Introduction

Incident Response and Malware Detection Using Traffic Analysis

By: Edward E. Ziots, CISSP, CISA, Security +, Network +

Profession: Security Engineer

Who Am I and what do I do?

- I am a security engineer, working for a large healthcare organization in the state of Rhode Island.
- The content contained within or my statements during this presentation do not reflect the opinions of my employer or technology vendors in any way shape or form.
- **Disclaimer**: Nothing in this presentation should constitute legal advice in dealing with incident response issues within your organization or business.

Incident Response Questions

- ## What is security incident response?

  Security incident response is the ability to detect and remediate problems that threaten people, process, technology or facilities. Resolution of these incidents is accomplished through an appropriate reaction to, and containment of, the problem that constitutes security incident response.

Note: Incident response is not always focused on computers and information systems, there are also physical attacks (facilities) and social engineering to consider.

- ## What is a computer security incident?

  A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies or standard security practices. (NIST SP 800—61)

Note: (Policies, process and procedures that are well understood and repeatable are critical to the success of the incident response capabilities).

Incident Response Questions (Cont'd)

- Why do we need security incident response?

  Incident response helps personnel to minimize loss or theft of information and disruption of services caused by various incidents. (NIST SP 800-61)

Note: Your incident response plans must cover any and all incidents that could possibly affect your organization. Do you know the current threats to your information systems and facilities?

- What is more important? The traffic coming into your network or the traffic leaving your network?

  Answer: Both, as you will learn later.

Compliance Regulations Concerning Incident Response (Cont'd)

HIPAA: Security Incident Response Procedures: Section 164.308(a)(6)

Key Activities: SP 800-66 Version 1, SP 800-61.

- Determine Goals of Incident Response.
- Develop and Deploy and Incident Response Team or Other Reasonable and Appropriate Response Mechanism.
- Develop and Implement Procedures to Respond to and Report Security Incidents.
- Incorporate Post-Incident Analysis into Updates and Revisions.

PCI-DSS 2.0: Section 12

- PCI-DSS 2.0 section 12.5.3 (Establish, document and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.

Compliance Regulations Concerning Incident Response (Cont'd)

PCI-DSS 2.0: Section 12

- PCI-DSS 2.0 section 12.5.3 (Establish, document and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
- PCI-DSS 2.0 section 12.9 (Implement an incident response plan. Be prepared to response immediately to a system breach)
- PCI-DSS 2.0 section 12.9.1 (Create an incident response plan to be implemented in the event of system breach).
- PCI-DSS 2.0 section 12.9.2 (Test the incident response plan at least annually)
- PCI-DSS 2.0 Section 12.9.3 (Designate specific personnel to be available on a 24/7 basis to respond to alerts)
- PCI-DSS 2.0 Section 12.9.4 (Provide appropriate training to staff with security breach responsibilities.)
- PCI-DSS 2.0 Section 12.9.5 (Include alerts from intrusion detection, intrusion prevention and file integrity monitoring systems.)
- PCI-DSS 2.0 Section 12.9.6 (Develop a process to modify and evolve the incident response plan according to lessons learned to incorporate industry developments.

Compliance Regulations Concerning Incident Response (Cont'd)

Sarbanes-Oxley Act of 2002

- Section 302: Establishes the responsibilities of the CEO and CFO for establishing and maintaining internal controls.
- Section 404: Requires management to assess the effectiveness of internal controls, obtain external validation of those controls, and provide assurances that financial/accounting processes are protected from unauthorized usage.
- Section 409: Requires real-time disclosures of material events.

Gramm-Leach Biliey Act (GLBA) Section 501 of Safeguard rules (501(b)

- Ensure the security and confidentiality of customer records and information
- Protect against any anticipated threats or hazards to the security or integrity of such records
- Protect against unauthorized access or use of such records or information which could result in substantial harm or inconvenience to any customer.

Note: Information Security Risk Assessment, Information Security Strategy, Information Security Controls, Security testing, Monitoring and Updating are part of the process that FFIEC recommends.

Compliance Regulations Concerning Incident Response (Cont'd)

NERC (North American Electric Reliability Corporation) (CIP-002, CIP-009)

- CIP-002-R3 Critical Asset Identification.
- CIP-003-R6 Change Control and Configuration Management
- CIP-005-R1.6 Documentation for Perimeter Assets
- CIP-005-R2 Electronic Access Controls
- CIP-005-R3 Monitoring Electronic Access
- CIP-005-R4 Cyber Vulnerability Assessment
- CIP-007-R2 Ports and Services
- CIP-007-R4 Malicious Software Prevention
- CIP-007-R6 Security Status Monitoring
- CIP-008-R1 Incident Response Plan

FISMA (The Federal Information Security Management Act) (Title III of E-Government Act of 2002)

Compliance Regulations Concerning Incident Response (Cont'd)

FISMA (The Federal Information Security Management Act) (Title III of E-Government Act of 2002). (Controls from NIST SP 800-53)

- CA-7 Continuous Monitoring.
- IR-5 Incident Monitoring.
- RA-3 Risk Assessment.
- RA-5 Vulnerability Scanning.
- SI-3 Intrusion Detection Tools and Techniques.
- CM-1 Configuration Management Policy and Procedures.
- CM-2 Baseline Configuration.
- CM-4 Monitoring Configuration Changes.

DOD Directive 8500.1 "Information Assurance"

- Information Assurance Implementation—requires that critical IT assets be protected with an intrusion detection system.

Incident Response Life-cycle

Incident Response Life-cycle (Cont'd)

Preparation:

•Creating an incident response policy and plan.

•Developing procedures for performing incident handling and reporting, based on the incident response policy. (Procedures need refined and communicated and practiced)

•Setting guidelines for communicating with outside parties regarding incidents. (Discussion between senior management and public relations/communications)

•Selecting a team structure and staffing model. (Senior Management)

•Establishing relationships between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies)

•Determining what services the incident response team should provide. (All requirements of incident response cycle as per NIST SP 800-61 Version 2) (Training, table-top exercises, cross training of staff, at least once a year if not more often)

•Staffing and training the incident response team. (Management, CSIRT lead)
On-call information, and call-trees in case of incident response plan activation.

•Who has the authority to invoke the incident response plan?

Incident Response Life-cycle (Cont'd)

Detection and Analysis:

Attack Vectors: External/Removable Media, Web Based (XSS, SQLi, Brute Force, DOS, DDOS), Email (Phishing, Malicious attachments, documents, or links), Impersonation (Social Engineering, MITM, Spoofing), Improper Usage (Violations of acceptable use policies (File sharing software, P2P networks) Loss or Theft of equipment (if contains EPHI or CC data could lead to violations of PCI-DSS or HITECH,HIPAA) Other: Anything that doesn't fit into the existing attack vectors.

What you should be looking for and doing within your information systems? (Base-lining)

•Review of exceptions auditing logs from information systems (Windows, Unix, etc) (Do you have the audit logs turned on? Are the logs exported on a regular basis to SEIM or event log management system? (Event Correlation)

•Filtering of traffic both ingress and egress at firewall systems looking for indicators of compromise. (Again these logs need to be sent to SEIM for trending and reporting.

•Review of logs from web servers (Apache, IIS, Tomcat)
Note: Do we see any web based attacks (SQLi, Directory Traversal, Brute-Force Password attack, Fuzzing attempts?)

•Review of security logs from SQL, Oracle etc etc.
Note: Anything that is out of the ordinary showing up in the logs, above the established baseline?

Incident Response Life-cycle (Cont'd)

Detection and Analysis:

•IPS and IDS Alerts logs. (What are your logs telling you, especially about the types of attacks and malicious traffic you are seeing on your network?)

