We can do better

• IDS only works if you have the right patterns, but how do you make those patterns smarter and more real-time?
  – Stop depending on the security vendor for DAT files and signature databases

• Tune your IDS to detect the threats that are custom to your environment
  – You need to extract & leverage the evidence that already exists in your own enterprise
Threat Intelligence Cycle

1. Adverse Event
2. Compromise Detected
3. Get Threat Intel from the host
4. Search Logs
5. Update NIDS
6. More Compromise
7. Scan for IOC’s
8. Reimage Machine
Evolving Threat Landscape
Evolving Threat Landscape

- Adversaries are funded and well equipped
- The bad guys are entrenched
- AV losing credibility
  - Web-based attack has 10%-45% chance of bypassing the AntiVirus protection (NSS, Q3 2010)
  - Exploit-based attack has 25%-97% chance of bypassing the AntiVirus protection (NSS, Q3 2010)
Social Networking

• A new way to target individuals and workers within a specific industry group
• It’s easy to create a false digital identity
Attack Vectors

• Spear-phishing
  – Booby-trapped documents
  – Fake-Links to drive-by websites

• Trap postings on industry-focused social networks
  – Forums, Groups (clinician list-servs, AMDIS, web forums)

• SQL injections into web-based portals
  – Employee benefit portals, external labs, etc.
Boobytrapped Documents

- Single most effective *focused* attack today
- Human crafts text
you *know* they will click it
Web-based attack

- Used heavily for large scale infections
- *Focused*, Social network targeting is possible
SQL Injection

www.somesite.com/somepage.php

SQL attack, inserts IFRAME or script tags
The web-based portal is quite helpful.
Using SEO tracker

<table>
<thead>
<tr>
<th>Domain</th>
<th>Common keywords</th>
<th>SE Keywords</th>
<th>SE Traffic</th>
<th>SE Traffic price</th>
<th>AdW Keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>google.com</td>
<td>93</td>
<td>2.5m</td>
<td>399.9m</td>
<td>863.1m</td>
<td>133.7k</td>
</tr>
<tr>
<td>wordpress.com</td>
<td>52</td>
<td>166</td>
<td>7.5k</td>
<td>7.1k</td>
<td>0</td>
</tr>
<tr>
<td>worldcare.org</td>
<td>41</td>
<td>101</td>
<td>1.5k</td>
<td>1.6k</td>
<td>0</td>
</tr>
<tr>
<td>newhealth.com</td>
<td>39</td>
<td>1.1k</td>
<td>156k</td>
<td>146.9k</td>
<td>0</td>
</tr>
<tr>
<td>redcross.org</td>
<td>34</td>
<td>442.2k</td>
<td>13.7m</td>
<td>19.8m</td>
<td>36.4k</td>
</tr>
<tr>
<td>wikipedia.org</td>
<td>32</td>
<td>17.1m</td>
<td>2702.2m</td>
<td>2204.7m</td>
<td>68</td>
</tr>
<tr>
<td>ebates.com</td>
<td>31</td>
<td>416</td>
<td>6.8k</td>
<td>3.6k</td>
<td>0</td>
</tr>
<tr>
<td>mediated.com</td>
<td>30</td>
<td>209</td>
<td>3.2k</td>
<td>3.6k</td>
<td>0</td>
</tr>
<tr>
<td>medicare.gov</td>
<td>26</td>
<td>125</td>
<td>9.9k</td>
<td>12.8k</td>
<td>1</td>
</tr>
<tr>
<td>medical.com</td>
<td>26</td>
<td>60</td>
<td>3.1k</td>
<td>3.3k</td>
<td>0</td>
</tr>
</tbody>
</table>

Full Report »
Error Messages (68 entries)
Really retarded error messages that say WAY too much!

Files containing juicy info (230 entries)
No usernames or passwords, but interesting stuff none the less.

Files containing passwords (135 entries)
PASSWORDS, for the LOVE OF GOD!!! Google found PASSWORDS!

Files containing usernames (15 entries)
These files contain usernames, but no passwords... Still, google finding use on a web site...

Footholds (21 entries)
Examples of queries that can help a hacker gain a foothold into a web server

Pages containing login portals (232 entries)
These are login pages for various services. Consider them the front door of a web site: more sensitive functions.

Pages containing network or vulnerability data (59 entries)
These pages contain such things as firewall logs, honeypot logs, network information, IDS logs... all sorts of fun stuff!

Sensitive Directories (61 entries)
Google’s collection of web sites sharing sensitive directories. The files contained here will vary from sensitive to uber-secret!

