TOMORROW
starts here.

# Cisco Sourcefire Advanced Malware Protection (AMP)

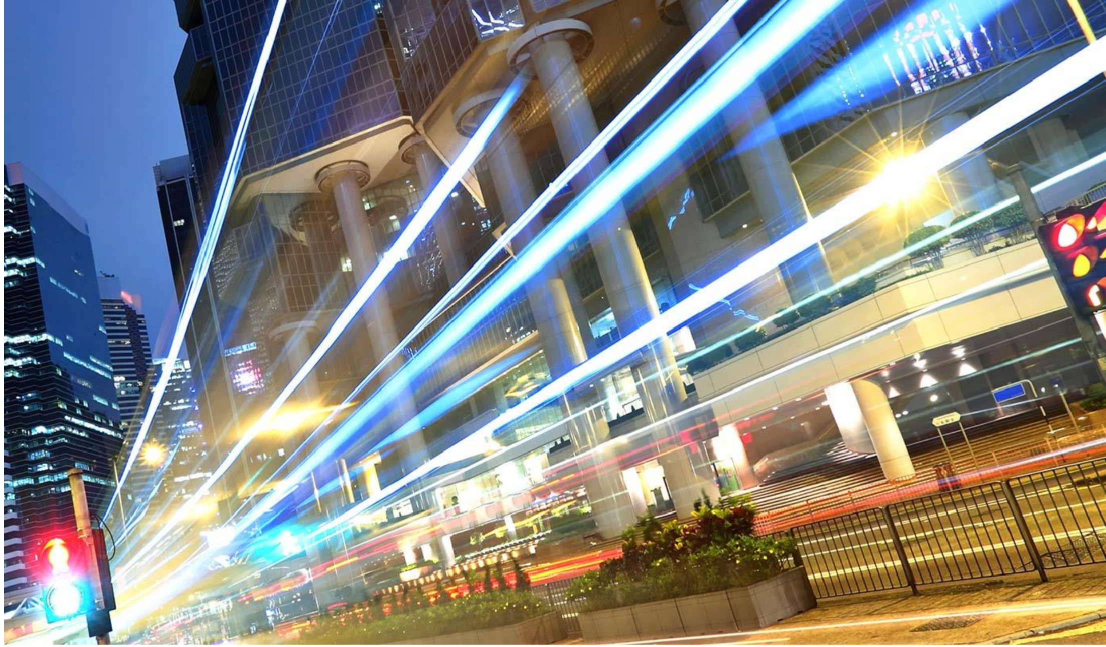
BRKSEC-2664

Jay Tecksingani
AMP CSE APJC

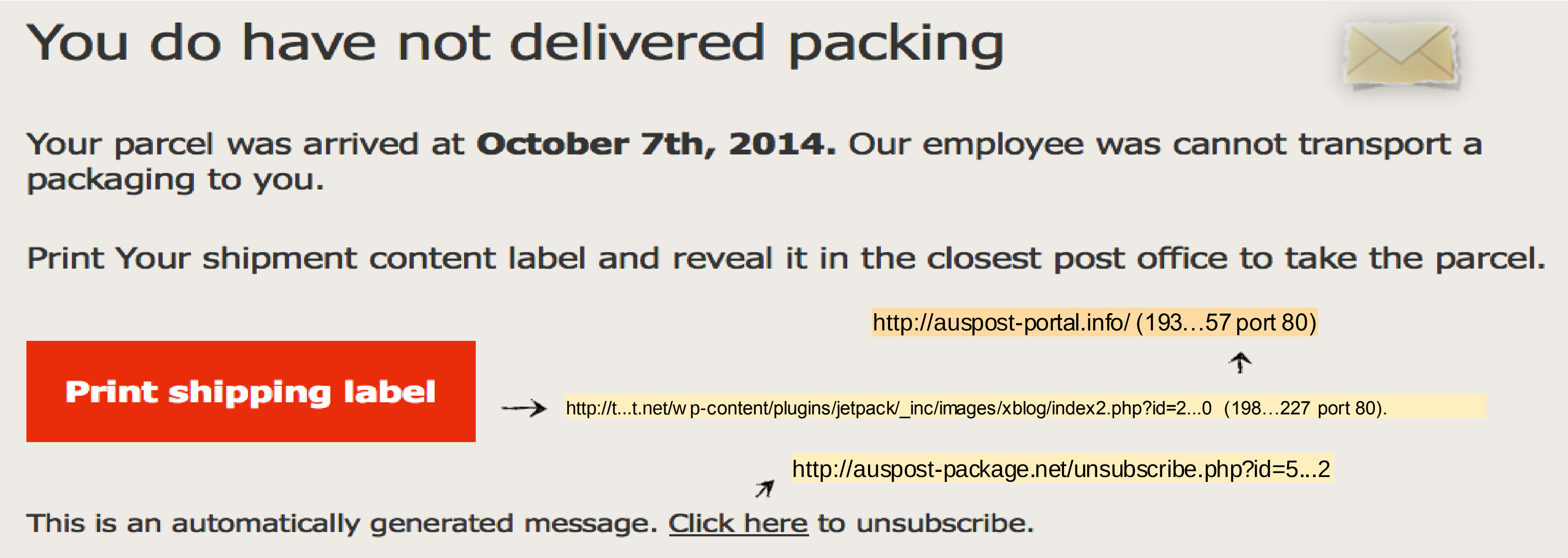
#clmel

Cisco live!

# Malware



- The Lure
- The Investigation
- Reasons for Success
- Simple Protection
- What’s been Missing ?
- Advanced Malware Protection



# You do have not delivered packing

Your parcel was arrived at **October 7th, 2014.** Our employee was cannot transport a packaging to you.