•Reports from Antivirus, Anti-malware products. (Yes still of some use and worth)

•Logs from Network infrastructure devices (routers, switches). (Extrusion Prevention, Brute Force attempts access network infrastructure etc etc)

•Network Flow (Jflow, Netflow, (help baseline the traffic on the network) (Profile systems and understanding the normal behaviors and traffic patterns)

•Packet Sniffing (Wireshark, Windump, Tcpdump) (Does your firewall have interfaces you can dump traffic in these formats (IE: Checkpoint)

•Reports from employees in the organization. (Social engineering, Phishing, Spear Phishing malicious attachments) (Yes you should encourage and reward your users for reporting these things)

•Reports from employees in other organizations. (Email compromised and spamming other organizations, businesses) (Usually means bad news if its coming from a user in your organization)

Incident Response Life-cycle (Cont'd)

Containment, Eradication and Recovery.

•Who is responsible for activating the incident response plan? (SOP)

Note: Remember back in the Planning phase this SOP should have been created and rehearsed with the members of the IR team.

•Who is notified about the incident? (SOP) (CISO, CIO, Senior Mgmt?) (Document everything and when you did it…)

•How is the incident documented? (SOP)
Note: This is critical for post mortem discussions and learning.

•What is the current effect of the incident, (High, Medium Low)
Note: What are the timelines for remediation? (Resources and time is commensurate with the severity of Incident)

•What is impact to the affected resource? (DOS, DDOS, Theft of Intellectual Property (IP), system level compromise, web site defacement, etc etc)

Questions: When do we get law enforcement involved if at all? What are the escalation procedures?

Incident Response Life-cycle (Cont'd)

Containment, Eradication and Recovery.

•Evidence Preservation (In case of legal proceedings) (Digital Forensics) (Chain of Custody, and evidence preservation)

•Identification of attacker (Country of origin? AS?) (Leads to egress filtering) (Where do we implement this?)

•Containment strategy (Pull the plug on the NIC, Firewall off the server? Etc etc) based on needed availability of the resource and the type of attack you are facing.

•Process and Procedures to restore systems to normal operations. (Can you trust your backups, how long have you been breached?)

Incident Response Life-cycle (Cont'd)

Post Incident Activity

•Lessons Learned (Post-mortem of CISRT, and Management) (What happened who, what where when and why)

Note: This is not a finger pointing exercise, its meant to constructively review what happened and how the incident was dealt with and resolved and what measures can be put in place to prevent future it again. (Remember an once of prevention is worth a pound of cure)

•How well did staff and management perform in dealing with the incident?

•What information was needed sooner? (communications and decision making process)

•Were there any steps or actions taken that might have inhibited the recovery? (Backups, IR plans and their implementations, lack of appropriate personnel to implement the IR plan)

•What would management and the IR team do differently the next time a similar incident occurs?

•What corrective actions can be implemented to prevent similar incidents in the future?

•What additional tools or resources are needed to detect, analyze and mitigate future incidents?

Incident Response Life-cycle (Cont'd)

Incident Data (What does it tell us?)

•Logs: What did the logs tell you about your attacker? (IOC)

•Packet Analysis (Did we learn anything from capturing packets from the system) (IOC)

•What did the IDS/IPS logs tell you about the methods your attacker utilized to attack your network or systems? (IOC)

•Are you willing to use the evidence in a court of law to prosecute those that are responsible for the attack (forensics, chain of custody for evidence gathered)

•How many of these types of incidents has the IR team had to respond too (Helpdesk tickets and the remediation and root cause of the issues?) (Time per incident, types of incidents, time to detection of incident, monetary damage from incidents?)

•What is the cost to the organization to maintain in house IR team capability? Should this be out-sourced?

•Have you updated your IR Checklists, improvement of tools and techniques to detect and remediate future incidents of a similar nature?

•Prevention of similar attacks by implementation of additional controls (Ingress/egress filtering, system level hardening, patch management, and vulnerability management, penetration testing?

Incident Response Life-cycle (Cont'd)

Lessons Learned

•Egress filtering at your systems and network and firewalls is as important to the incident response process and providing ingress filtering. (Think its your early warning system that something is not right)

•Understand to whom and where your systems communicate and plan to restrict traffic to only those endpoints and protocols that are needed and nothing else. (Isolation, Least Privilege)

•Learn from attacks to your users and systems and plan and implement controls that will reduce or eliminate the attack surface to your systems. (PT, VA, TM, RA).

•Enforce your policies, because some incidents wouldn't be incidents if your users followed the policies of the organization and was held accountable for non-compliance with policies. (Usually one of the main reason incidents happen in the first place)

•Ensure you have a plan in place to deal with incidents that could happen to your business/organization before you need to do incident response for real. (Remember even the best laid plans can go to hell in a hand basket minutes into an true incident response situation so be sure you can improvise and think on your feet.)

•Be proactive with scanning your network and understanding your traffic patterns looking for indicators of compromise (IOC).

Incident Response Life-cycle (Cont'd)

