

Living in Compromise to Advanced Persistent Threats

Eddie Schwartz, PMP, CISSP, CISA, CISM, ISSEP CSO, NetWitness Corporation eddie@netwitness.com



Agenda

- > Understanding the current cyber threat environment and what organizations can do to improve security visibility
- The need for situational awareness, network forensics and deeper inspection of network traffic
- >> Technology illustrations and specific cases
- > Final thoughts and Q&A







Cisco 2009 Mid-Year Security Report – Key Findings Summary

- » Top Threats:
 - Spear Phishing attacks, e.g. (H1N1/World Cup SPAM)
 - Poisoned websites and DNS "Drive-by" attacks
 - Pervasive botnet infection (e.g., ZeuS / Gumblar / Storm 2.0)
 - Social Networking / Mobility / Web 2.0
 - Cloud Computing protecting data
 - Data exfiltration
 - Product Vulnerabilities (e.g. Adobe, Microsoft, Oracle)

The Bottom Line THREATS ARE ALREADY ON THE INSIDE • EXPLOITS THAT MATTER HAVE ALREADY HAPPENED



4 | Copyright 2010 © All rights reserved. NetWitness Corporation







The Global Threat Landscape

- » Electronic Criminal Groups: Established Underground Industry (continued examples of successful large scale operations)
 - Organization: Low to High
 - Capability: High
 - Intent: High for financial gain
 - "Kneber" ZeuS BotNet information sold to anybody
- » Nation-Sponsored Activities: From Intelligence Gathering to Network-Centric Warfare
 - Organization: High
 - Capability: High
 - Intent: Connected to national policy
 - Operation Aurora, Titan Rain, etc.



- » Non-State Actors
 - Increasing interest from radical / extremist groups in cyberterror
 - "Hacking as a service"



5 | Copyright 2010 © All rights reserved. NetWitness Corporation



What Do These Organizations Want?

- » Nation-sponsored attacks on anything (critical infrastructure, defense industry base, etc.)
 - Designer malware directed at end users through spear phishing attacks
 - Covert channels and obfuscated network traffic
 - Low and slow data exfiltration
 - Rogue encryption
- » Organized criminal group attacks
 - Data from retail and banking POS and ATM systems
 - Infiltration of transaction processing systems in multiple industry sectors
 - Application layer, database and middleware systems with deep "personal information" and other "key" attributes







The Underground Economy





The Underground Data Marketplace

	Price List: VISA, MasterCard USA (with cvv2 code)							
Quantity	количество	идентификация	цена в \$USD					
	5-50	есть в продаже	5.0					
	51-100	есть в продаже	4.5					
	101-500	есть в продаже	4.0					
	501-1000	есть в продаже	3.0					
	1001-5000	есть в продаже	2.0					
	более 10000	есть в продаже	пишите					
	Если Вам нужно более отдельная скидка	е 10000 карт, свяжитесь с на	ами, для Вас будет					

Price in \$USD

Call for Bulk Pricing

(Other providers sold separately)

Source: iDEFENSE

8 | Copyright 2010 © All rights reserved. NetWitness Corporation







Advanced Persistent Threats (APT)



There ARE specific targets...

- Advanced the adversary can operate in the full spectrum of computer intrusion
- Persistent the adversary is driven to accomplish a mission
 - **Threat** the adversary is:
 - Organized
 - Funded
 - Motivated
 - Analysts speak of multiple "groups" consisting of dedicated "crews" with various missions

Source: Tao of Security Blog



So, Why Are Security Teams Failing to Detect APTs?



» People

- Underestimate the complexity and capability of the threat actors
- Security teams lack appropriate knowledge and experience
- >> Process
 - Organizations have misplaced IT measurements and program focus
 - i.e. focus on compliance vs. effective security operations and threat intelligence
- >> Technology
 - Current infrastructure is not well suited to fight APT
 - Holes in network visibility

💮 Google hackers duped system ad... 📘 🕂

The Washington Post

NEWS | POLITICS | OPINIONS | BUSINESS | LOCAL | SPORTS | ARTS & LIVING | GOING OUT GUIDE | JOBS | CARS | REAL ESTATE |SHOPPING

Google hackers duped system administrators to penetrate networks, experts say

By Ellen Nakashima Washington Post Staff Writer Wednesday, April 21, 2010; A15

The hackers who penetrated the computer networks of Google and more than 30 other large companies used an increasingly common means of attack: duping system administrators and other executives who have access to passwords, intellectual property and other information, according to cybersecurity experts familiar with the cases.

"Once you gain access to the directory of user names and passwords, in minutes you can take over a network," said George Kurtz, worldwide chief technology officer for McAfee, a Silicon Valley computer security firm that has been working with more than half a dozen of the targeted companies.

