delivers Integrated...



## File Reputation

- Blocks known and unknown files
- Reputation verdicts delivered by AMP cloud intelligence network

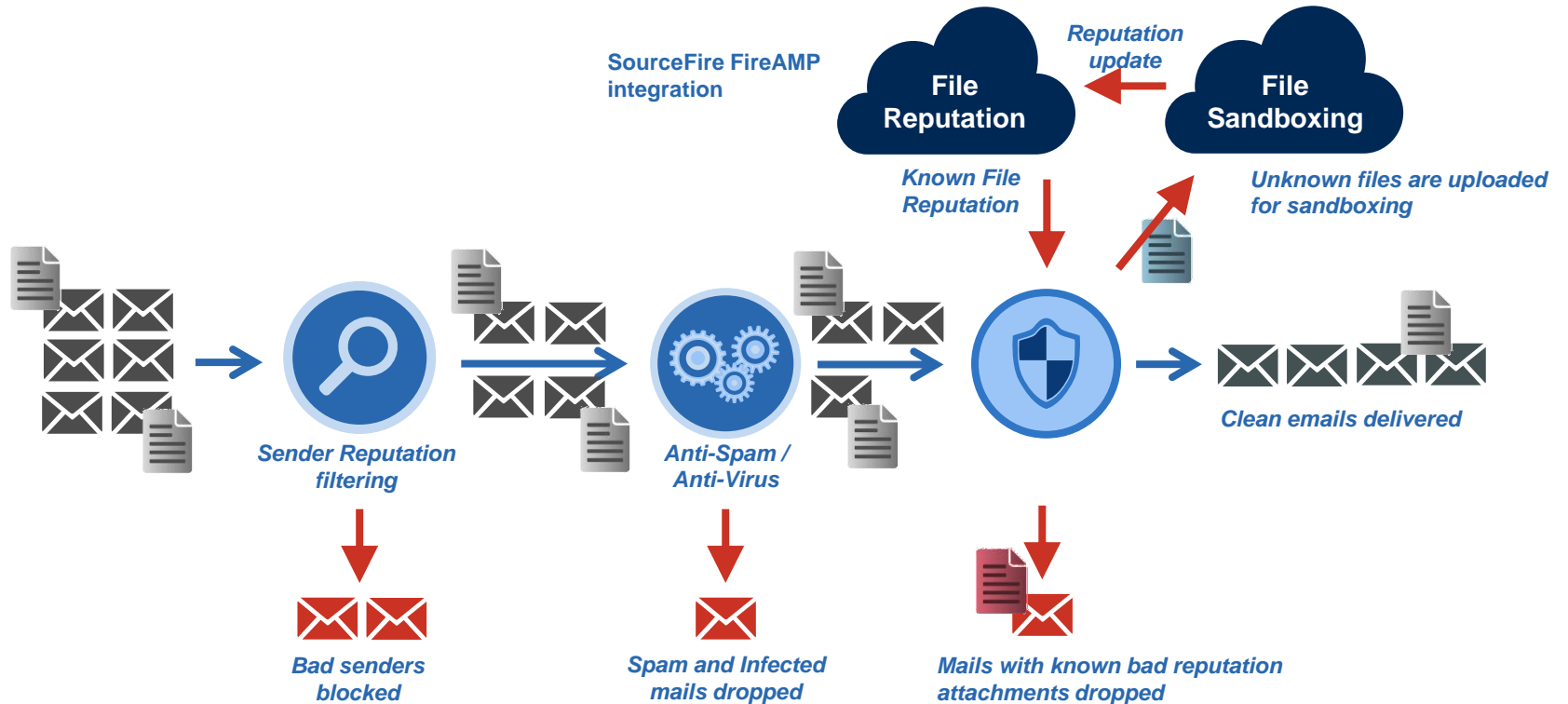
## File Sandboxing

- Behavioral analysis of unknown files
- Looks for suspicious behavior
- Feeds intelligence back to AMP cloud


## File Retrospection

- Continuous analysis of files that have traversed the gateway
- Retrospective alerting after an attack when file is determined to be malicious

# Advanced Malware Detection on Email



# Cisco AMP File Analysis Quarantine

Quarantine Name	Type	Messages	Default Action	Last Message Quarantined On	Size	Delete
File Analysis	Advanced Malware Protection	0	Retain 1 hour then Release	N/A	0	
Outbreak	Outbreak	0	Retention Varies Action: Release	N/A	0	
Policy	Policy	0	Retain 10 days then Delete	N/A	0	
Unclassified	Unclassified	0	Retain 30 days then Release	N/A	0	
Virus	Antivirus	0	Retain 30 days then Delete	N/A	0	