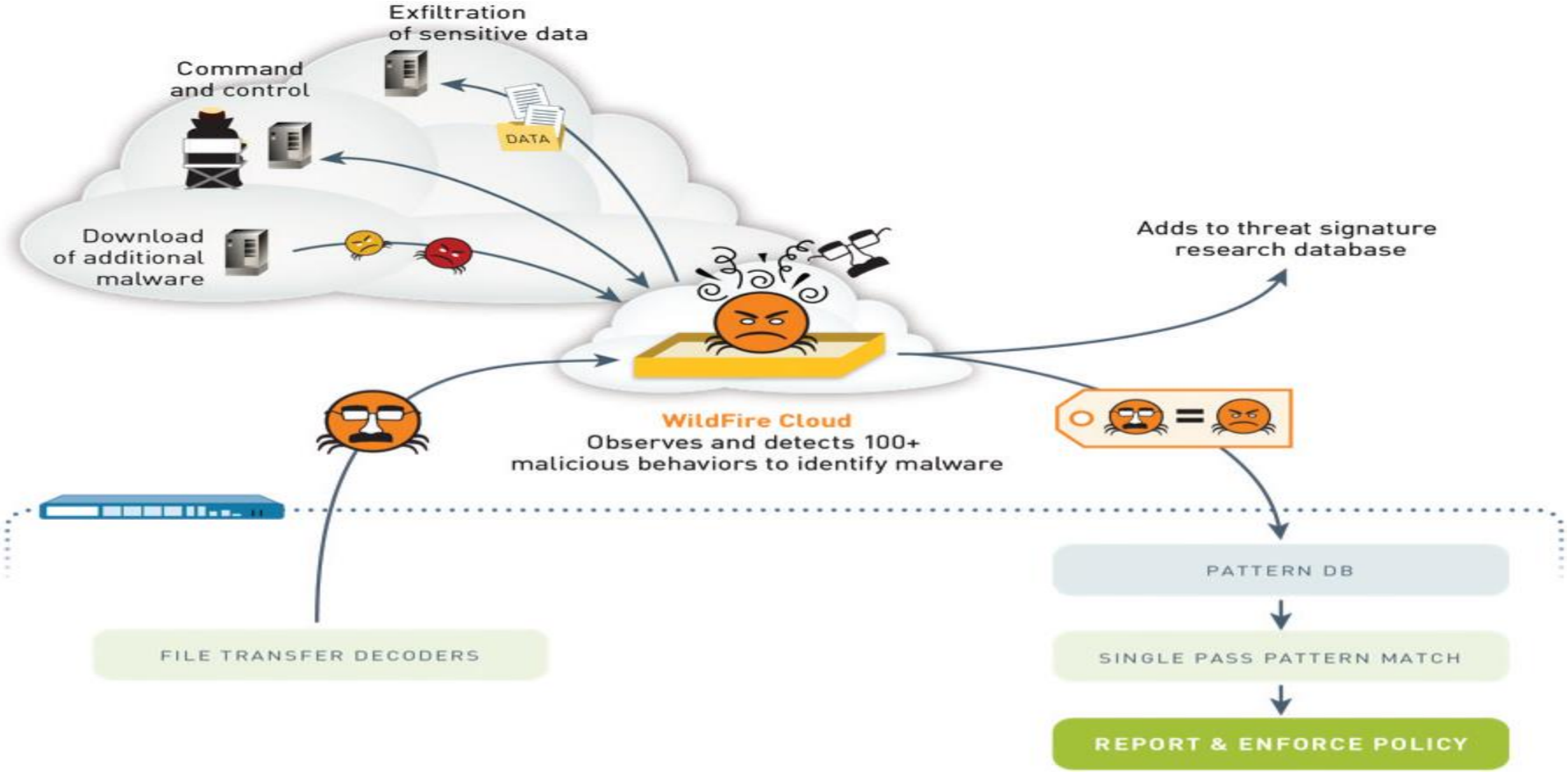
Lessons Learned Cont'd

•Ensure that you look at both encrypted and non-encrypted forms of traffic (yes malware can use encrypted channels to connect to command and control servers and malware sources)

•Ensure your systems are hardened from attack, patched regularly, and conduct frequent vulnerability scans to detect and remediate new vulnerabilities in systems.

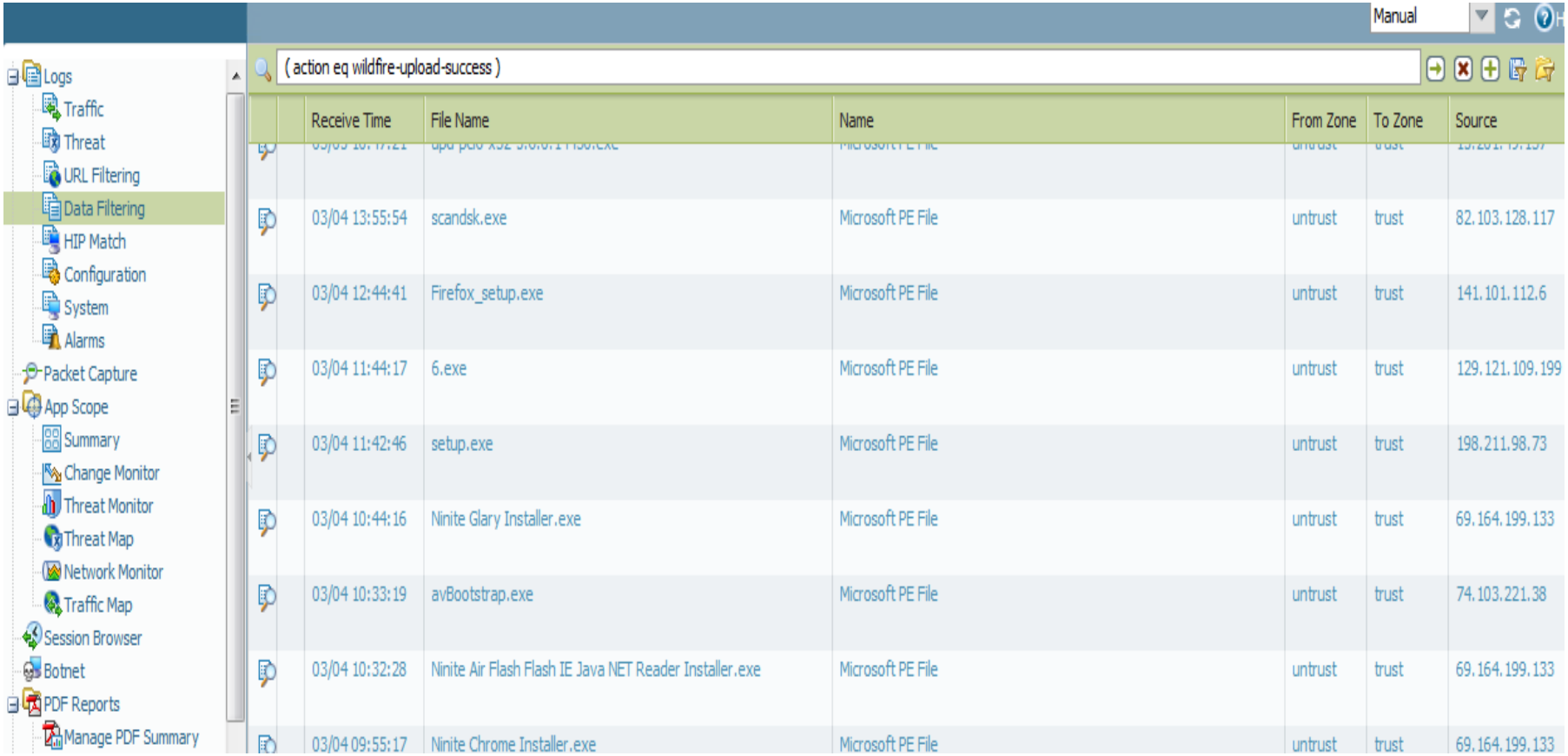
Palo Alto Wildfire

What is Wildfire and How does it work?



