



Check Point

SOFTWARE TECHNOLOGIES LTD.

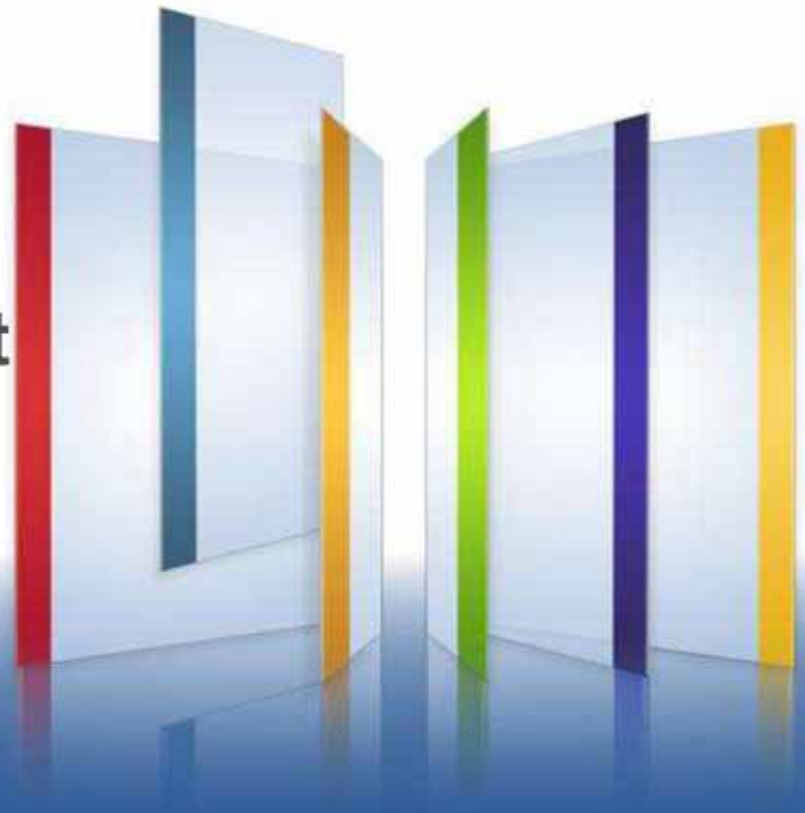
We Secure the Internet.

Securing Web 2.0 with Next Generation Web Security

Modern Threat Prevention

Rui Duro

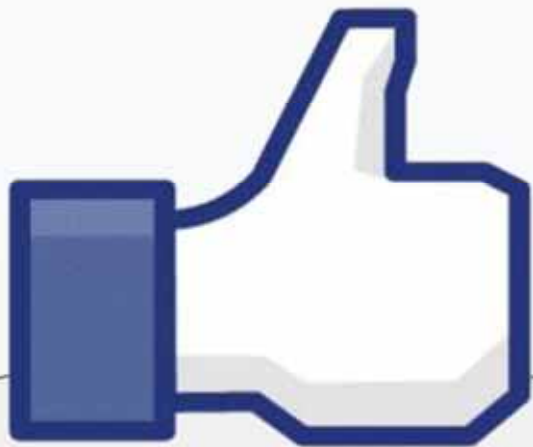
Sales Manager Portugal



Let's take a minute...



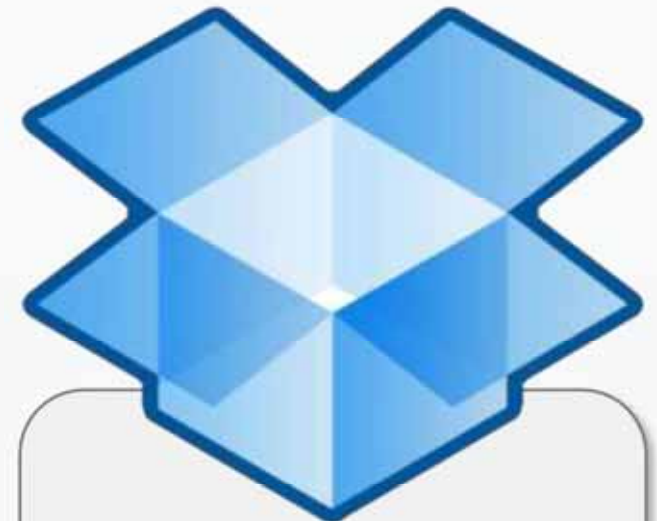
In an Internet Minute:



**1.9 Million
Likes**



**92,593 Hours
Viewed**



**694,444 Files
Uploaded**

The Web Evolves as Attack Vector:

Sites compromised to spread malware



Applications might pose security risk



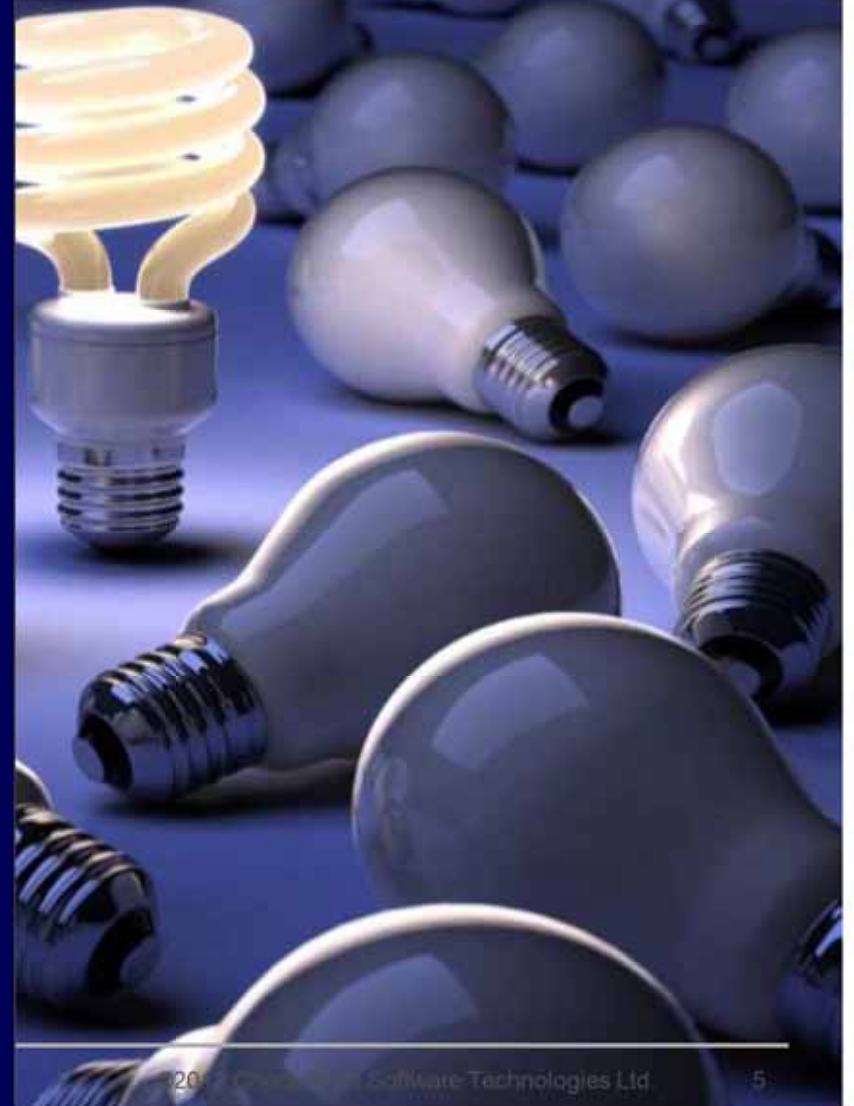
Sensitive data might be lost



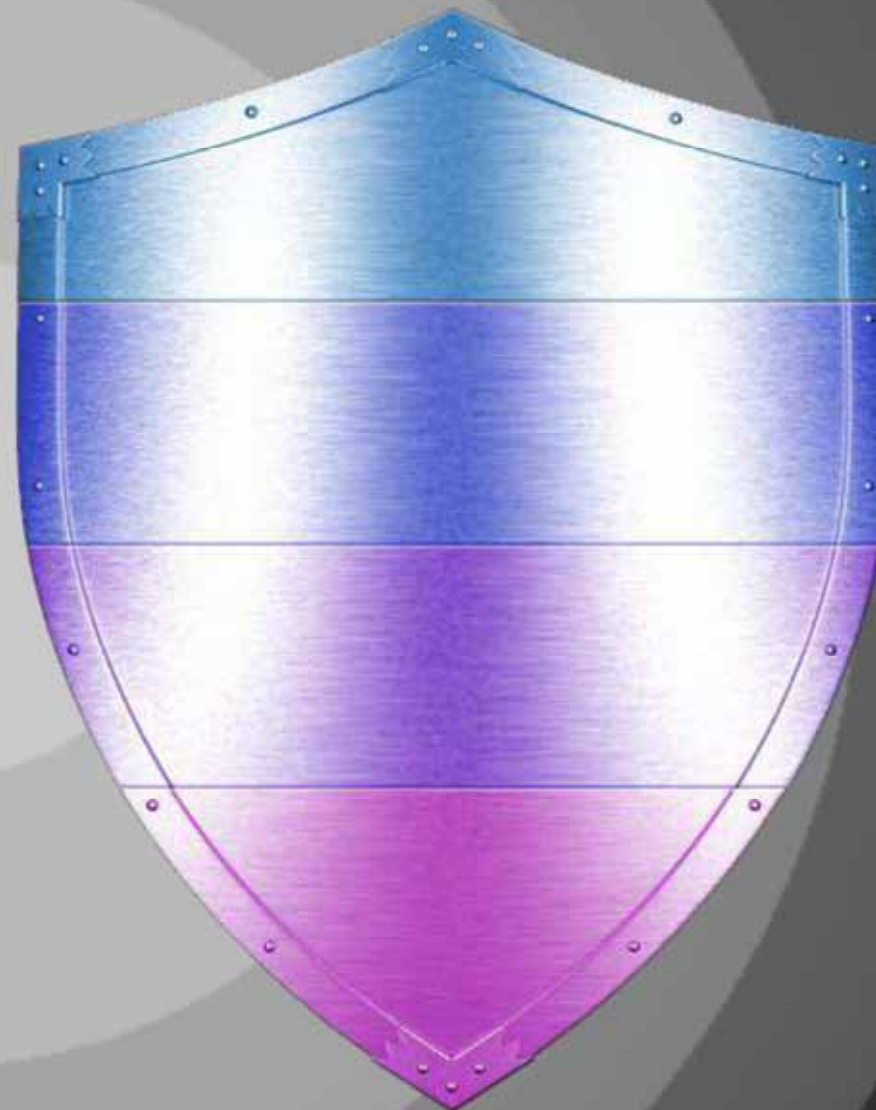
Social networks used in attacks



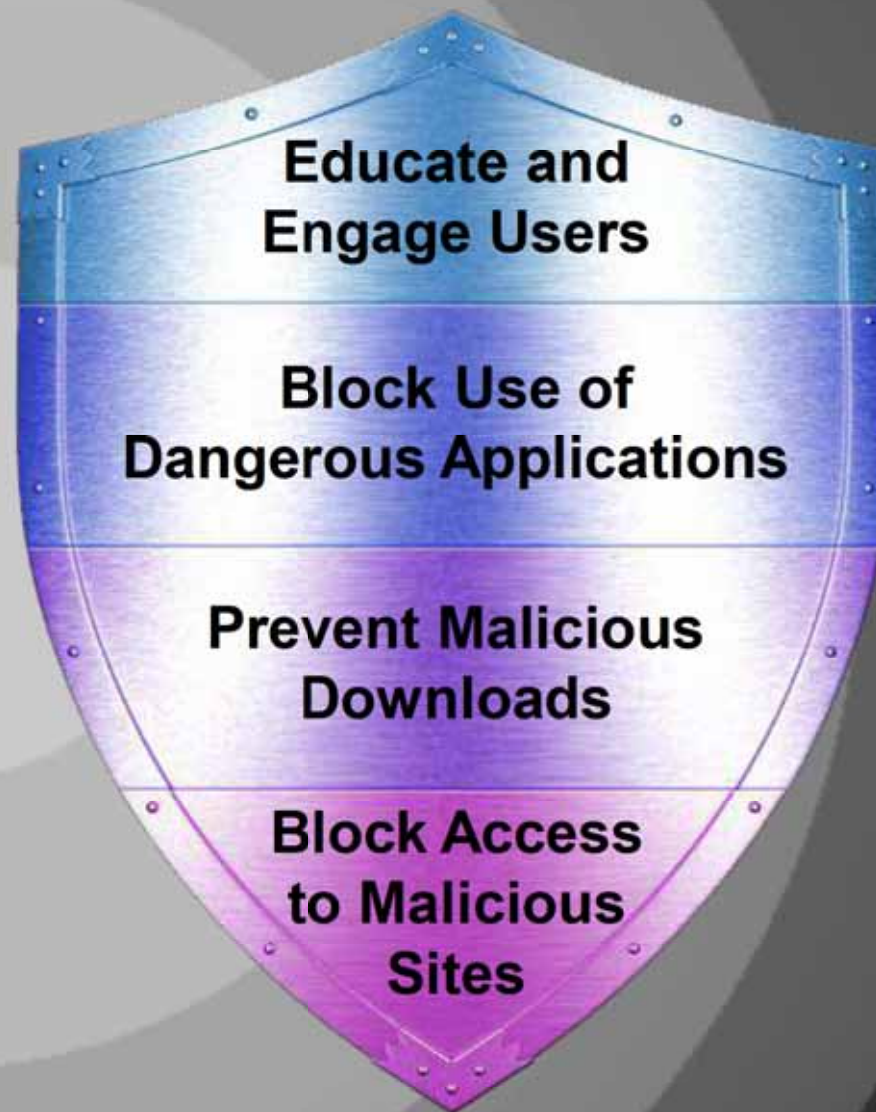
A New Approach Is Needed!



Multi-Layered Web Security



Check Point's Next Generation Secure Web Gateway



Layered Defenses & Software Blades



Legitimate Sites Compromised to Spread Malware



**“NBC Websites Hacked To Serve Citadel
Financial Malware”**

Information Week, February 22, 2013 09:50 AM

But Web is More Than Just URLs...

In **61%** of organizations,
a **P2P file sharing** application is used



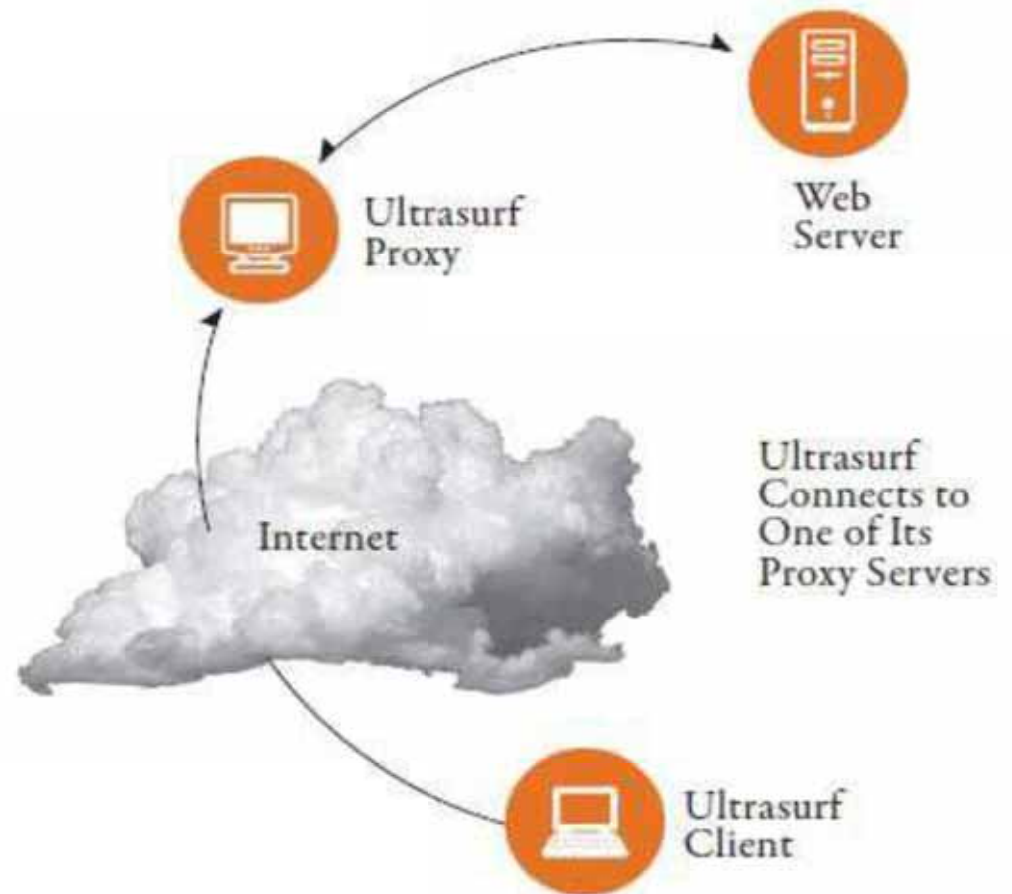
Heavily used to spread malware

Open back doors to the network

Legal liability for illegal downloads

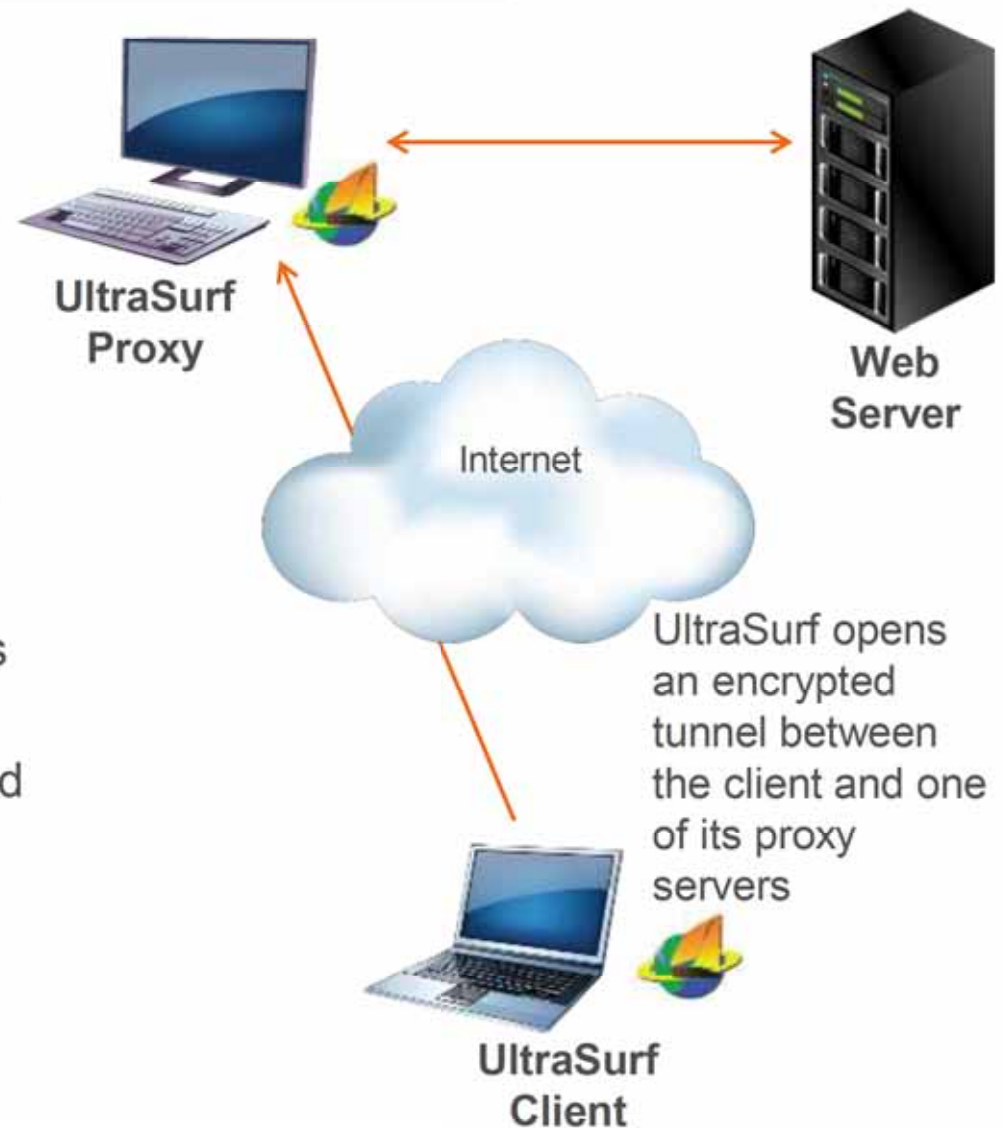
Anonymizers Used to Bypass the Security Policy

Some Applications are Highly Evasive!



UltraSurf Overview

- UltraSurf is a proxy client, originally aimed to bypass internet censorship to browse the internet freely.
- UltraSurf also has a very resilient design for discovering proxy servers:
 - A hard coded list of proxy server IPs built into the program
 - DNS requests, which return encoded IPs of proxy servers
 - Encrypted document on Google Docs / Amazon cloud
 - A cache file of proxy server IPs



Does Your Secure Web Gateway Look only at URLs?!

You Can't
Afford
to Look Only
Under the
Lamppost!



