



資訊安全趨勢與因應策略

郭旭傑 Joey Kuo
思科台灣 產品經理

There are two types of companies: those who **have been hacked**, and those who **don't yet know** they have been hacked.

John Chambers
Chief Executive Officer of Cisco



Security Challenges

It is a Community
that hides in plain
sight

avoids detection,
and attacks swiftly

60%
of data is
stolen in
hours

54%
of breaches
remain undiscovered
for months

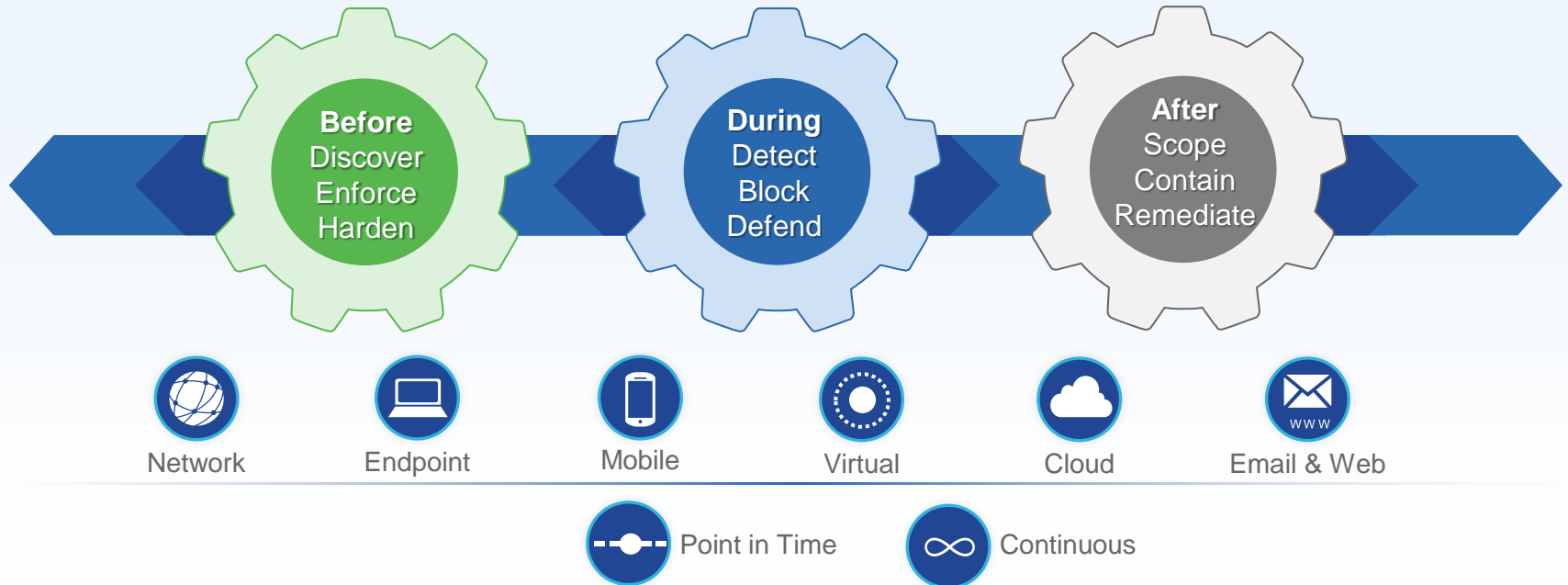
100%
of companies connect
to domains that host
malicious files or services

What would you do differently if you knew you were going to be compromised?



To defend against these advanced threats requires greater visibility and control across the full attack continuum

Attack Continuum





Before
See It, Control It

You can't protect what you can't see



Threats



Devices



Applications



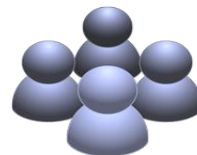
Flow



Vulnerabilities



OS



Users



Files



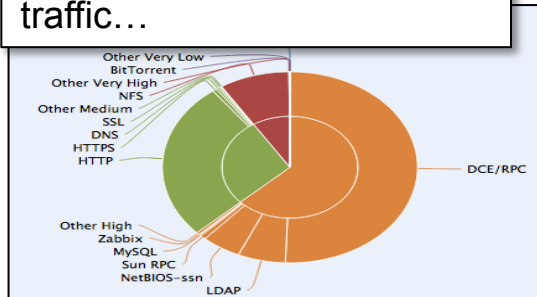
Network and endpoint awareness and context that provides environmental insights and automatically strengthens protection



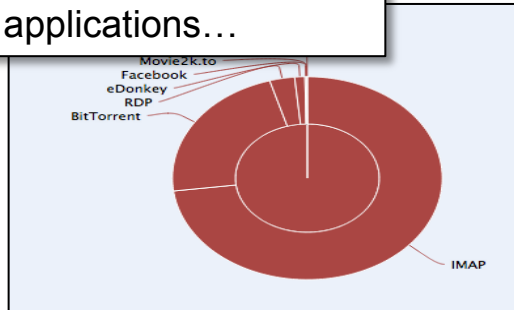
Before the Threat: Discover Your Environment

Before
See It, Control It

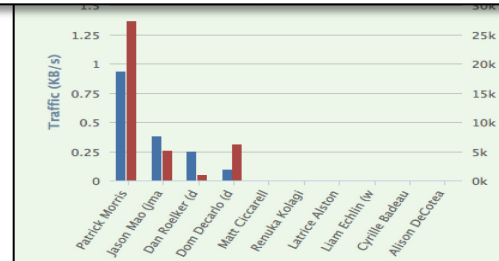
Browse all application traffic...



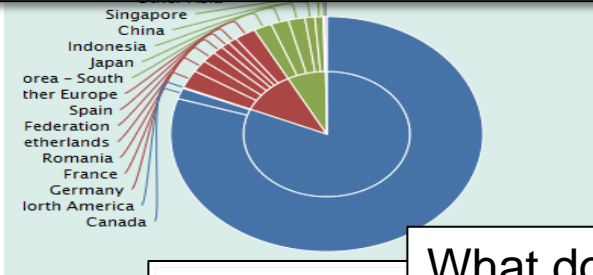
Look for risky applications...



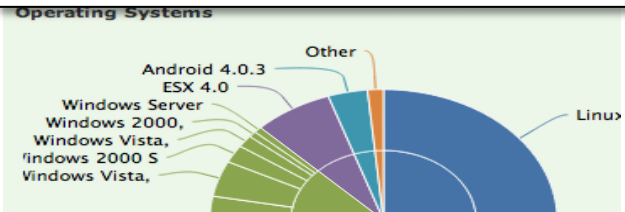
Who is using them?