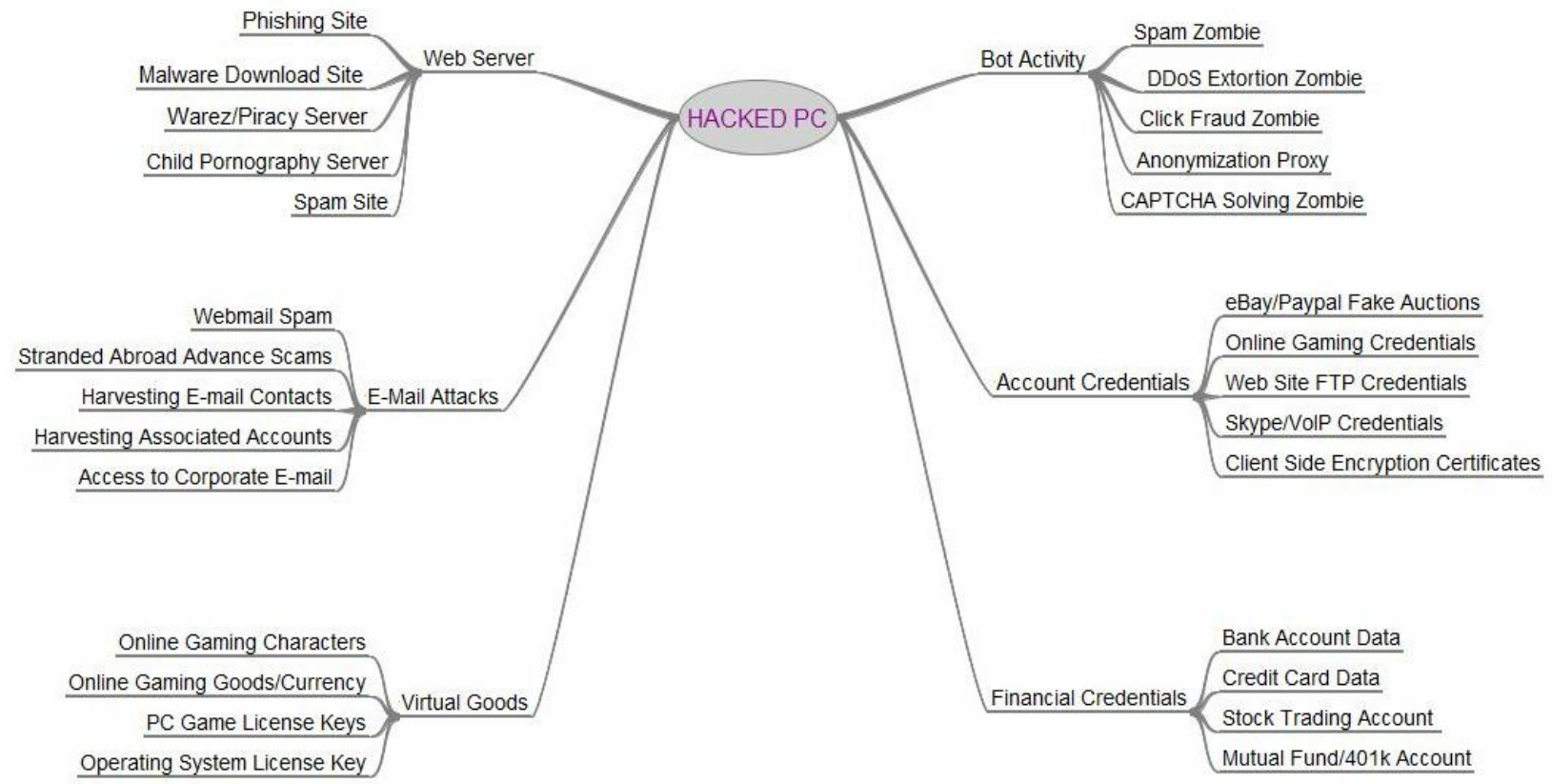
Palo Alto Wildfire

Wildfire in Action Looking at All Executable (PE)



Value in Malware Distribution

Value of a hacked PC



Malware Traffic Examples: Case 1

Case 1: What malware is this?

URL:	fresh-cache-node.com/1.exe		
Serial Number:			
SHA256:	a207ec38d59b105783ce034dac43c434dcc38f9c04d6e1d59bf8df2379338f58		
User:	Owned User	**Received:**	2/25/2013 12:10:42 PM
Attacker:	129.121.93.237 :80	**Victim:**	
Hostname /Mgmt. IP:	Palo Alto	**Application:**	web-browsing
Verdict:	Malware	Virus Coverage Information	

Malware Traffic Examples: Case 1 (Cont'd)

Case 1: Malware Behavior

Behavior

Created or modified files

Performed a host sweep

Spawned new processes

Listened on a specific port (backdoor behavior)

Deleted itself

Started or stopped a system service

Modified Windows registries

Modified registries or system configuration to enable auto start capability

Changed security settings of Internet Explorer

Attempted to sleep for a long period

Malware came from a malware domain

Communicated with new DNS server

Changed the Windows firewall policy

Malware Traffic Examples: Case 1 (Cont'd)

Case 1: Traffic Outbound

Protocol	IP Address	Country
UDP	68.99.236.133:16464	US
UDP	64.13.5.146:16464	US
UDP	77.121.250.84:16464	UA
UDP	76.31.86.134:16464	US
UDP	68.43.111.165:16464	US
UDP	95.235.64.134:16464	IT
UDP	2.94.189.170:16464	RU
UDP	111.188.83.88:16464	JP
UDP	82.140.54.148:16464	DE
UDP	189.46.167.114:16464	BR
UDP	116.203.87.182:16464	IN
UDP	117.200.139.143:16464	IN
UDP	190.79.200.122:16464	VE

Malware Traffic Examples: Case 1 (Cont'd)

Case 1: Indicators of Compromise

Registry	Action
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Personal	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{e86064ca-57e4-11e0-bef8-806d6172696f}\BaseClass	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Documents	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Desktop	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Desktop	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cookies	Set
HKCR\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}\InprocServer32\ThreadingModel	Set
HKCR\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}\InprocServer32	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Windows Defender	Delete
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-19\RefCount	Set
HKLM\SOFTWARE\Classes\CLSID\{5839FCA9-774D-42A1-ACDA-D6A79037F57F}\InprocServer32	Set
HKCU\Control Panel\Keyboard\InitialKeyboardIndicators	

Malware Traffic Examples: Case 1 (Cont'd)

Case 1: Indicators of Compromise

Process	Parent Process	Action
C:\sample.exe	explorer.exe	Create
C:\WINDOWS\system32\alg.exe	C:\WINDOWS\system32\services.exe	Terminate
C:\WINDOWS\system32\wscntfy.exe	C:\WINDOWS\system32\svchost.exe	Terminate
C:\WINDOWS\system32\userinit.exe	C:\WINDOWS\system32\winlogon.exe	Terminate
UNKNOWN	C:\sample.exe	Create
C:\sample.exe	explorer.exe	Terminate
UNKNOWN	C:\sample.exe	Terminate

Malware Traffic Examples: Case 1 (Cont'd)

Case 1: Indicators of Compromise

File	Process	Action
C:\RECYCLER\S-1-5-21-1004336348-362288127-725345543-500\$ae46e456ef90df271812f1460bbd369d\@	C:\sample.exe	Write
C:\RECYCLER\S-1-5-21-1004336348-362288127-725345543-500\$ae46e456ef90df271812f1460bbd369d\n	C:\sample.exe	Write
C:\Documents and Settings\LocalService\ntuser.dat.LOG	C:\WINDOWS\system32\winlogon.exe	Write
C:\Documents and Settings\LocalService\NTUSER.DAT	C:\WINDOWS\system32\winlogon.exe	Write
C:\RECYCLER\S-1-5-18\$ae46e456ef90df271812f1460bbd369d\@	C:\sample.exe	Write
C:\RECYCLER\S-1-5-18\$ae46e456ef90df271812f1460bbd369d\n	C:\sample.exe	Write
C:\sample.exe	UNKNOWN	Delete

Case 1: Conclusion and Actions

- **This was ZERO Access Root Kit Malware.**

Actions: (Suggested)

1. Lets determine the AS that this malware is coming from: use geoip.flagfox.net
2. Get a sample of the malware to analyze in virus total, and submit to your AV vendors for coverage updates
3. DNS black hole the query for the download site fresh-cache-node.com
4. Block egress all networks related to it.
5. Email Abuse at the ISP with the evidence.
6. Wipe and rebuild the endpoint system save no data, and ensure user changes credentials.
7. Review Web logs to determine what categories of information the user was viewing at the time of infection, make the adjustments to your security posture and follow your policies and procedures.
8. Create a traffic filter to look for this traffic outbound: ((port.dst eq 16471) or (port.dst eq 16464) or (port.dst eq 16465) or (port.dst eq 16470)) and (proto eq udp)

Malware Traffic Examples: Case 1 (Cont'd)