- Quarantine to store potential malware under investigation in sandbox
- System quarantine with standard functions
  - Release, Delete, Send Copy, and Delay scheduled exit
- Autorelease and rescan the message when file analysis is complete

# Advanced Malware Detection on Email

## Monitor >> File Analysis

Time Range: 90 days

17 Mar 2015 00:00 to 15 Jun 2015 13:36 (GMT +08:00) Data in time range:97.02 % complete

Completed Analysis Requests from This Appliance

Items Displayed 10

Displaying 1 - 10 of 15 items. << Previous | 1 | 2 | Next >>

File SHA256	Time of Analysis Request	Time Analysis Completed	Disposition
5e5eba2f...6b985f13	03 Jun 2015 10:01:32	03 Jun 2015 10:16:45	Clean
6a805619...caa79d1b	03 Jun 2015 10:01:31	03 Jun 2015 10:16:44	Clean
7a3db59e...172fc92f	03 Jun 2015 10:00:28	03 Jun 2015 10:13:08	Clean
9cd0ca08...04e89f52	03 Jun 2015 10:00:31	03 Jun 2015 10:12:18	Clean
187e0324...da1e7477	21 May 2015 17:12:07	21 May 2015 17:46:27	Malicious
01321ac7...80964b95	21 May 2015 17:12:03	21 May 2015 17:45:38	Malicious
34d4ffe1...d772f896	12 May 2015 15:45:23	12 May 2015 15:58:45	Malicious
102ea92e...79a68aee	12 May 2015 15:45:24	12 May 2015 15:58:13	Malicious
244e5dc0...065ed2ce	12 May 2015 15:44:21	12 May 2015 15:57:54	Malicious
160bab77...0c0b3145	12 May 2015 15:44:18	12 May 2015 15:57:28	Malicious

Displaying 1 - 10 of 15 items. << Previous | 1 | 2 | Next >>

Columns... | Export...

Pending Analysis Requests from This Appliance

No data was found in the selected time range



# Advanced Malware Detection on Email

## Monitor >> File Analysis

Time Range: 90 days		
17 Mar 2015 00:00 to 15 Jun 2015 13:36 (GMT +08:00)		
Completed Analysis Requests from This Appliance		
Displaying 1 - 10 of 15 items.		
File SHA256	Time of Analysis Request	Time Analysis Complete
5e5eba2f...6b985f13	03 Jun 2015 10:01:32	03 Jun 2015 10:16:45
6a805619...caa79d1b	03 Jun 2015 10:01:31	03 Jun 2015 10:16:44
7a3db59e...172fc92f	03 Jun 2015 10:00:28	03 Jun 2015 10:13:08
9cd0ca08...04e89f52	03 Jun 2015 10:00:31	03 Jun 2015 10:12:18
187e0324...da1e7477	21 May 2015 17:12:07	21 May 2015 17:46:27
01321ac7...80964b95	21 May 2015 17:12:03	21 May 2015 17:45:38
34d4fe1...d72f896	12 May 2015 15:45:23	12 May 2015 15:58:45
102ea92e...79a68aee	12 May 2015 15:45:24	12 May 2015 15:58:13
244e5dc0...065ed2ce	12 May 2015 15:44:21	12 May 2015 15:57:54
160bab77...0c0b3145	12 May 2015 15:44:18	12 May 2015 15:57:28
Displaying 1 - 10 of 15 items.		
Pending Analysis Requests from This Appliance		
No data was found in the selected time range		

General Information		
Analysis ID:	105702865	
Start time:	09:25:36Z	
Start date:	2015-05-21	
Number of analysed new started processes:	39	
Score:	100	
Status:	Complete	
Classification / Threat Score		
		Items Displayed 10
Factor	Score	Threat Level
AV Detection	1	Low
DDOS	30	Medium
Networking	52	High
Boot Survival	95	Very High
Stealing of Sensitive Information	1	Low
Persistence and Installation Behavior	100	Very High
Data Obfuscation	21	Low
Spreading	51	High
System Summary	69	High
HIPS / PFW / Operating System Protection Evasion	58	High
Export...		
Matching Signatures		
		Items Displayed 10
Signatures		
Scanner Search Results		
Too many similar processes found (Sandbox DDOS)		
Urls found in memory or binary data		
Downloads files from webservers via HTTP		
Found strings which match to known social media urls		
Performs DNS lookups		
Posts data to webserver		
Suspicious User Agent in HTTP Header		
Creates an undocumented autostart registry key		
Shows file infector / information gathering behavior (enumerates multiple directory for files)		