Connections by Initiator Country



On what operating systems?



What does their traffic look like over time?



FireSIGHT™ Awareness

The screenshot displays the Cisco FireSIGHT Awareness interface. At the top, there are navigation tabs: Overview, Analysis, Policies, Devices, Objects, and Endpoints. Below these are sub-tabs for Connection Events, Intrusion, Hosts, Users, Vulnerabilities, Correlation, and Custom. The main content area is titled 'Connection Events' and shows a table of connections with application details. A callout box on the left provides 'User Identity' for a specific connection, listing details like Username (cgillian), Authentication Protocol (LDAP), and Host History. A callout box in the center asks 'What other systems / IPs did user have, when?' and points to the Host History table. On the right, a detailed view of a host is shown, including Hostname, NetBIOS Name, Device (Hops), MAC Addresses (TTL), Host Type, Last Seen, Events, Intrusion Events, Current User, and Operating System. Below this, a table lists server applications and their versions. Another callout box asks 'Who is at the host' and points to the Current User field. A callout box asks 'OS & version Identified' and points to the Operating System section. A callout box asks 'Server applications and version' and points to the table of server applications. A callout box asks 'Client Applications' and points to the table of client applications. A callout box asks 'Client Version' and points to the version column in the client applications table. A callout box asks 'Application' and points to the application column in the client applications table. The bottom of the interface shows a table of connection events with columns for time, action, and status.

Who is at the host

OS & version Identified

Server applications and version

Client Applications

Client Version

Application

User Identity

Username cgillian
Authentication Protocol LDAP
First Name Charles
Last Name Gillian
Email charles.gillian@sourcefire.com
Department SF (ron)
Phone 867-5309

Host History

Hosts	2011-10-19 11:10:36	2011-10-20 11:10:36
10.4.10.117		
10.5.32.75		
10.4.10.116		
10.4.32.60		

Host Details:

Host: [REDACTED]
Hostname: [REDACTED]
NetBIOS Name: [REDACTED]
Device (Hops): mango (1)
MAC Addresses (TTL): [REDACTED] (VMware, Inc.) (127)
Host Type: Host
Last Seen: 2011-11-15 16:06:05
Events: View
Intrusion Events: Source Destination
Current User: [REDACTED] (LDAP)
Operating System: [REDACTED]

Vendor	Product	Version
Microsoft	Windows	2000,

Port	Application Protocol	Vendor and Version
189	pending	
1077	pending	
22	SSH	OpenSSH 5.1p1 Debian-6ubuntu2

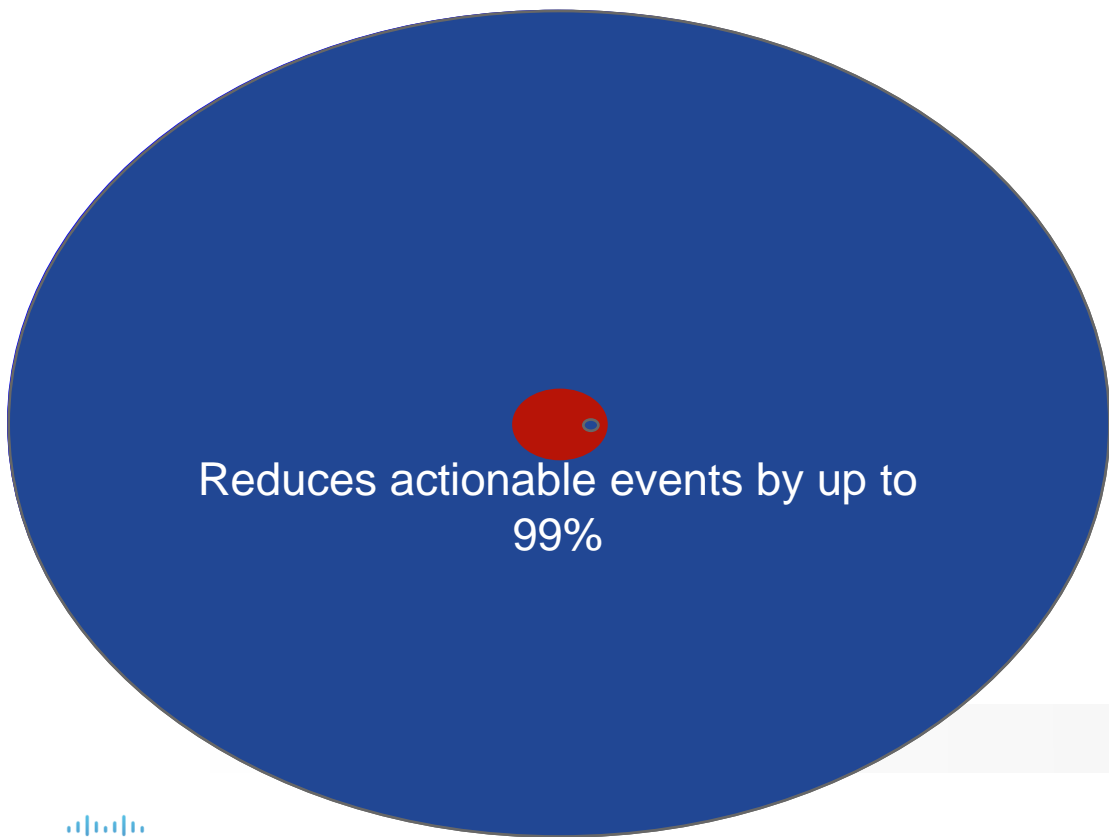
Protocol	Client	Version
<input type="checkbox"/>	DNS	
<input type="checkbox"/>	Google	
<input type="checkbox"/>	Google Safebrowsing	
<input type="checkbox"/>	IRC	
<input type="checkbox"/>	Internet Explorer	6.0
<input type="checkbox"/>	Internet Explorer	6.0
<input type="checkbox"/>	Internet Explorer	6.0

Application	Client	Version
<input type="checkbox"/>	Atom	
<input type="checkbox"/>	Blogger	
<input type="checkbox"/>	Dropbox	
<input type="checkbox"/>	Facebook	
<input type="checkbox"/>	Google	
<input type="checkbox"/>	Google	
<input type="checkbox"/>	Google APIs	
<input type="checkbox"/>	Google APIs	
<input type="checkbox"/>	Google Analytics	
<input type="checkbox"/>	Google Analytics	

Host History Table:

Time	Action	Status
2011-11-15 16:39:46	Allow	
2011-11-15 16:39:46	Allow	
2011-11-15 16:39:46	Allow	
2011-11-15 16:39:46	Trust	
2011-11-15 16:39:46	Trust	
2011-11-15 16:39:45	Trust	

事件管理？ How to manage thousands event per day?



