Trustwave®
SpiderLabs®

SecTor Security Conference

Monday Night Malware

Jibran Ilyas & Chris Pogue

Agenda

- Introduction
- Malware Intro
- Evolution of Attacks and Defenses
- Malware Types
- Demo (Infection and Detection)
- Conclusions
- Questions

About Us

Christopher Pogue
Managing Consultant for the Trustwave SpiderLabs

- Master's degree in Information Security
- Author of "Unix and Linux Forensic Analysis" by Syngress
- Author of the blog, "The Digital Standard"
- Chosen as a SANS "Thought Leader" in Digital Forensics
- Member of the USSS Electronic Crimes Task Force
- Speaker @ SANS "What Works in Incident Response" '09 and '10, The Computer Forensics Show '09 and '10, Direct Response Forum '09, SecTor '09 and '10, USSS ECTF - Miami Conference, The Next HOPE '10, BSIDESLV '10, DEF CON 18.
- Former US Army Signal Corps Warrant Officer
- Twitter Handle: @cpbeefcake

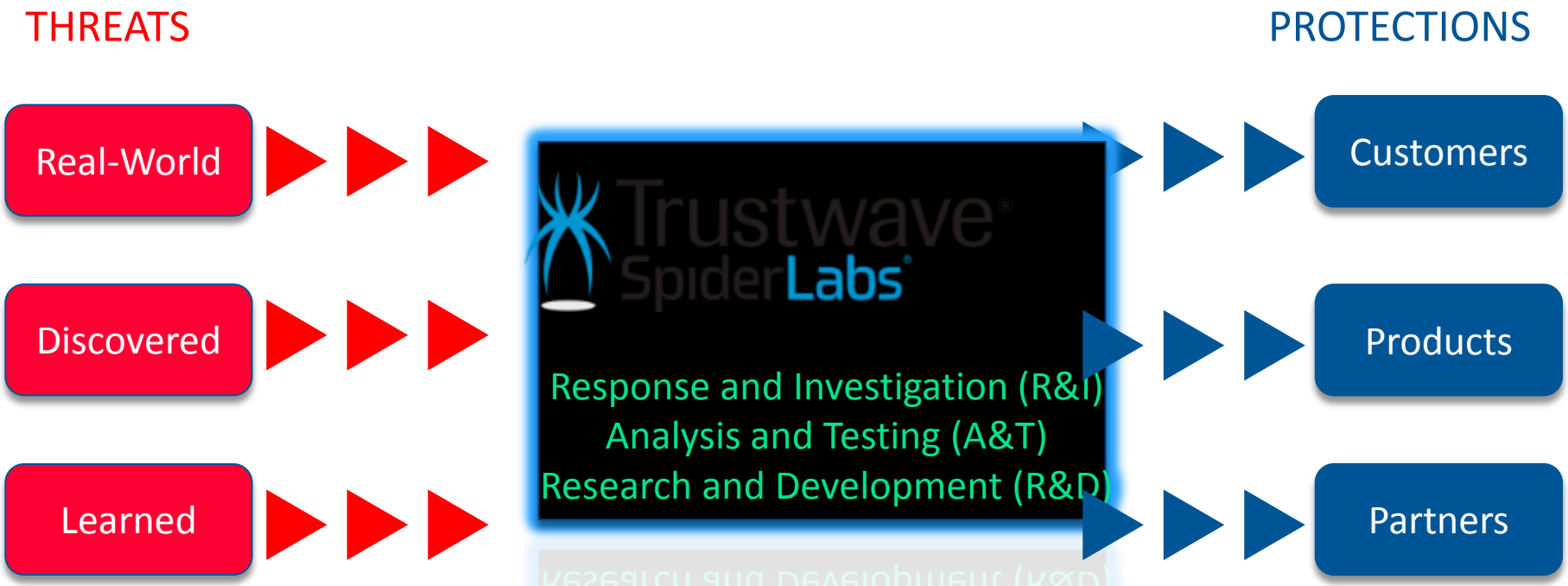
Introduction

Jibran Ilyas (@jibranilyas)

- Senior Forensic Investigator, SpiderLabs at Trustwave
- Speaker at several Global Security Conferences like Black Hat, DEF CON, SecTor, Source Barcelona, etc.
- Member of USSS Electronic Crimes Task Force
- Co-Author of Trustwave's Global Security Report
- Featured in Dark Reading, Infoworld, Threatpost, IT World and SearchSecurity
- Trained Law Enforcement in Forensics
- Masters Degree from Northwestern University
- Twitter Handle: @jibranilyas

Trustwave SpiderLabs®

Trustwave SpiderLabs uses real-world and innovative security research to improve Trustwave products, and provides unmatched expertise and intelligence to customers.



Trustwave® SpiderLabs®

Why the Monday Night Malware?

- **What is Malware:**
  - Malware, short for malicious software, is software used or created to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software. (Wikipedia)

- **Malware is dominating the hacking landscape**

- **The attackers design it to automate malicious activities; while investigators dig it to learn attacker behavior and sometimes even their identity**

Trustwave®

SpiderLabs®

Evolution of Intrusions and Data Breaches

Phase 1 - Simple

- **Attack: Smash n Grab**
  - Attackers would come into the network, look for the database containing Personally Identifiable Information (PII)
- **Detection: Very tough**
  - On a system with 80+GB, we needed to find that 'needle in the haystack' for the few minutes period that attackers accessed the network. With log retention rare, it was tough to discover the smoking gun

Phase 2 - Intermediate

- **Attack: Modification of Payment Application Config Files**
  - Since data was encrypted in the database, attackers targeted the plain text config files to toggle the debugging value from "False" to "True", to simply have the Payment Application do the work for attackers i.e. dump cardholder data in plain text file.

