Trustwave®

SpiderLabs℠

Cyber Crime
Past, Present and Future!

Jibran Ilyas
Senior Incident Response Consultant
MSIT 2009
Twitter: @jibranilyas

Agenda

- **About Trustwave's SpiderLabs and Source of Data**
- **Global view of Cyber Crime**
  - Reactive Engagements: Incident Response
  - Proactive Engagements: Penetration Testing
- **Malware Landscape Today**
- **Anatomy of a Successful Malware Attack**
- **Sample Analysis + Victim + Demo**
  - Sample SL2010-018 – Windows Credential Stealer
  - Sample SL2009-143 – Network Sniffer Rootkit
  - Sample SL2010-007 – Client-side PDF Attack
- **Conclusions**

Trustwave®

SpiderLabs℠

About SpiderLabs and Source of Data

About SpiderLabs

SpiderLabs is the advanced security team at Trustwave focused on incident response, penetration testing, application security and security research.

In addition, SpiderLabs provides thought leadership to the entire Trustwave organization and our clients.

SpiderLabs has responded to hundreds of security incidents, performed thousands of penetration tests and security tests hundreds of business applications for organizations ranging from the largest companies to nimble start-ups.

Members of the SpiderLabs teams are frequently asked to speak at global security conferences such as Black Hat, OWASP, SANS, and DEFCON.