Intrusion event



Vulnerable

(exploit targets known vulnerability)



Possibly vulnerable

(exploit targets OS and/or service)



Not vulnerable

(no service present)

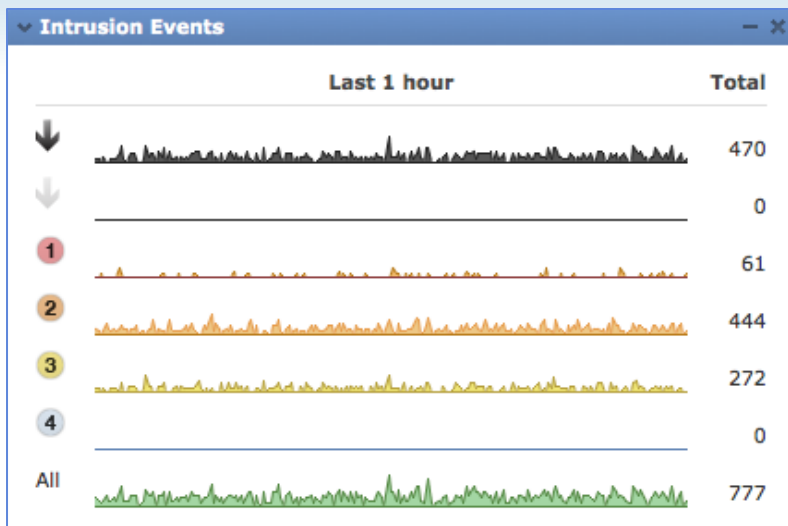


Not present

(no host present)

Correlation & Automation (自動化及關聯分析) - Cost Saving

Correlates all intrusion events to an impact of the attack against the target



Impact Flag

Administrator Action

Why



1

Act immediately, vulnerable

Event corresponds to vulnerability mapped to host



2

Investigate, potentially vulnerable

Relevant port open or protocol in use, but no vuln mapped



3

Good to know, currently not vulnerable

Relevant port not open or protocol not in use



4

Good to know, unknown target

Monitored network, but unknown host



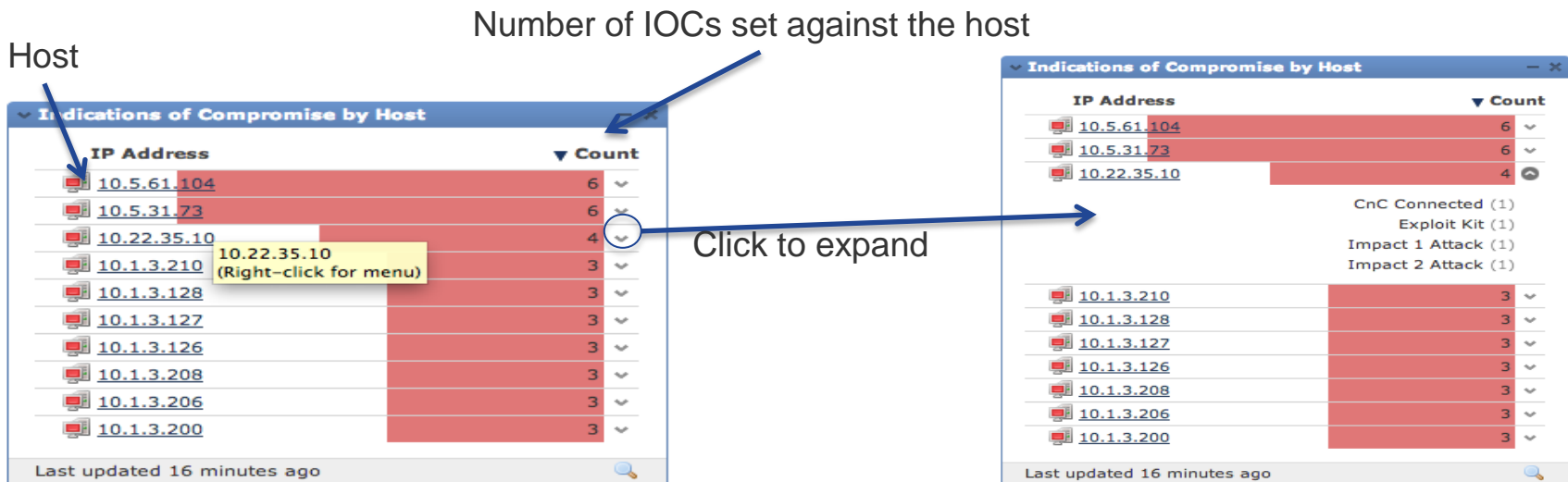
0

Good to know, unknown network

Unmonitored network

Indicators of Compromise (感染指標) Dashboard

- Because IOCs enable a quick way of classifying a host's potentially compromised state, having this data on a dashboard is desirable



Indicators of Compromise (感染指標)

Indications of Compromise (3)						Edit Rule States	Mark All Resolved
Category	Event Type	Description	First Seen	Last Seen			
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2013-09-17 16:46:28	2013-09-20 06:35:31			
CnC Connected	Security Intelligence Event - CnC	The host may be under remote control	2013-09-17 16:52:11	2013-09-20 03:55:45			
CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2013-09-17 20:09:23	2013-09-19 17:32:49			

