DEF CON 19
Malware Freakshow 3:
They're pwning er'body out there!

Nicholas J. Percoco & Jibran Ilyas
Agenda

• Introduction
• Evolution of Malware
• Sample Analysis + Victim + Demo
  • Sample SL2010-161 – Kameo (Grocery Store)
  • Sample SL2011-014 – Memory Dumper (Bar)
  • Sample SL2011-026 – Webcheck.dll (Work)
  • Sample SL2011-039 – Android Malware (Phone)
• Conclusions
Inspiration – “System Intruder”

“Well... There's malware on the interwebs. They're pwning all your systems, snatching your data up. So hide your cards, hide your docs, and hide your phone, 'cause they're pwning er'body out there!” – Zero Cool
Introduction – Who are these guys?

Nicholas J. Percoco (@c7five)
- Head of SpiderLabs at Trustwave
- Started my InfoSec career in the 90s
- 4\textsuperscript{th} DEF CON talk (2 more this weekend – Droid & SSL)
- Primary author of Trustwave’s Global Security Report

Jibran Ilyas (@jibranilyas)
- Senior Forensic Investigator, Spiderlabs at Trustwave
- 9 Years of InfoSec Experience
- Speaker at several Global Security Conferences like Black Hat, DEF CON, SecTor, Source Barcelona, etc.
- Masters degree from Northwestern University
Introduction – Why give a “Freakshow”? 

Exploits are commodities. 
Malware fuels the business of crime*.

*“They're pwning er'body out there!”
Introduction – What’s this about?

This the 3rd Iteration of this Talk

• 2009 – KeyLogger, MemDumper, Video Poker, Sniffer
• 2010 – MemDumper, Logon Credentials Stealer, Sniffer, Client-Side (PDF Malware)

New Targets This Year -> YOU

• Your Grocery Store
• Your Favorite Bar
• Your Work
• Your Smart Phone
Evolution of Malware - 2009

- Sloppy malware developers
- Just “testing the waters”
- No covert file system placement
- Noisy output files
- Easily detected using “Task Manager”
Evolution of Malware - 2010

• Started to use “tricky” names for executable

• Located in “system” folders

• Output still mainly in plain-text and written to disk

• Advanced tools can easily detect them

• Automated exfiltration in certain instances
Evolution of Malware - 2011

• Malware developers have grown up

• Completely subverting process analysis tools

• Many instances of ZERO data storage

• When data is stored it is ENCRYPTED

• More efficient methods resulting in small footprint

• Automation is “everywhere they want to be”
## Evolution of Malware – Network Sniffers

<table>
<thead>
<tr>
<th>Year</th>
<th>Notables</th>
</tr>
</thead>
</table>
| 2009 | • Obvious filenames  
      • Output was plain text (.cap extension)  
      • Attacker’s FTP credentials in executable |
| 2010 | • Filenames matched Windows system files  
      • Output compress and password protected  
      • Nightly auto-exfiltration functionality appeared |
| 2011 | • No output on disk  
      • Malware utilizes buffers (one to sniff, one to export)  
      • Real-time data exfiltration  
      • Encryption/Encoding of output data |
# Evolution of Malware – Memory Dumper

<table>
<thead>
<tr>
<th>Year</th>
<th>Notables</th>
</tr>
</thead>
</table>
| **2009** | • Malware kit required 3 executable files  
• No anti-forensics capabilities  
• Plain text output in “system” folders |
| **2010** | • Single executable  
• Kernel rootkit  
• Plain text output in “system folders” |
| **2011** | • Return of 3 executable files, but output file:  
• Time stomped after each update  
• Encrypted |
Evolution of Malware – Advanced Techniques

Malware Landscape Today

• **Anti-forensic features** are built into malware.
• Stolen **data is stored encrypted** and encryption algorithms are getting advanced.
• **Automated Exfiltration** features are built in so attackers don’t have to keep coming back to get the data.
• Data commonly being **exported on port 80** which is usually allowed for outbound access in most organizations.
• **Time stomping** is common.
• **Malware is a DLL** - injected into critical processes.
## Sample SL2010-161 – Kameo

