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
Malicious Software Infects Corporate Computers

By JOHN MARKOFF
Published: February 18, 2010

A malicious software program has infected the computers of more than 2,500 corporations around the world, according to NetWitness, a computer network security firm.

More than 75,000 computer systems had cyber attacks, security firm says

By Eilean Nakashima
Washington Post Staff Writer
Thursday, February 18, 2010

More than 75,000 computer systems at nearly 2,500 companies in the United States and around the world have been hacked in what appears to be one of the largest and most sophisticated attacks by cyber criminals discovered to date, according to a northern Virginia security firm.

Hackers in Europe and China successfully broke into computers at nearly 2,500 companies and government agencies over the last 18 months in a coordinated global attack that exposed vast amounts of personal and corporate secrets to theft, according to a computer-security company that discovered the breach.

The damage from the latest cyberattack is still being assessed, and affected companies are still being notified. But data compiled by NetWitness, the closely held firm that discovered the breaches, showed that hackers gained access to a wide array of data at 2,411 companies, from credit-card transactions to intellectual property.
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
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”
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

<table>
<thead>
<tr>
<th>Quantity Range</th>
<th>Availability</th>
<th>Price in $USD</th>
</tr>
</thead>
<tbody>
<tr>
<td>5-50</td>
<td>есть в продаже</td>
<td>5.0</td>
</tr>
<tr>
<td>51-100</td>
<td>есть в продаже</td>
<td>4.5</td>
</tr>
<tr>
<td>101-500</td>
<td>есть в продаже</td>
<td>4.0</td>
</tr>
<tr>
<td>501-1000</td>
<td>есть в продаже</td>
<td>3.0</td>
</tr>
<tr>
<td>1001-5000</td>
<td>есть в продаже</td>
<td>2.0</td>
</tr>
<tr>
<td>более 10000</td>
<td>есть в продаже</td>
<td>писите</td>
</tr>
</tbody>
</table>

Если Вам нужно более 10000 карт, свяжитесь с нами, для Вас будет отдельная скидка

(Other providers sold separately)

Source: iDEFENSE

Call for Bulk Pricing
Advanced Persistent Threats (APT)

» **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

There ARE specific targets...
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

The Washington Post

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 forensic 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' 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?

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

RISK = Threats x Assets x Vulnerabilities
??
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

» Reality
  ‣ Most anti-malware technologies are signature-based, 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

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?

Tom

...good question, Tom!
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
Implementing Next Generation Intrusion Detection, Analysis and Response

» 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 (exfiltration)?
» Who is using Skype and other technologies to transfer files out of our network?

» 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?
Understanding Advanced Threat Activity

THREE USE CASES:

- Website Drive By
- Spear Phishing Attack
- Understanding BotNet Activity
Examining Advanced Threats
A “Drive-By” Attack
### Initial Glance

**High DNS count**
- Mostly MX Servers
- High SMTP count

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS (19,254)</td>
<td>Mostly MX Servers</td>
</tr>
<tr>
<td>SMTP (6,835)</td>
<td>Mostly MX Servers</td>
</tr>
<tr>
<td>HTTP (482)</td>
<td>Mostly MX Servers</td>
</tr>
</tbody>
</table>

**Feed Name**
- MindSpring (536)
- mx4.mindspring.com (482)
- mx1.mindspring.com (481)
- mx2.mindspring.com (481)
- mx3.mindspring.com (481)
- Xpl (133)
- Yahoo.com (289)
- E.mxm.mail.yahoo.com (289)
- D.mxm.mail.yahoo.com (289)
- E.mxm.mail.yahoo.com (289)
- G.mxm.mail.yahoo.com (289)
- B.mxm.mail.yahoo.com (279)
- C.mxm.mail.yahoo.com (279)
- E.mxm.mail.yahoo.com (279)
- M2.hotmail.com (265)
- M1.hotmail.com (256)
- Mx4.hotmail.com (256)
- Normal.com (256)
- Mailin-04.mx.aol.com (213)