Sensitive Online Shopping Info (9 entries)
Examples of queries that can reveal online shopping info like customer data, suppliers, orders, creditcard numbers, credit card info, etc

Various Online Devices (201 entries)
This category contains things like printers, video cameras, and all sorts of cool things found on the web with Google.
My First Hit on `allinurl:~exchange/logon.asp` – I haven’t even started yet...
Perimeter-less Network

- Excuse me while I disconnect from the corporate network, I need to use my mobile hotspot to check facebook...
- The host matters more than ever
  - Regardless of the network data path, the data ends up on the host
Cyber Weapons Market

• Foreign Intelligence Services, Criminals, and Terrorist’s don’t need to have expert hackers, they can just buy exploits for money
  – Fully weaponized and ready to use
  – Mostly developed out of the Eastern Bloc
Selling Access to Your Network

- Access to your networks is being auctioned

---

**About InstallsDealer:**

You are welcome to the service for selling installs!
Advantages of working with us:
- Unique "clean installs" (uniqueness - 3 weeks)
- Flexible system of discounts depending on the transaction amount and frequency of transactions (discounts can reach 50%)
- Selection on any country in the world, except CIS
- Free test mixed-installs (10-100 pieces)
- Friendly-support
- Periodic special offers and super discounts! (check news or contact a support)
- Bonuses for regular customers!

**Our Rules:**

- Maximum file size - 500 kb
- Will not install antispy and affiliate programs
- Payments are accepted only on WMZ
- Just prepayment method

**Attention!**

Invite a friend: If a support from whom you bought installs, will invite a new buyer which will make an order for the amount of 100$, you will get a discount of 5-10% depending on the amount of the order.

**Our Price:**

<table>
<thead>
<tr>
<th>Country/Region</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK, CH</td>
<td>$175</td>
</tr>
<tr>
<td>DE, AT, ES</td>
<td>$160</td>
</tr>
<tr>
<td>DK, NO, SE</td>
<td>$155</td>
</tr>
<tr>
<td>BE, FR, IT</td>
<td>$150</td>
</tr>
<tr>
<td>CA, USA</td>
<td>$130</td>
</tr>
<tr>
<td>BR, AR</td>
<td>$60</td>
</tr>
<tr>
<td>Mix w/o asia</td>
<td>$30</td>
</tr>
<tr>
<td>Mix</td>
<td>$20</td>
</tr>
<tr>
<td>Asia</td>
<td>$10</td>
</tr>
<tr>
<td>Euromix</td>
<td>$130</td>
</tr>
</tbody>
</table>

© 2009 HBGary. All rights reserved.
They will install for you

Minimum is 1,000 installs – this would be about $100,000 for US installs.

<table>
<thead>
<tr>
<th>Region</th>
<th>Price</th>
<th>Installs per day</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mix (all countries)</td>
<td>$15</td>
<td>50-80k per day</td>
</tr>
<tr>
<td>Europe (mix without Asia)</td>
<td>$30</td>
<td>30-50k per day</td>
</tr>
<tr>
<td>Asia</td>
<td>$7</td>
<td>20-30k per day</td>
</tr>
<tr>
<td>United States</td>
<td>$100</td>
<td>5-20k per day</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>$160</td>
<td>500-1000 per day</td>
</tr>
<tr>
<td>Germany</td>
<td>$100</td>
<td>1000-2000 per day</td>
</tr>
<tr>
<td>Italy</td>
<td>$100</td>
<td>1000-2000 per day</td>
</tr>
<tr>
<td>Other Countries</td>
<td>$20-300</td>
<td>50-10000 per day</td>
</tr>
</tbody>
</table>
Recruiting All Exploiters

Pays per 1,000 infections

* http://www.secureworks.com/research/threats/ppi/*
Custom Crimeware Programming Houses

Welcome

December 14, 2009 — Posted by: Santasack

GeckoCode is a group of talented software developers whose skills cover a large range of software development, web design and graphics technologies. Our team of developers have extensive expertise in C/C++, legacy visual basic, .NET, PHP, database design and implementation, company logo and banner design... and much more.

We work with all kinds of clients, from large businesses to individuals, and we believe that custom software and graphic design should be accessible and affordable to anybody that requires such services.

We pride ourselves on taking a personal approach to our customers, no matter how small the job our main focus is that on completion our customer is happy and the solutions we provide fit their needs exactly.

We will develop you any kind of software deployed after project completion (yes, WE DO NOT CHARGE BY THE HOUR!)