Control All Aspects of Web



[http://www](http://www.playboy.com)
www.playboy.com
www.playboyfootball.com

URL Filtering



Not URL-based
beyond URLs

Application Control

Application Control Software Blade



- Detect and Control
 - ✓ Over **4,900** Applications
 - ✓ Over **240,000** Social Network Widgets
 - ✓ Over **130** Categories
- User-defined applications
- User and user-group granularity

Appwiki.checkpoint.com

URL Filtering Software Blade



















- Over **200 million** URLs
- Constantly updated
Cloud-based categorization
- User-defined Sites/Categories
- User and user-group granularity

Check Point Unifies URL Filtering and Application Control

 User/Group Granularity!

 Websites - URL Filtering



Source	Applications/Sites	Action
 Any	 Sex	 Block  Blocked Message
 John_Adams_Role	 TeamViewer	 Allow
 Marketing	 Vimeo  YouTube	 Ask  Company Policy  Once a day
 Any	 Unknown Traffic	 Block

 Applications - Application Control

 User Check Actions

Sharing is Not Always Caring...

80% of organizations use file storage and sharing applications

“Our investigation found that usernames and passwords **recently stolen** were used to sign in to Dropbox accounts”

Dropbox blog, July 31, 2012



Check Point's Next Gen Secure Web Gateway

Granularly Control Features Within Applications

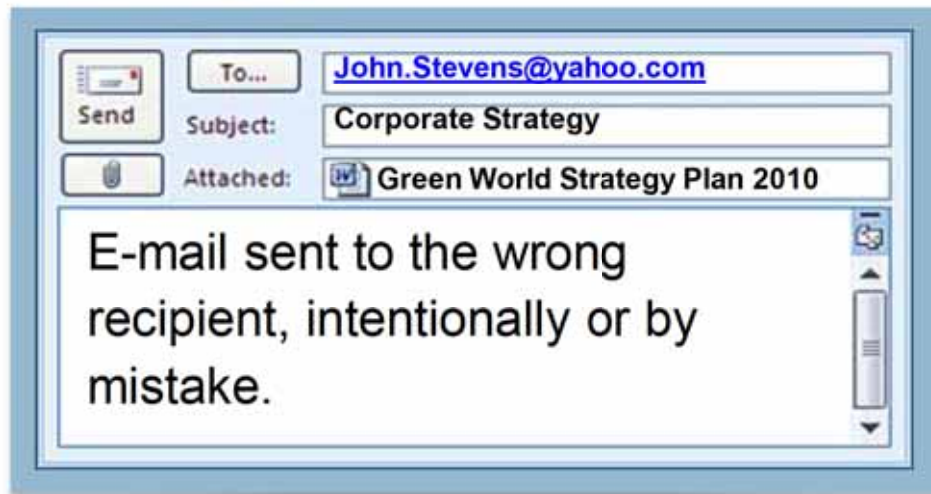


Applications/Sites	Action
 Amazon Cloud Drive-upload	 Block
 Box-uploading	 Blocked Message
 Dropbox-web upload	
 Google Docs-uploading	
 YouSendIt-upload	

Add DLP for extended data protection!



What is DLP?



Data breaches have happened to all of us

Social Media Used as Attack Vector



Spread malware



Gather information to be used
in targeted attacks

Blocking Won't Help...



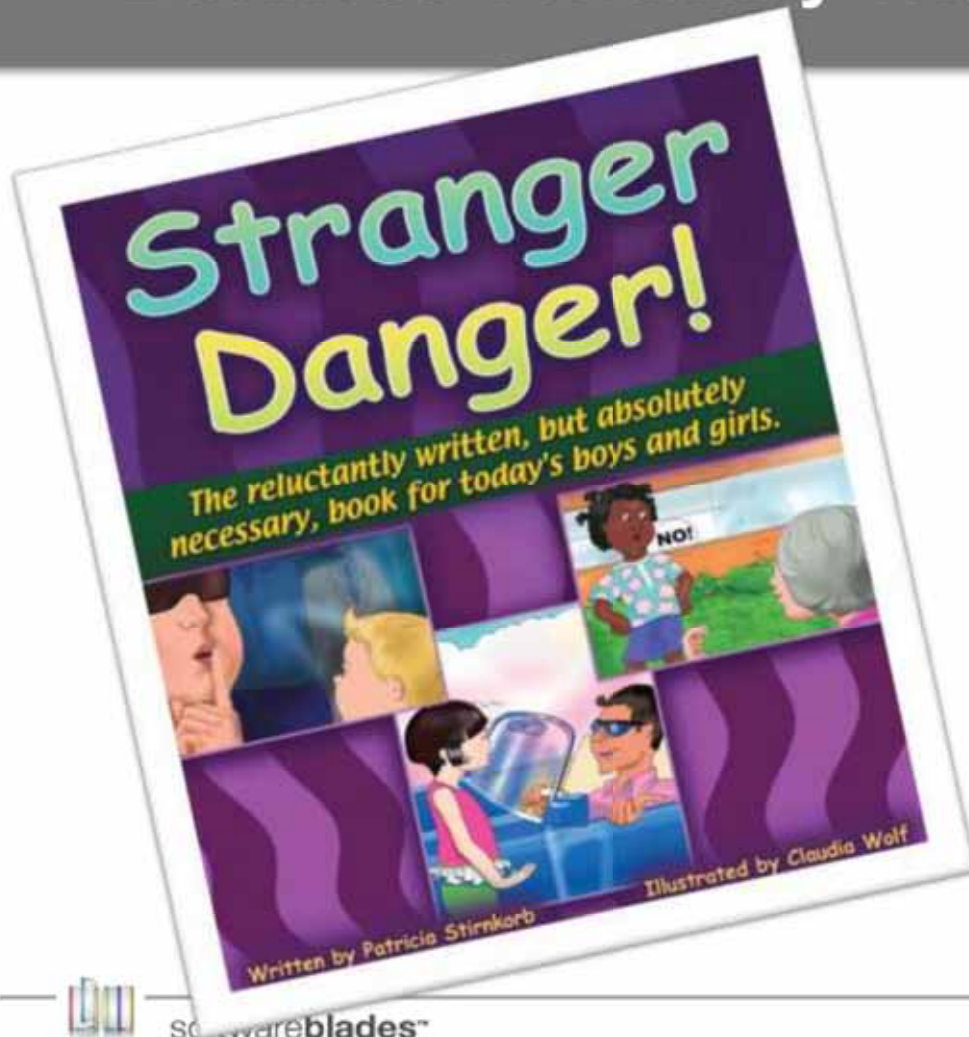
Sales



Engineer

Social media increasingly used in the business!

Does Your Secure Web Gateway Allow Business Continuity While Maintaining Security?



Kids know not to take candy
from strangers...

...Education is key!



Check Point's Next Gen Secure Web Gateway

Using Social Media Safely

Easily Educate and Engage End-Users

Before proceeding to use **Facebook**, please be aware:

- Fake Rihanna videos are actually a **virus** - **don't click!**
- **Cyber-criminals** might use Social Networks to gather information in preparation for an attack - **don't accept** friends you don't personally know!

OK, I Understand

Cancel

OK

Elementary...



Monitoring, analysis and reporting—
a critical part of Web security

Check Point's Next Gen Secure Web Gateway



Count	Application / Site	Primary Category
18	Facebook	Social Networking
33	YouTube	Video Streaming
24	google.com	Search Engines / Portals
4	pcmag.com	Computers / Internet
2	iTunes	Multimedia
8	metacafe.com	Media Sharing
11	LinkedIn	Social Networking

Web Browsing: ✔ Allow Copy Details Go to Policy...

Hannah Hash (204.0.0.52)
 metacafe.com (Media Sharing)
 Allow
 Today at 01:18:35

- Event Description:**
 Hannah Hash accessed metacafe.com today at 01:18:35
- Additional Data:**
 Rule Name: [Go to Policy](#)
 Data Transferred: 24.69 MB
 Origin: United States-gateway (75.0.1.245)



Check Point's Next Gen Secure Web Gateway

Executive Summary Reports:

3. Top Categories by Browse Time

5. Top Users and their Top Applications / Sites by Browsing Time

Top Users and their Top Applications / Sites by Browse Time						
User	Application / Site	Category	Risk	Bytes	Sessions	Browse Time (hh:mm:ss)
Eugenia Eyelash	YouTube	Video Streaming	2-Low	16.46 MB	1	12:10:11
	Windows Live Writer	Multimedia	2-Low	250.1 KB	1	02:33:44
	funnyjunk.com	Media Sharing	0-Unknown	53.46 KB	1	01:30:00
	metacafe.com	Media Sharing	0-Unknown	33.03 KB	1	01:21:00
	Total (4)				16.79 MB	4
Hayden Hash	YouTube	Video Streaming	2-Low	13.91 MB	1	00:41:10
	google.com	Search Engines / Portals	0-Unknown	69.15 KB	1	00:33:00
	metacafe.com	Media Sharing	0-Unknown	33.03 KB	1	00:20:11
	Total (3)				14.01 MB	3



Check Point's Next Gen Secure Web Gateway

Detailed user and group activity reports:

User Activity Report

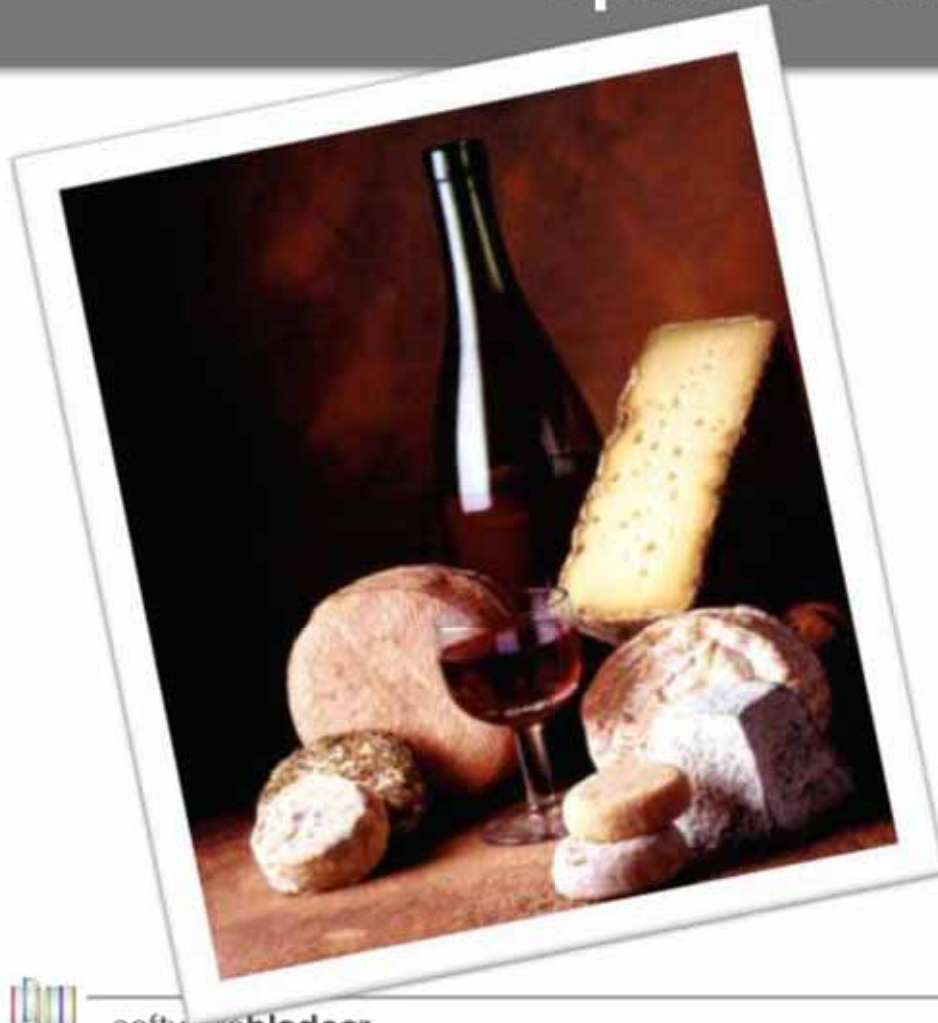
May 01, 2012 12:00 AM - May 14, 2012 11:59 PM
 User: Jared Josh(jaredjosh@myBiz.com)

