



## **Black Hat USA Malware Freakshow 2010**

**Nicholas J. Percoco & Jibran Ilyas**

# Agenda

---

- About Us
- Introduction
- What's a Malware Freakshow?
- Anatomy of a Successful Malware Attack
- Sample Analysis + Victim + Demo
  - Sample SL2009-127 – Memory Rootkit Malware
  - Sample SL2010-018 – Windows Credential Stealer
  - Sample SL2009-143 – Network Sniffer Rootkit
  - Sample SL2010-007 – Client-side PDF Attack
- Conclusions

# About Us

## **Nicholas J. Percoco** / Senior Vice President at Trustwave

- 15 Years in InfoSec / BS in Computer Science
- Built and Leads the SpiderLabs team at Trustwave
- Interests:
  - Targeted Malware, Attack Prevention, Mobile Devices
    - Business / Social Impact Standpoint

## **Jibran Ilyas** / Senior Security Consultant at Trustwave

- 8 Years in InfoSec / Masters in Infotech Management from Northwestern University
- Interests:
  - Antiforensics, Artifact Analysis, Real time Defense

# Introduction

---

## **We had a busy year!!**

- Over 200 incidents in 24 different countries
- Hundreds of Samples to pick from
- We picked the most interesting for you

## **New Targets This Year**

- Sports Bar in Miami
- Online Adult Toy Store
- International VoIP Provider
- US Defense Contractor

## **Malware Developers were busy updating/improving their code**

- Many improvements to avoid detection
- Maybe they saw our Freakshow last year 😊

# What's a Malware Freakshow?

## We have access to breached environments

- These environments contain valuable data
- Smash and Grab is old school
- Attackers spend average of 156 before getting caught
- With time, comes exploration and development
- Custom and Targeted Malware is the Norm, not the exception
- Gather and perform analysis on each piece of Malware
  - **A Malware Freakshow demos samples to the security community**
  - **Benefit: Learn the sophistication of the current threats**
  - **Goal: Rethink the way we alert and defend!!!**

# Anatomy of a Successful Malware Attack

## Malware development takes a methodical approach

- Step 1: Identifying the Target
- Step 2: Developing the Malware
- Step 3: Infiltrating the Victim
- Step 4: Finding the Data
- Step 5: Getting the Loot Out
- Step 6: Covering Tracks and Obfuscation (optional)

**Before we discuss the samples, we'll cover this process.**

# Anatomy – Step 1: Identifying the Target

## Target the Data that will lead to the Money

- Credit Card Data
  - Exists in plain text in many type of environments
  - Cash is just 4 hops away
    - [Track Data]->[Fake Card]->[Fraud]->[Sale of Goods]->[Cash]**
- ATM/Debit Card Data
  - Limited to only ATM Networks and places accepting debit
  - Need PIN as well
  - Cash is just 3 hops away
    - [Track Data+PIN]->[Fake Card]->[ATM Machine]->[Cash]**

# Anatomy – Step 2: Developing the Malware

**Depends on the Target System, but focus on the Big Three**

- Keystroke Logger
- Network Sniffer
- Memory Dumper
- *Disk Parser?*

## **Design Considerations**

- Naming Convention
  - blabla.exe – not the best name choice
  - svchost.exe – much better 😊
- Functionality
  - Slow and Steady wins the race
- Persistency and Data Storage



# Anatomy – Step 3: Infiltrating the Victim

Three basic methods of planting your malware:

- **The Physical Way**
  - “Hi, I’m Ryan Jones. Look over there. pwned”
- **The Easy Way**
  - “Nice to meet you *RDP* & your friend *default password*”
- **The Über Way**
  - 0days
  - “Silent But Deadly”

# Anatomy – Step 4: Finding the Data

## The Software Holds the “Secrets”

- **Task Manager**
  - Busy Processes == Data Processing
- **Process's Folders**
  - Temp Files == Sensitive Data
- **Configuration Files**
  - Debug Set to ON == Shields Down
- **The Wire**
  - Local Network Traffic == Clear Text

# Anatomy – Step 5: Getting the Loot Out

## Keep It Simple Stupid

- Little to no egress filtering, doesn't mean use TCP 31337
- Don't Reinvent to Wheel
  - FTP
  - HTTP
  - HTTPS
  - SMTP
- IT/Security Professional Look for Freaks
  - Traffic on high ports == suspicious

# Anatomy – Step 6: Covering Tracks and Obfuscation

## Don't Be Clumsy

- *Test the Malware First!*
  - Crashing Systems = Sorta Bad
  - Filling Up Disk Space = Real Bad
  - CMD Popping Up = Just Stupid

## Mess with the Cops

- MAC times to match system install dates
- Obfuscate Output file; even just slightly
- Pack the *Bag of Tricks*
- Automate, but Randomize Events
- Rootkits