Print Your shipment content label and reveal it in the closest post office to take the parcel.

http://auspost-portal.info/ (193…57 port 80)

**Print shipping label** → http://t...t.net/w p-content/plugins/jetpack/_inc/images/xblog/index2.php?id=2...0 (198…227 port 80).

http://auspost-package.net/unsubscribe.php?id=5...2

This is an automatically generated message. Click here to unsubscribe.

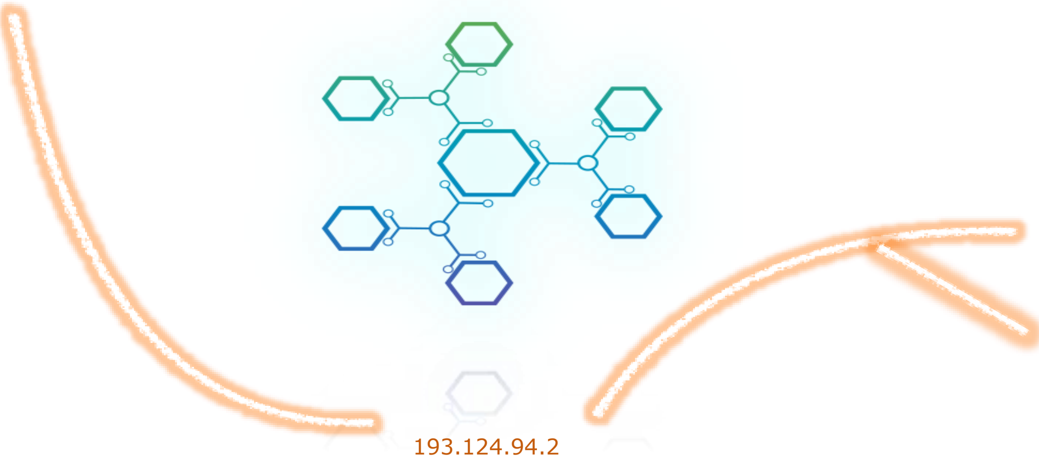
Typo’s - the obvious conclusion has long been “lost in translation”, however , INTENTIONAL Typos are meant to target unaware / distracted victims ! (attentive users will often delete these, causing no further concern to the criminals)

Stage #1: Compromise multitudes of WordPress WebSites - Setup Redirectors !
Stage #2: Register Multitudes of “similar” domain names through either Dynamic DNS or in different GEOs to Target
Stage #3: Setup fast-flux domains in different GEOs to the Target Victim Base

The URLs used are often ONE-TIME use URLS , tied to recipient email addresses = Slowing down TakeDowns / Investigations
Redirectors and Referrer IDs are often checked by the landing hosting Malware Server - to bypass investigative methods

AUSPOST-DELIVERY.COM
AUSPOST-DELIVERY.NET
AUSPOST-EPARCEL.COM
AUSPOST-EPARCEL.NET
**AUSPOST-HOME.COM**
AUSPOST-HOME.NET
AUSPOST-PACKAGE.COM
AUSPOST-PACKAGE.NET
AUSPOST-PARCEL.COM
AUSPOST-PARCEL.NET
AUSPOST-PORTAL.NET
AUSPOST-PORTAL24.NET
AUSPOST-SERVICE.COM
AUSPOST-SERVICE.NET
AUSPOST-SERVICES.COM
AUSPOST-SERVICES.NET
AUSPOST-TRACK.NET
AUSPOST-TRACK24.NET
AUSPOST-TRACKING.COM
AUSPOST-TRACKING.NET
AUSPOST-TRACKING24.COM
AUSPOST-TRACKING24.NET
AUSPOST-TRACKIT.COM
AUSPOST-TRACKIT24.COM
AUSPOST-US.COM