(1 out of 2)

Start Time	Application / Site	Risk	Category	Action	Traffic	Browse Time
14-May-2012 04:31:10 PM	Facebook	2 Low	Social Networking	Allow	12.3MB	00:23:47
14-May-2012 04:33:15 PM	bettingsitesreview.com	Unknown	Gambling	Allow	3.6KB	00:19:47
14-May-2012 04:41:12 PM	espn.com	Unknown	News / Media	Allow	3.6KB	00:19:47
14-May-2012 04:55:00 PM	YouTube	2 Low	Video Streaming	Allow	207.5MB	00:19:27
14-May-2012 05:01:12 PM	Gmail	3 Medium	Webmail	Allow	4KB	00:13:44
14-May-2012 05:02:28 PM	LinkedIn	2 Low	Social Networking	Allow	3KB	00:13:58
14-May-2012 05:05:10 PM	Twitter	2 Low	Social Networking	Allow	136MB	01:18:44
14-May-2012 05:22:33 PM	mIRC	4 High	Instant Messaging	Block	0B	00:00:00
14-May-2012 05:23:12 PM	Time.com	Unknown	News / Media	Allow	39.5KB	00:03:44



Does Your Secure Web Gateway Download Protection Updates Once a Day?!



Sometimes old is fine...

...Not in security!

Check Point's Next Gen Secure Web Gateway

Powered by Threat Intelligence

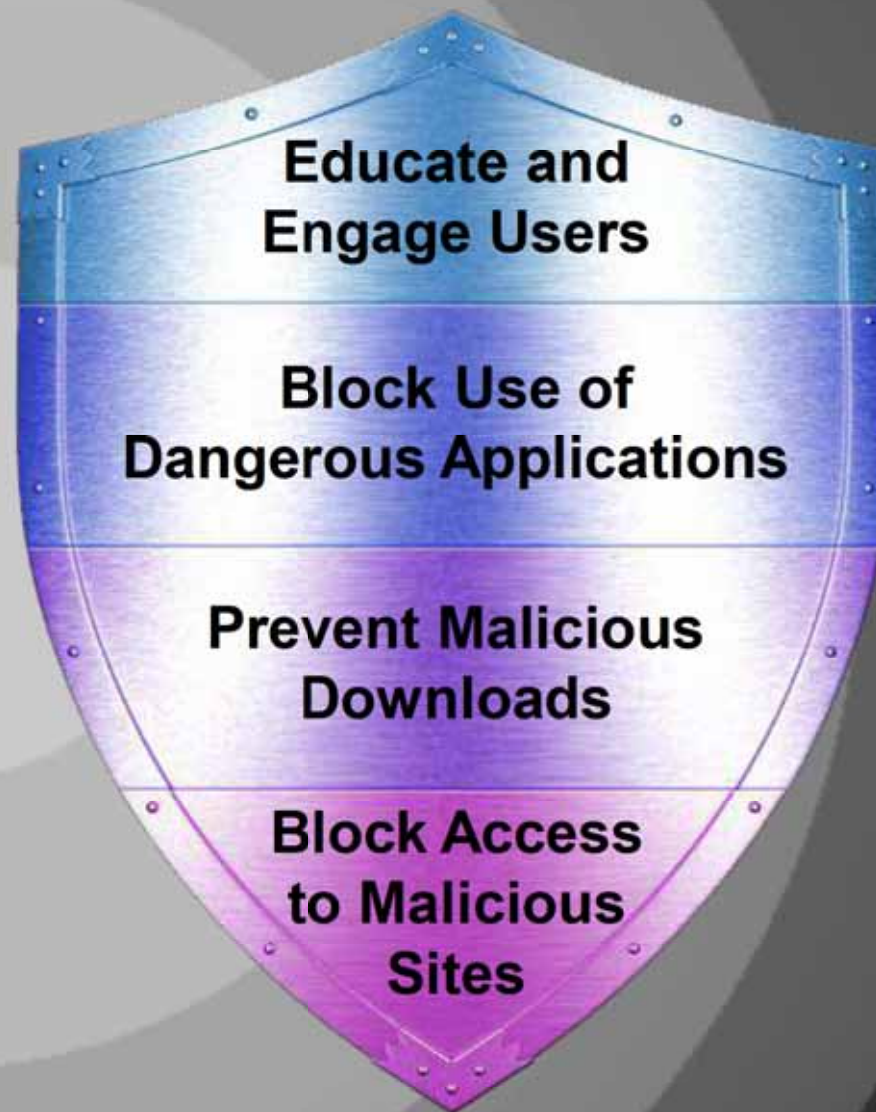


URL Filtering
constantly updated

Antivirus uses ThreatCloud—
a vast, collaborative threat
intelligence repository



Check Point's Next Generation Secure Web Gateway



Layered Defenses & Software Blades

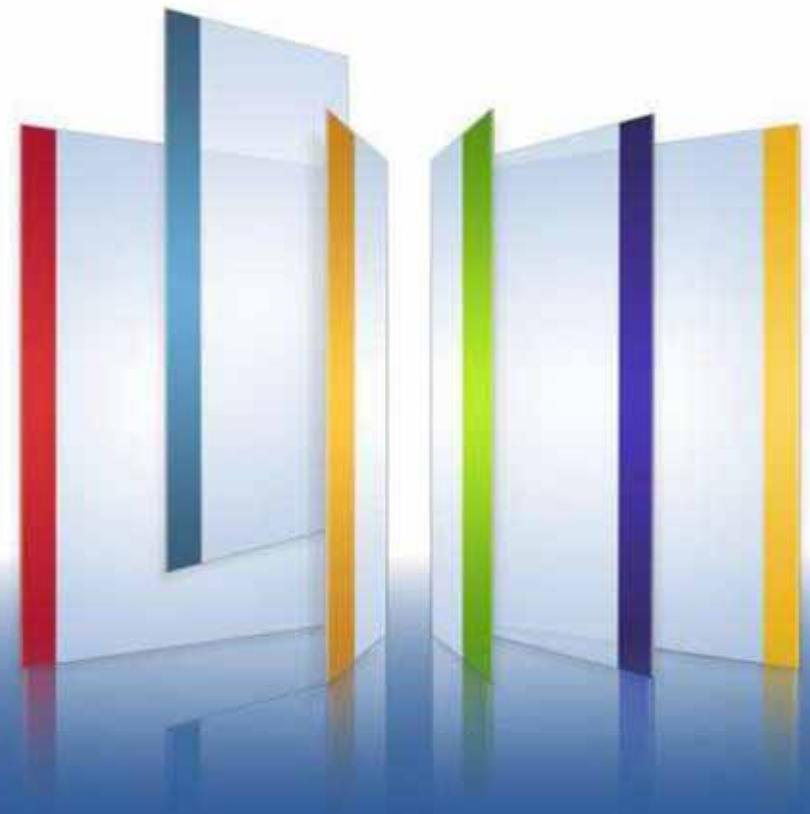




Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Modern Threat Prevention



Growing Security Challenges

Growing
Network
Complexity


Advanced Targeted
Attack





Growing Attacks
Sophistication


Growing
Regulatory
Requirements

Agenda

-  Examine Three Real Attacks

-  The Economy Behind Attacks

-  3 Modern Threat Prevention

-  4 Summary

Let's examine three real cases

Stuxnet – attack on Iran Nuclear Plant

Attack on RSA and Lockheed Martin

Syrian Attack



Let's examine three real cases

Stuxnet – attack on Iran Nuclear Plant

Attack on RSA and Lockheed Martin

Syrian Attack



Stuxnet

Drop Malware



Reprogram Controller (Payload)