Malware Backdoors

- Exploit Kits
- Web App Attacks
- CnC Connections
- Admin Privilege Escalations

Connections to Known CnC IPs

Malware Detections

- Office/PDF/Java Compromises
- Malware Executions
- Dropper Infections

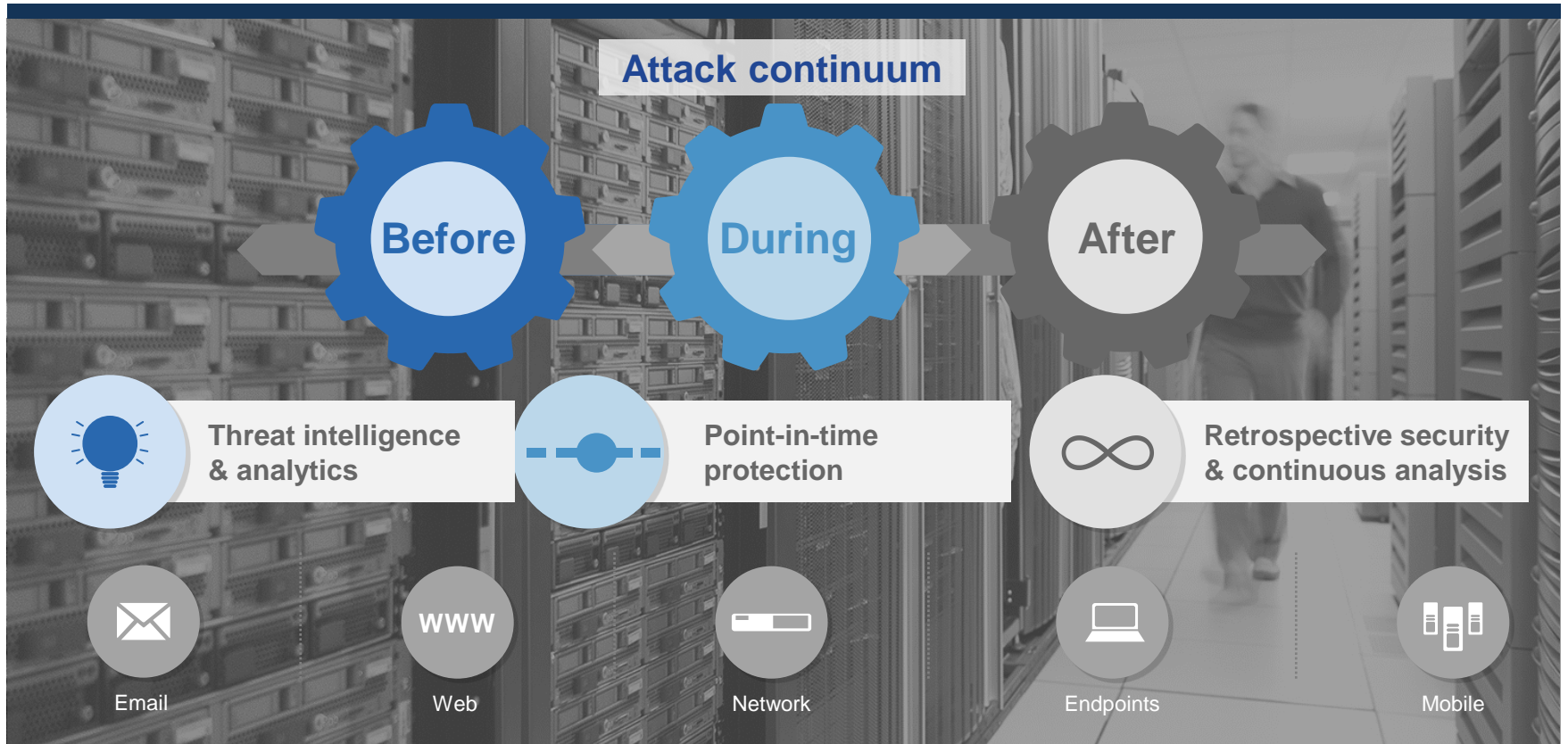
Advanced Persistent Threat & Advanced Malware

Is now a tool for financial gain

- Uses formal Development Techniques
 - Sandbox aware
 - Quality Assurance to evade detection
 - 24/7 Tech support available
- Has become a math problem
 - End Point AV Signatures ~20 Million
 - Total KNOWN Malware Samples ~100 M
 - AV Efficacy Rate ~50%

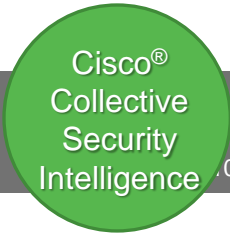


Cisco **Advanced Malware Protection** (AMP) across the entire attack continuum



Cisco **A**dvanced **M**alware **P**rotection

Built on unmatched collective security intelligence



1001 1101 1110011 0110011 101000 0110 00 1001 1101 1110011 0110011 101000 0110 00 0111000 0110 00 0111000 111010011 101 1100001 110 101000 0110 00 011100001110001110 1001 1101 1110011 0110011 101000 0110 00 1100001110001110



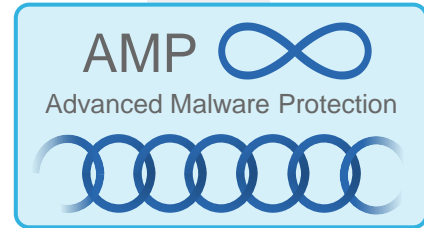
Automatic Updates in real time



1.6 million global sensors
 100 TB of data received per day
 150 million+ deployed endpoints
 600 engineers, technicians, and researchers
 35% worldwide email traffic

13 billion web requests
 24x7x365 operations
 4.3 billion web blocks per day
 40+ languages
 1.1 million incoming malware samples per day
 AMP Community
 Private/Public Threat Feeds

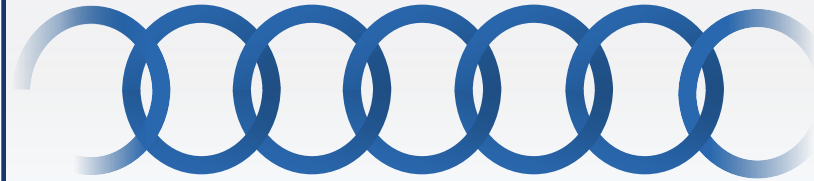
Talos Security Intelligence
 AMP Threat Grid Intelligence
 AMP Threat Grid Dynamic Analysis
 10 million files/month
 Advanced Microsoft and Industry Disclosures
 Snort and ClamAV Open Source Communities
 AEGIS Program



Cisco AMP Delivers A Better Approach

Point-in-Time Detection 一次性偵測 & Retrospective 回溯分析

Point-in-Time Protection
一次性偵測



File Reputation, Sandboxing

Retrospective Security
回溯分析



Continuous Analysis

Unique to Cisco® AMP

+ Possible ZeuS Variant Detected Severity: 100 Confidence: 100

- Process Modified an Executable File Severity: 95 Confidence: 95

Malware will modify executables on a system, to hide logs or other evidence. Also, by modifying various executables it can disable functionality in the system which may detect or hamper the operation of the malware. Lastly, it may be attempting to hide an executable, so that it appears to be a legitimate file. Please review the 'Disk Artifacts' section in order to view additional details about this file.