194.58…/16
193.124…/16



193.124.94.2

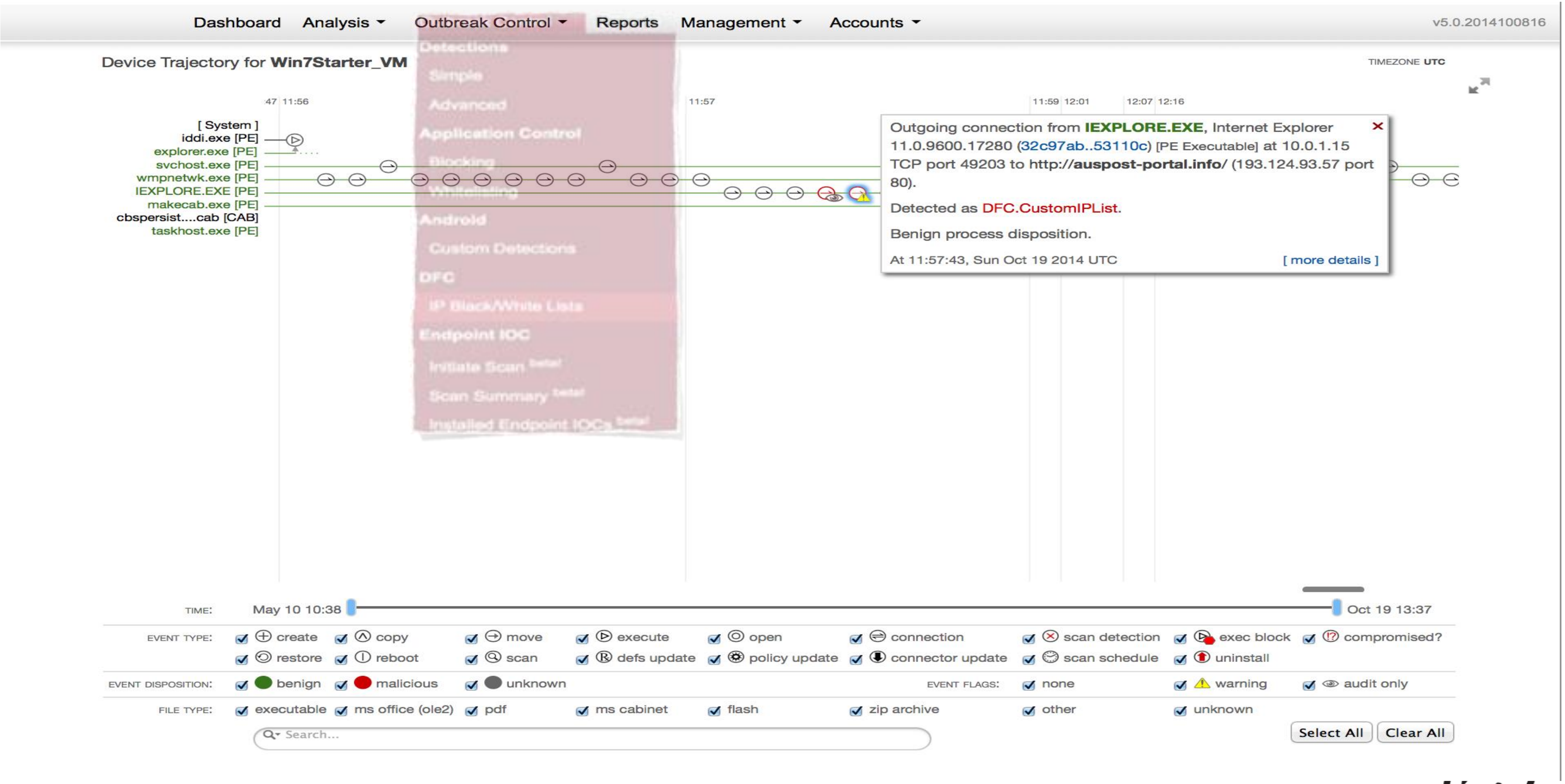
ROYALMAIL-BELGIE.COM
ROYALMAIL-BELGIQUE.COM
ROYALMAIL-CSI.COM
ROYALMAIL-DELIVERY.COM
ROYALMAIL-DIRECT.COM
ROYALMAIL-DIRECT.NET
ROYALMAIL-ECOMMERCE.COM
ROYALMAIL-EMHS.COM
ROYALMAIL-EMHS.NET
ROYALMAIL-EPARCEL.COM
ROYALMAIL-EPARCEL.NET
ROYALMAIL-GROUP.COM
ROYALMAIL-GROUP.NET
ROYALMAIL-GROUPLTD.COM
ROYALMAIL-GROUPLTD.NET
ROYALMAIL-INTERNATIONAL.COM
ROYALMAIL-LUXEMBOURG.COM
ROYALMAIL-MAIDSTONE.COM
ROYALMAIL-PARCEL24.COM
ROYALMAIL-PARCEL24.NET