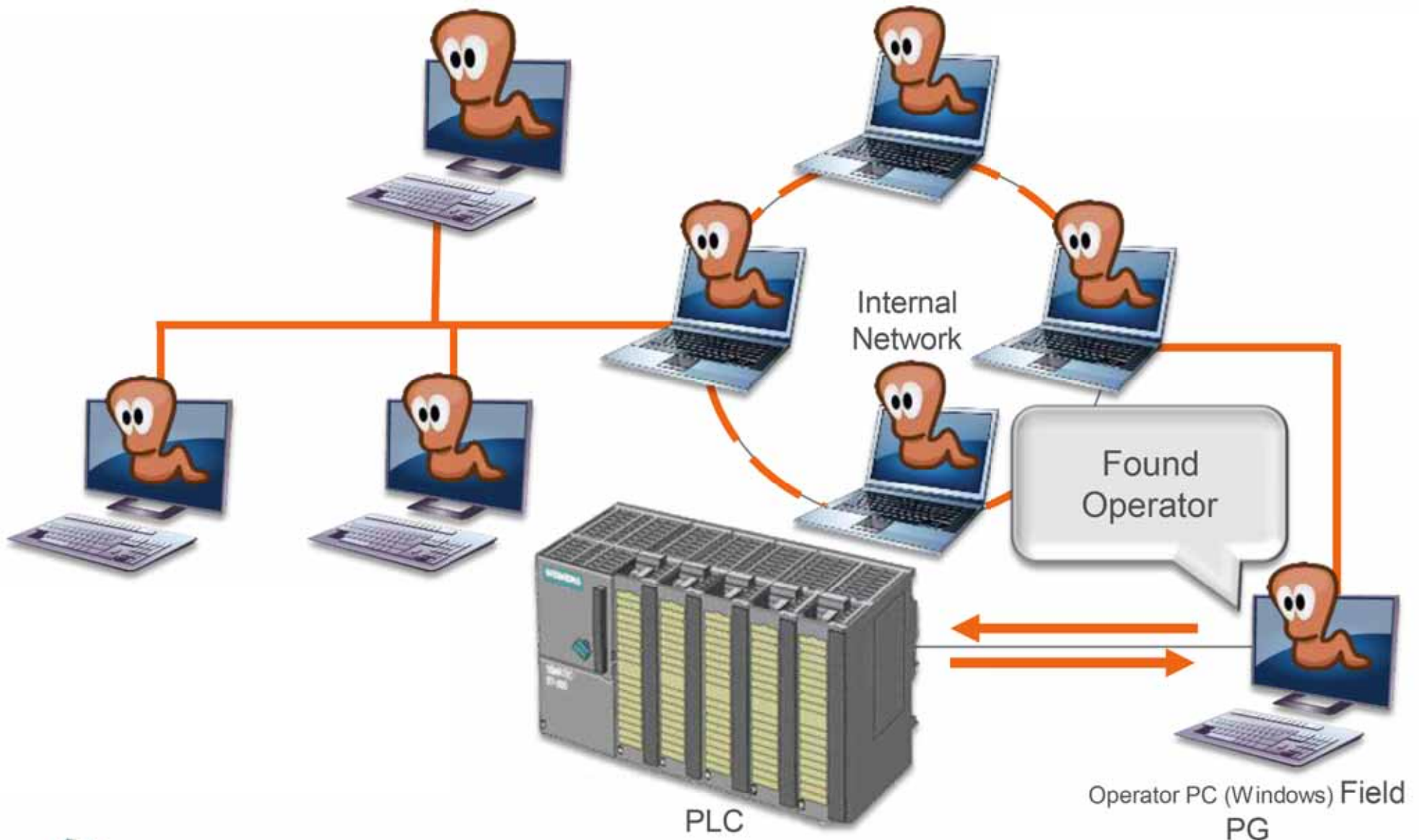
Mission Goal: No Nukes



Target: Centrifuge in Natanz



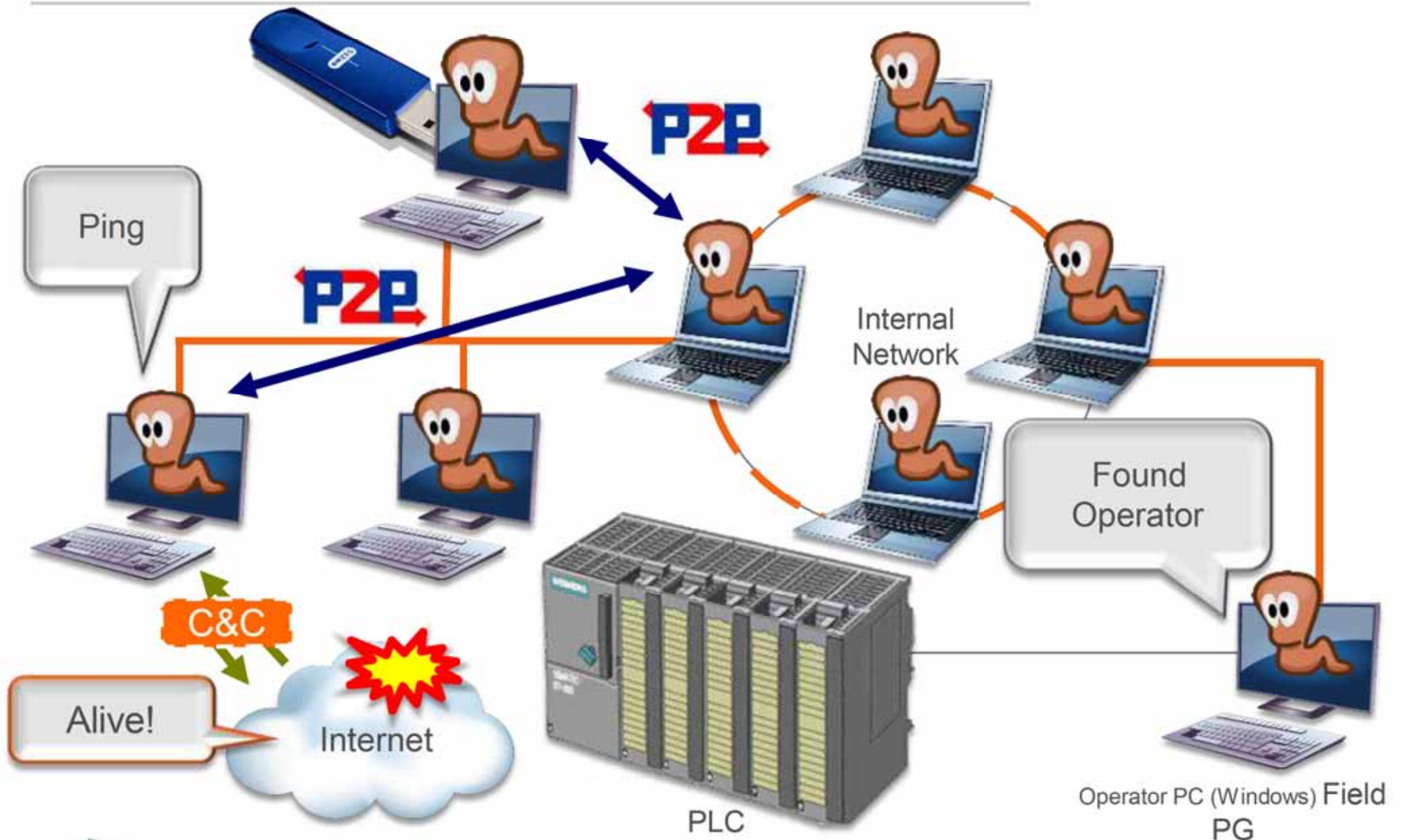
What's Going To Happen?



Step #1: Introduce Threat To Target Network



Step #2: Propagate



Step #3: Infecting The Target

When Stuxnet Reaches a Field PG,
It Installs a Trojan Horse That:

- Monitors PLC commands being written and read
- Infects a PLC by inserting bad commands
- Masks the fact the PLC is infected

Let's examine three real cases

Stuxnet – attack on Iran Nuclear Plant

Attack on RSA and Lockheed Martin

Syrian Attack



About RSA SecureID®

- RSA is the Security Division of EMC²
- Offers a variety of security solutions
(Access Control, DLP, Fraud Prevention etc.)
- Flagship product – SecureID
 - Benchmark for secure authentication solution
 - OTP Generator
- Two components:
 - Encryption algorithm
 - Symmetric key for encryption (seed)



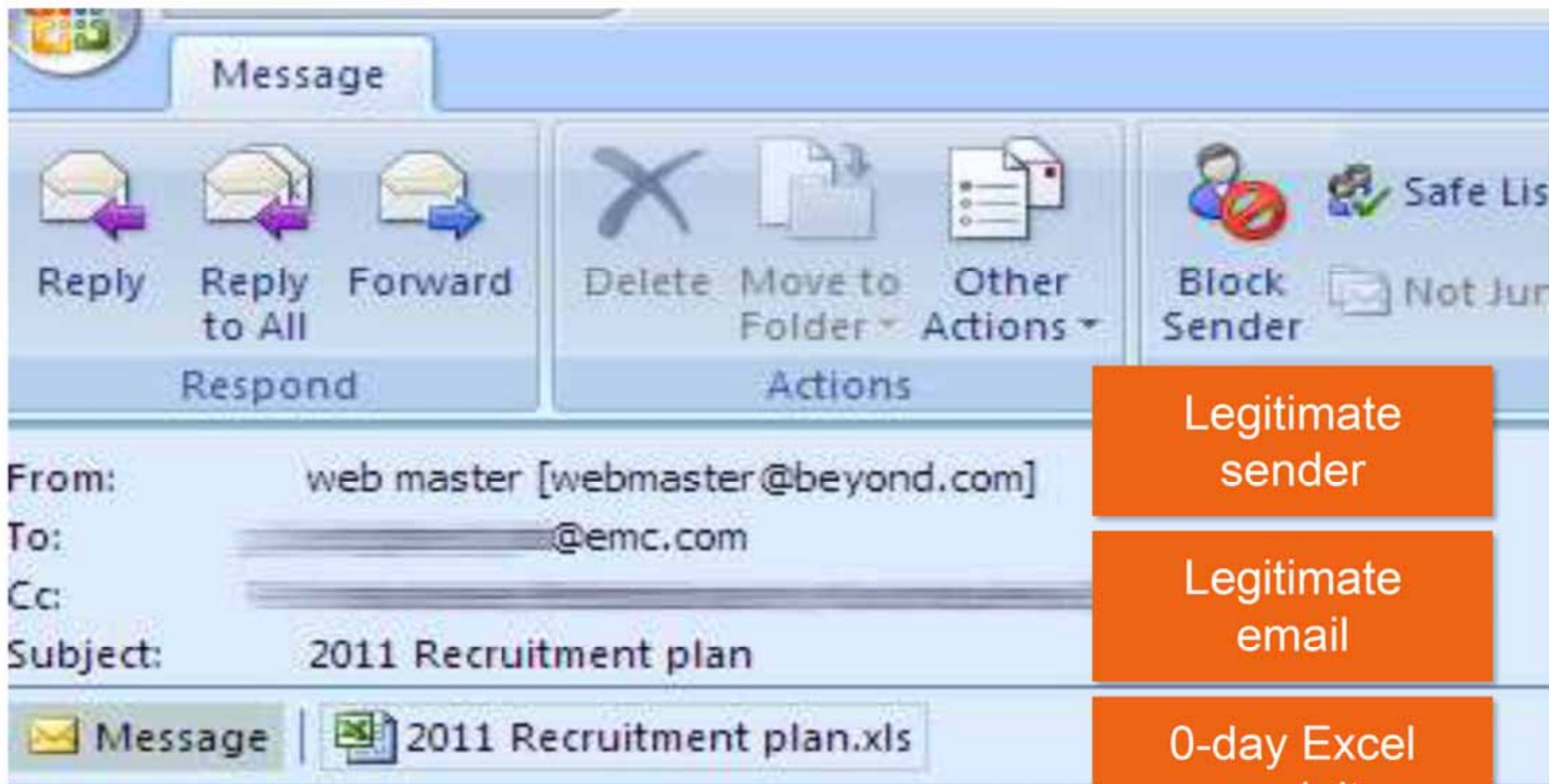
Lockheed: a staged attack

RSA

SOCIAL

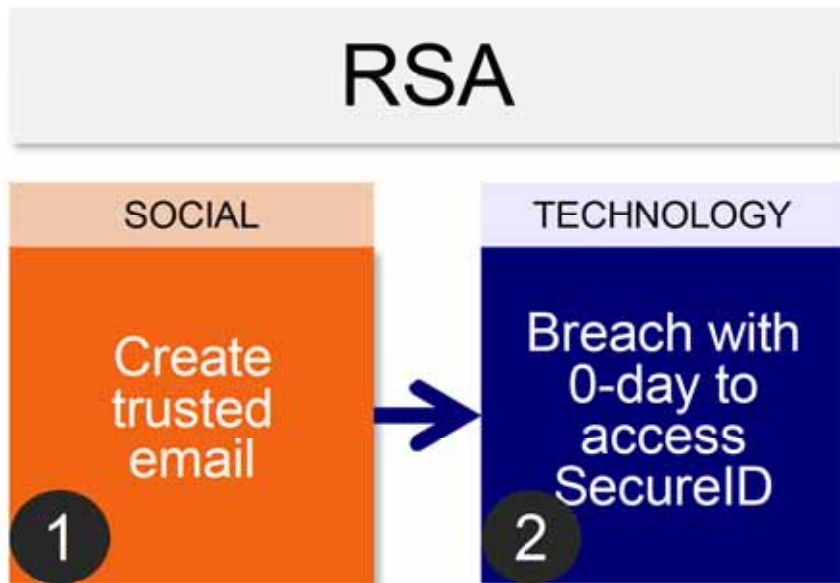
Create
trusted
email





I forward this file to you for review. Please open and view it.