Categories
Tags

persistence, obfuscation
executable, file, process, PE

Path	Process Name	Process ID
\Documents and Settings\Administrator\Application Data\Byumqu\nayb.exe	LATEST_ZeuS.exe	1120 (LATEST_ZeuS.exe)

+ Process Modified Autorun Registry Key Value Severity: 80 Confidence: 60

+ Process Modified File in a User Directory Severity: 70 Confidence: 80

+ Potential Sandbox Detection - Enumeration of ProductID Severity: 60 Confidence: 70

+ Process Created an Executable in a User Directory Severity: 60 Confidence: 95

+ Command Exe File Execution Detected Severity: 50 Confidence: 80

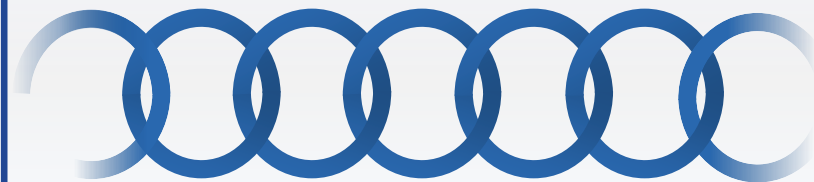
+ Potential Code Injection Detected Severity: 50 Confidence: 50

+ Executable with Encrypted Sections Severity: 30 Confidence: 30

Cisco AMP Delivers A Better Approach

Point-in-Time Detection 一次性偵測 & Retrospective 回溯分析

Point-in-Time Protection
一次性偵測



File Reputation, Sandboxing

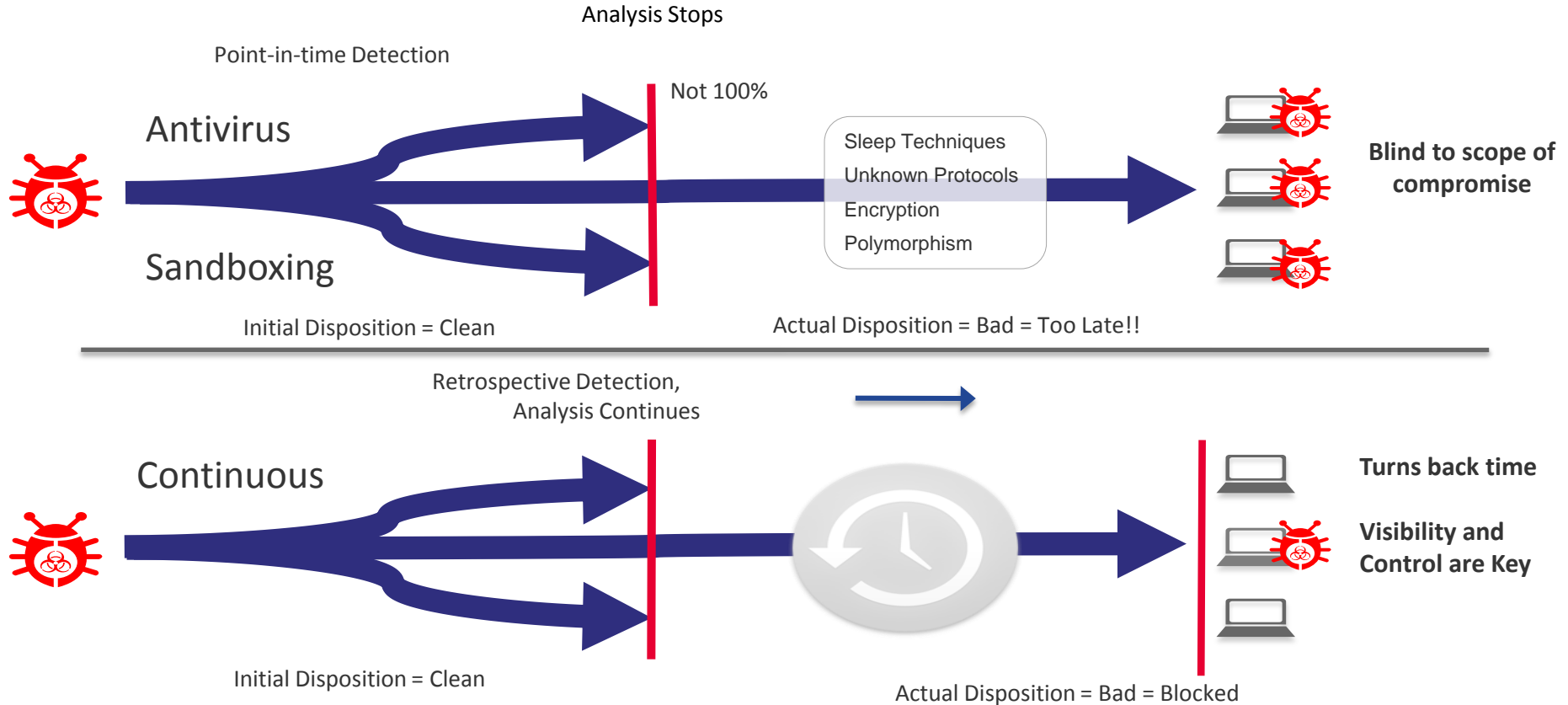
Retrospective Security
回溯分析



Continuous Analysis

Unique to Cisco® AMP

Retrospective (可回朔) 持續分析 vs. Point-in-Time Detection 一次性偵測



How Cisco AMP Works: Network File Trajectory Use Case

Overview **Analysis** Policies Devices Objects FireAMP Health System Help admin

Context Explorer Connections Intrusions **Files** Network File Trajectory Hosts Users Vulnerabilities Correlation Custom Search

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374
 File Name WindowsMediaInstaller.exe
 File Type MSEXE
 File Category Executables
 Current Disposition Malware
 Threat Score High

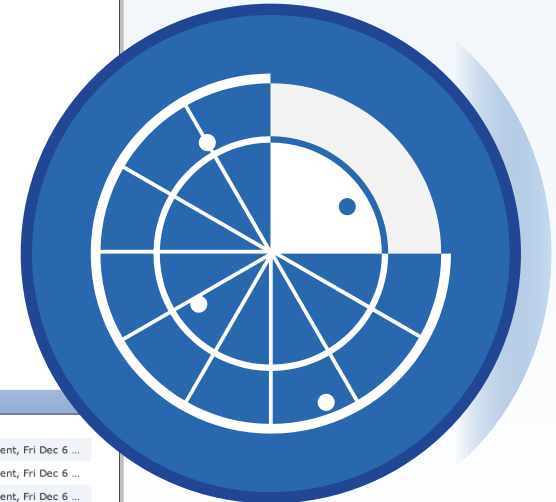
First Seen 2013-12-06 10:57:13 on 10.4.10.183
 Last Seen 2013-12-06 18:17:27 on 10.4.10.183
 Event Count 7
 Seen On 4 hosts
 Seen On Breakdown 2 senders → 3 receivers