Figuring out whom to target and how is the result of research, said Shawn Carpenter, a principal forensics analyst at the security firm NetWitness whose former job involved trying to hack into government agencies' Web sites to help them find their weak spots. "One of the first things we do is build up a dossier," he said. "What conferences has this person spoken at? What people do they know? Are they likely to open up this type of e-mail attachment if I spoof it as coming from a person who has sat on a panel with them?"

The essence of the attack is "exploiting those human tendencies of curiosity and trust," Carpenter said.

The targeting of personnel is only one aspect of a larger, more sophisticated operation that involves planning the mode of attack, reconnaissance inside a company's network, deciding what type of data to go after, and harvesting and analyzing the data, experts said.

"There's a life cycle of activities that occurs, involving many steps, both with human intelligence and electronic intelligence, to ultimately penetrate these organizations," said Eddie Schwartz, NetWitness's chief security officer. "When you're combining all of these techniques, this is the work of a highly organized group or groups that has specific targets in mind."

Staff researcher Julie Tate contributed to this report.







PEOPLE: Has Regulatory Compliance Improved Security Posture?



40 35 30 **CISO - CSI** 25 20 15 10 5 0 Strongly 3 5 Strongly Disagree Agree Source: Pam Fusco 11 | Copyright 2010 © All rights reserved. NetWitness Corporation NETWITNESS

CIO – Info Week

PROCESS: Do I/T Metrics Support Advanced Threat Management?





TECHNOLOGY: The Gaps in Status Quo Security - Firewalls



- » Intent
 - Prevent or limit unauthorized connections into and out of your network



» Reality

- Attackers use "allowed paths" (DNS, HTTP, SMTP, etc) to provide reliable and hard to detect C&C and exfiltration channels.
- » Even worse
 - Using encrypted tunnels to provide "reverse-connect" for full remote control capabilities.
- Some firewall technology is just beginning to evolve towards the application layer – but still susceptible to evasion



The Gaps in Status Quo Security – A/V

- » Intent
 - Prevent malicious code from running on an endpoint



From an A/V vendor forum...

Just a question on signatures...

Does the signature team not do Zeus/ZBot configuration files? We have submitted a number (20+) of ".bin" files over the last 6-8 weeks but have yet to see these files detected using "Official" signatures. Should we not submit these files?

» Reality

- Most anti-malware technologies are signaturebased, requiring constant signature updates, often lag
- » Even worse
 - eCrime crews create custom malware for high value targets and for routine campaigns, less likely to have timely signatures

...good question, Tom!

Tom

14 | Copyright 2010 © All rights reserved. NetWitness Corporation





The Gaps in Status Quo Security – IDS/IPS



- » Intent
 - Alert on or prevent known malicious network traffic



» Reality

- Attackers are using obfuscation methods to prevent IDS signatures from recognizing malicious traffic and client-side attacks that don't do "network-based" exploitation
- » Even worse
 - Intrusion Prevention Systems are largely left unimplemented or crippled due to fears of business impact



The End of Security? Nah....



Cyber Defense in 2010 and Beyond – What is Required?



- » Advanced threat detection and response requires a different approach:
 - > 24 x 7 SITUATIONAL AWARENESS
 - Applying the science of NETWORK FORENSICS to the art of incident response
 - Application-layer threat context and intelligence
- Enable security teams to view network traffic as conversations instead of individual packets or groups of IP addresses
- AGILITY to extend architecture to address emerging threat trends and integrate the intelligence of open and classified threat sources





17 | Copyright 2010 © All rights reserved. NetWitness Corporation

Implementing Next Generation Intrusion Detection, Analysis and Response





- Why is our top destination today a foreign IP address and protocol with whom we never communicate?
- » Why is our top destination port 15347?
- > How can I be sure this cyber incident is a false positive?

- Which security controls are being subverted in real-time?
- What is the magnitude of this Trojan or malware incident?
- Who is communicating with the enemy, cyber criminals, or other inappropriate entities
- Who is using policy evasion technologies such as TOR, ultrasurf, or PGP encryption?
- >> What is the potential source of an attack or breach (attribution)?
- » How is data leaving our organization (exfiltation)?
- Who is using Skype and other technologies to transfer files out of our network?







Understanding Advanced Threat Activity







Examining Advanced Threats

A "Drive-By" Attack



Initial Glance





Initial Glance





Email Content Review

>> Indicators show malware is spamming: White Supremacy Forum



Greetings brother!

The White Nationalism community would like to Welcome you to our new Whites-only web forum.

Here we discuss ways to deal with the jewish menace and the mud people invasion.

Click the link below to visit our site: http://f2bbs.com/

» But what about the random filenames?