Unlike other companies, we will quote accepted you will know from the outset as near as possible to the total project cost.

We provide full rights and ownership to the software/graphics over to you on project completion, and will provide you with detailed technical documents, flowcharts and time lines throughout the development period.

NO JOB TOO LARGE OR TOO SMALL

As well as large project development, we accept any kind of software/graphics related jobs. From simple website banner and logo designs right down to trivial technical support.

OUR PRICES WON'T BE BEATEN

We believe that our personal approach to customers needs, and the fact we take every customer’s current situation and overall goals into account before we even consider our quote means that you will not find a cheaper more personal solution to your custom software needs.

INSTANT MESSENGER AND LIVE WEB CHAT SUPPORT

Read more

December 14, 2009
Eleonore (exploit pack)

<table>
<thead>
<tr>
<th>browsers</th>
<th>traffic</th>
<th>loads</th>
<th>percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firefox 2.0.0</td>
<td>17</td>
<td>1</td>
<td>5.68</td>
</tr>
<tr>
<td>Firefox 3.0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Firefox 3.0.1</td>
<td>3</td>
<td>1</td>
<td>33.33</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>exploit</th>
<th>loads</th>
</tr>
</thead>
<tbody>
<tr>
<td>mem.c</td>
<td>1</td>
</tr>
<tr>
<td>Font_FireFox</td>
<td>1</td>
</tr>
<tr>
<td>op_telnet</td>
<td>2</td>
</tr>
<tr>
<td>DirectC_DS</td>
<td>3</td>
</tr>
<tr>
<td>Spreadsheet</td>
<td>4</td>
</tr>
<tr>
<td>ndac</td>
<td>12</td>
</tr>
<tr>
<td>pdf</td>
<td>58</td>
</tr>
</tbody>
</table>
# Tornado (exploit pack)

<table>
<thead>
<tr>
<th>Status</th>
<th>Exploit</th>
<th>Exploited</th>
<th>Last 24h</th>
<th>Last 1h</th>
<th>Breaking</th>
<th>Loads</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>MDAC (RDS)</td>
<td>0 (0%)</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>on</td>
<td>WVFI SetSlice</td>
<td>0 (0%)</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>on</td>
<td>VML</td>
<td>0 (0%)</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>on</td>
<td>MS06-044</td>
<td>0 (0%)</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>on</td>
<td>WMF Firefox</td>
<td>0 (0%)</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>on</td>
<td>WMF Opera 7</td>
<td>0 (0%)</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>on</td>
<td>QuickTime</td>
<td>0 (0%)</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>on</td>
<td>WinZip</td>
<td>0 (0%)</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>on</td>
<td>Zenturi</td>
<td>0 (0%)</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>on</td>
<td>Yahoo Webcam</td>
<td>0 (0%)</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>on</td>
<td>Opera 9-9.20</td>
<td>0 (0%)</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>on</td>
<td>XML Core Services</td>
<td>0 (0%)</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>off</td>
<td>empty</td>
<td>0 (0%)</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>off</td>
<td>empty</td>
<td>0 (0%)</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>on</td>
<td>Java bytecode(*)</td>
<td>0 (0%)</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>on</td>
<td>.ANI(*)</td>
<td>0 (0%)</td>
<td>0</td>
<td>0</td>
<td>0%</td>
<td>0 (0%)</td>
</tr>
</tbody>
</table>

**Totals:**
- 0 active exploits
- 0 exploited systems
- 0%
- 0 loads

**Exploits options**

- MDAC (RDS)
- WVFI SetSlice
- VML
- MS06-044
- WMF Firefox
- WMF Opera 7
- Zenturi
- Yahoo Webcam
- Opera 9-9.20
- XML Core Services
- empty
- empty
- empty
- Java code

© 2009 HBGary. All rights reserved.
Attribution
Sources of Intelligence

• Data at rest
• Data in motion
• Data in execution
  – This is the gap, and it exists only at the host
DISK FILE

In Memory Image

Internet Document
PDF, Active X, Flash
Office Document, Video, etc...

MD5 Checksum is white listed

Process is trusted

White listing on disk doesn’t prevent malware from being in memory

White listed code does not mean secure code

Public Attack-kits have used memory-only injection for over 6 years
**DISK FILE**

MD5 Checksum reliable

**IN MEMORY IMAGE**

MD5 Checksum is not consistent

Software Traits remain consistent

100% dynamic

Copied in full

Copied in part

In memory, traditional checksums don’t work
Software Traits remain consistent.