Trajectory

Events: Transfer, Block, Create, Move, Execute, Scan, Retrospective, Quarantine
 Dispositions: Unknown, Malware, Clean, Custom, Unavailable

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		



Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type [MSEXE](#)

File Category [Executables](#)

Current Disposition [Malware](#)

Threat Score ●●●○ [High](#)

First Seen

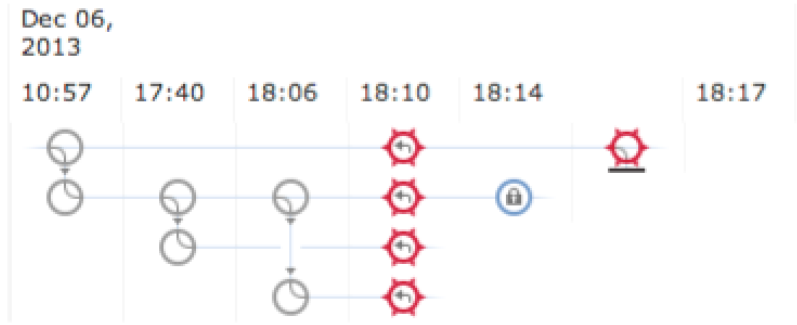
Last Seen

Event Count

Seen On

Seen On Breakdown

Trajectory



Events Transfer Block Create Move Execute Scan Retrospective Quarantine

Dispositions Unknown Malware Clean Custom Unavailable

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type [MSEXE](#)

File Category [Executables](#)

Current Disposition [Malware](#)

Threat Score ●●●○ [High](#)

First Seen

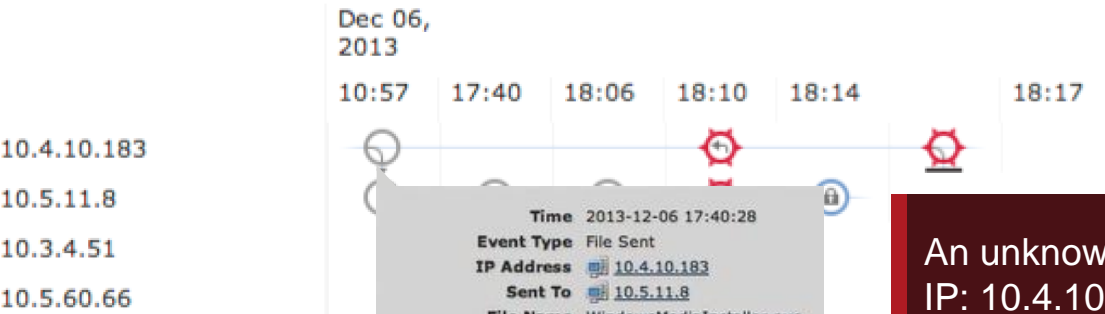
Last Seen

Event Count

Seen On

Seen On Breakdown

Trajectory



Time 2013-12-06 17:40:28

Event Type File Sent

IP Address [10.4.10.183](#)

Sent To [10.5.11.8](#)

File Name [WindowsMediaInstaller.exe](#)

Disposition [Unknown](#)

Action [Malware_Cloud_Lookup](#)

Application Protocol [HTTP](#)

Client [Firefox](#)

An unknown file is present on IP: 10.4.10.183, having been downloaded from Firefox

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type [MSEXE](#)

File Category [Executables](#)

Current Disposition [Malware](#)

Threat Score ●●●○ [High](#)

First Seen

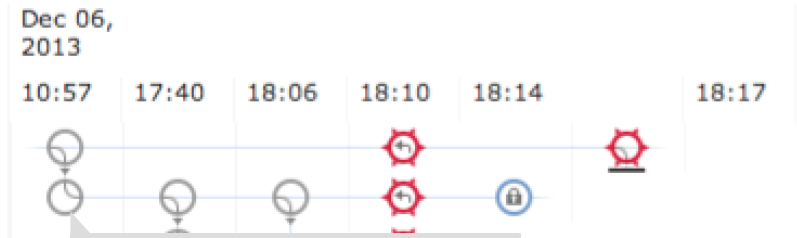
Last Seen

Event Count

Seen On

Seen On Breakdown

Trajectory



Time 2013-12-06 17:40:28

Event Type File Received

IP Address [10.5.11.8](#)

Received From [10.4.10.183](#)

File Name [WindowsMediaInstaller.exe](#)

Disposition [Unknown](#)

Action [Malware Cloud Lookup](#)

Application Protocol [HTTP](#)

Client [Firefox](#)

At 10:57, the unknown file is from IP 10.4.10.183 to IP: 10.5.11.8

- Events** Transfer
- Dispositions** Unknown

- Move
- Quarantine
- Custom
- Unavailable

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type [MSEXE](#)

File Category [Executables](#)

Current Disposition [Malware](#)

Threat Score ●●●○ [High](#)

First Seen

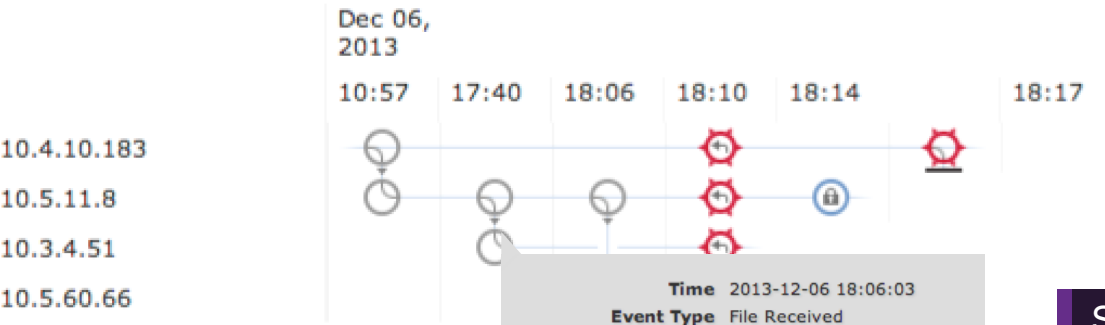
Last Seen

Event Count

Seen On

Seen On Breakdown

Trajectory



Time 2013-12-06 18:06:03

Event Type File Received

IP Address [10.3.4.51](#)