Lockheed: a staged attack





Hackers get access to SecurID tokens used to protect an estimated 40M employees of large enterprises



**RSA hack enabled
2 more attacks**

27

MAY

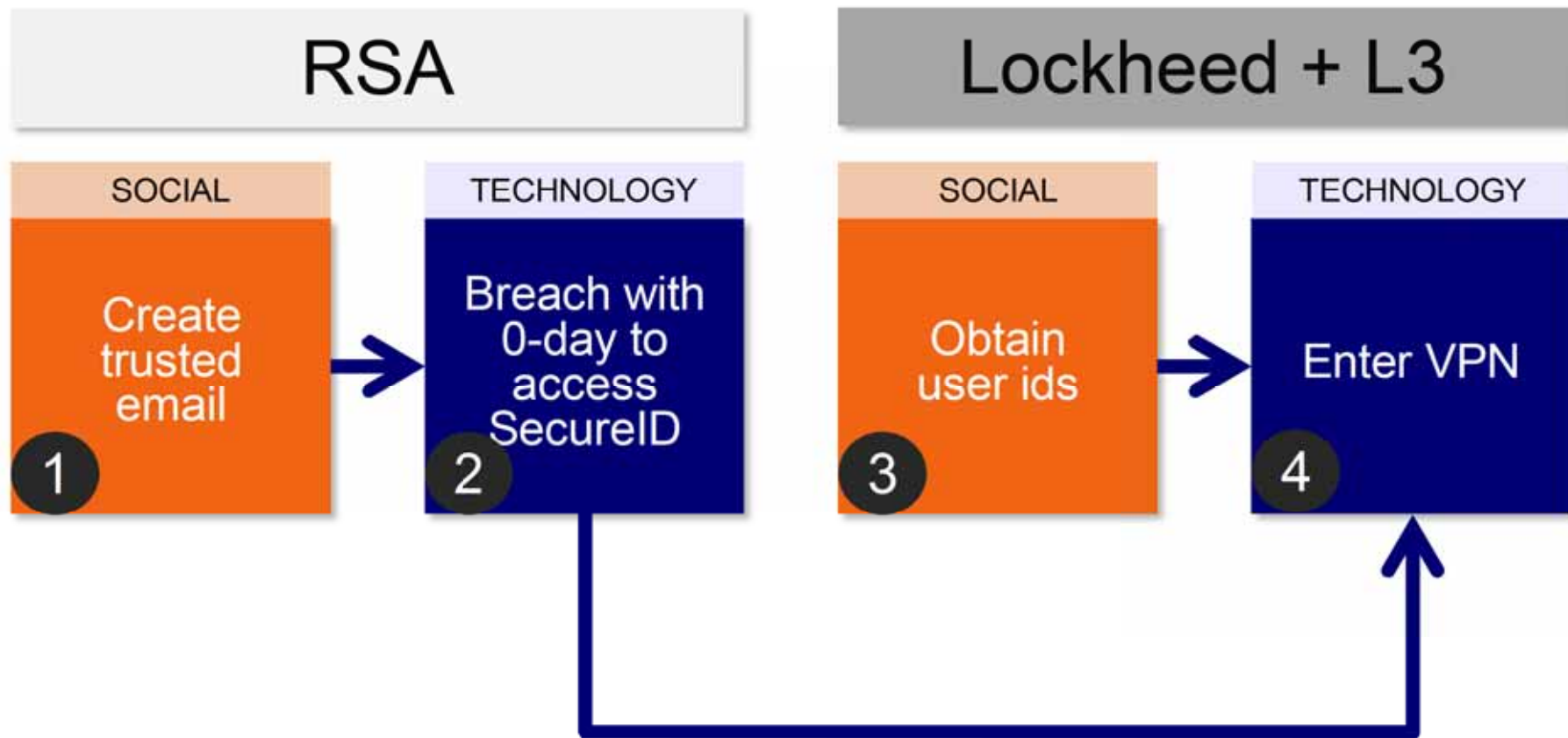
**Lockheed
Martin**

01

JUN

L3

Lockheed: a staged attack



Let's examine three real cases

Stuxnet – attack on Iran Nuclear Plant

Attack on RSA and Lockheed Martin


Syrian Attack


The Attack Against the Syrian Ministry of Foreign Affairs





- Leaked from Syrian Ministry (by Anonymous)
- CVE-2010-0188 – tiff vulnerability in PDF
- Installs custom built malware
- Sent from a proxy in Seoul, Korea
- C&C Communications to China



-  Examine Three Real Attacks

-  The Economy Behind Attacks

-  3 Modern Threat Prevention

-  4 Summary

2012 Top Vulnerable Applications



Adobe Reader

30 Critical
Exploits



Java

17 Critical
Exploits



Microsoft Office

16 Critical
Exploits



Adobe Flash

57 Critical
Exploits



Firefox



Internet Explorer





Exploit Price List


ADOBE READER	\$5,000-\$30,000
MAC OSX	\$20,000-\$50,000
ANDROID	\$30,000-\$60,000
FLASH OR JAVA BROWSER PLUG-INS	\$40,000-\$100,000
MICROSOFT WORD	\$50,000-\$100,000
WINDOWS	\$60,000-\$120,000
FIREFOX OR SAFARI	\$60,000-\$150,000
CHROME OR INTERNET EXPLORER	\$80,000-\$200,000
IOS	\$100,000-\$250,000




Agenda

-  Examine Three Real Attacks

-  The Economy Behind Attacks

-  3 Modern Threat Prevention

-  4 Summary

Threat Prevention

Full Coverage of Attack Vectors and Surfaces

Implement Controls

		Manual					
		DDoS					
		Malware					
Indicator Sharing	Correlation	Signatures	IPS	Anti-DDoS	Anti-Virus	Anti-Bot	Threat Emulation
		Reputation	IPS	Anti-DDoS	Anti-Virus	Anti-Bot	Threat Emulation
		Behavior	IPS	Anti-DDoS		Anti-Bot	Threat Emulation
		Emulation				Anti-Bot	Threat Emulation
		Human Validation	IPS	Anti-DDoS	Anti-Virus	Anti-Bot	Threat Emulation
		Known / Unknown					
		Network / Servers / Clients					

Endpoint Security, IPS and Network A/V are the first layers of Defense

INFILTRATION

USB STICK
AUTORUN

PROPAGATION

0-DAY
EXPLOIT

WORM USING
KNOWN EXPLOITS

Endpoint security can block the use of non-encrypted USB sticks

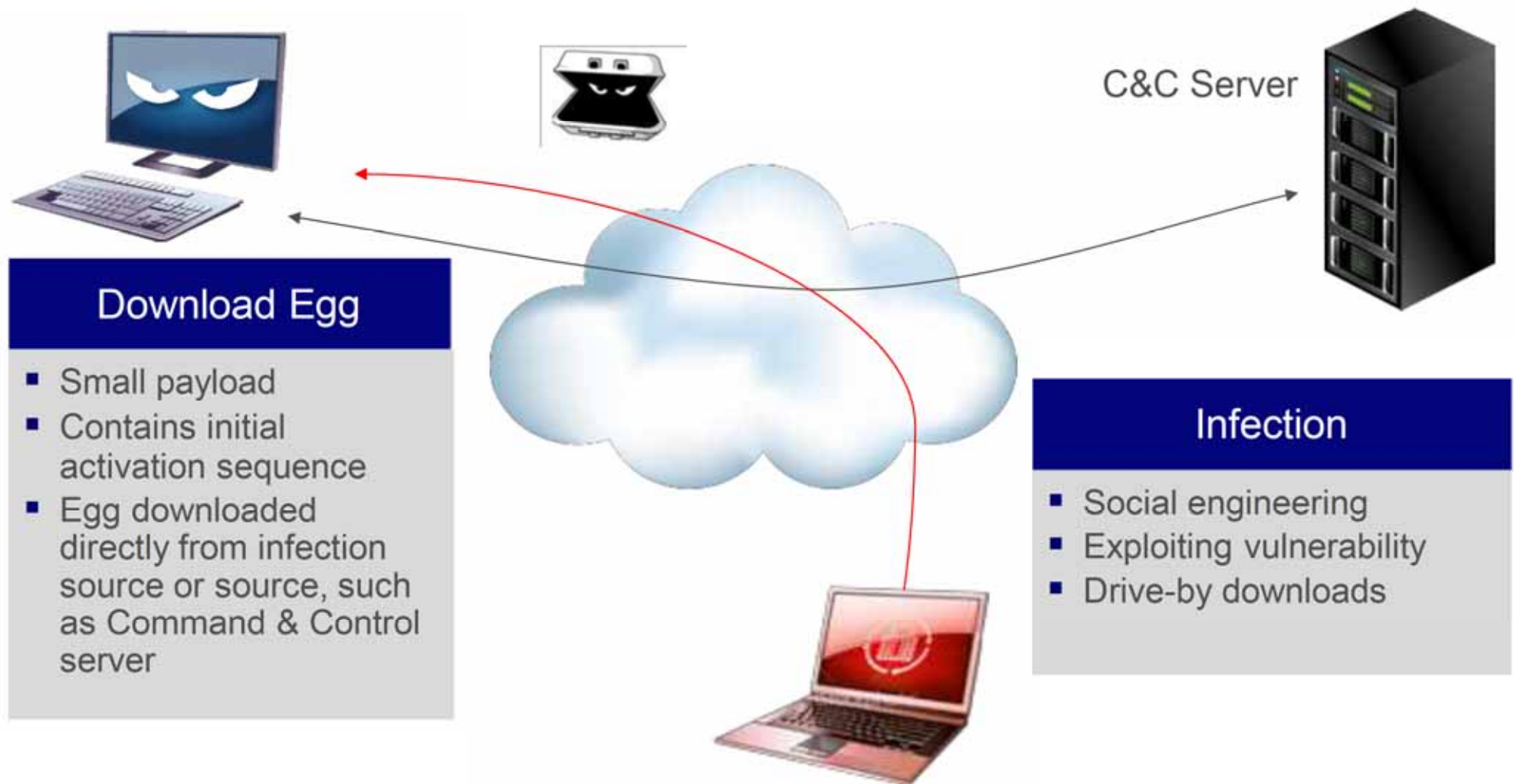


IPS can block the propagation of the worm



You can still get infected...