Case 1: Conclusion and Actions

Actions: (Suggested)

root@bt:~# dig fresh-cache-node.com

; <<>> DiG 9.7.0-P1 <<>> fresh-cache-node.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37143
;; flags: qr rd ra; QUERY: 1, ANSWER: 14, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;fresh-cache-node.com. IN A
;; ANSWER SECTION:

fresh-cache-node.com.	1179	IN	A	129.121.94.235 (NEXCESS.NET LLC (AS36444)
fresh-cache-node.com.	1179	IN	A	129.121.95.229 (NEXCESS.NET LLC (AS36444)
fresh-cache-node.com.	1179	IN	A	129.121.96.231 (NEXCESS.NET LLC (AS36444)
fresh-cache-node.com.	1179	IN	A	129.121.97.225 (NEXCESS.NET LLC (AS36444)
fresh-cache-node.com.	1179	IN	A	129.121.98.233 (NEXCESS.NET LLC (AS36444)
fresh-cache-node.com.	1179	IN	A	129.121.99.223 (NEXCESS.NET LLC (AS36444)
fresh-cache-node.com.	1179	IN	A	129.121.100.223 (NEXCESS.NET LLC (AS36444)
fresh-cache-node.com.	1179	IN	A	129.121.101.220 (NEXCESS.NET LLC (AS36444)
fresh-cache-node.com.	1179	IN	A	129.121.102.209 (NEXCESS.NET LLC (AS36444)
fresh-cache-node.com.	1179	IN	A	129.121.103.211 (NEXCESS.NET LLC (AS36444)
fresh-cache-node.com.	1179	IN	A	129.121.104.201 (NEXCESS.NET LLC (AS36444)
fresh-cache-node.com.	1179	IN	A	129.121.91.228 (NEXCESS.NET LLC (AS36444)
fresh-cache-node.com.	1179	IN	A	129.121.92.234 (NEXCESS.NET LLC (AS36444)
fresh-cache-node.com.	1179	IN	A	129.121.93.237 (NEXCESS.NET LLC (AS36444)

Malware Traffic Examples: Case 1 (Cont'd)

Case 1: Conclusion and Actions

Countries that are invovled in this malware:
USA: 46 Networks
Ukraine: 4 Networks
Italy: 5 Networks
Russia: 4 Networks
Japan: 6 Networks
Germany: 5 Networks
Brazil: 6 Networks
India: 16 Networks
Venezuela: 4 Networks
Taiwan: 24 Networks
Bosnia and Herzegovina: 3 Networks
Korea: 2 Networks
Canada: 4 Networks
Europe: 2 Networks
Spain: 3 Networks
Israel: 3 Networks
Hungary: 2 Networks
France: 7 Networks
Romania: 4 Networks
Bulgaria: 3 Networks
Mylasia: 1 Network
Hong Kong: 1 Network
Serbia: 1 Network
Poland: 7 Networks
Sweden: 1 Network
China: 1 Network
Lativa: 1 Network
Belgium: 1 Network
Argentina: 1 Network
Philippines: 1 Network
Turkey: 3 Network
Kyrgyzstan: 1 Network
SwitzerLand: 1 Network

Malware Traffic Examples: Case 2

Case 2: What malware is this?

URL:	gq1-attach.ymail.com/us.f1635.mail.yahoo.com/ya/securedownload?		
Serial Number:			
SHA256:	4a6ab406f82e620a24e25d717ba04657d9b2ef254d7d853233ba2d077c0bcdf3		
User:	Owned User	**Received:**	3/6/2013 10:43:40 AM
Attacker:	206.190.57.60 :80	**Victim:**	
Hostname/ Mgmt. IP:	Palo Alto	**Application:**	yahoo-mail
Verdict:	Malware	Virus Coverage Information	

Malware Traffic Examples: Case 2 (Cont'd)

Case 2: What malware is this?

The file "235-2352352375623724634782384528354823548234823462875 48.pdf.exe" is uploaded from firewall Palo Alto at 2013-03-06 10:43:40.
URL: gq1-attach.ymail.com/us.f1635.mail.yahoo.com/ya/securedownload?

Application:Yahoo-Mail (Maybe good idea to ban yahoo mail? or limit downloads from this?)

Malware Traffic Examples: Case 2 (Cont'd)

Case 2: Malware Behavior

Created or modified files
Started a process from a user document folder
Spawned new processes
Contained unknown TCP/UDP traffic
Listened on a specific port (backdoor behavior)
Deleted itself
Injected code into another process

Registered a file as auto-start from a local directory

Modified registries or system configuration to enable auto start capability

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

Malware came from a malware domain
Visited an unregistered domain
IP country different from HTTP host TLD
Visited a malware domain
Changed the Windows firewall policy

Malware Traffic Examples: Case 2 (Cont'd)

Case 2: Outbound Traffic

Phone home to: on port 8080 tcp.
POST 50.28.90.36/forum/viewtopic.php Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)
POST 50.28.90.36/forum/viewtopic.php Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)
POST 50.28.90.36/forum/viewtopic.php Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)
POST 50.28.90.36/forum/viewtopic.php Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)
POST 50.28.90.36/forum/viewtopic.php Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)
POST 50.28.90.36/forum/viewtopic.php Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)
POST 50.28.90.36/forum/viewtopic.php Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)
POST 50.28.90.36/forum/viewtopic.php Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)
POST 74.207.227.67/forum/viewtopic.php Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)
POST 74.207.227.67/forum/viewtopic.php Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)
POST 74.207.227.67/forum/viewtopic.php Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)
POST 74.207.227.67/forum/viewtopic.php Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)
POST 50.28.90.36/forum/viewtopic.php Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)
POST 74.207.227.67/forum/viewtopic.php Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)
POST 50.28.90.36/forum/viewtopic.php Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)
POST 50.28.90.36/forum/viewtopic.php Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)

TCP 50.28.90.36:8080 US Liquid Web, Inc. (AS32244) (site:elenskids.com)
TCP 74.207.227.67:8080 US Global Net Access, LLC (AS3595) (Site:li69-67.members.linode.com)

http://www.threatexpert.com/report.aspx?md5=bfe7c4846823174cbcbb10de9daf426b

Malware Traffic Examples: Case 2

Domain:Generated and some are lookup for phone home:
halzcmgmlofdeduilvljhdmwocayceivpaxgmftwindnfeynv.net (nothing resolves via nslookup or dig)
asov.info (nothing resolves via nslookup or dig)
google.ru 173.194.75.94
ovnrtsbixhmhexzguvodmpbtcnr.org (Nothing resolves via nslookup or dig)
hmmbdiauibnzqsdushmcugzhufiu.com (Nothing resolves via nslookup or dig)
deqowcpmrfenjjnzhhpzdxgy.com (Nothing resolves via nslookup or dig)
www.google.com ;; ANSWER SECTION:

google.com.	276	IN	A	74.125.228.70
google.com.	276	IN	A	74.125.228.66
google.com.	276	IN	A	74.125.228.68
google.com.	276	IN	A	74.125.228.73
google.com.	276	IN	A	74.125.228.72
google.com.	276	IN	A	74.125.228.69
google.com.	276	IN	A	74.125.228.65
google.com.	276	IN	A	74.125.228.78
google.com.	276	IN	A	74.125.228.71
google.com.	276	IN	A	74.125.228.64
google.com.	276	IN	A	74.125.228.67

zlrgtcjblmzgyjrvcqsaqcqxkgqpb.ru (Nothing resolves via nslookup or dig)
google.com (Same as above)
clskfefatogekdapbormveunvhulj.com (Nothing resolves via nslookup or dig)
mrlrroduolordacqobobibjrm.info (Nothing resolves via nslookup or dig)
fmvwnrsmzovxceazdwiflvkjmzdi.ru (Nothing resolves via nslookup or dig)
wkpdqjrrobqkbtoftknrdhjbqs.biz (Nothing resolves via nslookup or dig)
www.google.ru
But when I searched google.ru I found the following (For each of the generated sites)
virustracker.info/text/Blocklist_combined.txt ZeuS_Gameover (Domains)

Malware Traffic Examples: Case 2 (Cont'd)