Random Filename Analysis









Geographic Activity Map



27 | Copyright 2010 © All rights reserved. NetWitness Corporation







BOT Examination Summary

- Clearly using host to SPAM
- Using HTTP for Command and Control
 - .png PUT
- Global BOT
- Top domain name in HTTP C&C traffic is "adoresong.com".
 - Adoresong.com was one of the domains that was used during the social engineering spam that Waledac used
- Spam could be cover for other data exfiltration activity





Case Study

Understanding a Custom ZeuS-based APT Spear Phishing Attack

Advanced Threats Are More Prevalent Than You Think



- There are many commercial and non-commercial variants of Trojans such as ZeuS that have been developed by eCrime groups for specific targets of interest:
 - Banks, DIB, specific government agencies in U.S. and Europe
- » Numerous signs of collaboration among malware writers, including "best practices" for improving techniques for detection avoidance and resilience (e.g. ZeuS and Waledac collaboration noted in NetWitness "Kneber" report)

C:\WINDOWS\system32\cmd.exe - zsbcs.exe listen -ipv4 -cp:3333 -bp:6666 - 0 C:\Documents and Settings\test\Desktop>zsbcs.exe ZeuS BackConnect Server 2.0.0.0. Standard Edition Build time: J61. Usage: zsbcs.exe <command> -<switch 1> -<switch N> (Connands>
listen Start a backconnect server for one bot. Switches> Suppresses display of sign-on banner. Listen on IPv4 port. Listen on IPv6 port. nologo ipu4 ipv6 ICP port for accepting a connection from bot. ICP port for accepting a connection from ?lient. bp:[port] cp:[port] \Documents and Settings\test\Desktop>zsbcs.exe listen -ipv4 -cp:3333 -bp:6666 ZeuS BackConnect Server 2.0.0.0. Standard Edition Build time: <\$980. Listening on IPv4 port 6666. Listening on IPv4 port 3333.

Press Ctrl+C key to shutdown server. Waiting for incoming connections <port of bot: 6666, port of client: 3333>...

Source: iSightpartners

- New features, such as the inclusion of robust Backconnect reverse proxy capabilities
- Many of these non-commercial variants are invisible to typical security tools





Continued Targeted Attacks Against USG Assets



- During the last year+ there has been an ongoing campaign associated with forged emails containing targeted ZeuS infections
- > Typical scenario is email from some "reliable" email address containing spear phishing text of interest and link to custom ZeuS site
- » Parallels: this approach directly imitates non-USG mass eCrime ZeuS approaches

Subject: DEFINING AND DETERRING CYBER WAR From: ctd@nsa.gov U.S. Army War College, Carlisle Barracks, PA 17013-5050 December 2009 **DEFINING AND DETERRING CYBER WAR** Since the advent of the Internet in the 1990s, not all users have acted in cyberspace for peaceful purposes. In fact, the threat and impact of attack in and through cyberspace has continuously grown to the extent that cyberspace has emerged as a setting for war on par with land, sea, air, and space, with increasing potential to damage the national security of states, as illustrated by attacks on Estonia and Georgia. Roughly a decade after the advent of the Internet, the international community still has no codified, sanctioned body of norms to govern state action in cyberspace. Such a body of norms, or regime, must be established to deter aggression in cyberspace. This project explores the potential for cyber attack to cause exceptionally grave damage to a state's national security, and examines cyber attack as an act of war. The paper examines efforts to apply existing international norms to cyberspace and also assesses how traditional concepts of deterrence apply in cyberspace. The project concludes that cyber attack, under certain conditions, must be treated as an act of war, that deterrence works to dissuade cyber aggression, and provides recommendations to protect American national interests.





"DPRK has carried out nuclear missile attack on Japan"



- Email with bogus message about a missile attack on Japan by the DPRK received by member of the intelligence community
- >> The sender's email from this example is forged <u>nic@dni.gov</u>
 - Other forged senders used in same phish e.g., <u>ODNI@dia.mil</u>, <u>SSC@dia.mil</u>
- The email contained "tear lines" and fake classification markings (i.e. "U//FOUO") in an attempt to look legitimate
- The sophistication level is fairly low; there is one obvious grammatical error, the far-fetched claims in the email can be quickly disproved, and the phish requires user action (open linked file) to successfully install the malware
- Despite the low sophistication level of the spear phish, it reeled in numerous victims before the command & control server was deactivated – it was good enough





Subject: DPRK has carried out nuclear missile attack on Japan

Office of the Director of National Intelligence INTELLIGENCE BULLETIN UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U//FOUO) DPRK has carried out nuclear missile attack on Japan

05 March 2010

(U//FOUO) Prepared by Defense Intelligence Agency

(U//FOUO) Today, March 05, 2010 at 01.41 AM local time (UTC/GMT -5 hours), US seismographic stations recorded seismic activity in the area of Okinawa Island (Japan). According to National Geospatial-Intelligence Agency, Democratic People's Republic of Korea has carried out an average range missile attack with use of nuclear warhead. The explosion caused severe destructions in the northern part of the Okinawa island. Casualties among the personnel of the US military base are being estimated at the moment.