Botnet Operation: The Infection

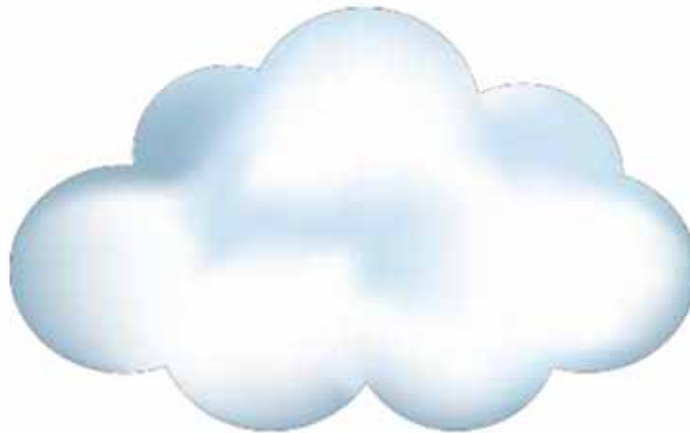


Botnet Operation: Self -Defense



Self Defense

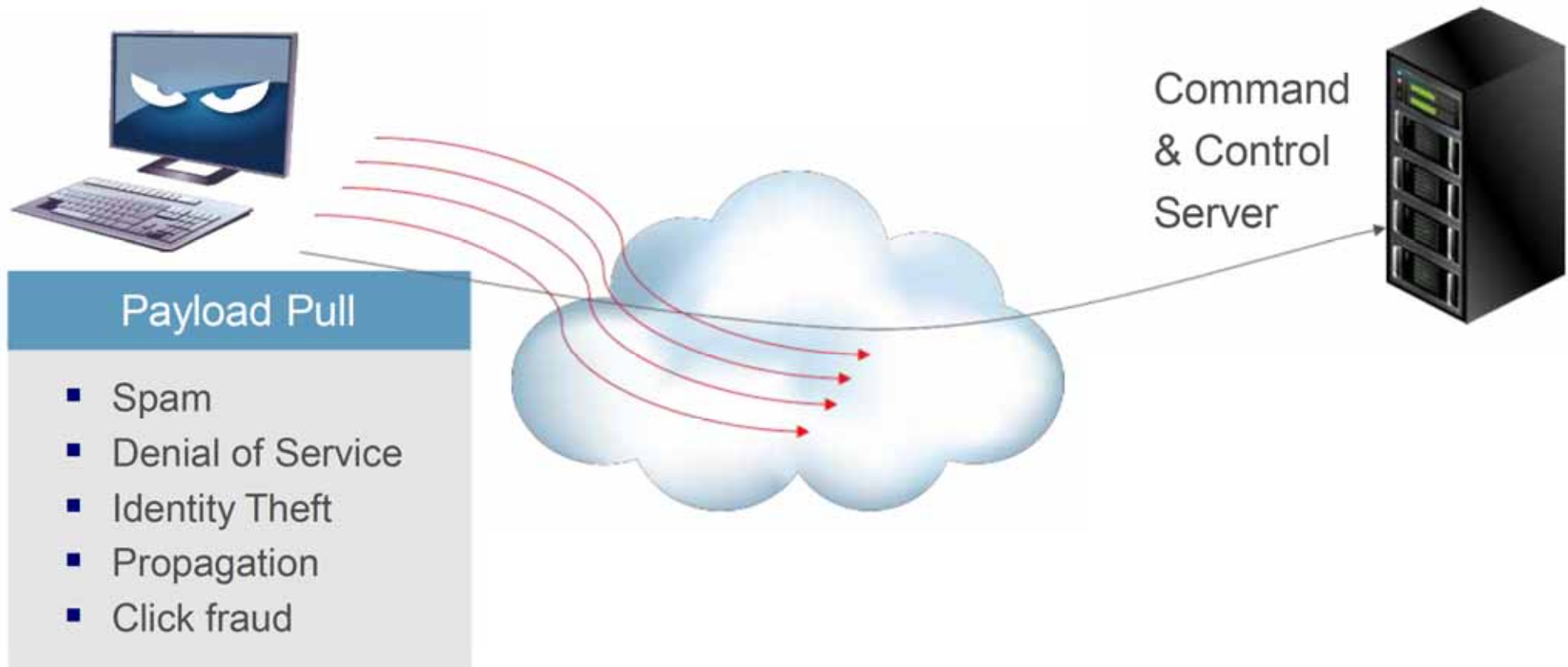
- Stop Anti-Virus service
- Change "hosts" file
- Disable Windows Automatic Updates
- Reset system restore points



Command
& Control
Server



Botnet Operation: The Damages





Anti-Bot Software Blade

DISCOVER and STOP Bot Attacks

Discover
Bot infections

Multi-tier
discovery

Command and
Control
IP/URL/DNS



Communication
patterns



Attack
signs and types



Prevent
Bot damage

Stop traffic to
remote operators



Investigate
Bot infections

Extensive
forensics tools



Maximum security with
multi-gig performance

1

- Detect Command & Control sites and drop zones
- Over 250 millions addresses in ThreatCloud™
- Real time updates

2

- Over 2000 bots' family unique communication patterns
- Dozen of behavioral patterns







3

- Over 2 million outbreaks



The Unknown

Check Point Multi-Layered Threat Prevention

	<h2>IPS</h2>	<p>Stops exploits of known vulnerabilities</p>	
	<h2>Antivirus</h2>	<p>Block download of malware infested files</p>	
	<h2>Anti-Bot</h2>	<p>Detect and prevent bot damage</p>	

Protecting Against Unknown Attacks

Reputation based

- Sender email addresses / mail server IP
- MD5 of the PDF or malware
- *Ineffective against targeted attack – no reputation data*

Signature based

- Match on the exploit
- Match on the malware
- Match on the CnC communication
- Limited due to lack of prior *knowledge, variants and obfuscation*

Introducing Check Point Threat Emulation Software Blade



Instant protection against unknown threats



Threat Emulation – Malicious Attachment Example



Exploiting Zero-day vulnerabilities

2012 Top Vulnerable Applications

 Adobe Reader 30 critical exploits	 Java 17 critical exploits	 Office Microsoft Office 16 critical exploits
 Adobe Flash 57 critical exploits	 FireFox 91 critical exploits	 Internet Explorer 14 critical exploits

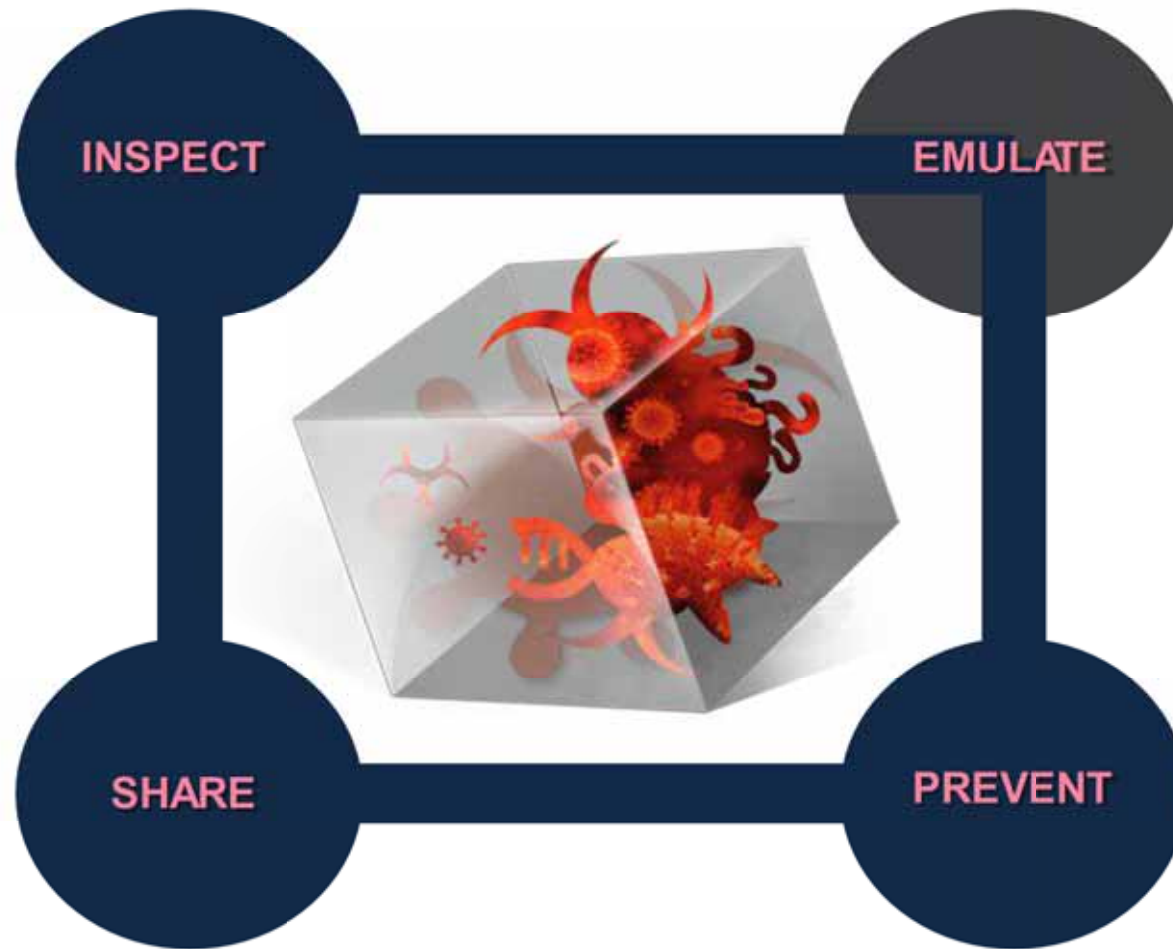
New vulnerabilities



Countless new variants

An average of 70,000 to 100,000 new malware samples are created and distributed each day