ROYALMAIL-PPI-LABELS.COM
ROYALMAIL-SERVICE.COM
ROYALMAIL-SERVICE.NET
ROYALMAIL-TRACKING.NET
ROYALMAIL-TRACKING24.COM
ROYALMAIL-TRACKING24.NET

Multiple domains registered @ orderbox-dns.com

Resolve to a few Subnets located in an address space allocated to Reg-RU = Moscow, Russia

The IP addresses reverse resolve to multiple domains, most notably ROYALMAIL

Royal Mail Services hit by CryptoLocker Scam earlier this year !



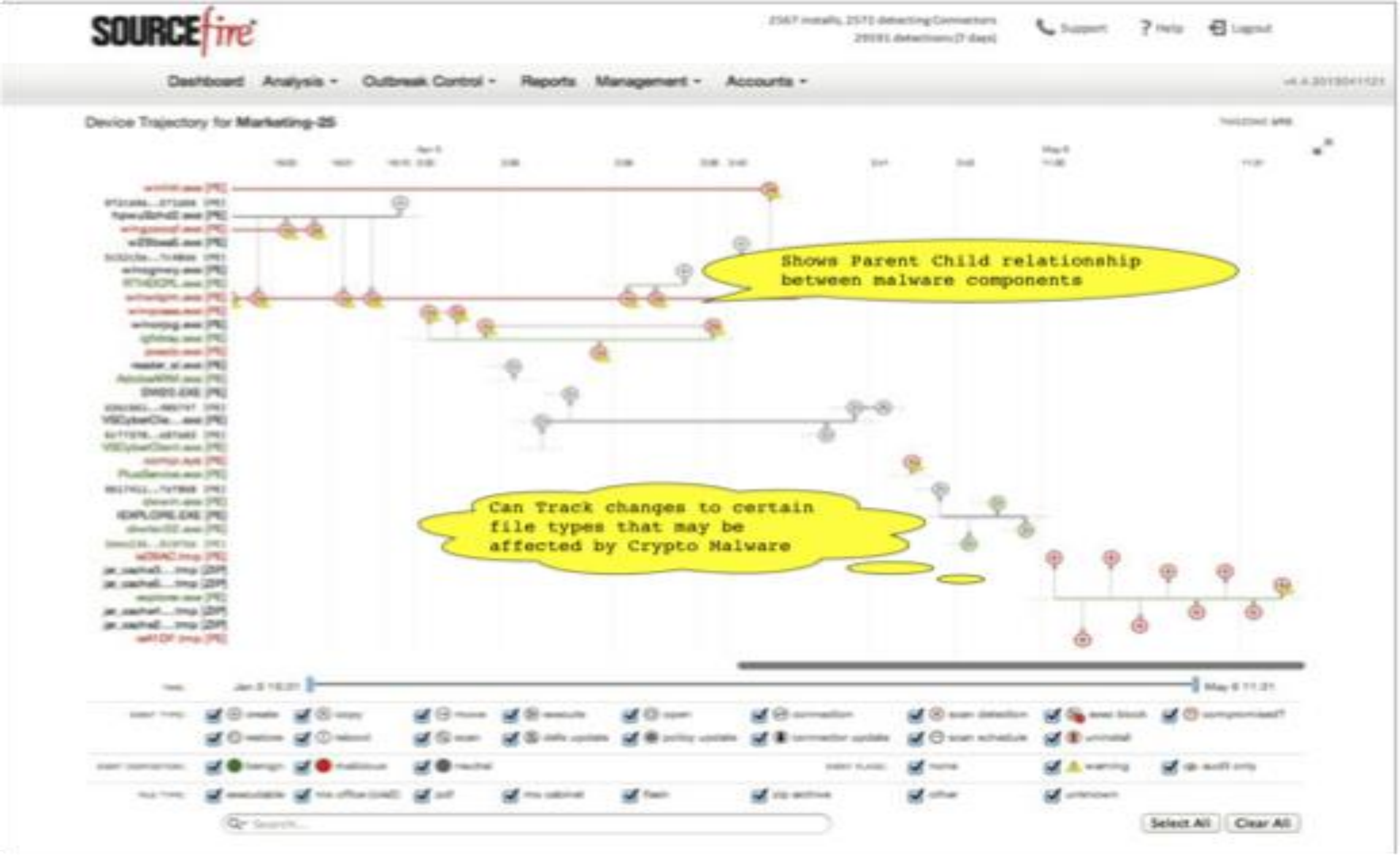
Device Trajectory for **Win7Starter_VM**