(U//FOUO) In connection with the occurred events, it is necessary for the personnel of the services listed below to be ready for immediate mobilization:

CENTRAL INTELLIGENCE AGENCY Phone: (703) 482-0623

DEFENSE INTELLIGENCE AGENCY Phone: (202) 231-8601 Email: DIA-PAO@dia.mil

DEPARTMENT OF ENERGY: OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE Phone: 1-202-586-5000 Email: The.Secretary@hq.doe.gov

DEPARTMENT OF HOMELAND SECURITY: OFFICE OF INTELLIGENCE AND ANALYSIS Phone: (202) 282-8000

DEPARTMENT OF STATE: BUREAU OF INTELLIGENCE AND RESEARCH Phone: (202) 647-4000

33 | Copyright 2010 © All rights reserved. NetWitness Corporation

DEPARTMENT OF THE TREASURY: OFFICE OF INTELLIGENCE AND ANALYSIS Phone: (202) 622-2000

DRUG ENFORCEMENT ADMINISTRATION: OFFICE OF NATIONAL SECURITY INTELLIGENCE Phone: (202) 307-1000

FEDERAL BUREAU OF INVESTIGATION NATIONAL SECURITY BRANCH Phone: (202) 324-3000

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY Phone: (703) 755-5900

NATIONAL RECONNAISSANCE OFFICE Phone: (703) 808-1198

NATIONAL SECURITY AGENCY Phone: 1-800-688-6115 Email: NIASC@nsa.gov

UNITED STATES AIR FORCE Phone: (251) 441-6215/6211

UNITED STATES ARMY Phone: 1-888-550-2769

UNITED STATES COAST GUARD Phone: (202) 372-2100

UNITED STATES MARINE CORPS Phone: (202) 372-4411

UNITED STATES NAVY Phone: (202) 372-2020

NETWITNESS

(U//FOUO) Additional information can be found in the following report:

http://dnicenter.com/docs/report.zip

Office of the Director of National Intelligence Washington, D.C. 20511



"DPRK has carried out nuclear missile attack on Japan"



> Only 1 of 42 AV vendors indentified the file as malicious on 03.05.2010

34 | Copyright 2010 © All rights reserved. NetWitness Corporation

File report.exe received on 2010.03.05 14:01:07 (01C) Current status: finished Result: 1/42 (2.38%)					
Compact				Print result	
Antivirus	Version	Last Update	Result		
a-squared	4.5.0.50	2010.03.05	-		
AhnLab-V3	5.0.0.2	2010.03.05	-		
AntiVir	8.2.1.180	2010.03.05	-		
Antiy-AVL	2.0.3.7	2010.03.05	-		
Authentium	5.2.0.5	2010.03.05	-		
Avast	4.8.1351.0	2010.03.05	-		
Avast5	5.0.332.0	2010.03.05	-		
AVG	9.0.0.730	2010.03.05	-		
BitDefender	7.2	2010.03.05	-		
CAT-QuickHeal	10.00	2010.03.05	-		
ClamAV	0.96.0.0-git	2010.03.05	-		
Comodo	4091	2010.02.28	-		
DrWeb	5.0.1.12222	2010.03.05	-		
eSafe	7.0.17.0	2010.03.04	-		
eTrust-Vet	35.2.7341	2010.03.05	-		
F-Prot	4.5.1.85	2010.03.04	-		
F-Secure	9.0.15370.0	2010.03.05	-		
Fortinet	4.0.14.0	2010.03.04	-		
GData	19	2010.03.05	-		
Ikarus	T3.1.1.80.0	2010.03.05	-		
Jiangmin	13.0.900	2010.03.05	-		
K7AntiVirus	7.10.990	2010.03.04	-		
Kaspersky	7.0.0.125	2010.03.05	-		
McAfee	5910	2010.03.04	-		
McAfee+Artemis	5910	2010.03.04	-		
McAfee-GW-Edition	6.8.5	2010.03.05	-		
Microsoft	1.5502	2010.03.05	-		
NOD32	4918	2010.03.05	-		
Norman	6.04.08	2010.03.05	-		
nProtect	2009.1.8.0	2010.03.05	-		

"DPRK has carried out nuclear missile attack on Japan"



- » AV effectively "neutered" by overwriting the OS hosts file
- Attempts to retrieve updates from vendor update server hosts routed to 127.0.0.1
- » Result: if AV didn't pick up the malware initially, it never will now