OS Loader

IN MEMORY IMAGE

Packer #1
Packer #2
Decrypted
Original

Physical memory tends to get around the ‘packing’ problem.

Software Traits remain consistent.
MD5 Checksums all different

Software Traits remain consistent

Same malware compiled in three different ways
Humans

• Attribution is about the human behind the malware, not the specific malware variants
• Focus must be on human-influenced factors

We must move our aperture of visibility towards the human behind the malware
Intel Value Window

Lifetime →
Minutes Hours Days

Blacklists

Signatures

Checksums

IP Address

DNS name

NIDS sans address

Protocol

Hooks

Install

ATTRIBUTION-Derived

Developer Toolmarks

Algorithms

Install
Intelligence Spectrum

<table>
<thead>
<tr>
<th>Blacklists</th>
<th>Net Recon C2</th>
<th>Developer Fingerprints</th>
<th>TTP</th>
<th>Social Cyberspace DIGINT</th>
<th>Physical Surveillance HUMINT</th>
</tr>
</thead>
</table>

**Nearly Useless**
- MD5 Checksum of a single malware sample

**Sweet Spot**
- IDS signatures with long-term viability
- Predict the attacker’s next moves

**Nearly Impossible**
- SSN & Missile Coordinates of the Attacker
Developer Fingerprints

- Communications Functions
- Installation & Deployment Method
- Command & Control Functions
- Compiler Environment
- Stealth & Antiforensic Techniques

Sample
- Malware
- Packing
The Flow of Forensic Toolmarks

- Core ‘Backbone’ Sourcecode
- Tweaks & Mods
- 3rd party Sourcecode
- 3rd party libraries

Compiler

Runtime Libraries

Machine

Time
Paths
MAC address

Sample

Malware
Packing

Developer
Archaeology layer

Net Recon C2

Developer Fingerprints

TTP

Actions / Intent (attacker’s behavior, as opposed to code)

Installation + Deployment method

Command + Control (primary outer loops)

CNA (spreader) CNE (search and exfil tools)

COMS (code level view, as opposed to network sniff)

Defensive / Antiforensics (usually a packer, easily changed)

Exploit weaponization / delivery vehicle

Shellcode

DNS, C2 Protocol, Encryption Method (high rate of change)
Rule #1

• The human is lazy
  – The use kits and systems to change checksums, hide from A/V, and get around IDS
  – They DON’T rewrite their code every morning
Rule #2

• Most attackers are focused on rapid reaction to network-level filtering and black-holes
  – Multiple DynDNS C2 servers, multiple C2 protocols, obfuscation of network traffic

• They are not-so-focused on host level stealth
  – Most malware is simple in nature, and works great
  – Enterprises rely on A/V for host, and A/V doesn’t work, and the attackers know this
Rule #3

- Physical memory is King
  - Once executing in memory, code has to be revealed, data has to be decrypted
Attribution Example: Paths
Paths

Developer

- Core ‘Backbone’ Sourcecode
- Tweaks & Mods
- 3rd party Sourcecode
- 3rd party libraries

Machine

Compiler

- Time
- Paths
- MAC address

Runtime Libraries

Sample

- Malware
- Packing
Example: Gh0stNet
Ghost Rat

Ghost Rat (or Gh0st RAT) is a Trojan horse for the Windows platform that the operators of GhostNet use of the most sensitive computer networks on Earth. It is a cyber spying computer program. The “RAT” part to the name of Ghost Rat comes from the phrase “Remote Administration Tool”. The operators of Ghost Rat use the RAT's ability to complete, real-time control. Such a computer can be controlled or inspected by its hackers, and effectively on the camera and audio-recording functions of an infected computer that has such capabilities, enabling

GhostNet

GhostNet (simplified Chinese: 幽灵网; traditional Chinese: 幽靈網; pinyin: Yōu Líng Wǎng) is the name given by researchers at the Information Warfare Monitor to a large-scale cyber spying operation discovered in March 2009. Its command and control infrastructure is based mainly in the People’s Republic of China and has infiltrated high-value political, economic and media locations in 103 countries. Computer systems belonging to embassies, foreign ministries and other government offices, and the Dalai Lama’s Tibetan exile centers in India, London and New York City were compromised. Although the control infrastructure is based mainly in the People’s Republic of China and has infiltrated high-value political, economic and media locations in 103 countries. Computer systems belonging to embassies, foreign ministries and other government offices, and the Dalai Lama’s Tibetan exile centers in India, London and New York City were compromised. Although the
GhostNet: Dropper

This program cannot be run in DOS mode

Embedded executable

NOTE: Packing is not fully effective here
GhostNet: Dropper

This program cannot be run in DOS mode.