# Advanced Malware Detection on Email

The Info message is:

amp Retrospective verdict received. SHA256:  
6652aeacb5e59e2e5dd5837e7944898df3096f338d8b7675633a0d7a41296b99, Verdict:  
malicious, Reputation Score: 0, Spyname: W32.6652AEACB5-100.SBX.VIOC

amp Retrospective verdict received. SHA256:  
78aa7ffef517aaa1644a7f85d0f91a310e00ca14c44f337ce99e19ed166389d, Verdict:  
malicious, Reputation Score: 0, Spyname: W32.78AA7FFEEF-100.SBX.VIOC

amp Retrospective verdict received. SHA256:  
8bfa6a7569e3ab2a6a6d09e025a6ea3d1bb2678405ab2acc487e46c961358dba, Verdict:  
malicious, Reputation Score: 0, Spyname: W32.8BFA6A7569-100.SBX.VIOC

amp Retrospective verdict received. SHA256:  
9f04c068158482a09491f7ccd4856bfae4a27a989ee38aa5a0e968a22c080d43, Verdict:  
malicious, Reputation Score: 0, Spyname: W32.Variant:Reputation.17ik.1201

Version: 8.5.6-073

Serial Number: 4220BFA1592470FD9E87-507356929B60

Timestamp: 13 Jul 2014 04:11:48 -0500

# Advanced Malware Detection on Email

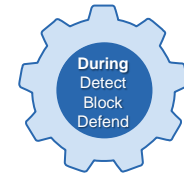
## Without AMP:

Thu May 21 17:01:44 2015 Info: MID 12831 interim AV verdict using McAfee **CLEAN**  
Thu May 21 17:01:44 2015 Info: MID 12831 interim AV verdict using Sophos **CLEAN**  
Thu May 21 17:01:44 2015 Info: MID 12831 antivirus negative  
Thu May 21 17:01:44 2015 Info: MID 12831 attachment 'SWIFT--20MT103.zip'  
Thu May 21 17:01:44 2015 Info: MID 12831 queued for delivery  
Thu May 21 17:01:44 2015 Info: Delivery start DCID 27904 MID 12831 to RID [0]  
Thu May 21 17:01:45 2015 Info: Message done DCID 27904 MID 12831 to RID [0]  
Thu May 21 17:01:45 2015 Info: MID 12831 RID [0] Response '2.6.0 <555D9EF4.6020400@iron.run > [InternalId=11] Queued mail for delivery'  
Thu May 21 17:01:45 2015 Info: Message finished MID 12831 done

## With AMP:

Thu May 21 17:16:43 2015 Info: MID 12832 interim AV verdict using McAfee CLEAN  
Thu May 21 17:16:43 2015 Info: MID 12832 interim AV verdict using Sophos CLEAN  
Thu May 21 17:16:43 2015 Info: MID 12832 antivirus negative  
Thu May 21 17:16:43 2015 Info: MID 12832 AMP file reputation verdict : **CLEAN**  
Thu May 21 17:16:44 2015 Info: MID 12832 attachment 'SWIFT--20MT103.zip'  
Thu May 21 17:16:44 2015 Info: MID 12832 quarantined to "File Analysis" (File Analysis Pending:file unknown)  
Thu May 21 17:16:44 2015 Info: Message finished MID 12832 done  
==  
Thu May 21 17:54:39 2015 Info: MID 12832 released from quarantine "File Analysis" (File Analysis completed) t=2275  
Thu May 21 17:54:39 2015 Info: MID 12832 released from all quarantines  
Thu May 21 17:54:39 2015 Info: MID 12832 matched all recipients for per-recipient policy manzhu in the inbound table  
Thu May 21 17:54:42 2015 Info: MID 12832 AMP file reputation verdict : **MALWARE**  
Thu May 21 17:54:42 2015 Info: Message aborted MID 12832 Dropped by amp  
Thu May 21 17:54:42 2015 Info: Message finished MID 12832 done

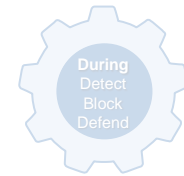
# Cisco AMP – License based



Description	Status	Time Remaining	Expiration Date
File Reputation	Active	258 days	28 Feb 2016 12:30 (GMT +08:00)
File Analysis	Active	258 days	28 Feb 2016 12:30 (GMT +08:00)

Existing customers with valid support contracts can evaluate the AMP feature by making a request to GLO at [licensing@cisco.com](mailto:licensing@cisco.com).