35 | Copyright 2010 © All rights reserved. NetWitness Corporation

This is a sample HOSTS file used by Microsoft TCP/IP for Windows. # This file contains the mappings of IP addresses to host names. Each # entry should be kept on an individual line. The IP address should # be placed in the first column followed by the corresponding host name. # The IP address and the host name should be separated by at least one # space. # Additionally, comments (such as these) may be inserted on individual lines or following the machine name denoted by a '#' symbol. For example: 102.54.94.97 rhino.acme.com # source server 38.25.63.10 # x client host x.acme.com 5(.0.0.1 localhost 127.0.0.1 downloads-eu1.kaspersky-labs.com 127.0.0.1 downloads2.kaspersky-labs.com 127.0.0.1 downloads4.kaspersky-labs.com 12. 0.1 downloads1.kaspersky-labs.com 127.0.0.1 dov xy-Labs.com 127.0.0.1 rads.mcafee.com 127.0.0.1 liveupdate.symantecliveupdate.com 127.0.0.1 liveupdate.symantec.com 127.0.0.1 liveupdate.symantec.d4p.net 127.0.0.1 update.symantec.com 127.0.0.1 download7.avast.com 127.0.0.1 download6.avast.com 127.0.0.1 download5.avast.com 127.0.0.1 download4.avast.com 127.0.0.1 download3.avast.com 127.0.0.1 download2.avast.com 127.0.0.1 download1.avast.com 127.0.0.1 avu.zonelabs.com 127.0.0.1 retail.sp.f-secure.com 127.0.0.1 retail01.sp.f-secure.com 127.0.0.1 retail02.sp.f-secure.com 127.0.0.1 acs.pandasoftware.com 127.0.0.1 pccreg.antivirus.com 127.0.0.1 dl1.antivir.de 127.0.0.1 dl2.antivir.de 127.0.0.1 dl3.antivir.de 127.0.0.1 dl4.antivir.de 127.0.0.1 fr.mcafee.com 127.0.0.1 mcafee.com 127.0.0.1 antivirus.cai.com 127.0.0.1 ftp.esafe.com 127.0.0.1 ftp.europe.f-secure.com 127.0.0.1 ftp.symantec.com 127.0.0.1 us.mcafee.com 127.0.0.1 security.symantec.com 127.0.0.1 download.mcafee.com 127.0.0.1 shop.symantec.com 127.0.0.1 dispatch.mcafee.com 127.0.0.1 f-secure.com NETV 127.0.0.1 kaspersky.com 127.0.0.1 mast.mcafee.com 127.0.0.1 secure.nai.com

Copyright (c) 1993-1999 Microsoft Corp.

127.0.0.1 sophos.com



Infection Progression – Nothing Unusual

- » After a user clicks on the link, the file "report.zip" is downloaded from dnicenter.com
- » If user opens the file, the malware is installed
- Malware is actually a Zeus variant; author used techniques to hamper reverse-engineering / analysis of the binary

	💽 NetWitness Investigator 9			
Domain name: dnicenter.com	: <u>Collection Edit V</u> iew <u>B</u> ookmarks <u>H</u> istory <u>H</u> elp			
Status: Active	All Data			
Protection Status: public (make contact info private at http://www.now.cn/domain/domainPrivate.php)	Image: Welcome Image: Open K Image:	4 Þ ×		
Registrant: Name: ???????? Address: Volodarskiy City: Izjevsk Province/state: Taliban Country: AU Postal Code: 519000 Administrative Contact: Name: ???????? Organization: ??????????? Address: Volodarskiy City: Izjevsk Province/state: Taliban Country: AU Postal Code: 519000 Phone: +84.4562425583 Fax: +84.4562425583 Fax: +84.4562425583 Email: abuseemaildhcp@gmail.com	Time Service Size Events 2010- IP / 53.44 00:0C:29:31:9D:73 -> 00:0B:6C:BA:C4:FF Mar-06 TCP / KB 192.168.0.32 -> 115.100.250.105 21:30:12 HTTP KB 192.168.0.32 -> 115.100.250.105 View View 1052 -> 80 (http) View KB action: get directory: /docs/ filename: report.zip extension: zip Client: moznia/+.0 alias.ip: 115.100.250.105 alias.host: dnicenter.com content: application/zip content: application/zip content: application/zip content: application/zip content: application/zip content: apglication/zip content: application/zip content: apglication/zip content: application/zip content: apglication/zip content: apglication/zip content: apglication/zip content: apglicatin fo: 388298 or, dst: Beijing Yiliyou Date Co.,Ltd	Displaying 1 - 20 of 169		
	organization and a second and a			



Further Network Forensics Evidence...