Case 2: Outbound Traffic

First Malware download :**Remember outbound communications after original infection.**
80.11.230.234/gkmYH.exe France Telecom S.A. (AS3215)
(Site:LVelizy-156-46-21-234.w80-11.abo.wanadoo.fr)

Malware Traffic Examples: Case 2 (Cont'd)

Case 2: Outbound Traffic

Second Malware Download:
axelditter.de/w91qZ5.exe IP:195.93.201.42 nocyo GmbH (AS44335) (Site:willy.kundenserver42.de)
Outbound Traffic
UDP 99.68.30.82:14974 US for SBIS- (AS7132)
UDP 155.212.138.69:23731 US One Communications Corporation (AS14751)
UDP 64.219.121.189:13503 US for SBIS- (AS7132)
UDP 50.72.177.24:25517 CA Shaw Communications Inc. (AS6327) (CA)
UDP 96.57.35.109:14435 US Cablevision Systems Corp. (AS6128)
UDP 66.117.77.134:15387 US Visionary Communications, Inc. (AS10835)
UDP 94.67.185.188:26120 GR Ote SA (Hellenic Telecommunications Organisation) (AS6799) (Greece)
UDP 71.42.56.253:22652 US BRIGHT HOUSE NETWORKS, LLC (AS33363)
UDP 151.49.166.206:10117 IT WIND Telecomunicazioni S.p.A. (AS1267)
UDP 142.176.125.203:10568 CA Bell Aliant Regional Communications, Inc. (AS855)
UDP 24.120.165.58:21251 US Cox Communications Inc. (AS22773)
UDP 108.211.64.46:23323 US AT&T Services, Inc. (AS7018)
UDP 69.39.74.6:14775 US 123.Net, Inc. (AS12129)
TCP 74.125.224.144:80 US Google Inc. (AS15169)
UDP 85.9.95.205:15080 IR Pishgaman Kavir Yazd (AS34918) (IRAN!)
UDP 194.94.127.98:25549 DE Verein zur Foerderung eines Deutschen Forschungsnetzes e.V. (AS680)
UDP 99.95.152.226:27763 US SBIS- (AS7132)
UDP 199.243.220.218:15242 CA Bell Canada (AS577)
UDP 184.156.76.158:23986 US Digital Teleport Inc. (AS22561)
UDP 87.203.112.174:19469 GR Ote SA (Hellenic Telecommunications Organisation) (AS6799)
TCP 74.125.224.151:80 US Google Inc. (AS15169)

Malware Traffic Examples: Case 2 (Cont'd)

Case 2: Outbound Traffic

Third Malware Download:
02e4047.netsolhost.com/wxe2V6.exe IP: 206.188.192.175 InterNIC Registration Services (AS6245)
(Site:vux.netsolhost.com)
UDP 99.68.30.82:14974 US
UDP 155.212.138.69:23731 US
UDP 64.219.121.189:13503 US
UDP 50.72.177.24:25517 CA
UDP 96.57.35.109:14435 US
UDP 66.117.77.134:15387 US
UDP 94.67.185.188:26120 GR
UDP 71.42.56.253:22652 US
UDP 151.49.166.206:10117 IT
UDP 142.176.125.203:10568 CA
UDP 24.120.165.58:21251 US
UDP 108.211.64.46:23323 US
UDP 69.39.74.6:14775 US
TCP 74.125.224.144:80 US
UDP 85.9.95.205:15080 IR
UDP 194.94.127.98:25549 DE
UDP 99.95.152.226:27763 US
UDP 199.243.220.218:15242 CA
UDP 184.156.76.158:23986 US
UDP 87.203.112.174:19469 GR
TCP 74.125.224.151:80 US

Malware Traffic Examples: Case 2 (Cont'd)

Case 2: Outbound Traffic

Fourth Malware Download:
a761119.sites.myregisteredsite.com/ab8bkn.exe 209.237.150.20 Web.com, Inc. (AS36476)
(Site:2190575.sites.myregisteredsite.com)
UDP 99.68.30.82:14974 US
UDP 155.212.138.69:23731 US
UDP 64.219.121.189:13503 US
UDP 50.72.177.24:25517 CA
UDP 96.57.35.109:14435 US
UDP 66.117.77.134:15387 US
UDP 94.67.185.188:26120 GR
UDP 71.42.56.253:22652 US
UDP 151.49.166.206:10117 IT
UDP 142.176.125.203:10568 CA
UDP 24.120.165.58:21251 US
UDP 108.211.64.46:23323 US
UDP 69.39.74.6:14775 US
TCP 74.125.224.144:80 US
UDP 85.9.95.205:15080 IR
UDP 194.94.127.98:25549 DE
UDP 99.95.152.226:27763 US
UDP 199.243.220.218:15242 CA
UDP 184.156.76.158:23986 US
UDP 87.203.112.174:19469 GR
TCP 74.125.224.151:80 US

Malware Traffic Examples: Case 2 (Cont'd)

Case 2: Outbound Traffic

Fifth Malware Download:
www.fragmentschen.de/tZ5GdC4.exe 81.169.145.148 STRATO STRATO AG (AS6724) (Site:w94.rzone.de)
UDP 99.68.30.82:14974 US
UDP 155.212.138.69:23731 US
UDP 64.219.121.189:13503 US
UDP 50.72.177.24:25517 CA
UDP 96.57.35.109:14435 US
UDP 66.117.77.134:15387 US
UDP 94.67.185.188:26120 GR
UDP 71.42.56.253:22652 US
UDP 151.49.166.206:10117 IT
UDP 142.176.125.203:10568 CA
UDP 24.120.165.58:21251 US
UDP 108.211.64.46:23323 US
UDP 69.39.74.6:14775 US
TCP 74.125.224.144:80 US
UDP 85.9.95.205:15080 IR
UDP 194.94.127.98:25549 DE
UDP 99.95.152.226:27763 US
UDP 199.243.220.218:15242 CA
UDP 184.156.76.158:23986 US
UDP 87.203.112.174:19469 GR
TCP 74.125.224.151:80 US

Malware Traffic Examples: Case 2 (Cont'd)

Case 2: Outbound Traffic

Sixth Malware Download:
d1003686.stwadmin.net/ymNFAt6N.exe 91.189.180.61 ServeTheWorld (AS34989) (Norway)
Site:linweb15.avaboo.net
UDP 99.68.30.82:14974 US
UDP 155.212.138.69:23731 US
UDP 64.219.121.189:13503 US
UDP 50.72.177.24:25517 CA
UDP 96.57.35.109:14435 US
UDP 66.117.77.134:15387 US
UDP 94.67.185.188:26120 GR
UDP 71.42.56.253:22652 US
UDP 151.49.166.206:10117 IT
UDP 142.176.125.203:10568 CA
UDP 24.120.165.58:21251 US
UDP 108.211.64.46:23323 US
UDP 69.39.74.6:14775 US
TCP 74.125.224.144:80 US
UDP 85.9.95.205:15080 IR
UDP 194.94.127.98:25549 DE
UDP 99.95.152.226:27763 US
UDP 199.243.220.218:15242 CA
UDP 184.156.76.158:23986 US
UDP 87.203.112.174:19469 GR
TCP 74.125.224.151:80 US

Malware Traffic Examples: Case 2 (Cont'd)