<table>
<thead>
<tr>
<th>Vitals</th>
<th>Code Name: Best Supporting Actor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename: Kameo.exe</td>
<td></td>
</tr>
<tr>
<td>File Type: PE 32-bit</td>
<td></td>
</tr>
<tr>
<td>Target Platform: Windows</td>
<td></td>
</tr>
</tbody>
</table>

### Key Features
- Malware has minimal file and registry activity.
- Malware sniffs magnetic stripe data of credit cards and puts it in a buffer XYZ.
- In a separate thread, malware sends the data in buffer XYZ to hacker server via port 80.
- Exported data is encoded to defeat monitoring tools.
- There is no storage of intercepted data on disk at anytime.

### Victim
- Your Grocery Store
Demo Demo Demo Demo!
# Sample SL2011-014 – Memory Dumper

<table>
<thead>
<tr>
<th>Vitals</th>
<th>Code Name: Son of Brain Drain</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Filename: Winboot.exe</td>
</tr>
<tr>
<td></td>
<td>File Type: PE 32-bit</td>
</tr>
<tr>
<td></td>
<td>Target Platform: Windows</td>
</tr>
</tbody>
</table>

## Key Features
- Malware is installed as Windows service.
- Winboot.exe invokes two other processes: One dumps memory of processes, other parses data.
- Malware executables are time stomped to OS Install time.
- Output file is time stomped despite regular read/writes.
- Output file is encrypted.

## Victim

Your Favorite Bar
Demo Please!
# Sample SL2011-026 – Webcheck.dll

<table>
<thead>
<tr>
<th>Vitals</th>
<th>Code Name: Napoleon's Victory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename: Webcheck.dll</td>
<td>File Type: Win32 DLL</td>
</tr>
<tr>
<td>Target Platform: Windows</td>
<td></td>
</tr>
</tbody>
</table>

## Key Features

- 10KB DLL gets injected into explorer.exe
- Malware is packed so strings can’t be read.
- Monitors a specific process and records data processed by it in a hidden and encrypted file.
- At 2am, data is FTP’ed to attacker’s server.
- Outgoing file is encrypted has extension of zip file but is not actually a zip file.

## Victim

<table>
<thead>
<tr>
<th>Your Work</th>
</tr>
</thead>
</table>
This Sh*t is Live (Demo)
## Sample SL2011-039 – Android Malware

<table>
<thead>
<tr>
<th>Vitals</th>
<th>Code Name: ZiTFO (aka Zitmo)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Filename: zitmo.apk</td>
</tr>
<tr>
<td></td>
<td>File Type: Android Package</td>
</tr>
<tr>
<td></td>
<td>Target Platform: Android</td>
</tr>
</tbody>
</table>

### Key Features
- Registers an intent filter looking for SMS_RECEIVED events
- Sets this filter with a priority of 1000 (highest)
- Prevents everything else from seeing SMS messages
- Send the content of the message to the attacker’s website
- It does NOT do any form of content analysis
  - Attackers are likely collecting a lot junk texts
- It ironically appears on the phone as a package by Trusteer called “Rapport” which is used by banks to specifically prevent this type of SMS interception attack

### Victim
You
Oh No3s!
(Android Demo)
Conclusions

**Windows Malware is All Grown Up**
- We have seen the same type of malware advance over the last three years.

**Mobile Malware is Just Taking it First Steps**
- This is a new, but interesting area where we will likely see the most growth.
- Attacks are PLENTY of targets

**Where will be next year?**
- Predictions:
  - iOS/Android Malware w/ Advanced Features
  - Mobile DDoS and Spam Bots
  - Malware Focused on Stealing Corporate Credentials
Special Thanks

Eric Monti
Ryan Merritt
Sean Schulte
Zack Fasel
Zero Cool
Contact Us:

Nicholas J. Percoco / npercoco@trustwave.com / @c7five

Jibran Ilyas / jilyas@trustwave.com / @jibranilyas