**Errors (8 items)**
- access denied (769)
- not found (156)
- method not allowed (12)
- forbidden (9)
- bad request (5)
- request entity too large (4)
- unauthorized (2)
- not implemented (1)

**Source Country**
- United States (557)
- Germany (16)
- Russian federation (16)
- Ukraine (12)
- United Kingdom (12)
- Canada (100)
- Australia (7)
- Romania (6)
- Italy (5)
- Japan (4)
- France (5)
- Poland (5)
- Spain (5)
- Sweden (5)
- Switzerland (3)
- Austria (2)
- Belarus (2)
- Belgium (2)
- Bulgaria (2)
- Hong Kong (2)

**Destination Country**
- United States (31,359)
- Russia (20,100)
- Germany (4,449)
- China (3,505)
- France (2,980)
- Poland (2,143)
- Ukraine (1,586)
- Romania (1,495)
- Italy (1,415)
- China (1,317)
- Netherlands (1,319)
- Brazil (1,042)
- Sweden (978)
- India (938)
- Spain (801)
- Japan (737)
- Bulgaria (777)
- Korea, Republic of (71)

**Source Organization**
- Internet access point corporation (9,002)
- Margo 15 medical enterprises (6,737)
- Internet specialists west (6,390)
- America online (2,154)
- Microsoft corp. (2,154)
- Inktomi corporation (740)
- Google (12)
- Comcast cable (10)
- Oco Cym (10)
- Earthlink (7)
- Road runner (7)
- Jidt internet services (6)
- Kbs internet, wholesale isp/dsl provider (6)
- Outblaze ltd. (6)
- Point net (3)
- Theplanet.com internet services (5)
- Yahoo! broadcast services (5)
- Universa laet manheim (4)
- Yahoo! (4)

**Destination Organization**
- Internet access point corporation (1,261)
- Margo 15 medical enterprises (2,399)
- Internet specialists west (3,399)
- America online (906)
- Hosted telephone company (816)
- Atlassia company (671)
- Google (640)
- Jidt internet services (555)
- Inktomi corporation (454)
- Point net (339)
- Yahoo! (357)
- Road runner (352)
- Comcast cable (314)
- Earthlink (307)
- Yahoo! broadcast services (210)
- Cox communications (139)
- Kbs internet, wholesale isp/dsl provider (133)

**E-mail Address**
- Jerry@sox.edu (9)
- Igazolin@westriv.com (9)
- Gal@nilode.com (8)
- Magnel@quiliences.com (8)
- Somm_nguen@falconlabs.com (8)
- Yahoo@cisco.com (8)
- Dawn.buey.price@powersperrlin.com (7)
- Gerd.palagashetty@inl.com (7)
- Alex@hymail.ru (6)
- Son Nguyen @ philips.com (6)
- Axiuslab@systemsinc.com (6)
- Benjamin@unitedhealthcare.com (6)
- Bordes@ms24.hinet.net (6)
- C101@psecon.ru (6)
- faiq@fairmail.net (6)
- D_p@bigmink.net (6)
- Eike@Kwc.net (6)
- Eileen.cesio@pearsorted.com (6)
- Franklin@pip.ru (6)
2300+ email addresses

Single email subject

Randomly generated filenames
Email Content Review

» Indicators show malware is spamming: White Supremacy Forum

NetWitness Reconstruction for session ID: 4382 (Source 192.168.1.107 - 1463, Target 64.18.4.14

From: "Dennis Dillard" <magnolov@quinties.com>
To: <sgazclid@westriv.com>
Subject: Welcome brother!
Date: Sat, 18 Jul 2009 07:21:24 -0500

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

**Breadcrumb**

**Likely HTTP**

Filename (80 items):

- acefuux.png (2)
- aga.png (2)
- aintsw.png (2)
- alblacckicazvcwh.png (2)
- blcicw.png (2)
- blp.png (2)
- bssux.png (2)
- burhwyrytm.png (2)
- dwuicnvm.png (2)
- ebecm.png (2)
- fhtbzyf.png (2)
- fscov.png (2)
- fytex.png (2)
- hicsq.png (2)
- hicsq.png (2)
- hicsq.png (2)
- hicsq.png (2)
Session detail for HTTP

HTTP-PUT random named PNGs?