Case 2: Outbound Traffic

Seventh Malware Download:
pm.aixsol.com/aUC1.exe 50.63.174.128 GoDaddy.com, LLC (AS26496) Site:ip-50-63-174-128.ip.secureserver.net
UDP 99.68.30.82:14974 US
UDP 155.212.138.69:23731 US
UDP 64.219.121.189:13503 US
UDP 50.72.177.24:25517 CA
UDP 96.57.35.109:14435 US
UDP 66.117.77.134:15387 US
UDP 94.67.185.188:26120 GR
UDP 71.42.56.253:22652 US
UDP 151.49.166.206:10117 IT
UDP 142.176.125.203:10568 CA
UDP 24.120.165.58:21251 US
UDP 108.211.64.46:23323 US
UDP 69.39.74.6:14775 US
TCP 74.125.224.144:80 US
UDP 85.9.95.205:15080 IR
UDP 194.94.127.98:25549 DE
UDP 99.95.152.226:27763 US
UDP 199.243.220.218:15242 CA
UDP 184.156.76.158:23986 US
UDP 87.203.112.174:19469 GR
TCP 74.125.224.151:80 US

Malware Traffic Examples: Case 2 (Cont'd)

Case 2: Indicators of Compromise

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Personal	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{e86064ca-57e4-11e0-bef8-806d6172696f}\BaseClass	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Documents	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Desktop	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Desktop	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cookies	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Local AppData	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Local AppData	Set
HKCU\Software\Microsoft\Tiloq\2ag6de3g	Set
HKCU\Software\Microsoft\Tiloq\2f894f0i	Set
HKCU\Software\Microsoft\Tiloq\2f894f0i	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\{F9919B46-0289-AD40-A2AF-DA84B0D0F996}	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\internat.exe	

Malware Traffic Examples: Case 2 (Cont'd)

Case 2: Indicators of Compromise

HKCU\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC\LDAP Server ID	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\Bigfoot\LDAP Server ID	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\VeriSign\LDAP Server ID	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\WhoWhere\LDAP Server ID	Set
HKCU\Software\Microsoft\Internet Account Manager\Server ID	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\PreConfigVer	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\PreConfigVerNTDS	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC\Account Name	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC\LDAP Server	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC\LDAP Search Return	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC\LDAP Timeout	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC\LDAP Authentication	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC\LDAP Simple Search	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC\LDAP Bind DN	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC\LDAP Port	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC\LDAP Resolve Flag	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC\LDAP Secure Connection	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC\LDAP User Name	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\Active Directory GC\LDAP Search Base	

Malware Traffic Examples: Case 2 (Cont'd)

Case 2: Indicators of Compromise

HKCU\Software\Microsoft\Internet Account Manager\Accounts\Bigfoot\Account Name	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\Bigfoot\LDAP Server	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\Bigfoot\LDAP URL	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\Bigfoot\LDAP Search Return	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\Bigfoot\LDAP Timeout	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\Bigfoot\LDAP Authentication	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\Bigfoot\LDAP Simple Search	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\Bigfoot\LDAP Logo	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\VeriSign\Account Name	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\VeriSign\LDAP Server	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\VeriSign\LDAP URL	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\VeriSign\LDAP Search Return	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\VeriSign\LDAP Timeout	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\VeriSign\LDAP Authentication	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\VeriSign\LDAP Search Base	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\VeriSign\LDAP Simple Search	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\VeriSign\LDAP Logo	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\WhoWhere\Account Name	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\WhoWhere\LDAP Server	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\WhoWhere\LDAP URL	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\WhoWhere\LDAP Search Return	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\WhoWhere\LDAP Timeout	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\WhoWhere\LDAP Authentication	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\WhoWhere\LDAP Simple Search	Set
HKCU\Software\Microsoft\Internet Account Manager\Accounts\WhoWhere\LDAP Logo	Set
HKCU\Software\Microsoft\Internet Account Manager\Default LDAP Account	

Malware Traffic Examples: Case 2 (Cont'd)

Case 2: Indicators of Compromise

HKCU\Software\Microsoft\WAB\WAB4\Wab File Name	Set
HKCU\Software\Microsoft\WAB\WAB4\OlkContactRefresh	Set
HKCU\Software\Microsoft\WAB\WAB4\OlkFolderRefresh	Set
HKCU\Identities\Changing	Delete
HKCU\Identities\IncomingID	Delete
HKCU\Identities\OutgoingID	Delete
HKCU\Identities\{7A323C99-BE29-4352-AFB7-C158712E22C9}\Identity Ordinal	Set
HKCU\Identities\Identity Ordinal	Set
HKCU\Software\Microsoft\Tiloq\2f894f0i	Set
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\DisableNotifications	Set
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List\10219:UDP	Set
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List\17850:TCP	Set
HKCU\Software\Microsoft\Tiloq\170gi752	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\MigrateProxy	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer	Delete
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride	Delete
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL	Delete
HKLM\SYSTEM\ControlSet001\Hardware Profiles\0001\Software\Microsoft\windows\CurrentVersion\Internet Settings\ProxyEnable	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings	Set
HKCU\Control Panel\Keyboard\InitialKeyboardIndicators	

Malware Traffic Examples: Case 2 (Cont'd)

Case 2: Indicators of Compromise

Process	Parent Process	Action
C:\sample.exe	explorer.exe	Create
C:\Documents and Settings\Administrator\Application Data\Nyib\mijof.exe	C:\sample.exe	Create
C:\WINDOWS\system32\userinit.exe	C:\WINDOWS\system32\winlogon.exe	Terminate
C:\Documents and Settings\Administrator\Application Data\Nyib\mijof.exe	C:\sample.exe	Terminate
UNKNOWN	C:\sample.exe	Create
C:\sample.exe	explorer.exe	Terminate
UNKNOWN	C:\sample.exe	Terminate
C:\WINDOWS\system32\update.exe	C:\WINDOWS\system32\cmd.exe	Terminate
C:\WINDOWS\system32\cmd.exe	C:\WINDOWS\explorer.exe	Terminate
C:\WINDOWS\system32\wscntfy.exe	C:\WINDOWS\system32\svchost.exe	Terminate

Malware Traffic Examples: Case 2 (Cont'd)

Case 2: Indicators of Compromise

File	Process	Action
C:\Documents and Settings\Administrator\Application Data\Nyib\mijof.exe	C:\sample.exe	Delete
C:\Documents and Settings\Administrator\Application Data\Nyib\mijof.exe	C:\sample.exe	Write
C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab	C:\WINDOWS\system32\cmd.exe	Write
C:\Documents and Settings\Administrator\Local Settings\Temp\tmp67a4ac22.bat	C:\sample.exe	Write
C:\sample.exe	UNKNOWN	Delete
C:\Documents and Settings\Administrator\Local Settings\Temp\tmp67a4ac22.bat	UNKNOWN	Delete
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\4PI385IJ\google[1].htm	C:\WINDOWS\explorer.exe	Delete

Case 2: Conclusion and Actions

This malware was Zbot.

• Each sample came from different sites and AS over the globe.
• Each sample had the same outbound traffic characteristics
• And each same has the same hash using sha1deep therefore could add this into Application White listing solutions and ban it.
•root@bt:~/malware/zbot# sha1deep *.exe
•ca087461129af44abddb3f831fa73ebb42787051 /root/malware/zbot/ab8bkn.exe
•ca087461129af44abddb3f831fa73ebb42787051 /root/malware/zbot/aUC1.exe
•ca087461129af44abddb3f831fa73ebb42787051 /root/malware/zbot/gkmYH.exe
•ca087461129af44abddb3f831fa73ebb42787051 /root/malware/zbot/tZ5GdC4.exe
•ca087461129af44abddb3f831fa73ebb42787051 /root/malware/zbot/wxe2V6.exe
•ca087461129af44abddb3f831fa73ebb42787051 /root/malware/zbot/w91qZ5.exe
•ca087461129af44abddb3f831fa73ebb42787051 /root/malware/zbot/ymNFAt6N.exe

•We found that the first malware, downloaded seven other malware executables, that was the same bot, and the domains that was associated with the outbound communications was apart of a Russian Banking Trojan domains.