Outgoing connection from **IEXPLORE.EXE**, Internet Explorer 11.0.9600.17280 (32c97ab..53110c) [PE Executable] at 10.0.1.15 TCP port 49203 to http://**auspost-portal.info**/ (193.124.93.57 port 80).

Detected as DFC.CustomIPList.

Benign process disposition.

At 11:57:43, Sun Oct 19 2014 UTC [ more details ]



Shows Parent Child relationship between malware components

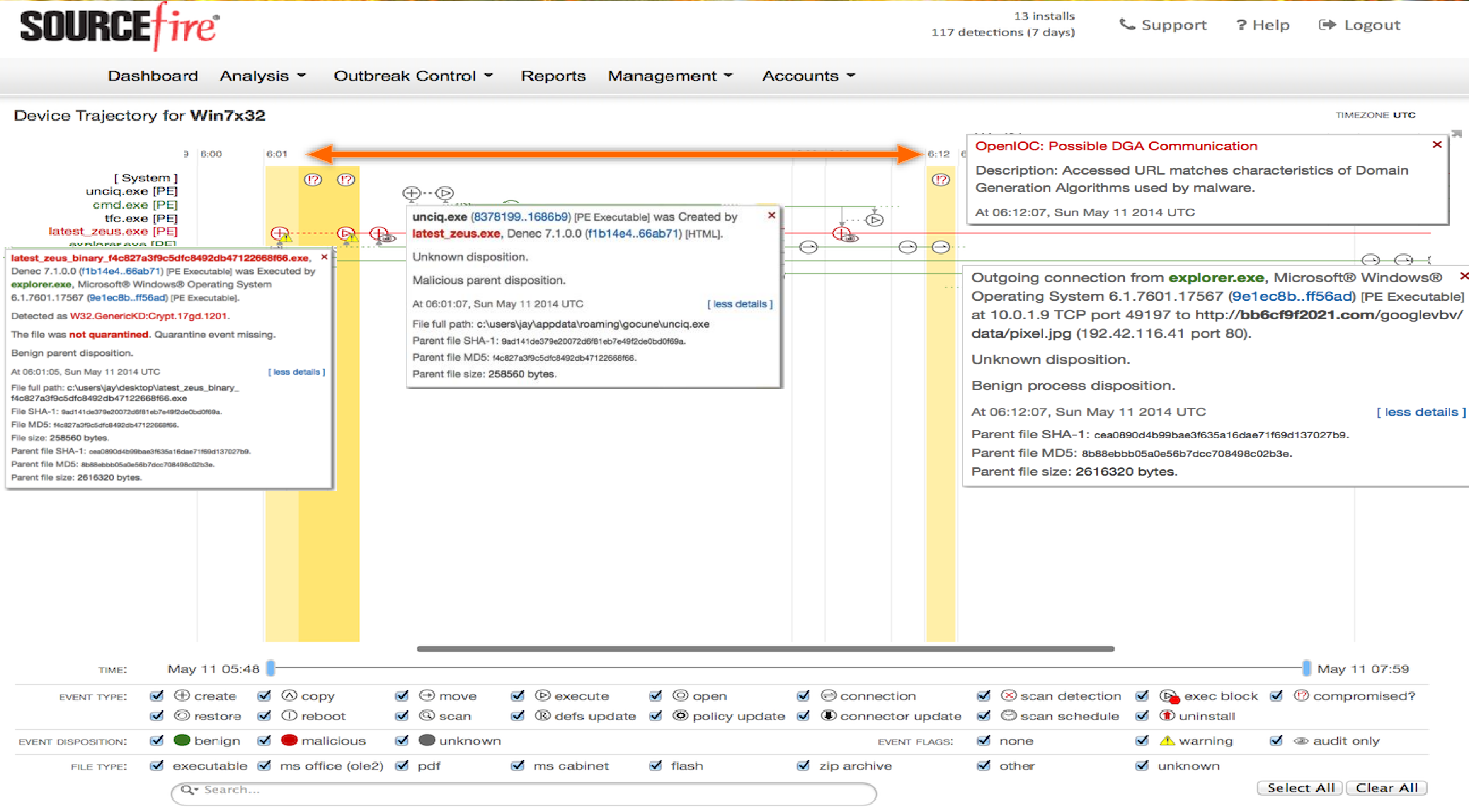
Can Track changes to certain file types that may be affected by Crypto Malware