## Sample SL2009-127 – Memory Rootkit Malware

<b>Vitals</b>	<b>Code Name:</b>	Capt. Brain Drain
	<b>Filename:</b>	ram32.sys
	<b>File Type:</b>	PE 32-bit, Kernel Driver
	<b>Target Platform:</b>	Windows
<b>Key Features</b>	<ul style="list-style-type: none"><li>• Installs malware as a rootkit to stay hidden from process list</li><li>• Checks all running processes in kernel for track data</li><li>• Output dumped to file w/ “HIDDEN” and “SYSTEM” attributes</li><li>• Character substitution in output file to avoid detection</li><li>• At set time daily, malware archives data and flushes the data from output file to avoid duplication of stolen data</li></ul>	
<b>Victim</b>	<p><b>Sports Bar in Miami</b></p> <ul style="list-style-type: none"><li>• An elite location that attracts celebrities</li><li>• IT operations outsourced to Third Party</li><li>• Owner throws away security and compliance notices as monthly IT expenses “give him a headache”.</li><li>• POS System is also a DVR server</li></ul>	

## **Sample SL2009-127 – Memory Rootkit Malware**

---

# **It's Demo Time!**

## Sample SL2010-018 – Windows Credential Stealer

<b>Vitals</b>	<b>Code Name:</b>	Don't Call Me Gina
	<b>Filename:</b>	fsgina.dll
	<b>File Type:</b>	Win32 Dynamic Link Library
	<b>Target Platform:</b>	Windows
<b>Key Features</b>	<ul style="list-style-type: none"><li>• Loads with Winlogon.exe process</li><li>• Changes Windows Authentication screen to a "Domain login" screen.</li><li>• Stores stolen credentials in ASCII file on system</li><li>• Only stores successful logins</li><li>• Attempts exporting logins via SMTP to an email address.</li></ul>	
<b>Victim</b>	<b>Online Adult Toy Store</b> <ul style="list-style-type: none"><li>• A 100 person company on the West Coast of USA.</li><li>• Outsourced website hosting and dev to a low cost provider</li><li>• Admin page allows uploads of files</li><li>• Database stores card data for 10 minutes post transaction</li></ul>	

## **Sample SL2010-018 – Windows Credential Stealer**

---

# **Another Demo!**



## Sample SL2009-143 – Network Sniffer Rootkit

<b>Vitals</b>	<b>Code Name:</b>	Clandestine Transit Authority
	<b>Filename:</b>	winsrv32.exe
	<b>File Type:</b>	PE 32-bit
	<b>Target Platform:</b>	Windows
<b>Key Features</b>	<ul style="list-style-type: none"><li>• Components of malware embedded inside it - Ngrep, RAR tool and Config file</li><li>• Uses rootkit to hide malware from Task Manager</li><li>• Ngrep options contains Track Data regular expression</li><li>• At the end of the day, it RARs and password protects the temporary output file and creates new file for next day.</li><li>• Exports compressed and password protected data via FTP</li></ul>	
<b>Victim</b>	<b>International VoIP Provider</b> <ul style="list-style-type: none"><li>• Seven person company (~80,000 active customers)</li><li>• 2 methods of payment: website or kiosk</li><li>• Data Center was in barn; was home to 20 farm cats</li><li>• Payment Switch support outsourced to 3<sup>rd</sup> party</li></ul>	

## Sample SL2009-143 – Network Sniffer Rootkit

---

# Demo #3!

## Sample SL2010-007 – Client-Side PDF Attack

<b>Vitals</b>	<b>Code Name:</b>	<b>Dwight's Duper</b>
	<b>Filename:</b>	Announcement.pdf
	<b>File Type:</b>	Portable Document Format
	<b>Target Platform:</b>	Windows
<b>Key Features</b>	<ul style="list-style-type: none"><li>• Malware attached in targeted email looks to be normal PDF</li><li>• PDF contains Oday exploit (in January it was).</li><li>• Shell code executes upon PDF launch</li><li>• Shell code calls a batch file which steals all *.docx, xlsx, pptx and txt files from user's My Documents folder</li><li>• Stolen files are compressed, password protected and sent to FTP over TCP port 443</li></ul>	
<b>Victim</b>	<b>US Defense Contractor</b> <ul style="list-style-type: none"><li>• Provides analytics service to US Military</li><li>• No inbound access allowed from the Internet without VPN</li><li>• Egress filtering set to only allow TCP ports 80 and 443</li><li>• Extremely secure environment compared to previous 3</li></ul>	

## Sample SL2010-007 – Client-Side PDF Attack

---

**Last One!**

# Conclusions (What we learned in the past year)

## Customization of Malware

- One size fits all is not the mantra of attackers today

## Slow and Steady wins the race

- Malware writers are not in for quick and dirty hacks. Since data is stolen in transit, persistency is the key.

## AntiForensics

- Detection is not easy for these new age malware. MAC times are modified; random events configured and protection from detection built in.

## Automation

- Attackers adding layers to malware to automate tasks so that they don't have to come in to the system and risk detection.

## Not Slowing Down

- Since Malware Freakshow last year at DEF CON 17, the techniques have improved significantly.



## Contact Us:

**Nicholas J. Percoco / [npercoco@trustwave.com](mailto:npercoco@trustwave.com) / @c7five**

**Jibran Ilyas / [jilyas@trustwave.com](mailto:jilyas@trustwave.com) / @jibranilyas**