The embedded executable is tagged with Chinese PRC Culture code.
GhostNet: Dropper

The embedded executable is extracted to disk. The extracted module is **not packed**. PDB path reveals malware name, E: drive.

This program cannot be run in DOS mode

E:\ghost\Server\Release\install.pdb

Embedded PDB Path
For Immediate Defense...

MD5 of the Gh0stNet dropper.EXE

PDB Path found within extracted EXE

Query: “Find Attacker’s PDB Path”

RawVolume.File.BinaryData contains "gh0st\"

← Useless →

Human →
Link Analysis

The web reveals Chinese hacker sites that reference the “gh0st\" artifact.
GhostNet: Backdoor

The dropped EXE is loaded as svchost.exe on the victim. It then drops another executable, a device driver.
Our defense...

Query: “Find Attacker’s PDB Path”

RawVolume.File.BinaryData contains “gh0st\”

Even if we had not known about the second executable, our defense would have worked. This is how moving towards the human offers predicative capability.
What do we know...

i386 directory is common to device drivers. Other clues:
1. sys directory
2. ‘SSDT’ in the name

SSDT means System Service Descriptor Table – this is a common place for rootkits and HIPS products to place hooks.

Also, embedded strings in the binary are known driver calls:
1. IoXXXX family
2. KeServiceDescriptorTable
3. ProbeForXXXX

KeServiceDescriptorTable is used when SSDT hooks are placed. We know this is a hooker.
What do we know...

| 6D 70 6C 65 74 | ....à.IofComplete |
| 01 49 6F 44 65 | eRequest..N.IoDe |
| 00 50 01 49 6F | leteDevice..P.Io |
| 6C 69 63 4C 69 | DeleteSymbolicLi |
| 76 69 63 65 44 | nk..O.KeServiceD |
| 62 6C 65 00 00 | escriptorTable.. |
| 72 69 74 65 00 | A.ProbeForWrite. |
| 65 61 64 00 00 | @.ProbeForRead.. |
| 61 6E 64 6C 65 | _except_handle |
| 61 74 65 53 79 | r3..F.IoCreateSy |
| 00 3D 01 49 6F | mbolicLink..=..Io |
| 65 00 00 19 04 | CreateDevice |

IofCompleteRequest, IoCreateDevice, IoCreateSymbolicLink, and friends are used when the driver communicates to usermode. This means there is a usermode module (a process EXE or DLL) that is used in conjunction with the device driver.

When communication takes place between usermode & kernelmode, there will be a device path.
For Immediate Defense...

MD5 of the Gh0stNet dropper.EXE

Device Path of the kernel mode driver and the Symbolic Link name

Query: “Find Rootkit Device Path or Symlink”

Physmem.WindowsObject.Name

contains

“RESSDT”
A readme file on Kasperky’s site references a Ressdt rootkit.
TMC

e:\gh0st\server\sys\i386\RESSDT.pdb

e:\job\gh0st\Release\Loader.pdb

.?AVCgh0stDoc@@

.?AVCgh0stApp@@

.?AVCgh0stView@@

Cgh0stView

Cgh0stDoc

e:\job\gh0st\Release\gh0st.pdb

C:\gh0st3.6_src\HACKER\i386\HACKE.pdb

\gh0st3.6_src\Server\sys\i386\CHENQI.pdb

Already at version 3.6

Rootkit

Dropper

GUI (MFC)