Malware Traffic Examples: Case 2 (Cont'd)

Case 2: Conclusion and Actions

• So does AV really stop these types of threats if most of them can't even detect in their signatures (Of course not)
•According to Virustotal the only AV vendors that knew about this was. (Sorry if your current AV wasn't on the list but we told you AV isn't going to always catch these things)
•Kaspersky
•Mcafee
•Microsoft
•Panda
•Pctools
• Remediation (Get the samples to your AV vendors for submission), Block the infecting websites with your web filter.
•Egress filter the serving sites and the phone home networks, and notify the ISP's of the networks via abuse email channels with the proof. If you have
•Application White listing in place, make sure you put the hashes of the files into your block list.
•Make sure the users machine is wiped clean (DBAN and reimage or bare metal rebuild) and make sure the user is educated

Malware Traffic Examples: Case 3

Case 3: What malware is this?

URL:	rcaretrospect.org/soft4.exe		
Serial Number:			
SHA256:	0c7943cb3e57c1b8a56d5d5cda64535ce715174dec3f30cc7e6446694400f9f4		
User:	Owned User	**Received:**	2/19/2013 2:20:58 PM
Attacker:	91.238.83.63 :80	**Victim:**	
Hostname/Mgmt. IP:	Palo Alto	**Application:**	web-browsing
Verdict:	Malware	Virus Coverage Information	

Malware Traffic Examples: Case 3 (Cont'd)

Case 3: Analysis of Behavior

Behavior

Created or modified files

Deleted itself

Modified Windows registries

Modified registries or system configuration to enable auto start capability

Changed security settings of Internet Explorer

Created an executable file in a user document folder

Attempted to sleep for a long period

Used direct IP instead of host name

Malware came from a malware domain

Malware Traffic Examples: Case 3 (Cont'd)

Case 3: Outbound Traffic Analysis

Method	URL	User Agent
GET	103.4.225.41/api/stats/install/?ts=7588b9e869bde32b05410129e679ecac7cf377d5&affid=51800&ver=3070025&group=dap	Mozilla/5.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/5.0);(b:2600;c:INT-2C60;l:09)
GET	103.4.225.41/api/urls/?ts=7588b9e869bde32b05410129e679ecac7cf377d5&affid=51800	Mozilla/5.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/5.0);(b:2600;c:INT-2C60;l:09)

http://urlquery.net/report.php?id=1076123

Malware Traffic Examples: Case 3 (Cont'd)

Case 3: Outbound Traffic Analysis

Protocol	IP Address	Country
TCP	103.4.225.41:80	HK

Malware Traffic Examples: Case 3 (Cont'd)

Case 3: Indicators of Compromise

Registry	Action
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Personal	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{e86064ca-57e4-11e0-bef8-806d6172696f}\BaseClass	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Documents	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Desktop	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Desktop	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cookies	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cookies	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\History	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\E89BEF5C5FE338350000E89B06C83F1B	Set

Malware Traffic Examples: Case 3 (Cont'd)

Case 3: Indicators of Compromise

Process	Parent Process	Action
C:\sample.exe	explorer.exe	Create
C:\WINDOWS\system32\userinit.exe	C:\WINDOWS\system32\winlogon.exe	Terminate

File	Process	Action
C:\sample.exe	C:\sample.exe	Delete
C:\Documents and Settings\All Users\Application Data\E89BEF5C5FE338350000E89B06C83F1B**E89BEF5C5FE338350000E89B06C83F1B.exe**	C:\sample.exe	Write
C:\Documents and Settings\All Users\Application Data\E89BEF5C5FE338350000E89B06C83F1B\E89BEF5C5FE338350000E89B06C83F1B.ico	C:\sample.exe	Write

Case 3: Conclusions and Actions

• This sample was **Fake AV**, seen by a lot of Antivirus vendors according to Virustotal.
• This sample was apart of a campaign as we seen in outbound website traffic. (Pay Per install Malware Economics)
•Sandbox analysis will disclose IOC of the malware on the endpoint.
• Remediation (Get the samples to your AV vendors for submission), Block the infecting websites with your web filter.
• Make sure the user password is changed after the endpoint is remediated.
•Egress filter the serving sites and the phone home networks, and notify the ISP's of the networks via abuse email channels with the proof.
•Application White listing in place, make sure you put the hashes of the files into your block list.
•Make sure the users machine is wiped clean (DBAN and reimage or bare metal rebuild) and make sure the user is educated

Resources Utilized

•Books: Extrusion Detection, Richard Bejtlich, Addison-Wesley.
•Books: Tao of Network Security Monitoring, Richard Bejtlich, Addison-Wesley
•Books: Hacking Exposed, Malware and Root kits (Davis, Bodmer, Lemasters (Mcgraw Hill)
•Books: Windows Forensic Analysis, Carvey, Syngress Press.
•Practical Packet Analysis: Chris Sanders, No Starch Press.

•Tools: Fiddler HTTP proxy, Paros Proxy, BurpSuite
•Tools: Palo Alto ™ Wildfire Malware Sandbox
•Tools: Virustotal
•Tools: Backtrack Penetration Test Platform R3 (Various tools)
•Tools: Palo Alto Next Generation Firewall, IPS, Web Filtering Solution. (Palo Alto Networks ™.

•Useful Websites for Malware Analysis and Tracking:
•Malware.dontneedcoffee.com
•http://www.gfi.com/malware-analysis-tool/ (Gfi Malware Sandbox)
•http://labs.alienvault.com/labs/index.php/projects/open-source-ip-reputation-portal/lastest-ips/ (Current Threat feed of malware seen across the globe)
•http://zeltser.com/reverse-malware/analyzing-malicious-documents.html (Analyzing Malicious Documents Cheat sheet (Lenny Zeltser)
•http://wepawet.iseclab.org/index.php (Malware Analysis of JavaScript, PDF and files)

Resources Utilized (Cont'd)

- **Useful Websites for Malware Analysis and Tracking: Cont'd.**
- **http://jsbeautifier.org/ (JavaScript deobfuscation into readable format)**
- **http://jsunpack.jeek.org/ (JavaScript unpacker can also check pdf, html and .js files)**
- **http://www.malwaredomains.com/**
- **https://palevotracker.abuse.ch/ (Palevo Tracker from abuse.ch)**
- **https://spyeyetracker.abuse.ch/ (Spyeye tracker from abuse.ch)**
- **https://zeustracker.abuse.ch/ (Zeus tracker from abuse.ch)**
- **http://scanurl.net/**
- **http://www.google.com/safebrowsing/diagnostic?site=AS:24940 (Google Safe browsing by AS number)**
- **http://sitevet.com/db/asn/AS16265 (Look up malicious actions seen by AS)**
- **http://vurldissect.co.uk/**
- **http://www.threatexpert.com**

- **SANS Articles:**
- **https://isc.sans.edu/diary/Wipe+the+drive%21++Stealthy+Malware+Persistence+Mechanism+-+Part+1/15394**
- **https://isc.sans.edu/diary/Wipe+the+drive%21++Stealthy+Malware+Persistence+-+Part+2/15406**
- **https://isc.sans.edu/diary/Wipe+the+drive%21++Stealthy+Malware+Persistence+-+Part+3/15448**
- **Symantec Article (Pay Per Install Malware Network)**
- **http://www.symantec.com/connect/blogs/pay-install-new-malware-distribution-network**