Suspicious query string

International destination

... 807 more of these HTTP Sessions....
Content Analysis

HTTP Put

Encoded/Encrypted content

Breadcrumb
Geographic Activity Map
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

Service Type (1 item)
  - HTTP (848)

Action Event (2 items)
  - put (744) - get (64)

Hostname Alias (20 items)
  - adoresong.com (14) - guide.opendns.com (14) - labs.iddefense.com (7) - col.stb.s-msn.com (3) - rad.msn.com (3) - www-go-b-ads2.msn.com (2) - ad.doubleclick.net (1) - ads2.msn.com (1) - b.ads1.msn.com (1) - c.msn.com (1) - clients1.google.com

Errors (7 items)
  - not found (16) - method not allowed (12) - forbidden (9) - bad request (5) - request entity too large (4) - unauthorized (2)
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)

» New features, such as the inclusion of robust Backconnect reverse proxy capabilities

» Many of these non-commercial variants are invisible to typical security tools

Source: iSightpartners
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.

Source: iSight Partners
“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 – nic@dni.gov
  ‣ Other forged senders used in same phish – e.g., ODNI@dia.mil, SSC@dia.mil
- 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@dla.mil

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

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

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

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

NATIONAL GEOGRAPHIC 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: (231) 441-6215/6211

UNITED STATES ARMY
Phone: 1-888-550-2760

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

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

UNITED STATES NAVY
Phone: (202) 372-2020

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

http://drnicenter.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
“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
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
Further Network Forensics Evidence...

» ZeuS configuration file download

» This type of problem recognition can be automated
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.”


Malware stealing files of interest to the drop server in Minsk

FTP drop server still is resolving to same address

Early on March 8, 2010, server cleaned out and account disabled

username: mao2 password: [captured]
Files harvested from victim machines in drop server (located in Minsk, Belarus)