Doc/View is usually MFC

Rootkits

© 2009 HBGary. All rights reserved.
**gh0st RAT, source code, team, and forum**

www.wolfexp.net

---

**C. Rufus Security Team »Forum Statistics**

<table>
<thead>
<tr>
<th>Forum</th>
<th>User name</th>
<th>Management titles</th>
<th>Last visit</th>
<th>Leave days</th>
<th>Posts</th>
<th>Last 30 days post</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulletin Board</td>
<td>Indifferent</td>
<td>Forum Administrator</td>
<td>2010-6-28 23:38</td>
<td>16</td>
<td>91</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Comfortable reincarnation</td>
<td>Forum Administrator</td>
<td>2009-9-21 10:09</td>
<td>296</td>
<td>114</td>
<td>0</td>
</tr>
<tr>
<td>Article Cache</td>
<td>Disappear and then disappear</td>
<td>Super Moderator</td>
<td>2009-11-28 00:29</td>
<td>229</td>
<td>474</td>
<td>0</td>
</tr>
<tr>
<td>Forum Director</td>
<td>xi4oyu</td>
<td>Moderator</td>
<td>2010-6-21 12:32</td>
<td>23</td>
<td>69</td>
<td>0</td>
</tr>
<tr>
<td>General Discussion</td>
<td>Jackie Chan</td>
<td>Super Moderator</td>
<td>2009-10-16 20:23</td>
<td>271</td>
<td>86</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Sad fish</td>
<td>Moderator</td>
<td>2010-1-15 16:40</td>
<td>180</td>
<td>228</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Little Zhi</td>
<td>Super Moderator</td>
<td>2010-3-21 17:25</td>
<td>115</td>
<td>58</td>
<td>0</td>
</tr>
<tr>
<td>Today, irrigation water, say tomorrow, then</td>
<td>Alone naughty</td>
<td>Forum Administrator</td>
<td>2010-6-25 20:00</td>
<td>19</td>
<td>268</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Soul Harbour</td>
<td>Super Moderator</td>
<td>2010-7-12 23:58</td>
<td>2</td>
<td>175</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Disappear and then disappear</td>
<td>Super Moderator</td>
<td>2009-11-28 00:29</td>
<td>229</td>
<td>474</td>
<td>0</td>
</tr>
</tbody>
</table>

© 2009 HBGary. All rights reserved.
Attribution Example: Timestamps
Timestamps

Developer

Core ‘Backbone’ Sourcecode
Tweaks & Mods
3rd party Sourcecode
3rd party libraries

Compiler

Runtime Libraries

Time
Paths
MAC address

Machine

Sample
Malware
Packing
PE Timestamps

Module timestamp*

time_t (32 bit)

The ‘Imv’ command in WinDBG will show this value..

Debug timestamp

time_t (32 bit)

This is present if an external PDB file is associated with the EXE

*This is not the same as NTFS file times, which are 64 bit and stored in the NTFS file structures.
Timestamp Formats

• **time_t** – 32 bit, seconds since Jan. 1 1970 UTC
  – 0x3DE03E0A ← usually start with ‘3’ or ‘4’
    • ‘3’ started in 1995 and ‘4’ ends in 2012
  – Use ‘ctime’ function to convert

• **FILETIME** – 64 bit, 100-nanosecond intervals since Jan. 1 1600 UTC
  – 0x01C195C2.5100E190 ← usually start with ‘01’ and a letter
    • 01A began in 1972 and 01F ends in 2057
  – Use FileTimeToSystemTime(), GetDateFormat(), and GetTimeFormat() to convert
Compile times extracted from ‘soysauce’ backdoor program.
For Immediate Defense...

Compile time

Useless

Human

Query: “Find Modules Created Within Attack Window”

<table>
<thead>
<tr>
<th>RawVolume.File.CompileTime</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt; 3/1/2010</td>
</tr>
<tr>
<td>&lt; 3/31/2010</td>
</tr>
</tbody>
</table>
Attribution Example: Sourcecode
Source Code Clues

• Bad guys keep re-using their same source code
# Source Code Trade!

## Programming

<table>
<thead>
<tr>
<th>Category</th>
<th>Posts</th>
<th>Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ASM</strong></td>
<td>802</td>
<td>249</td>
</tr>
<tr>
<td>Snippets, code donations, source codes, questions and answers go here.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Basic</strong></td>
<td>21563</td>
<td>3250</td>
</tr>
<tr>
<td>Snippets, code donations, source codes, questions and answers go here.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderator: sotpot</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>C &amp; C++</strong></td>
<td>3630</td>
<td>776</td>
</tr>
<tr>
<td>Snippets, code donations, source codes, questions and answers go here.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderator: Velocihaxtor</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>.NET</strong></td>
<td>3417</td>
<td>706</td>
</tr>
<tr>
<td>C#, VB.NET, J#, Mono, ASP.NET, ADO.NET</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Other Languages</strong></td>
<td>473</td>
<td>195</td>
</tr>
<tr>
<td>Scripting, Java, Ada, D, Matlab, Ruby, Perl, and so forth.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Pascal/Delphi</strong></td>
<td>7071</td>
<td>1495</td>
</tr>
<tr>
<td>Snippets, code donations, source codes, questions and answers go here.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web Developments</strong></td>
<td>2257</td>
<td>447</td>
</tr>
<tr>
<td>Web - PHP / ASP / HTML / MySQL / Perl / CSS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderator: dime111</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Last post by M4xCoding in Re: [FASM] "Hrrhr Hack … on October 10, 2010, 02:31:07 am*