# AMP Provides Continuous Retrospective Security



## Breadth and Control Points



Email



Endpoints



Web



Network




IPS




Devices

## Telemetry Stream

➤  File fingerprint and metadata

➤  File and network I/O

➤  Process information

## Continuous Feed

```
1100001110001110 1001 1101 1110011 01100  
101 1110011 0110011 101000 0110 00 011100  
111010011101 1100001110001110 1001 1101
```



## Continuous Analysis



## Content & URL Filter



# Outstanding URL Defense

Many Ways of Protecting End Users from Malicious or Inappropriate Links

发件人: [redacted]  
收件人: [redacted]  
抄送: [redacted]  
主题: [redacted]

发送时间: 2015/5/20 (周三) 9:33

**OA系统通行证**

亲爱的OA通行证用户:  
您的帐号 [redacted] 近期发生了一次异常登录, 请核实以下详情:  
登录异常

登录时间	2015-5-20 9:33:02
登录地点	江苏省 (114.232.205.*)
登录产品	邮箱客户端(通过POP3/IMAP协议)

如非您本人操作, 请您立即验证您的帐户!

[验证帐户](#)  
OA通行证  
2015-5-20  
本电子邮件地址不能接受回复邮件。有关详情, 请访问 [OA通行证帮助中心](#)。

<http://xxx.xxx.xxx/urlProcess/urlProcessor.do?mailID=2111628803&urlID=176200&taskID=87988&mail=xxxxxxx%40qq.com&test=0&pa18url=http%3A%2F%2Foa-admin.sevnice.cn.com:82/mail%2F%3FAa1%3DAa201503271714110001%26mail%3Dxxxxxxxxx%40qq.com%26mt%3D1%26mp%3Dnull>

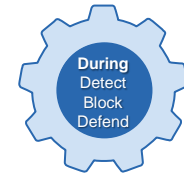


- From a good source, hacked email account
- Link to a famous insurance company site
- Use an unsafe function as a redirect service
- Finally redirect customer to a phishing site

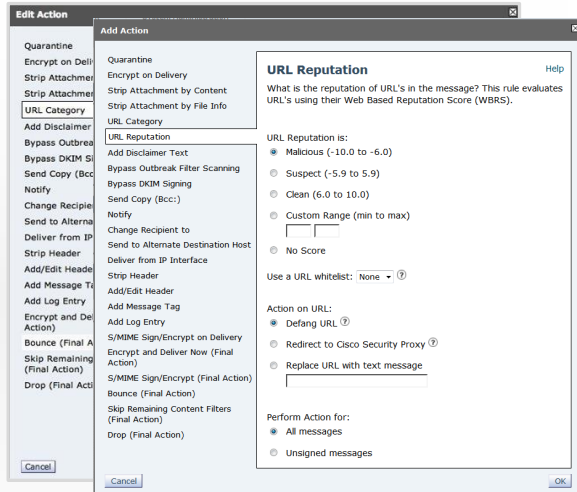


# Outstanding URL Defense

Many Ways of Protecting End Users from Malicious or Inappropriate Links



Email Contains URL  
Web Rep and/or Web Cat



URL  
Analysis

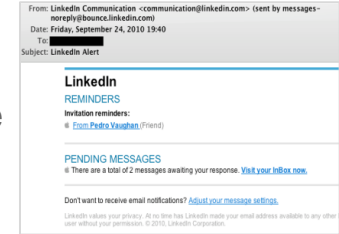


Send to Cloud

Rewrite

Defang

Replace



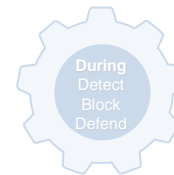
[BLOCKEDwww.playboy.comB](#)  
[LOCKED](#)  
[BLOCKEDwww.proxy.orgBLO](#)  
[CKED](#)

“This URL is blocked by policy”

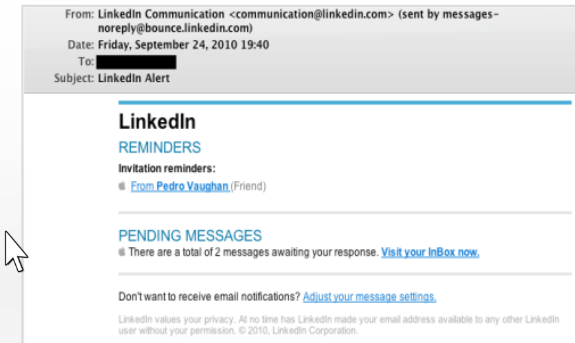
Automated with Outbreak Filters or Manual

# Outstanding URL Defense

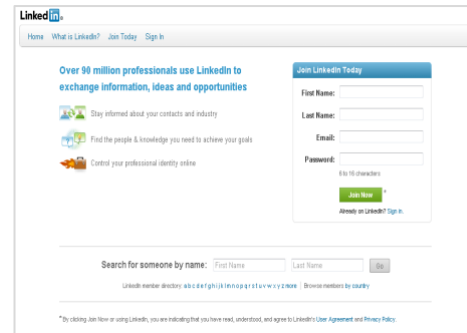
## Defend Against Blended Attacks



Link is clicked



Website is clean



Website is blocked

**Cisco Security**

**The requested web page has been blocked**

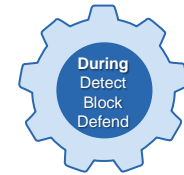
**http://www.threatlink.com**

Cisco Email and Web Security protects your organization's network from malicious software. Malware is designed to look like a legitimate email or website which accesses your computer, hides itself in your system, and damages files.