<table>
<thead>
<tr>
<th>File Path</th>
<th>Permissions</th>
<th>Size</th>
<th>Date</th>
<th>Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>explorer.exe</td>
<td>71440</td>
<td>1584455</td>
<td>7/15/2011</td>
<td>9B49D93D57DE8CBB8F73C945B765502D</td>
</tr>
<tr>
<td>explorer.exe</td>
<td>71440</td>
<td>1584455</td>
<td>7/15/2011</td>
<td>9B49D93D57DE8CBB8F73C945B765502D</td>
</tr>
<tr>
<td>explorer.exe</td>
<td>71440</td>
<td>1584455</td>
<td>7/15/2011</td>
<td>9B49D93D57DE8CBB8F73C945B765502D</td>
</tr>
<tr>
<td>explorer.exe</td>
<td>71440</td>
<td>1584455</td>
<td>7/15/2011</td>
<td>9B49D93D57DE8CBB8F73C945B765502D</td>
</tr>
<tr>
<td>explorer.exe</td>
<td>71440</td>
<td>1584455</td>
<td>7/15/2011</td>
<td>9B49D93D57DE8CBB8F73C945B765502D</td>
</tr>
<tr>
<td>explorer.exe</td>
<td>71440</td>
<td>1584455</td>
<td>7/15/2011</td>
<td>9B49D93D57DE8CBB8F73C945B765502D</td>
</tr>
<tr>
<td>explorer.exe</td>
<td>71440</td>
<td>1584455</td>
<td>7/15/2011</td>
<td>9B49D93D57DE8CBB8F73C945B765502D</td>
</tr>
<tr>
<td>explorer.exe</td>
<td>71440</td>
<td>1584455</td>
<td>7/15/2011</td>
<td>9B49D93D57DE8CBB8F73C945B765502D</td>
</tr>
<tr>
<td>explorer.exe</td>
<td>71440</td>
<td>1584455</td>
<td>7/15/2011</td>
<td>9B49D93D57DE8CBB8F73C945B765502D</td>
</tr>
<tr>
<td>explorer.exe</td>
<td>71440</td>
<td>1584455</td>
<td>7/15/2011</td>
<td>9B49D93D57DE8CBB8F73C945B765502D</td>
</tr>
<tr>
<td>explorer.exe</td>
<td>71440</td>
<td>1584455</td>
<td>7/15/2011</td>
<td>9B49D93D57DE8CBB8F73C945B765502D</td>
</tr>
<tr>
<td>explorer.exe</td>
<td>71440</td>
<td>1584455</td>
<td>7/15/2011</td>
<td>9B49D93D57DE8CBB8F73C945B765502D</td>
</tr>
<tr>
<td>explorer.exe</td>
<td>71440</td>
<td>1584455</td>
<td>7/15/2011</td>
<td>9B49D93D57DE8CBB8F73C945B765502D</td>
</tr>
<tr>
<td>explorer.exe</td>
<td>71440</td>
<td>1584455</td>
<td>7/15/2011</td>
<td>9B49D93D57DE8CBB8F73C945B765502D</td>
</tr>
<tr>
<td>explorer.exe</td>
<td>71440</td>
<td>1584455</td>
<td>7/15/2011</td>
<td>9B49D93D57DE8CBB8F73C945B765502D</td>
</tr>
<tr>
<td>explorer.exe</td>
<td>71440</td>
<td>1584455</td>
<td>7/15/2011</td>
<td>9B49D93D57DE8CBB8F73C945B765502D</td>
</tr>
<tr>
<td>explorer.exe</td>
<td>71440</td>
<td>1584455</td>
<td>7/15/2011</td>
<td>9B49D93D57DE8CBB8F73C945B765502D</td>
</tr>
<tr>
<td>explorer.exe</td>
<td>71440</td>
<td>1584455</td>
<td>7/15/2011</td>
<td>9B49D93D57DE8CBB8F73C945B765502D</td>
</tr>
</tbody>
</table>

FTP drop hosted in Minsk, with directory listing of 14 compromised hosts containing exfiltrated data
Time graph of beaconing activity and metadata showing comms to C&C server – all via “allowed pathways”
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)
» Commercial sectors represented: Telecommunications, Financial 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

- Facebook: 3800
- Yahoo: 2600
- Hi5: 2500
- Metroflog: 1250
- Sonico: 650
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.
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

<table>
<thead>
<tr>
<th>Data Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewalls, Gateways, etc.</td>
<td>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.</td>
</tr>
<tr>
<td>IDS and AV</td>
<td>Sometimes the first indicator of a problem, for known exploits. Can produce false positives and is signature based.</td>
</tr>
<tr>
<td>NetFlow</td>
<td>Network performance management and network behavioral anomaly detection (NBAD) tools. Indicators of changes in traffic flows within a given time slice.</td>
</tr>
<tr>
<td>DLP</td>
<td>Data leakage protection based on defined data types and security policies. Limited to specific protocols and contexts.</td>
</tr>
<tr>
<td>SEIM</td>
<td>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.</td>
</tr>
<tr>
<td>Real-time Network Forensics (NetWitness)</td>
<td>Collects the richest network data. Provides a deeper level of advanced threat identification and analysis and traffic reconstruction.</td>
</tr>
</tbody>
</table>
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.netwitnes.com
» For me: eddie@netwitnes.com
» Join over 30,000 other security experts and download the freeware:
  ‣ Web: http://download.netwitnes.com
» Twitter:
  ‣ @netwitnes
» Blog: http://www.networkforensics.com