Pathology – An Awareness Concern

- The malware used in the DPRK spear phish examined here attempted FTP connections to the host "grepsync.com," which resolves to an IP address in Belarus (86.57.246.177)
- Nart Villeneuve, Chief Research Officer at the well-respected SecDev.cyber Group, pointed out in recently published research that the FTP drop zone for exfiltrated information in a similar spear phishing attack involving Zeus (packupdate.com) resolved to the same IP address in Belarus – 86.57.246.177
- In the excellent piece published by Nart, he states, "...Following the publication of the article by Brian Krebs, attackers took portions of his article and used them as a lure in further spear phishing attacks."
- "The 'Kneber' Botnet, Spear Phishing Attacks and Crimeware," Infowar Monitor, Nart Villeneuve, published March 1, 2010
 - http://www.infowar-monitor.net/2010/03/the-kneber-botnet-spear-phishing-attacks-andcrimeware/





Files harvested from victim machines in drop server (located in Minsk, Belarus)



1 -										
LSHODE (86										
250 UK, LUFT	encluirec	cory is 7								
TTP2_LS	in=65535		460	ment						
227 Entering	g Passive i	10de (86,57,2	46,177,40	9,224	н)= — — — — — — — — — — — — — — — — — — —					
150 Accepted	data con	nectionsin								
drwxr-xr-x	16 942	925	4096	Mar	7 15:51					
drwxr-xr-x	16 942	925	4096	Mar	7 15:51	Nwarel				
drwxr-xr-x	2 942	925	4096	Mar	7 09:41	1mKQgN	Atcs2S	DAX9		
drwxrexrext	2 942	925	4096	Mar	7 15:14	3L×1XU	JmDK8ZJ1	NglZ		
drwxr-xr-x	2 942	925	4096	Mar	7 08:33	Ci70rp	QKSUwol	- JIP		
drwxr-xr-x	2 942	925	4096	Mar	7 07:59	ELUSOE	3h9FXvaj	jc87		
drwxr-xr-x	2 942	925	4096	Mar	7 08:18	GSR40g	;iKFGLn	(ruy -		
drwxr-xr-x	2 942	925	4096	Mar	7 07:38	UK9zG1	LidWGrDS	Бүур		
drwxr-xr-x	2 942	925	4096	Mar	7 15:53	MNnPU2	(VIBqCs)	LKKP		
drwxr-xr-x	2 942	925	4096	Mar	7 10:24	VfwG92	cOE8Fd9	ЭЈ1у —		
drwxr-xr-x	2 942	925	4096	Mar	7 13:03	hMomRt	fEWnnCYo	oWGD 👘		
drwxr-xr-x	2 942	925	4096	Mar	7 11:05	mPm4J8	BknriULL			
drwxr-xr-x	2 942	925	4096	Mar	7 07:57	_gk0tD4	4Qp7Wd6V	/w1w		
drwxr-xr-x	2 942	925	4096	Mar	7 07:38	uzs0BF	°aXU3Bi2	ZEQR		
drwxr-xr-x	2 942	925	4096	Mar	7 06:59	yzZTtt	hcHRlK	KdJ f		
drwxr-xr-x	2 942	925	4096	Mar	7 07:07	z 5wyTr	Az7CQ9	fniY 🖪		
226-Options:										
226 16 match	nes total								D. Graces	AA sind I
ftp> cd yzZT	TtbhcHRlKK	1Jf								WEB FILLIN D
250 OK. Curr	rent direct	tory is /yzZT	tbhcHRlKk	(dJf						
ftp> ls										
227 Entering	g Passive I	Mode (86,57,2	46,177,10	09,14	Distance in and					
150 Accepted	data con	nection								
drwxr-xr-x	2 942	925	4096	Mar	7 06:59					
drwxr-xr-x	16 942	925	4096	Mar	7 15:51					
-rw-rr	1 942	925	39904	Mar	7 06:54	1051a1	LlowaDer	ns.pdf		
-rw-rr	1 942	925	65307	Mar	7 06:54	780e0e	91ccb6	dbf6e	6udymvin	7.pdf
-rw-rr	1 942	925	452141	Mar	7 06:55	AFL-CI	0-Obama	a.pdf		
-rw-rr	1 942	925	11776	Mar	7 06:55	EXCEL	.XLS			
-rw-rr	1 942	925	92795	Mar	7 06:55	JULOSE	B-Elec.r	odf		
-rw-rr	1 942	925	41011	Mar	7 06:55	Katrir	haFactS	heetEi	nal.odf	
-rw-rr	1 942	925	54895	Mar	7 06:56	Obama	odf			
-rw-rr	1 942	925	335765	Mar	7 06:56	ObamaB	Bluepri	htFord	hange.odf	
-rw-rr	1 942	925	40639	Mar	7 06:56	PC 08	Obama r	odf.		
-rw-rr	1 942	925	66601	Mar	7 06:56	PPP Pe	nn Rele	ease @	40208.ndf	
-rw-rr	1 942	925	237882	Mar	7 06:57	Senato	ur Ohama	thn.e		
-rw-rr	1 942	925	97792	Mar	7 06:57	VBATes	st Word	2K. doc		
- rw-rr	1 942	925	10752	Mar	7 06:57	WINWOR	208.000			
- rw-rr	1 942	925	1066858	Mar	7 06:59	XPL ANE	D Ohama	a Eupo	raising o	df
- rw-rr	1 942	925	828	Mar	7 06:59	C. d11			a a bring i p	
- rw-rr	1 942	925	16	Mar	7 06:59	hslit				
- ru - r r	1 942	925	20	Mar	7 06:59	Users	- d11			
- Fills Face Face	1 942	925	124499	Main	7 06:54	aBdfc3	86246524	tee3eb	iem6byog	h ndf
- FM- F F	1 942	G025 D1 0	43582	Mar	7 06:55	narale	0240050	506160	S odf	879 N & &
- FW-FF	1 942	005///	45505	Mar	7 06:55	obawa	full.+			d f
226 Option	5 C 4010 442 - 51	vsinc, 34 aggr Fiddle	1074021	nar	, 00,50	obalia	Turren	-x (- 0-	20-2000.p	
226-0ptrons:	a -d -L									
ftp>	ies total									
T CD S		Subject					Date Rev	-bavia		- D