Dynamic, real-time inspection via HTTP

# Outstanding URL Defense

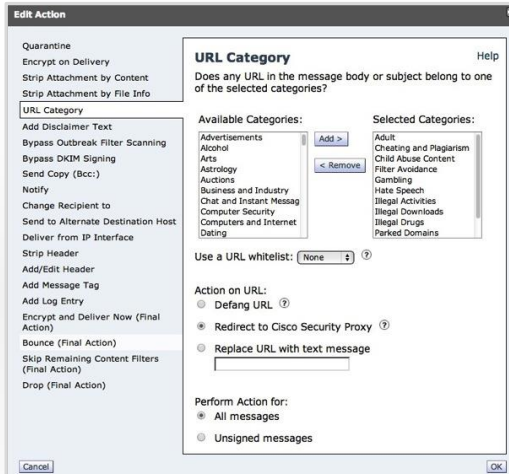
80 Category



Email Contains URL  
Web Rep and/or Web Cat

## 80 Categories

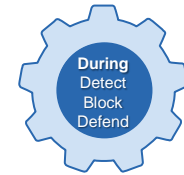
- Adult
- Advertisements
- Alcohol
- Arts
- Astrology
- Auctions
- Business and Industry
- Chat and Instant Messaging
- Cheating and Plagiarism
- Child Abuse Content
- Computer Security
- Computers and Internet
- Dating
- Digital Postcards
- Dining and Drinking
- Dynamic and Residential
- Education
- Entertainment
- Extreme
- Fashion
- File Transfer Services
- Filter Avoidance
- Finance
- Freeware and Shareware
- Gambling
- Games
- Government and Law
- Hacking
- Hate Speech
- Health and Nutrition
- Humor
- Illegal Activities
- Illegal Downloads
- Illegal Drugs
- Infrastructure and Content Delivery
- Networks
- Internet Telephony
- Job Search
- Lingerie and Swimsuits
- Lotteries
- Mobile Phones
- Nature
- News
- Non-Governmental Organizations
- Non-Sexual Nudity
- Online Communities
- Online Storage and Backup
- Online Trading
- Organizational Email
- Parked Domains
- Peer File Transfer
- Personal Sites
- Photo Searches and Images
- Politics
- Pornography
- Professional Networking
- Real Estate
- Reference
- Religion
- SaaS and B2B
- Safe for Kids
- Science and Technology
- Search Engines and Portals
- Sex Education
- Shopping
- Social Networking
- Social Science
- Society and Culture
- Software Updates
- Sports and Recreation
- Streaming Audio
- Streaming Video
- Tobacco
- Transportation
- Travel
- Unclassified
- Weapons
- Web Hosting
- Web Page Translation
- Web-Based Email



Automated with Outbreak Filters or Manual

# Outstanding URL Defense

Many Ways of Protecting End Users from Malicious or Inappropriate Links



Content Filter Settings	
Name:	URL_Filtering
Currently Used by Policies:	manzhu
Description:	
Order:	22 (of 32)

Conditions			
Add Condition...			Apply rule: If one or more conditions match
Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(-10.00, 10.00, "")	
2	Message Body	only-body-contains("验证", 1)	

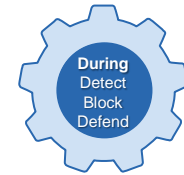
Actions			
Add Action...			
Order	Action	Rule	Delete
1	Quarantine	quarantine("BAD URL")	