*Last post by SqUeEzEr in Re: Meltfile [Module] on Today at 04:41:25 am*

*Last post by nedo5050 in Re: C++ & the Environment… on Yesterday at 10:18:54 am*

*Last post by efrides in Re: serial for .NET React… on Yesterday at 07:40:29 pm*

*Last post by Mi4night in Re: [Python] Rapidshare A… on Yesterday at 09:53:30 pm*

*Last post by xaf0n in Re: Problems with Epeius… on Yesterday at 11:52:38 pm*

*Last post by P3H3X in Re: Need free hosting… on Today at 02:29:54 am*
Tracking Source Code

Core 'Backbone' Sourcecode
Tweaks & Mods
3rd party Sourcecode
3rd party libraries

Compiler
Runtime Libraries

Time
Paths
MAC address

Machine

Sample
Malware
Packing

Developer

© 2009 HBGary. All rights reserved.
Main Functions

• Main
  – Same argument parsing
  – Init of global variables
  – WSAStartup
• DllMain
• ServiceMain
Service Routines

- Install / Uninstall Service
- RunDll32
- Service Start/Stop
- ServiceMain
- ControlService
Skeleton of a service

DllMain()
{
    // store the HANDLE to the module in a global variable
}

ServiceMain()
{
    // RegisterServiceCtrlHandler & store handle to service in global variable
    // call SetServiceStatus, set PENDING, then RUNNING
    // call to main malware function(s)
}

ServiceCtrlHandler_Callback
{
    // handle various commands, start/stop/pause/etc
}

Sleep loop at end

dwWaitHint

Size of local buffer

Hard coded sleep( ) times
Main_Malware_Function
{
  // do stuff
}

InstallService()
{
  // OpenSCManager
  // CreateService
}

UninstallService()
{
  // OpenSCManager
  // DeleteService
}
Filename Creation

• Log files, EXE’s, DLL’s
• Subdirectories
• Environment Variables
• Random numbers
Case Study: Chinese APT

2005 posting of similar source code, includes poster’s handle.
Case Study: Chinese APT

Continued searching will reveal many, many references to the base source code of this malware.

All malware samples for this attacker are derived from this basic framework, but many additions & modifications have been made.
3rd Party SourceCode

- Core ‘Backbone’ Sourcecode
- Tweaks & Mods
- 3rd party Sourcecode
- 3rd party libraries

Compiler
- Runtime Libraries
- Time
- Paths
- MAC address

Machine

Sample
- Malware
- Packing
Format Strings

• These are written by humans, so they provide good uniqueness

http://%s:%d/%d%04d
Searching for:
- “Unable to determine” &
- “Unknown type!”

Reveals that the attacker is using the source-code of BO2k for cut-and-paste material.
```c
#define Command kmd

boxp_beta7/srv_system/main.h

81:  char *sRpmeminfo;
     // Reply: "Memory: %dM in use: %d%%  Page file: %dM free: %dM"
82:  char *sRplerrsk;
     // Reply: "Unable to determine.\n"
83:  char *sRplskrmv;
     // Reply: "Removable\n"
87:  char *sRplskram;
     // Reply: "Ramdisk\n"
88:  char *sRplskuk;
     // Reply: "Unknown type!\n"
89:  char *sRplskinfo;
     // Reply: " Bytes free: %u MB(%s)/%u MB(%s)"

prdownloads.sourceforge.net/boxp/boxp_beta7_src.zip - GPL - C - More from boxp_beta7_src.zip

boxp_beta6/srv_system/cmd_system.cpp

510:  case 0:
511:    api->plstrcat(svReply, "Unable to determine.\n");
512:    break;

548:    default:
549:      api->plstrcat(svReply, "Unknown type!\n");
550:      break;
```

```c
srp_system/cmd_system.cpp

334:    case 0:
335:      lstrcat(svReply, "Unable to determine.\n");
336:      break;

360:    default:
361:      lstrcat(svReply, "Unknown type!\n");
362:      break;
```

```c
prdownloads.sourceforge.net/bo2k/bo2kdev_src_1.1.1.zip - LGPL - C++
```
Mutex Names

Mutex names remain consistent at least for one infection-push, as they are designed to prevent multiple-infections for the same malware.
Link Analysis