- **Detection: Easier**
  - Again, the attackers 'on air' time was little and we had to dig deep to find out the time period. If the files with cardholder data would be present, then we were able to correlate the MAC times with attackers' entry.

Phase 3, 4, 5, 6 … Advanced

- **Attack: Targeted Malware Infection**
  - After POS vendors locked down debugging feature and required databases to be encrypted, attackers moved to the "In Transit" attacks i.e. they created malware to steal the data while it was in transit.

- **Detection: Investigators' delight**
  - The more hacker/malware activity on the system, the better for investigators. With malware running on the system, there are too many places where evidence can be discovered from e.g. Memory, Disk, Log Files, Prefetch Files, Registry, etc.

Targeted Malware

Customized

- Malware developers a taking a methodical approach to study target systems and environments and testing before developing their toolkits.

Persistent

- Once planted on a system, the malware must survive reboots and even upgrades to be successful while propagating slowly to similar systems.

Covert

- These types of malware go unnoticed for months, even within environments with IT Security "best practices" in place.

Automated

- Targeted malware will do the job for the attackers, leaving them to just wait to receive data being harvested.

Trustwave®

SpiderLabs®

Attackers vs. Forensicators

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
2012	• All features of 2011 + the following: • Heavily packed executable • Breaks POS application's encryption

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	• 3 executables return, each with distinct function
	  • Time stomping for malware files and output file
	  • Malware Output file encrypted

2012	• Single executable • Botnet Architecture (malware fetches settings from server) • Data is exfiltrated in real time via HTTPS

Evolution of Forensic Techniques

Year	Notables
2009	• Shotgun Analysis
2010	• Live Analysis and Memory Analysis
2011	• Timeline Analysis
2012	• Heavy Focus on Anti-Forensics countermeasures • Network Analysis along with all developments from 2009-2011

Demo #1

Demo Scenario

- **A high-profile Hotel in Toronto gets compromised**
- **Attacker steals cardholder data and sells it on Black Market**
- **When cards are used fraudulently, credit card brands find out about the common point of purchase i.e. Hotel**
- **Card Brands require forensic investigation with a clear goal of finding out the risk window of cardholder data exposure so that they can notify all card issuers.**
- **The Hotel's internal IT didn't detect the breach and hired outside forensic consultants to find the breach and remove the malware**

Goals of the Attacker

- **Install Malware on Targeted System Only**
- **Make Malware Persistent**
- **Hide Tracks on the system and the network**
- **Apply Anti Forensic measures**
- **Encrypt Malware Output File**
- **Test the Malware before leaving**

Goals of the Investigator

- **Find the System that aggregates the data**
- **Conduct Live Analysis to find malicious files**
- **Find how the malware got to the system and where from**
- **Check for Anti Forensic measures**
- **Determine Timeframe of the Attack**
- **Conclusively determine what data was taken**
- **Do it in a reasonable timeframe**

MFT Analysis

- **Look at the $Standard_Information and $File_Name attributes**
  - The system and user can interact with the $S_I attribute
  - The Kernel is the ONLY thing that interacts with the $F_N attribute
  - Anti-Forensics WILL NOT affect the $F_N attribute
  - Makes attempts seem silly…VERY obvious!

Timestomping Example

BAM! Anti-Forensics – Schmanti-Schmorensics…

32324 FILE 348 1 0x38 4 1
0x0010 96 0 0x0000 0x0000
M: Mon Jun 23 12:28:52 2003 Z
A: Tue Sep 28 21:34:57 2010 Z
C: Tue Sep 28 00:18:58 2010 Z
B: Mon Jun 23 12:28:52 2003 Z ← ***Modified*** **birth date**
0x0030 112 0 0x0000 0x0000
FN: inetmgr.exe Parent Ref: 29 Parent Seq: 1
M: Wed Jun 2 17:51:20 2010 Z
A: Wed Jun 2 17:51:20 2010 Z
C: Wed Jun 2 17:51:20 2010 Z
B: Wed Jun 2 17:51:20 2010 Z ← ***Accurate*** **birth date**
0x0080 72 1 0x0000 0x0000

Conclusions

- **Don’t take malware on its face value**
  - Dig deep for hidden features and check for time stomping
- **Utilize all detection techniques to check your data**
  - Behavioral Analysis of Malware, Master File Table, Timeline, System logs, Prefetch Files, Internet History, etc.
- **Learn the attacker behavior / patterns.**
  - Every case should aid in contributing towards “Expert Eyes”

Tools and Resources

- **Mactime.pl**
  - http://wiki.sleuthkit.org/index.php?title=Mactime
- **MFT Analysis**
  - http://code.google.com/p/winforensicaanalysis/downloads/detail?na me=mft.pl
- **Log2Timeline**
  - http://log2timeline.net
- **The Digital Standard (Tutorials to use the tools)**
  - http://thedigitalstandard.blogspot.com

Trustwave®
SpiderLabs®

Contact Us:

Jibran Ilyas / jilyas@trustwave.com / @jibranilyas
Christopher Pogue / cepogue@trustwave.com / @cpbeefcake

www.trustwave.com/spiderlabs @SpiderLabs