Add Action	
<input type="checkbox"/> Quarantine	<b>URL Reputation</b> <a href="#">Help</a> What is the reputation of URL's in the message? This rule evaluates URL's using their Web Based Reputation Score (WBRS).  URL Reputation is: <input checked="" type="radio"/> Malicious (-10.0 to -6.0) <input type="radio"/> Suspect (-5.9 to 5.9) <input type="radio"/> Clean (6.0 to 10.0) <input type="radio"/> Custom Range (min to max) [ ] [ ] <input type="radio"/> No Score  Use a URL whitelist: None [?] [?]  Action on URL: <input checked="" type="radio"/> Defang URL [?] <input type="radio"/> Redirect to Cisco Security Proxy [?] <input type="radio"/> Replace URL with text message [ ]  Perform Action for: <input checked="" type="radio"/> All messages <input type="radio"/> Unsigned messages
<input type="checkbox"/> Encrypt on Delivery	
<input type="checkbox"/> Strip Attachment by Content	
<input type="checkbox"/> Strip Attachment by File Info	
<input type="checkbox"/> URL Category	
<input type="checkbox"/> URL Reputation	
<input type="checkbox"/> Add Disclaimer Text	
<input type="checkbox"/> Bypass Outbreak Filter Scanning	
<input type="checkbox"/> Bypass DKIM Signing	
<input type="checkbox"/> Send Copy (Bcc:)	
<input type="checkbox"/> Notify	
<input type="checkbox"/> Change Recipient to	
<input type="checkbox"/> Send to Alternate Destination Host	
<input type="checkbox"/> Deliver from IP Interface	
<input type="checkbox"/> Strip Header	
<input type="checkbox"/> Add/Edit Header	
<input type="checkbox"/> Add Message Tag	
<input type="checkbox"/> Add Log Entry	
<input type="checkbox"/> S/MIME Sign/Encrypt on Delivery	
<input type="checkbox"/> Encrypt and Deliver Now (Final Action)	
<input type="checkbox"/> S/MIME Sign/Encrypt (Final Action)	
<input type="checkbox"/> Bounce (Final Action)	
<input type="checkbox"/> Skip Remaining Content Filters (Final Action)	
<input type="checkbox"/> Drop (Final Action)	
<input type="button" value="Cancel"/>	<input type="button" value="OK"/>

Automated with Outbreak Filters or Manual

# Outstanding URL Defense

Many Ways of Protecting End Users from Malicious or Inappropriate Links

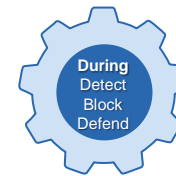


Wed Jun 17 16:44:31 2015 Info: New SMTP ICID 117 interface TEST (10.75.49.228) address 10.140.20.78 reverse dns host unknown verified no  
Wed Jun 17 16:44:31 2015 Info: ICID 117 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS rfc1918  
Wed Jun 17 16:44:31 2015 Info: Start MID 13063 ICID 117  
Wed Jun 17 16:44:31 2015 Info: MID 13063 ICID 117 From: <123@ironlab.com.cn>  
Wed Jun 17 16:44:31 2015 Info: MID 13063 ICID 117 RID 0 To: <manzhu@ironlab.com.cn>  
Wed Jun 17 16:44:31 2015 Info: MID 13063 using engine: SPF Verdict Cache using cached verdict  
Wed Jun 17 16:44:31 2015 Info: MID 13063 SPF: helo identity postmaster@[10.140.20.78] None  
Wed Jun 17 16:44:31 2015 Info: MID 13063 using engine: SPF Verdict Cache using cached verdict  
Wed Jun 17 16:44:31 2015 Info: MID 13063 SPF: mailfrom identity 123@ironlab.com.cn None  
Wed Jun 17 16:44:31 2015 Info: MID 13063 Message-ID '<5581338D.8040405@ironlab.com.cn>'  
Wed Jun 17 16:44:31 2015 Info: MID 13063 Subject 'malicious URL'  
Wed Jun 17 16:44:31 2015 Info: MID 13063 ready 742 bytes from <123@ironlab.com.cn>  
Wed Jun 17 16:44:31 2015 Info: MID 13063 matched all recipients for per-recipient policy manzhu in the inbound table  
Wed Jun 17 16:44:31 2015 Info: ICID 117 close  
Wed Jun 17 16:44:31 2015 Info: MID 13063 interim verdict using engine: CASE spam negative  
Wed Jun 17 16:44:31 2015 Info: MID 13063 using engine: CASE spam negative  
Wed Jun 17 16:44:31 2015 Info: MID 13063 interim AV verdict using Sophos CLEAN  
Wed Jun 17 16:44:31 2015 Info: MID 13063 antivirus negative  
Wed Jun 17 16:44:31 2015 Info: MID 13063 URL http://malware.testing.google.test/testing/malware/ has reputation -9.33 matched url-reputation-rule  
Wed Jun 17 16:44:31 2015 Info: MID 13063 quarantined to "BAD URL" (content filter:URL\_Filtering)  
Wed Jun 17 16:44:31 2015 Info: Message finished MID 13063 done