Received From [10.5.11.8](#)

File Name [WindowsMediaInstaller.exe](#)

Disposition [Unknown](#)

Action

Application Protocol [NetBIOS-ssn \(SMB\)](#)

Seven hours later the file is then transferred to a third device (10.3.4.51) using an SMB application

Events Transfer Block

Dispositions Unknown Malware Quarantine

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type [MSEXE](#)

File Category [Executables](#)

Current Disposition [Malware](#)

Threat Score [High](#)

First Seen

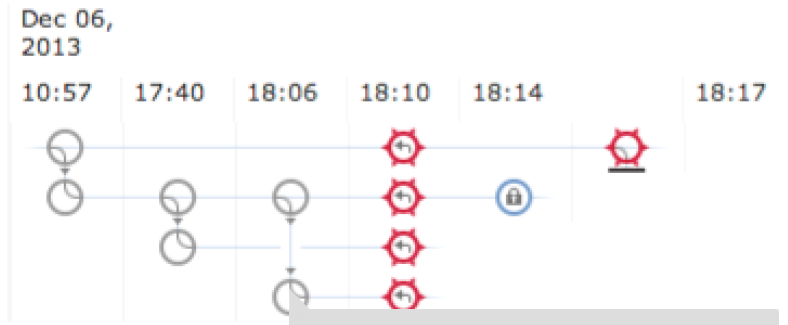
Last Seen

Event Count

Seen On

Seen On Breakdown

Trajectory



Events Transfer Block

Dispositions Unknown Malware

Time 2013-12-06 18:10:03

Event Type File Received

IP Address 10.5.60.66

Received From 10.5.11.8

File Name [WindowsMediaInstaller.exe](#)

Disposition Unknown

Action

Application Protocol NetBIOS-ssn (SMB)

The file is copied yet again onto a fourth device (10.5.60.66) through the same SMB application a half hour later

Quarantine

able

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type [MSEXE](#)

File Category [Executables](#)

Current Disposition [Malware](#)

Threat Score ●●●○ [High](#)

First Seen

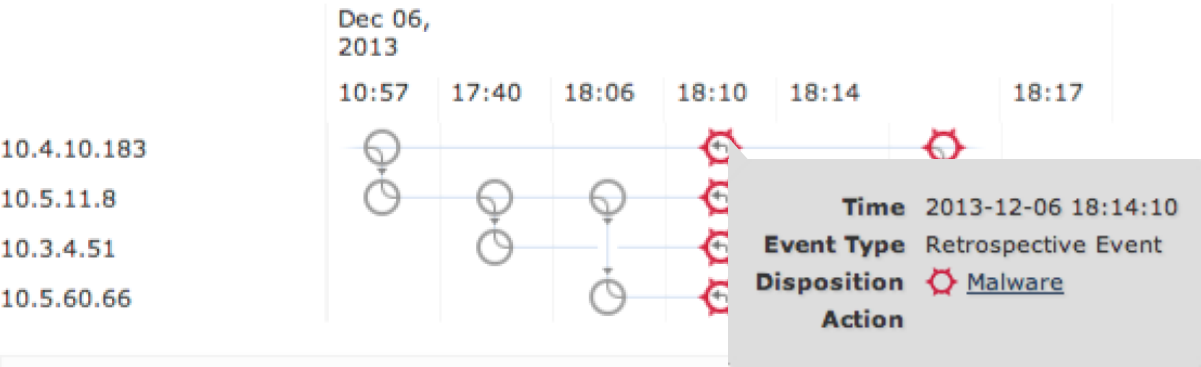
Last Seen

Event Count

Seen On

Seen On Breakdown

Trajectory



The Cisco Collective Security Intelligence Cloud has learned this file is malicious and a retrospective event is raised for all four devices immediately.

Events Transfer Block Create Move Execute Scan Retrospective Quarantine

Dispositions Unknown Malware Clean Custom Unavailable

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type [MSEXE](#)

File Category [Executables](#)

Current Disposition [Malware](#)

Threat Score [High](#)

First Seen

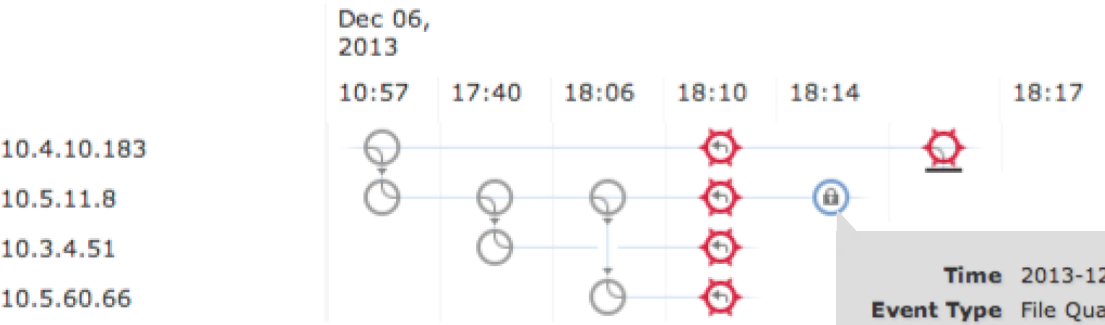
Last Seen

Event Count

Seen On

Seen On Breakdown

Trajectory



At the same time, a device with the FireAMP endpoint connector reacts to the retrospective event and immediately stops and quarantines the newly detected malware

Time 2013-12-06 18:14:23

Event Type File Quarantined

IP Address [10.5.11.8](#)

File Name [WindowsMediaInstaller.exe](#)

Disposition [Malware](#)

Action

Events Transfer Block Create Retrospective Quarantine

Dispositions Unknown Malware Clean Quarantine

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type [MSEXE](#)

File Category [Executables](#)

Current Disposition [Malware](#)

Threat Score ●●●○ [High](#)