**We need to Track Tracks changes to the following files**
MSEXE, PDF, SCRIPT,HTML,HTML_UTF16,GRAPHICS, TEXT_ASCII, TEXT_UTF8, TEXT_UTF16LE, TEXT_UTF16BE,RTF, RIFF,MSCHM, MSCAB,MSOLE2,MSSZDD,ZIP,RAR,7Z,BZ,GZ,ARJ,ZIPSFX,RARSFX,CABSFX,ARJSFX,NULSFT,AUTOIT,ISHIELD_MSI,SFX BINHEX,MAIL,TNEF,BINARY_DATA,CRYPTFF,UUENCODED,SCRENC,POSIX_TAR,OLD_TAR,ELFMACHO,MACHO_UNIBIN,SIS,SWF,CPIO_OD,CPIO_NEWC,CPIO_CRC

Crypto - affects several types of media, graphics and document files

~ track undetected processes - that otherwise continue to damage your system !
Device File Trajectory clearly to show changes to multiple file types - that can be affected by CryptoLocker

IOC is an advanced behavioural methodology that can be used to flag data corruption and even exfiltration like activity !



Device Trajectory for **Win7x32**

**latest_zeus_binary_f4c827a3f9c5dfc8492db47122668f66.exe**, Denec 7.1.0.0 (f1b14e4..66ab71) [PE Executable] was Executed by **explorer.exe**, Microsoft® Windows® Operating System 6.1.7601.17567 (9e1ec8b..ff56ad) [PE Executable].

Detected as W32.GenericKD:Crypt.17gd.1201.

The file was **not quarantined**. Quarantine event missing.

Benign parent disposition.

At 06:01:05, Sun May 11 2014 UTC [ less details ]

File full path: c:\users\jay\desktop\latest_zeus_binary_f4c827a3f9c5dfc8492db47122668f66.exe

File SHA-1: 9ad141de379e20072d6f81eb7e49f2de0bd0f69a.

File MD5: f4c827a3f9c5dfc8492db47122668f66.

File size: 258560 bytes.

Parent file SHA-1: cea0890d4b99bae3f635a16dae71f69d137027b9.

Parent file MD5: 8b88ebbb05a0e56b7dcc708498c02b3e.

Parent file size: 2616320 bytes.

**unciq.exe** (8378199..1686b9) [PE Executable] was Created by **latest_zeus.exe**, Denec 7.1.0.0 (f1b14e4..66ab71) [HTML].

Unknown disposition.

Malicious parent disposition.

At 06:01:07, Sun May 11 2014 UTC [ less details ]

File full path: c:\users\jay\appdata\roaming\gocune\unciq.exe

Parent file SHA-1: 9ad141de379e20072d6f81eb7e49f2de0bd0f69a.

Parent file MD5: f4c827a3f9c5dfc8492db47122668f66.

Parent file size: 258560 bytes.

OpenIOC: Possible DGA Communication

Description: Accessed URL matches characteristics of Domain Generation Algorithms used by malware.

At 06:12:07, Sun May 11 2014 UTC

Outgoing connection from **explorer.exe**, Microsoft® Windows® Operating System 6.1.7601.17567 (9e1ec8b..ff56ad) [PE Executable] at 10.0.1.9 TCP port 49197 to http://**bb6cf9f2021.com**/googlevbv/data/pixel.jpg (192.42.116.41 port 80).

Unknown disposition.

Benign process disposition.

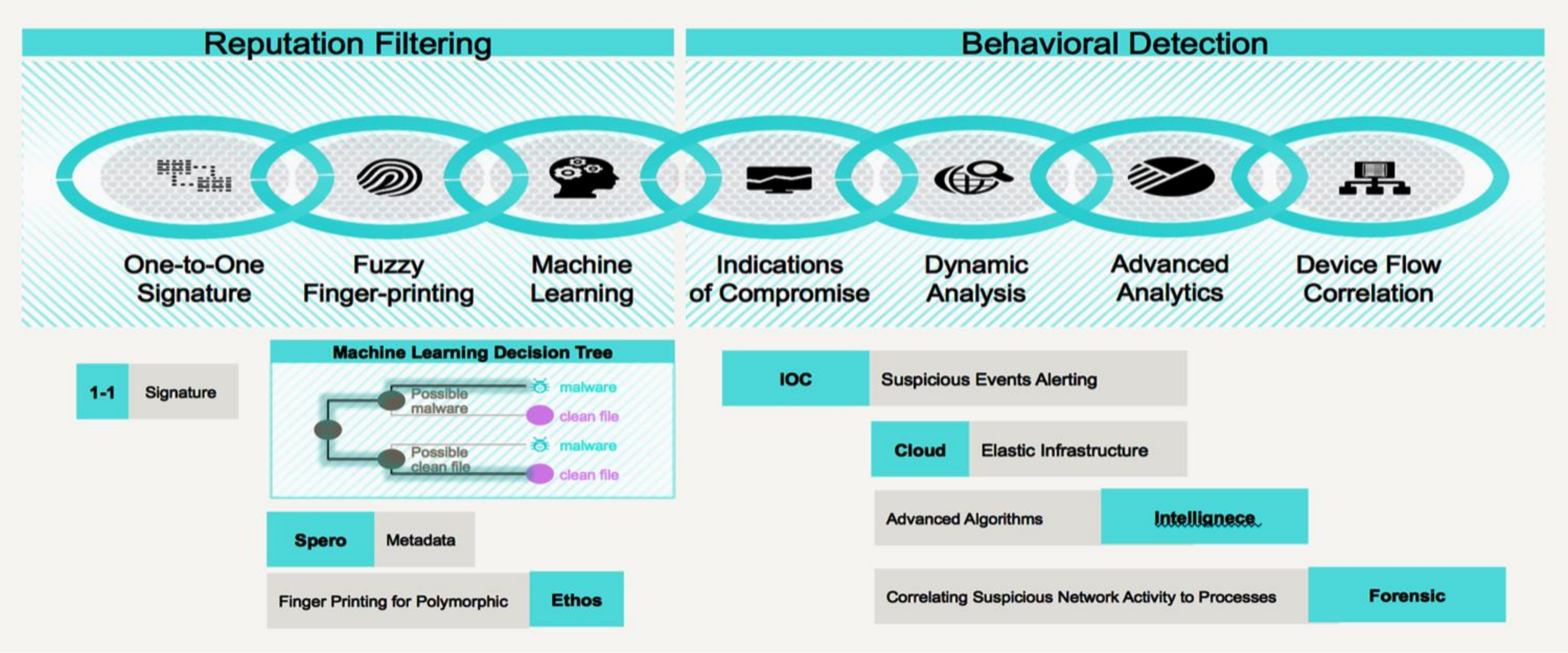
At 06:12:07, Sun May 11 2014 UTC [ less details ]