Today checked out Hook键盘记录器。
不知道为会么写文件的时候会出错。
贴关键代码，看来得解决这个问题才行啊。

```c
void WriteChar(char* sText)
{
    //加锁
    HANDLE hMetux = OpenMutex(MUTEX_ALL_ACCESS, FALSE, "PsKey400");
    if(hMetux != NULL)
        WaitForSingleObject(hMetux, 300);

    FILE fp;
    if ((fp = &fopen(m_CharFileName,"ab")) == NULL)
    {
        MessageBox(NULL,"打开了出错","打开了出错",MB_OK);
        fclose(fp);
    }
    if (fwrite(sText,strlen(sText),1,fp) != 1)
    {
        MessageBox(NULL,"写入出错","写入出错",MB_OK);
        fclose(fp);
    }
    fclose(fp);
```
GhostNet: Searching for sourcecode

Search source code of the ‘Net

Large grouping of constants

Google code search labs

Search public source code.
Further refine the search by including ‘WAVE_FORMAT_GSM610’ in the search requirements...
We discover a nearly perfect ‘c’ representation of the disassembled function. Clearly cut-and-paste.

We can assume most of the audio functions are this implementation of ‘CAudio’ class – no need for any further low-level RE work.
Attribution Example:
Command and Control
Command & Control

- Communications Functions
- Installation & Deployment Method
- Command & Control Functions
- Compiler Environment
- Stealth & Antiforensic Techniques

Sample
- Malware
- Packing

Developer
Command and Control

- Remote attackers must communicate with embedded access, this is their primary weakness
- We need to detection signatures for these COMS channels
API Usage

- Once code is decrypted, remote access behaviors are always the same – if you have host access this is a great way to detect compromise.
Command and Control

Once installed, the malware phones home...

<table>
<thead>
<tr>
<th>TIMESTAMP</th>
<th>SOURCE COMPUTER USERNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>VICTIM IP</td>
<td>ADMIN?</td>
</tr>
<tr>
<td>OS VERSION</td>
<td>HD SERIAL NUMBER</td>
</tr>
</tbody>
</table>
C&C Hello Message

1) this queries the uptime of the machine..
2) checks whether it's a laptop or desktop machine...
3) enumerates all the drives attached to the system, including USB and network...
4) gets the windows username and computername...
5) gets the CPU info... and finally,
6) the version and build number of windows.
Command and Control Server

• The C&C system may vary
  – Custom protocol (Aurora-like)
  – Plain Old URL’s
  – IRC (not so common anymore)
  – Stealth / embedded in legitimate traffic

• Machine identification
  – Stored infections in a back end SQL database
A) Command is stored as a number, not text. It is checked here.

B) Each individual command handler is clearly visible below the numerical check

C) After the command handler processes the command, the result is sent back to the C&C server
Attribution Example: Algorithms
GhostNet: Screen Capture Algorithm

- Loops, scanning every 50th line (cY) of the display.
- Reads screenshot data, creates a special DIFF buffer.
- LOOP: Compare new screenshot to previous, 4 bytes at a time.
  - If they differ, enter secondary loop here, writing a ‘data run’ for as long as there is no match.
How to apply attribution
Continuous Protection

• The bad guys are going to get in. Accept it.
• Because intruders are always present, you need to have a continuous countering force to detect and remove them.
• Your continuous protection solution needs to get smarter over time – it must learn how the attackers work and get better at detecting them. Security is an intelligence problem.
The Breakdowns

• #1 – Trusting the AV
  – AV doesn’t detect most malware, even variants of malware that it’s supposed to detect

• #2 – Not using threat intelligence
  – The only way to get better at detecting intrusion is to learn how to detect them next time

• #3 – Not preventing re-infection
  – If you don’t harden your network then you are just throwing money away
The Intelligent Perimeter

- Connect host-based intelligence back to the perimeter security devices
- Extract any C2 / DNS / Protocol from physical memory and apply to NIDS
Host System Analysis

• Address all three of these:
  – Physical Memory
  – Raw Disk (forensically sound)
  – Live Operating System (for speed, agentless)

• Be able to extract artifacts from all three sources
Timelines

• Any timestamped event, regardless of source
• Make easy to extract in one step
  – User registry
  – Event log
  – MFT
  – Temporary internet files
  – Prefetch
  – Etc...
Malware Analysis

• This needs to be easy
• No more disassembly, just show me the strings!
The Solution

- Inoculate
- Update NIDS
- Intelligent Perimeter
- Adverse Event
- Compromise Detected
- More Compromise
- Scan Hosts
- Artifacts
- Malware Analysis
- Timelines
- Host Analysis
- Reimage Machine
- Get Threat Intel
Thank you

HBGary, Inc.
www.hbgary.com

For copies of this slide deck contact
Karen Burke
karen@hbgary.com