First Seen

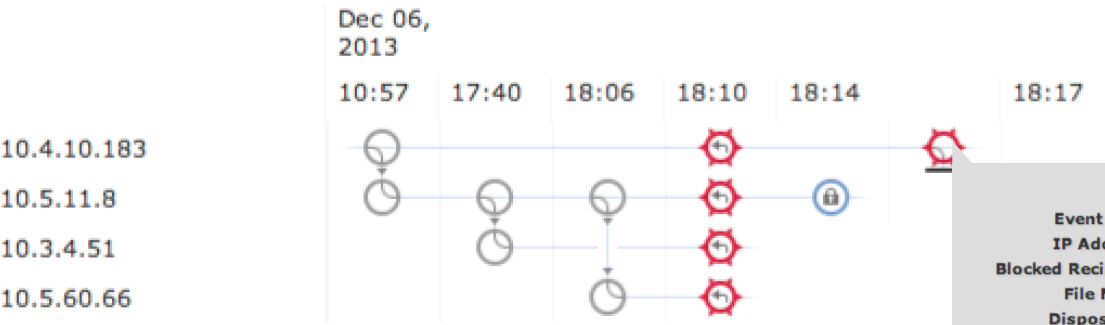
Last Seen

Event Count

Seen On

Seen On Breakdown

Trajectory



8 hours after the first attack, the Malware tries to re-enter the system through the original point of entry but is recognized and blocked.

Time 2013-12-06 18:17:27

Event Type File Sent

IP Address [10.4.10.183](#)

Blocked Recipient [10.5.11.8](#)

File Name [WindowsMediaInstaller.exe](#)

Disposition [Malware](#)

Action [Malware Block](#)

Application Protocol HTTP

Client Firefox

- Events** Transfer Block Create Move
- Dispositions** Unknown Malware Clean Custom Unavailable

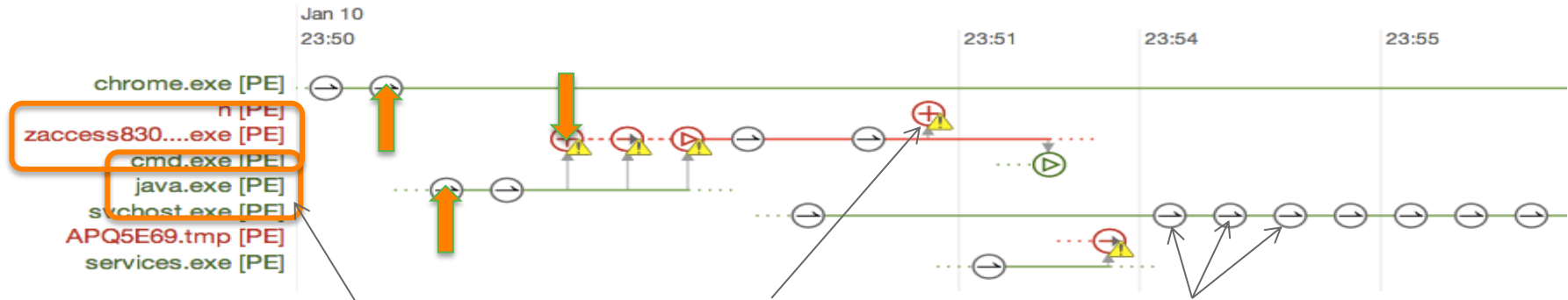
retrospective Quarantine

Device Trajectory

- Break the reinfection lifecycle with fast root cause analysis





Outgoing connection from Google Chrome 24.0.1312.52 (62ca2bc..59a3cb), most common filename chrome.exe, at TCP port 1156 to http://10.180.0.144:8888/exploit.html (10.180.0.144 port 8888).
Neutral disposition.
At 23:50:44, Thu Jan 10 2013 UTC

Device Trajectory for Java-0-Day



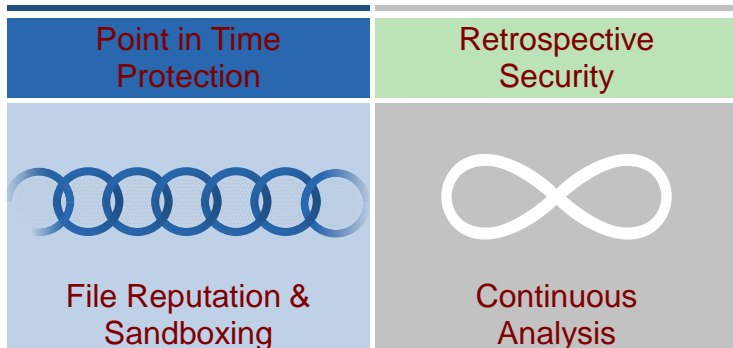
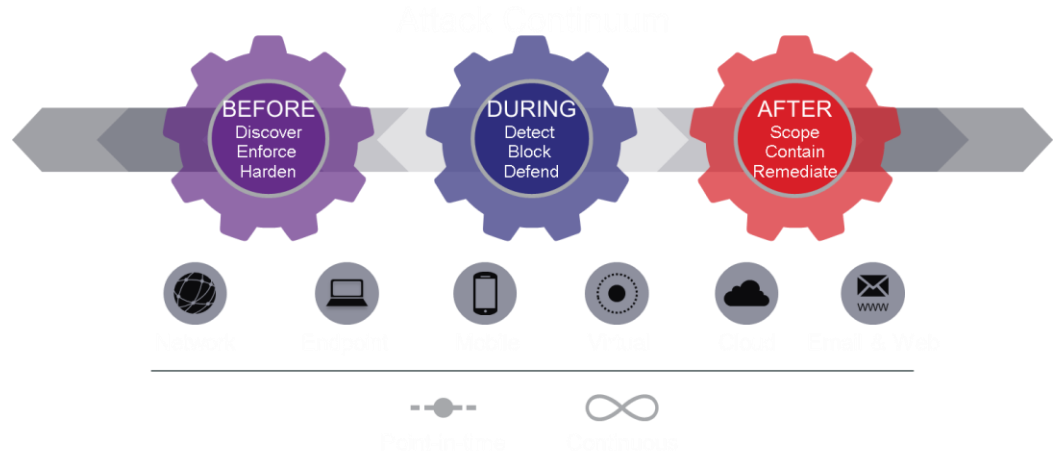
There Are Several Ways You Can Deploy AMP



Deployment Options				
	Email and Web; AMP on Cisco® ASA CWS	AMP for Networks (AMP on FirePOWER Network Appliance)	AMP for Endpoints	AMP Private Cloud Virtual Appliance
Ideal for	New or existing Cisco CWS, Email /Web Security	IPS/NGFW/AMP Appliance	Windows, Mac, Android, virtual machines	High-Privacy Environments

Key Take Away

1. 能見度 (可視性)
2. 自動化
3. 可回溯、調查及鑑識





TOMORROW starts here.

Thank You