DATA READING



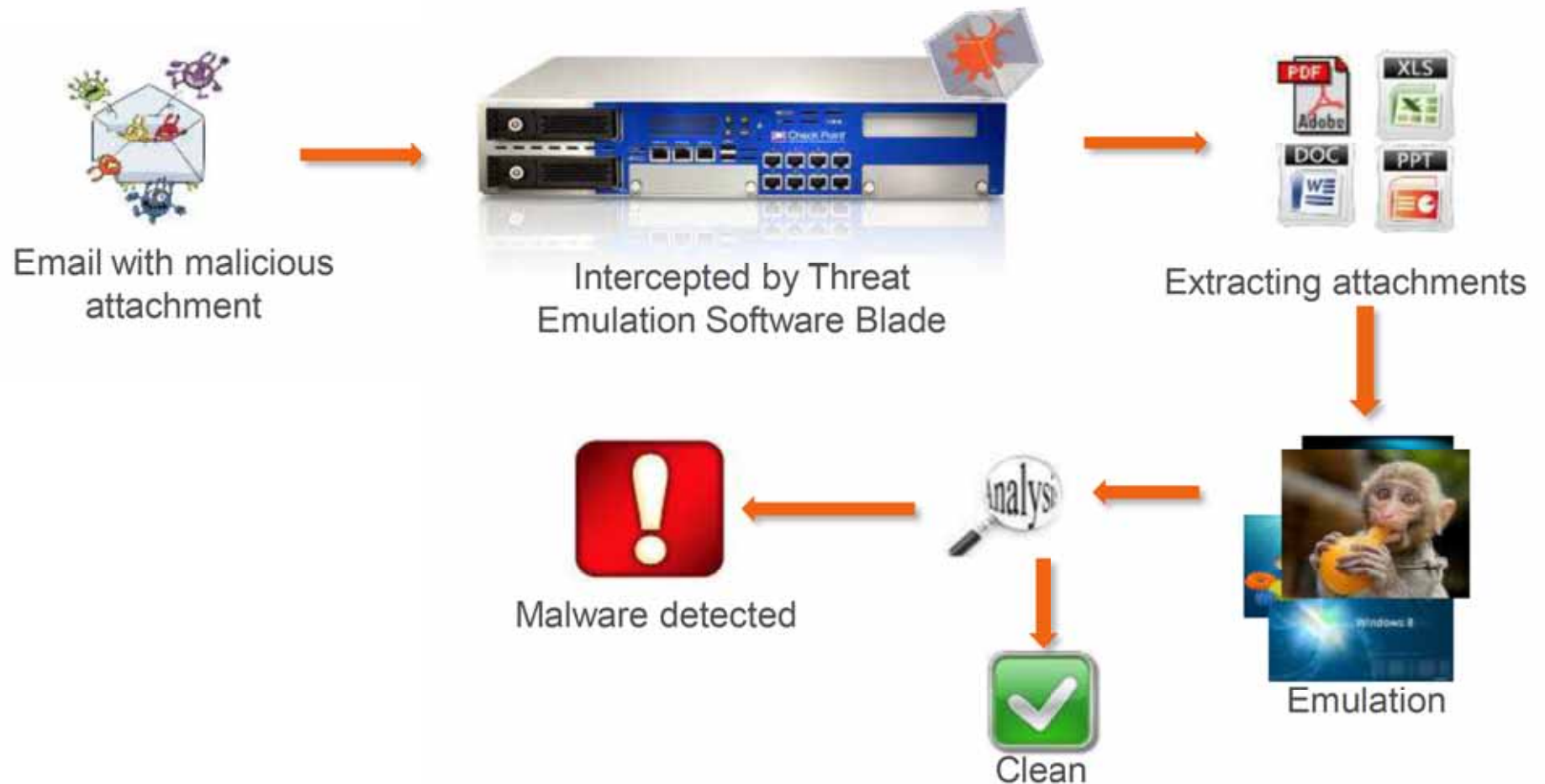
Stop undiscovered attacks with **Check Point Threat Emulation**

ThreatCloud Emulation Service



**Entire Enterprise can Verify files with
Check Point ThreatCloud Emulation Service**

Threat Emulation – Malicious Attachment Example



We know what should happen when opening a legitimate document ('White List')

The entire system activity is monitored for unexpected behavior

Any document which causes abnormal behavior can be safely consider as malicious

We monitor network activity, file system & registry changes, process activity & more



Syrian Attack Fed to the Threat Emulation

Malware Report

Emulated On: Windows XP Acrobat 7 Office 2010

Generated by Threat Emulation®, on 1

 **syrian.pdf**
Malicious Activity Detected

Type pdf
MD5
SHA

Executes the malware

Drops malware
(‘explorer.exe’ in temp directory)
Detected by Threat Emulation

Contact CnC

 **37 Affected Files**
9 Files Created | 28 Files Modified | 1 File Deleted

C:\\$ConvertToNonresident
C:\Documents and Settings\admin\Local Settings\Temp\1.dat
C:\Documents and Settings\admin\Local Settings\Temp\964.PDF
C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe

 **1 Affected Processes**
1 Process Created | 0 Processes Terminated | 0 Processes Crashed

C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe

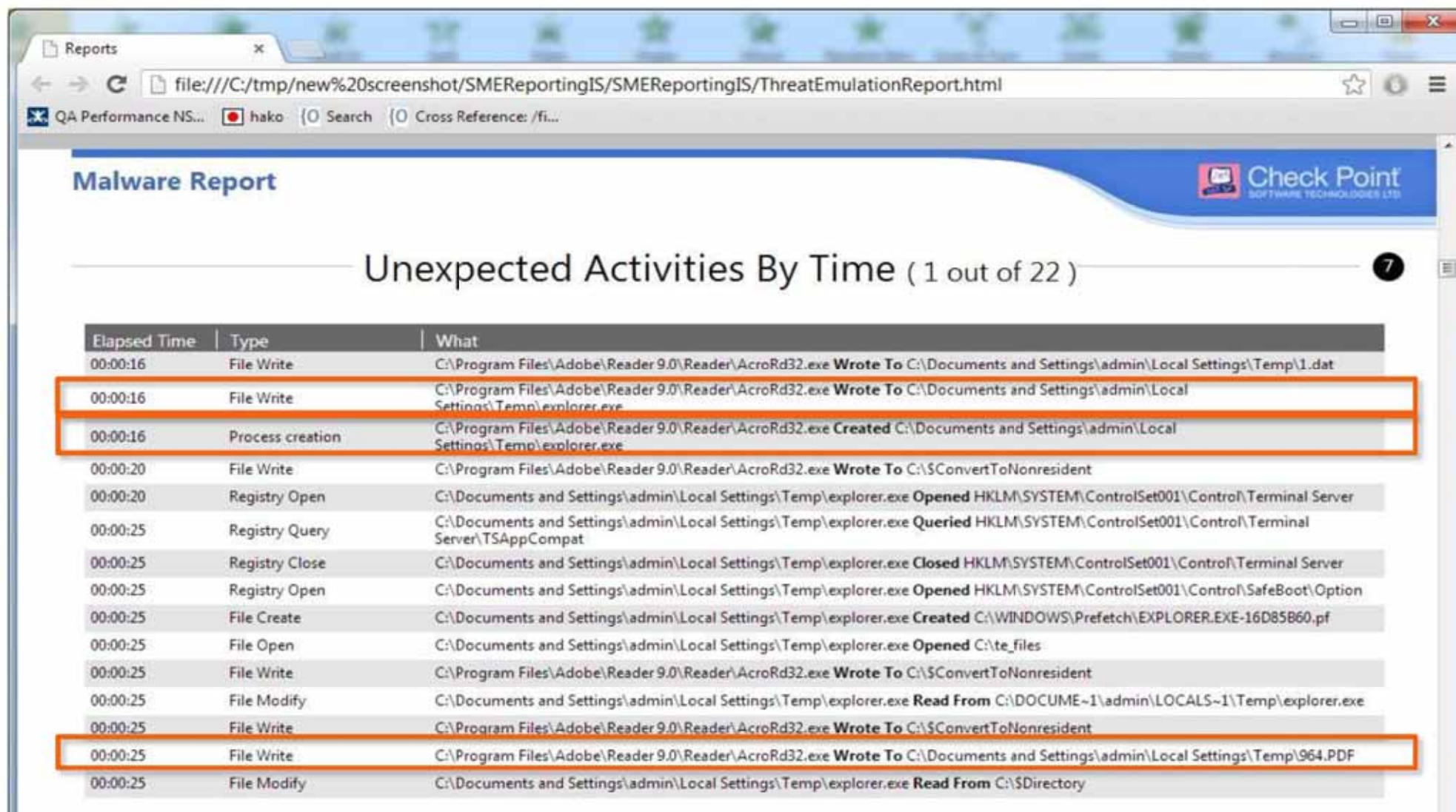
 **3 Affected Registry Keys**
3 Entries Set | 0 Entries Deleted

HKCU
HKCU\Control Panel\Desktop
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings

 **1 Attempted Network Connections**

sureshreddy1.dns05.com

Syrian Attack Fed to the Threat Emulation



The screenshot displays a web browser window with the URL `file:///C:/tmp/new%20screenshot/SMEReportingIS/SMEReportingIS/ThreatEmulationReport.html`. The page title is "Malware Report" and it features the Check Point logo. The main heading is "Unexpected Activities By Time (1 out of 22)". Below this is a table with three columns: "Elapsed Time", "Type", and "What". Several rows in the table are highlighted with orange borders, indicating suspicious or unexpected activities.

Elapsed Time	Type	What
00:00:16	File Write	C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe Wrote To C:\Documents and Settings\admin\Local Settings\Temp\1.dat
00:00:16	File Write	C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe Wrote To C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe
00:00:16	Process creation	C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe Created C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe
00:00:20	File Write	C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe Wrote To C:\\$ConvertToNonresident
00:00:20	Registry Open	C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe Opened HKLM\SYSTEM\ControlSet001\Control\Terminal Server
00:00:25	Registry Query	C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe Queried HKLM\SYSTEM\ControlSet001\Control\Terminal Server\TSAppCompat
00:00:25	Registry Close	C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe Closed HKLM\SYSTEM\ControlSet001\Control\Terminal Server
00:00:25	Registry Open	C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe Opened HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Option
00:00:25	File Create	C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe Created C:\WINDOWS\Prefetch\EXPLORER.EXE-16D85B60.pf
00:00:25	File Open	C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe Opened C:\te_files
00:00:25	File Write	C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe Wrote To C:\\$ConvertToNonresident
00:00:25	File Modify	C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe Read From C:\DOCUME~1\admin\LOCALS~1\Temp\explorer.exe
00:00:25	File Write	C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe Wrote To C:\\$ConvertToNonresident
00:00:25	File Write	C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe Wrote To C:\Documents and Settings\admin\Local Settings\Temp\964.PDF
00:00:25	File Modify	C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe Read From C:\\$Directory


Over **280** Million Addresses Analyzed for Bot Discovery


Over **12** Million Malware Signatures


Over **1** Million Malware-Infested Sites


150,000 updates
per day



-  Examine Three Real Attacks

-  The Economy Behind Attacks

-  3 Modern Threat Prevention

-  4 Summary

Summary and Recommendations

- Attacks vectors are numerous. Need to protect from the Known but also from the Unknown.
- Set expectations internally on what you are trying to protect against
- Choose a strategic Threat Prevention vendor capable of delivering Multi Layer defenses
- Collaboration with other organizations through a program like ThreatCloud is becoming a key.
- Check Point provide full spectrum of solutions verified by 3rd party labs.



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Thank You!