Parent file SHA-1: cea0890d4b99bae3f635a16dae71f69d137027b9.

Parent file MD5: 8b88ebbb05a0e56b7dcc708498c02b3e.

Parent file size: 2616320 bytes.

# Technologies We Use to Help us Fight Malware



## Reputation Filtering

- One-to-One Signature
- Fuzzy Finger-printing
- Machine Learning

## Behavioral Detection

- Indications of Compromise
- Dynamic Analysis
- Advanced Analytics
- Device Flow Correlation

**1-1** Signature

**Machine Learning Decision Tree**

**Spero** Metadata

Finger Printing for Polymorphic **Ethos**

**IOC** Suspicious Events Alerting

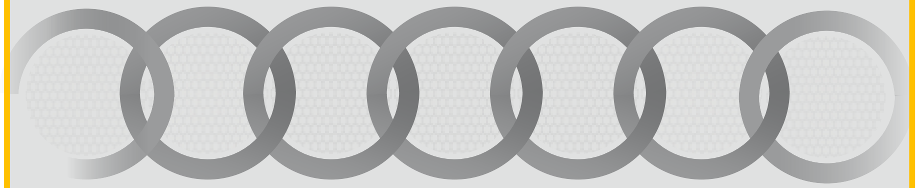
**Cloud** Elastic Infrastructure

Advanced Algorithms **Intellignece**

Correlating Suspicious Network Activity to Processes **Forensic**

# Cisco AMP Delivers A Better Approach

## Point-in-Time Detection

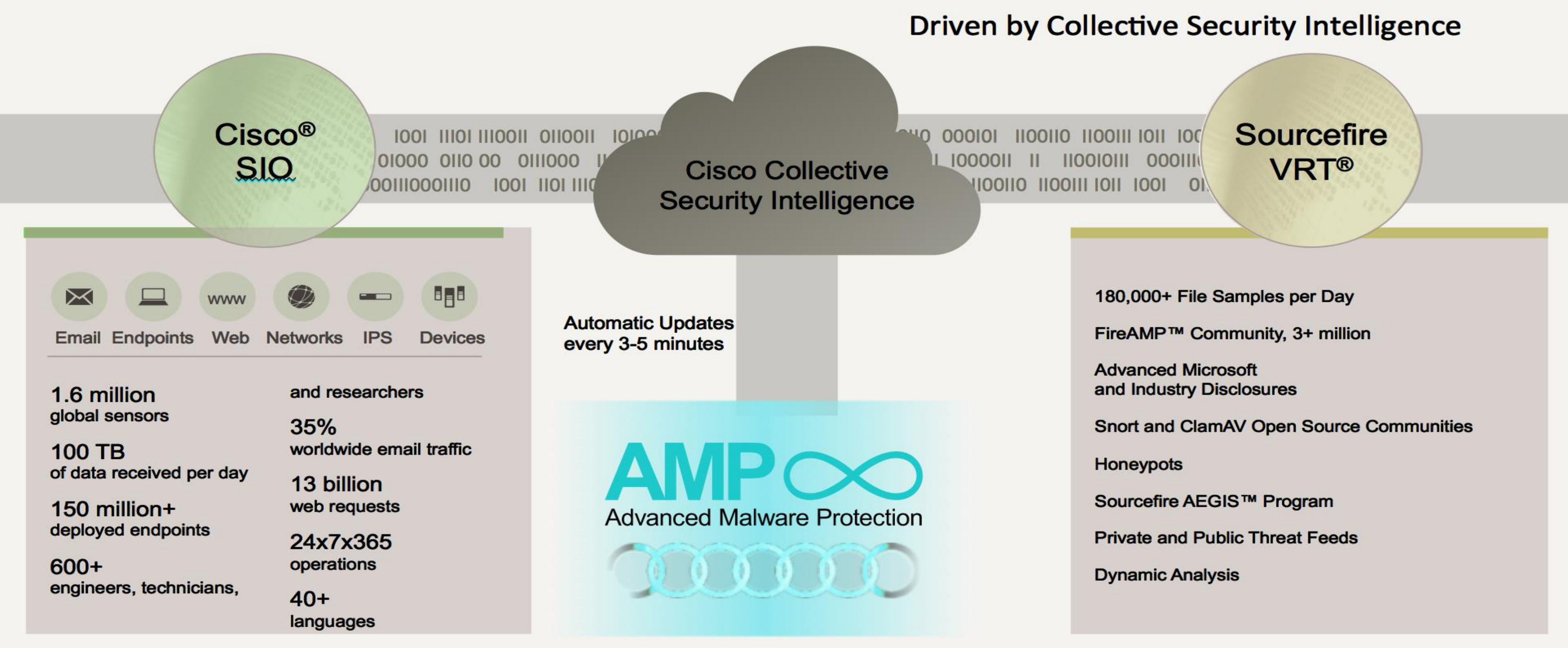


File Reputation & Behavioural Detection

## Retrospective Security

Continuous Protection

# AMP is an Important Part of the Cisco Response



Driven by Collective Security Intelligence

Cisco® SIO

Cisco Collective Security Intelligence

Sourcefire VRT®

Email Endpoints Web Networks IPS Devices

**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

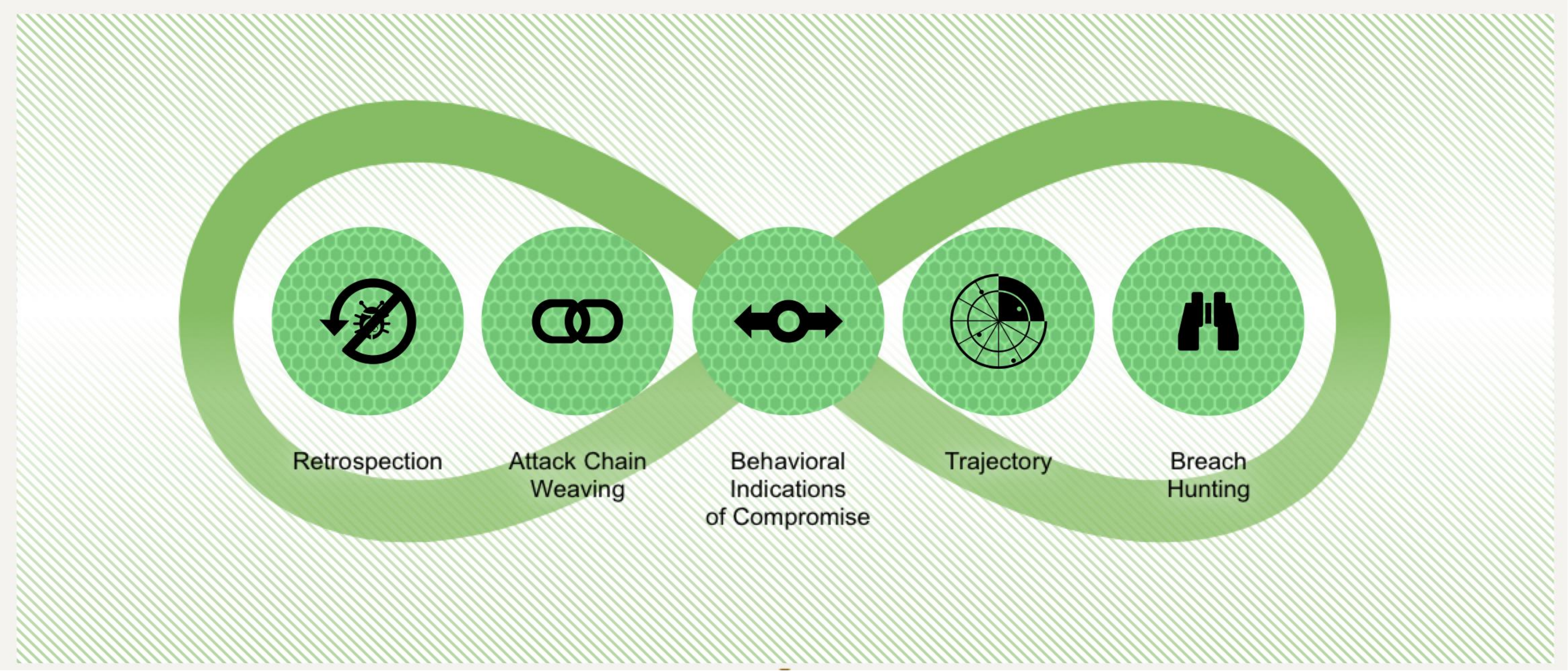
**40+**
languages

Automatic Updates every 3-5 minutes

AMP
Advanced Malware Protection

- 180,000+ File Samples per Day
- FireAMP™ Community, 3+ million
- Advanced Microsoft and Industry Disclosures
- Snort and ClamAV Open Source Communities
- Honeypots
- Sourcefire AEGIS™ Program
- Private and Public Threat Feeds
- Dynamic Analysis