Automated with Outbreak Filters or Manual

# Outstanding URL Defense

Many Ways of Protecting End Users from Malicious or Inappropriate Links



## Messages in Quarantine: "BAD URL"

Messages in Quarantine: "BAD URL"				Message Details	
Action on selected items on page ▾ Release Delete More Actions...				Test for Viruses: <a href="#">Start Test</a>	
<input type="checkbox"/>	Sender ▲	Recipient	Subject	Received	Send Copy To: E-Mail Addresses, comma separated: <input type="text"/> <a href="#">Send</a>
<input type="checkbox"/>	123@ironlab.com.cn	manzhu@ironlab.com.cn	malicious URL	17 Jun 2015 16:44 (GMT +08:00)	Envelope Sender: 123@ironlab.com.cn
<input type="checkbox"/>	123@ironlab.com.cn	manzhu@ironlab.com.cn	It may trick victims	17 Jun 2015 16:42 (GMT +08:00)	Recipients: manzhu@ironlab.com.cn
<input type="checkbox"/>	123@ironlab.com.cn	manzhu@ironlab.com.cn	Fwd: http://tinyurl...	17 Jun 2015 16:41 (GMT +08:00)	Subject: malicious URL

Headers
Received-SPF: None (c170123.ironlab.com.cn: no sender authenticity information available from domain of 123@ironlab.com.cn) identity=mailfrom; client-ip=10.140.20.78; receiver=c170123.ironlab.com.cn; envelope-from="123@ironlab.com.cn"; x-sender="123@ironlab.com.cn"; x-conformance=spf_only
Received-SPF: None (c170123.ironlab.com.cn: no sender authenticity information available from domain of postmaster@[10.140.20.78]) identity=hello; client-ip=10.140.20.78; receiver=c170123.ironlab.com.cn; envelope-from="123@ironlab.com.cn"; x-sender="postmaster@[10.140.20.78]"; x-conformance=spf_only

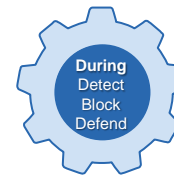
  

Message
<a href="http://malware.testing.google.test/testing/malware/">http://malware.testing.google.test/testing/malware/</a>

Automated with Outbreak Filters or Manual

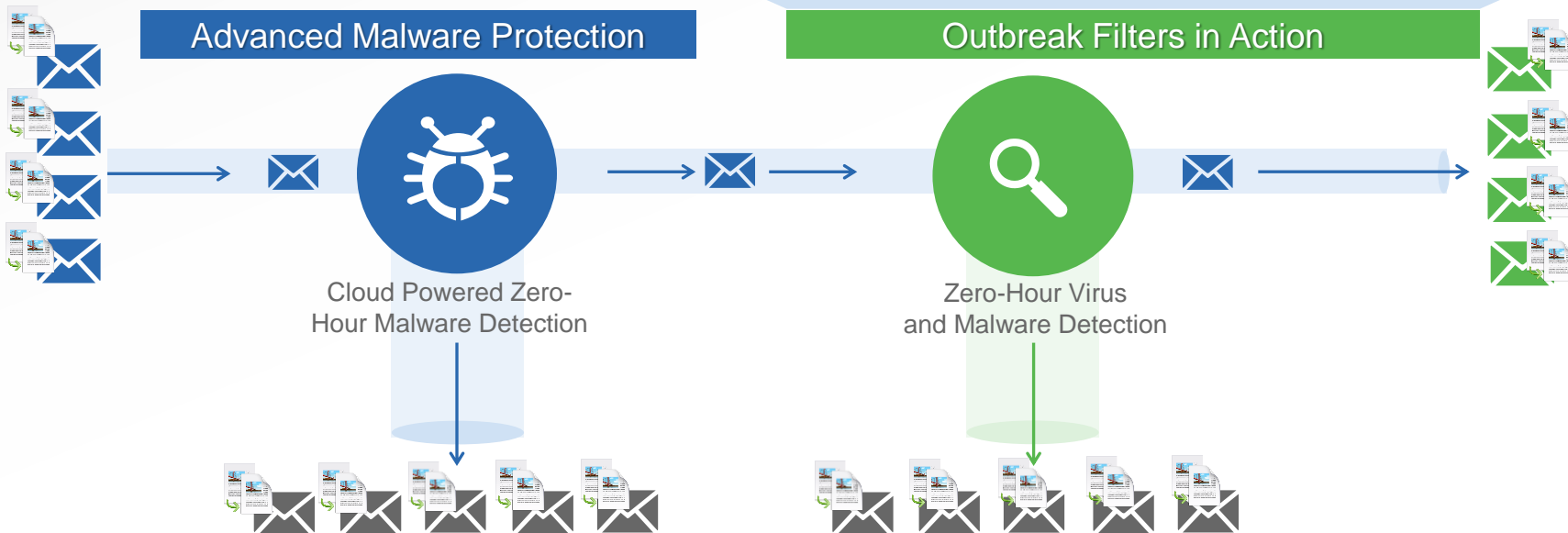
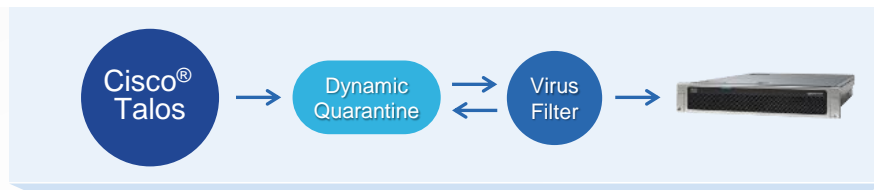
# Outbreak Filters