 FTP drop hosted in Minsk, with directory listing of 14
 compromised hosts containing exfiltrated data

40 | Copyright 2010 © All rights reserved. NetWitness Corporation

NETWITNESS

S Ne	NetWitness Investigator 9 > Time graph of beaconing activity and							
: <u>⊂</u> ol	lection	Edit View Bookmarks History Help		metadata show	ing comms to C&C			
All Da	ata	North Korea > suspicious_indicators		server – all via '	"allowed pathways"			
6	No 🛞	orth Korea 🔀						
Collect		123 abc 👔 👪 🗂 📾 🚔 🌄 🚔		_	_		_	
tion	Time	Graph of Session Traffic (Sessions Per Minute)						
	Sessions	0.75 0.5 0.25 0.25				2010-03-08 06:15 >		
		Alerts (1 item)	💽 NetWitness Investigator 9				. = x	
	•	suspicious_indicators_php_files (134)	Collection Edit ⊻iew Bookmark	s <u>H</u> istory	Help			
		Service Type (1 item)	All Data		North Korea > suspicious_indicat	brs_php_files >	 ∢ ⊳ ×	
	\overline{a}	TCP Destination Port (1 item)	Page 1 of 7					
	~	Source IP Address (1 item)	2010-Mar- 06 21:37:3	IP / TCP 4 HTTP	Size Events / 1.02 00:0C:29:31:9D:73 -> 0 K8 192.168.0.32 -> 115.14	0:08:6C:BA:C4:FF 0.250.105		
	~	Destination IP address (1 item)			2 1054 -> 80 (http) 2 payload: 468 2 medium: 1			
		Destination Country (1 item)	View		Cp.flags: 27 Control to the streams: 2 Control to the streams: 10			
	9	china (134)			🧑 lifetime: 2 9 action: put			
	ø	Action Event (1 item) put (134)			directory: /templtes/a1 []] []] filename: s.php []] extension: php	6ext/int3xs/		
	.txt	Extension (1 item) php (134)			client: Mozilla/4.0	D5		
	6	Filename (1 item) s.php (134)			2=ugov_dcs040_00117135	.com S&n=1&v=16778770&i=sbnm&s=0&sp=0&lcp=0π	r=0	
		Ethernet Source [open]			Content: text/html			
		Ethernet Destination [open]			City.dst: Beijing Latdec.dst: 39.928902 Congdec.dst: 116.38829 Rog.dst: Beijing Yiliyou (98 Date Co.,Ltd.		
		IP Protocol (1 item)	3			ators_php_files	>	
							.:	



Case Study

The "Kneber" BotNet



Kneber ZeuS Botnet Statistics

- » 75,000 systems compromised with ZeuS Trojan
- >> Over half of the compromised systems also infected with Waledac
- » 68,000 stolen credentials
- » 2,000 stolen SSL certificate files
- Data cache includes complete credentials and dossier-level data sets including dumps of entire IE protected storage of individual machines
- » Victim organizations include 2,500 public (federal, state, local) and commercial sector entities (400 U.S.-based)
- Services, Online and Conventional Retail, Technology, Healthcare, Energy, Oil and Gas, Aerospace, Entertainment, Education
- » 196 countries
- > Only one month of captured data (roughly 80Gb of data analyzed)







Many Amateur (?) Criminal Opportunities



/

Compromised Credentials – Top 5



Kneber's Focus on Social Networking and E-mail





Significance of Kneber

- NetWitness found evidence that the Kneber crew has multiple data gathering goals and has been operating across the globe in a coordinated manner for over a year
- The focus in this data cache on user credentials suggests the ultimate consumer of data could be groups other than organized crime, e.g.: nation-sponsored or terrorist groups
- Both the malicious Trojans resident on the infected systems themselves and the data harvested by Kneber could be used to conduct information operations against a target with material impact:
 - Using Facebook identities and other information to steal government secrets or contractor designs for weapons
 - Using email social networking or email accounts as a vehicle for spear phishing attacks for advanced persistent threats (APT)
- The coexistence of ZeuS and Waledac suggests the goals of resilience and survivability and potential deeper cross-crew collaboration in the criminal underground





