Trustwave®
SpiderLabs®

SecTor 2011

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 SL2011-039 – Android Malware (Phone)
  - Sample SL2011-026 – Webcheck.dll (Work)
- Conclusions

Copyright Trustwave 2011

Introduction – Who are these guys?

Nicholas J. Percoco (@c7five)

- Head of SpiderLabs at Trustwave
- Started my InfoSec career in the 90s
- Primary author of Trustwave's Global Security Report
- Research featured on MSNBC, The Wall Street Journal, Fox News, USA Today, Forbes, NPR, Dark Reading, etc.

Jibran Ilyas (@jibranilyas)

- Senior Forensic Investigator, SpiderLabs at Trustwave
- Speaker at several Global Security Conferences like Black Hat, DEF CON, SecTor, Source Barcelona, etc.
- Masters degree from Northwestern University
- Member of USSS Electronic Crimes Task Force

Copyright Trustwave 2011

Introduction – Why give a "Freakshow"?

Exploits are commodities.

Malware fuels the business of crime*.

***"They're pwning er'body out there!"**

Copyright Trustwave 2011

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

Copyright Trustwave 2011

Evolution of Malware – Network Sniffers

Year	Notables
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

Copyright Trustwave 2011

Evolution of Malware – Memory Dumper

Year	Notables
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

Copyright Trustwave 2011

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”

Copyright Trustwave 2011

Sample SL2010-161 – Kameo – Network Sniffer

Vitals	**Code Name:**	**Best Supporting Actor**
	Filename:	Kameo.exe
	File Type:	PE 32-bit
	Target Platform:	Windows
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**	

Copyright Trustwave 2011

Trustwave SpiderLabs

Sample SL2010-161 – Kameo

Demo!

Copyright Trustwave 2011

Sample SL2011-014 – Memory Dumper

Vitals	**Code Name:**	**Son of Brain Drain**
	Filename:	Winboot.exe
	File Type:	PE 32-bit
	Target Platform:	Windows
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**	

Copyright Trustwave 2011

Trustwave SpiderLabs

Sample SL2011-014 – Memory Dumper

Demo #2!

Copyright Trustwave 2011

Sample SL2011-039 – Android Malware

Vitals	**Code Name:**	**ZiTFO (aka Zitmo)**
	Filename:	zitmo.apk
	File Type:	Android Package
	Target Platform:	Android
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**	

Copyright Trustwave 2011

Trustwave SpiderLabs

Sample SL2011-039 – Android Malware

Demo #3

Copyright Trustwave 2011

Trustwave SpiderLabs

Sample SL2011-026 – Webcheck – Browser Sniffer

Vitals	**Code Name:**	**Napoleon's Victory**
	Filename:	Webcheck.dll
	File Type:	Win32 DLL
	Target Platform:	Windows
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	**Your Work**	

Copyright Trustwave 2011

Trustwave SpiderLabs

Sample SL2011-026 – Webcheck.dll

Demo #4

Copyright Trustwave 2011

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

Copyright Trustwave 2011

Special Thanks

Ryan Merritt

Sean Schulte

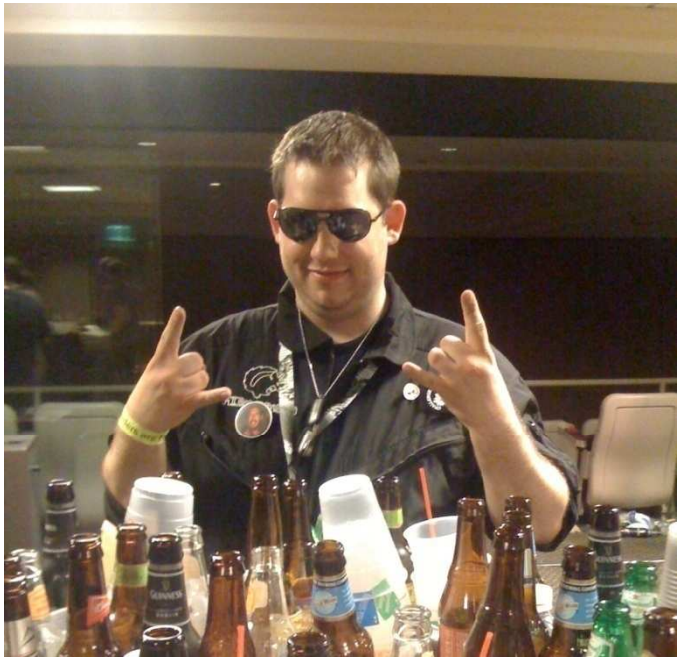
Zack Fasel

Nathan Glick

Zero Cool

Copyright Trustwave 2011

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

Copyright Trustwave 2011

Trustwave®
SpiderLabs®

Contact Us:

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

Jibran Ilyas / jilyas@trustwave.com / @jibranilyas