# Cisco AMP Defends With Retrospective Security



Retrospection

Attack Chain Weaving

Behavioral Indications of Compromise

Trajectory

Breach Hunting

# FireAMP Agent

File Samples are only sent if configured to do so in the connector policy

**The Messaging Subsystem:**

The endpoint's MAC and IP address

The user name

Execution privilege at the time of the detection

The SHA-256 of the offending file and parent process

The name of the parent and any child processes

The time of the event

The file type

Where the file was quarantined

The username is only sent if configured to do so in the connector policy

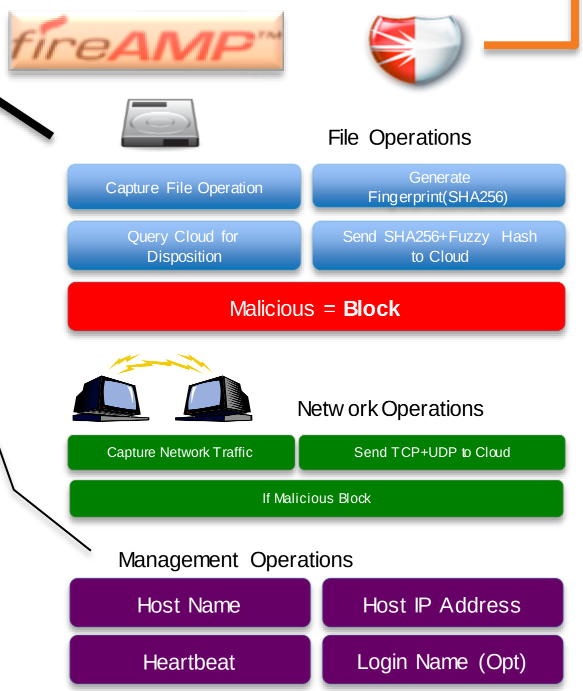
**The Ping2 Message**

**– a periodic "phone home"**

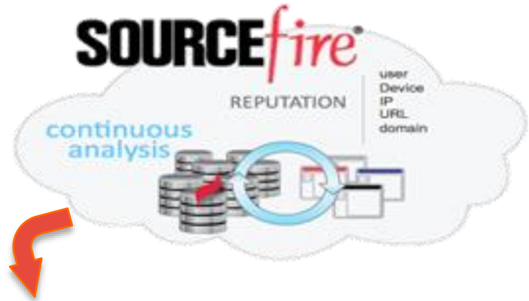
It handles retrospective detection (a.k.a Cloud Recall™)

Handles policy updates

*Other components: libclamav, Tetra*



SSL Port 443
Port 32137



**Detection Publishing – Detection**

Custom signatures pushed to the endpoint connectors.

Cross referencing of files and signatures is done in the cloud

Self-updating, which limits endpoint/cloud communications

**Large-scale data processing**

File samples are provided to the cloud for processing

Low latency for detection

Advanced analytic engines

Uses machine-learning engines to refine signatures

**Collective Intelligence**

FireAMP customer data is not shared with any other entity

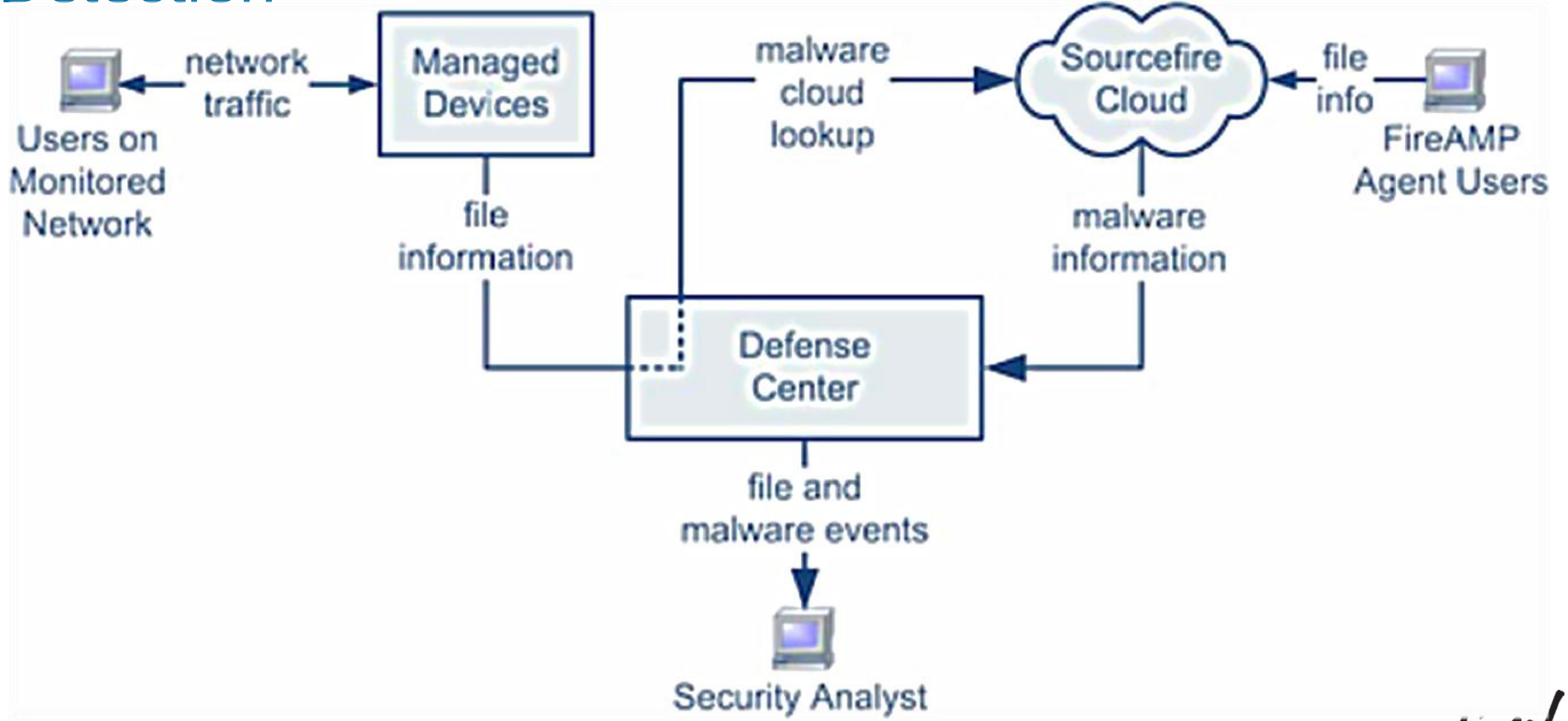
Decision making in real-time

Reporting

**Remote File Fetch**

Upload files from the clients on which they were seen to the cloud

# Combined Network-Based and Endpoint Malware Detection



“If you KNEW you were going to be compromised,
would you DO security differently?”

M Roesch

# Advanced Malware Protection

# Demo

# Q & A

# Complete Your Online Session Evaluation

**Give us your feedback and receive a Cisco Live 2015 T-Shirt!**

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm

**Learn online with Cisco Live!**
Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com

# Thank you.

cisco