## Zero Hour URL and File Based Malware Protection



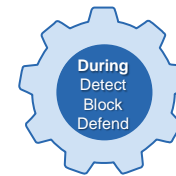
### Outbreak Filters Advantage

- Average lead time\*: Over 13 hours
- Outbreaks blocked\*: 291 outbreaks
- Total incremental protection\*: Over 157 days



# Outbreak Filters

## Zero Hour URL and File Based Malware Protection



Lead-times of Cisco's protection against the 20 most recent Malware outbreaks delivered via email.

Malware Name	Cisco	Sophos	McAfee	Trend Micro	Symantec
Mal/Generic-L	FIRST 2015/06/18 05:30 UTC	+0d 3h 0m	Not Published	Not Published	Not Published
Troj/Agent-ANXS	FIRST 2015/06/18 05:10 UTC	+0d 11h 25m	Not Published	+0d 12h 35m	Not Published
Troj/Limites-Z	FIRST 2015/06/18 03:40 UTC	+0d 12h 55m	Not Published	+0d 6h 0m	Not Published
Mal/Generic-L	FIRST 2015/06/18 02:15 UTC	+0d 14h 20m	Not Published	Not Published	Not Published
Troj/MSIL-DJA	FIRST 2015/06/18 00:42 UTC	+0d 15h 53m	Not Published	+0d 4h 3m	Not Published
Troj/DocDL-RJ	+1d 6h 39m	+1d 7h 15m	+1d 0h 0m	FIRST 2015/06/16 15:45 UTC	+1d 1h 35m
Troj/MSIL-DIS	FIRST 2015/06/17 21:25 UTC	+0d 6h 30m	Not Published	Not Published	Not Published
Troj/MSIL-DIZ	FIRST 2015/06/17 21:25 UTC	+0d 6h 30m	Not Published	Not Published	Not Published
Mal/Generic-L	FIRST 2015/06/17 17:10 UTC	+0d 3h 30m	Not Published	Not Published	Not Published
Troj/DocDL-RJ	+0d 0h 27m	+0d 7h 15m	FIRST 2015/06/17 15:45 UTC	+0d 4h 5m	Not Published
Troj/DocDI-QH	FIRST 2015/06/17 09:02 UTC	+0d 4h 43m	Not Published	+0d 3h 38m	+0d 17h 43m
Troj/DocDI-QH	FIRST 2015/06/17 06:54 UTC	+0d 6h 51m	Not Published	Not Published	Not Published
Mal/Generic-L	FIRST 2015/06/17 03:35 UTC	+0d 10h 10m	Not Published	Not Published	Not Published
Mal/Generic-I	FIRST 2015/06/17 01:50 UTC	+0d 6h 35m	Not Published	+0d 11h 50m	Not Published
Mal/Generic-L	FIRST 2015/06/17 01:20 UTC	+0d 7h 5m	Not Published	+0d 12h 20m	Not Published
Mal/Wonton-BB	FIRST 2015/06/17 01:10 UTC	+0d 12h 35m	Not Published	Not Published	+0d 16h 10m
Mal/Generic-L	+0d 2h 0m	+0d 10h 40m	Not Published	FIRST 2015/06/16 21:45 UTC	+0d 19h 35m
Mal/Generic-L	+3d 8h 5m	+3d 11h 40m	FIRST 2015/06/13 15:15 UTC	Not Published	Not Published
Mal/MSIL-ON	FIRST 2015/06/16 21:00 UTC	+0d 5h 55m	Not Published	Not Published	+0d 20h 20m
Troj/Agent-ANLL	FIRST 2015/06/16 20:50 UTC	+0d 20h 20m	Not Published	Not Published	Not Published

Last Updated: 2015/06/19 03:00 UTC







*TOMORROW starts here.*

Learn more at [www.cisco.com/go/esa](http://www.cisco.com/go/esa)