46 | Copyright 2010 $\ensuremath{\mathbb{O}}$ All rights reserved. NetWitness Corporation



Conclusions

Building Continuous Monitoring Around Common Threat Vectors



- » Data leakage
 - PII, SSN, DL, DoB, Address, etc.
 - Organization-specific content
- » Compliance monitoring and measurement
- » Counter-Intelligence
 - Outbound Network Activity
 - Inbound Network Activity
 - Top Email Competition Outbound
 - Top Email Competition Inbound
 - Email Outbound with Attachment
 - Email Outbound with Crypto

- » Network Management
 - Top IPs Initiating DMZ Sessions
 - Top IP DNS Zone Transfer
 - Externally initiated streams
 - External Access Attempt to Internal Fileserver
 - Internal DNS Server Comm with External Hosts
 - Top FTP IP Destinations by Byte Count
 - Top FTP Users
 - Top FTP Files Deleted
 - Top FTP Files Up/Downloaded
 - Top Files FTP'd
 - Top FTP Passwords
 - Top FTP Files by Byte Count
 - Top IP Addresses by 'Anonymous' FTP







Improving Incident Response and Visibility



- » MalCode / Hacker Related
 - BOTNet Activity
 - SQL Injection Scanner Executables
 - Malicious Email Attachments
 - Log "Hacking"
 - Root Access
 - password file access
 - Hacker research (URLs, hostname, newsgroups)
 - Hacker Application file Names
 - External to Internal Direct Jet
 - Username/login Buffer Overflow
 - QueryString Parameter Overflow
 - SQL Injection Scanner Executables
 - Unix commands in URL

- Web Browser as Attack Tool (phf Attack)
- IIS Buffer Overflow Attempt
- IRC Malicious Download
- IRC Malicious Open
- FTP Malicious Download
- FTP Malicious Upload
- > Anomalous Activity
 - Top IP HTTP not over port 80
 - Top IP non-HTTP over port 80
 - Top IP non-FTP over port 21
 - Top IP non-SMTP over port 25
 - TOP IP non-DNS over Port 53
 - TOP IP SSH not over port 22
 - TOP IP SSL not over 443
 - Top IP non-SSL over 443







Enforcing Security Controls

- » System Administrative
 - Top Files Accessed
 - Top Files Printed
 - Administrative Accounts
 - Most Active Email
 - Most Active Logins
 - Most Active Logoffs
 - Failed Windows Login
 - Default Cisco Router Passwords
 - Top Database Users
 - SQL Query (meta count)
 - Database by Bandwidth
 - Top IP Running Oracle
 - Top IP Running MSSQL
 - Unencrypted DB Access

- » I/T Asset Misuse
 - Gnutella/TOR/Tunneling
 - Clear-text passwords
 - Content Crypto
 - Unusual Services
 - Anonymizers
 - Yahoo Message Board Post
 - Google Message Board Post
 - Warez URL
 - Porn Sites
 - Auction Sites
 - Gambling Sites
 - Wireless Protocols
 - 2 MACS using 1 IP
 - Source Code
 - Job Searching
 - Google Searching







Understanding the Relative Value of Network Security Data



	Data Source	Description					
lest < Lowest	Firewalls, Gateways, etc.	Overwhelming amounts of data with little context, but can be valuable when used within a SEIM and in conjunction with full packet capture and network forensics reviews.					
	IDS and AV	Sometimes the first indicator of a problem, for known exploits. Can produce false positives and is signature based.					
	NetFlow	Network performance management and network behavioral anomaly detection (NBAD) tools. Indicators of changes in traffic flows within a given time slice.					
	DLP	Data leakage protection based on defined data types and security policies. Limited to specific protocols and contexts.					
	SEIM	Correlates IDS and other network and security event data and dramatically improves signal to noise ratio. Is valuable to the extent that data sources have useful information and are properly integrated.					
	Real-time Network Forensics (NetWitness)	Collects the richest network data. Provides a deeper level of advanced threat identification and analysis and traffic reconstruction.					

51 | Copyright 2010 © All rights reserved. NetWitness Corporation

High







Conclusions

- Advanced threats require a new approach to network monitoring and cyber threat analysis
- Improved situational awareness requires the use of network forensics, full packet capture, session analysis and fusion of live threat data into sensor grids



- > Enterprise information security programs can benefit significantly through:
 - Continuous augmented awareness
 - Improved incident responses through shortened time to problem recognition and resolution
 - Reduced impact and cost related to cyber incidents
 - More effective threat intelligence and investigations



Contact / Q&A

- » For More Information Contact: http://www.netwitness.com
- » For me: <u>eddie@netwitness.com</u>
- >> Join over 30,000 other security experts and download the freeware:
 - Web: <u>http://download.netwitness.com</u>
- » Twitter:
 - @netwitness
- » Blog: <u>http://www.networkforensics.com</u>