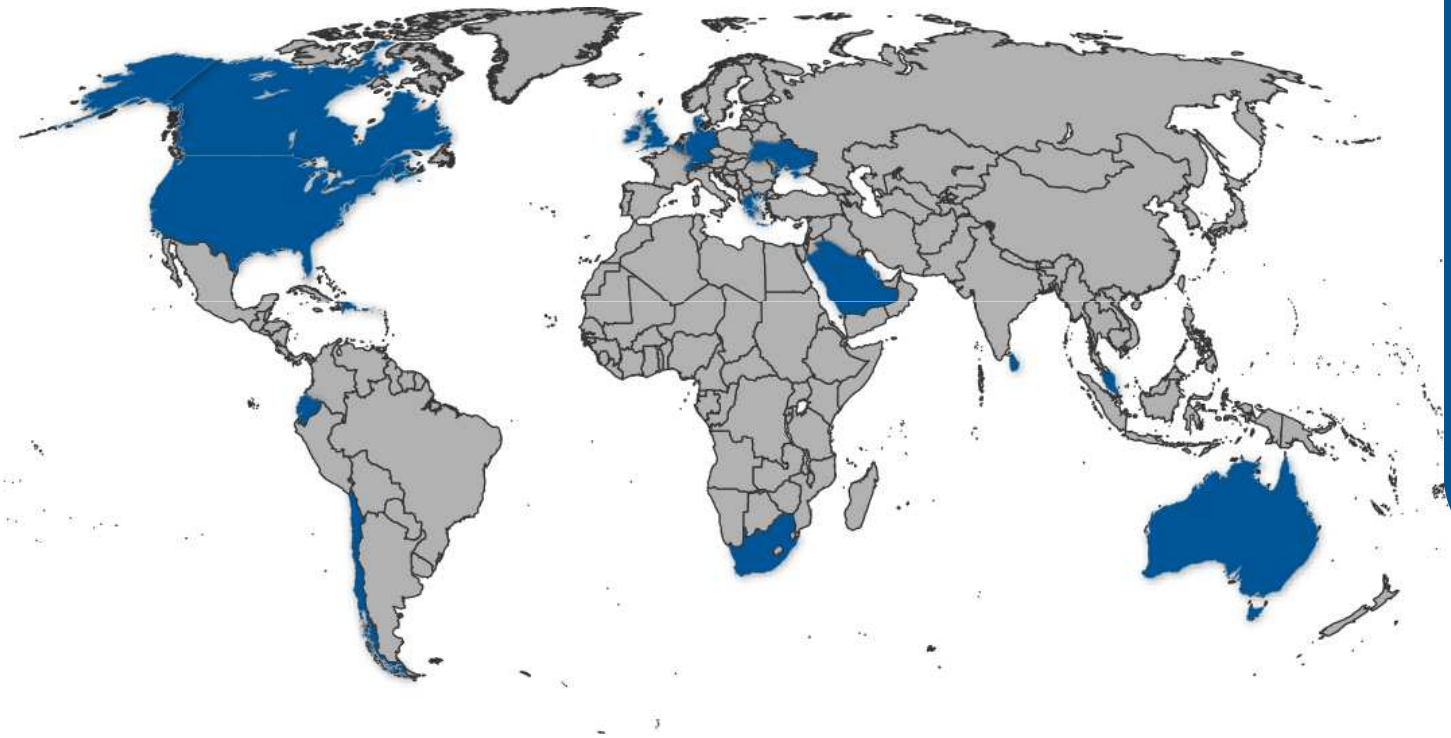
Trustwave®

SpiderLabs℠

Global Security Report 2010

Incident Response – About the Sample Set

In 2009, SpiderLabs performed 218 breach investigations in 24 countries



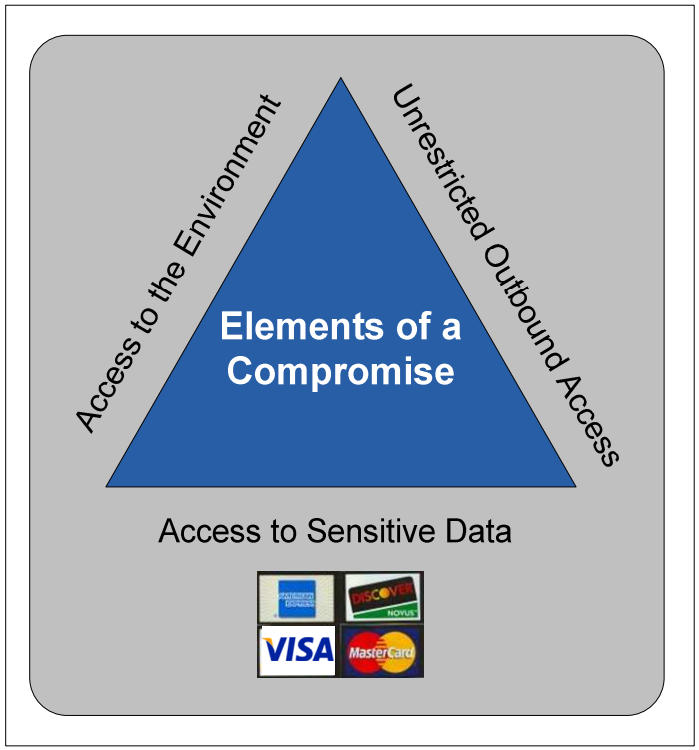
Australia
Belgium
Canada
Chile
China
Cyprus
Denmark
Dominican Republic
Ecuador
Germany
Greece
Ireland
Luxembourg
Malaysia
Puerto Rico
Saudi Arabia
South Africa
Sri Lanka
Switzerland
Ukraine
United Arab Emirates
United Kingdom
United States
Virgin Islands

Trustwave® SpiderLabs℠

Anatomy of a Data Breach

Three Components:

1. Initial Entry
2. Data Harvesting
3. Exfiltration



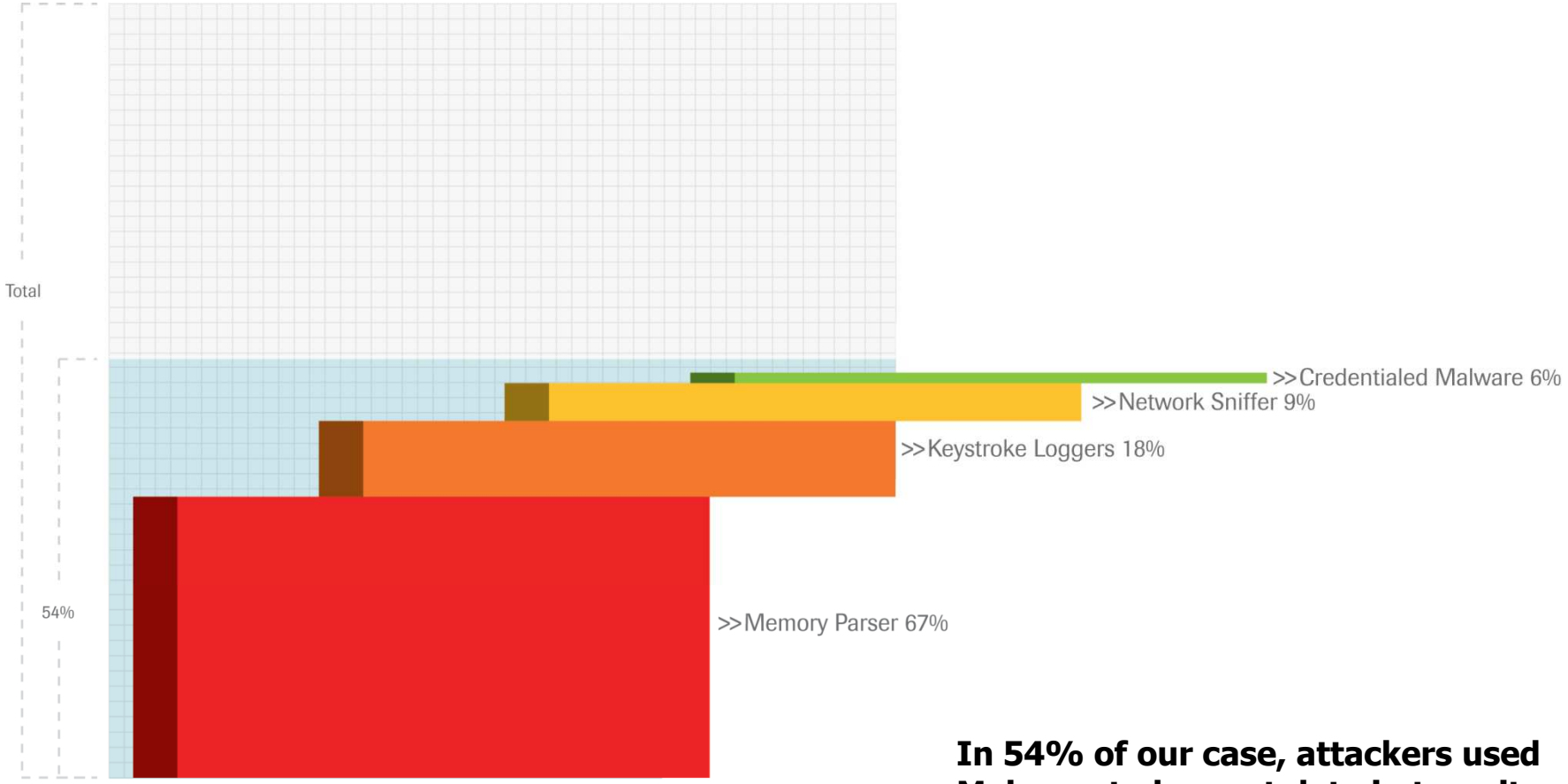
Anatomy of a Data Breach – Initial Entry

Top Methods of Entry Included:

- **Remote Access Applications**
  - Remote Desktop, VNC, pcAnywhere
- **3rd Party Connections**
  - MPLS, ATM, frame relay
- **SQL Injection**
- **Email Trojan**
  - We will see an example soon
- **Physical Access**

Anatomy of a Data Breach – Data Harvesting

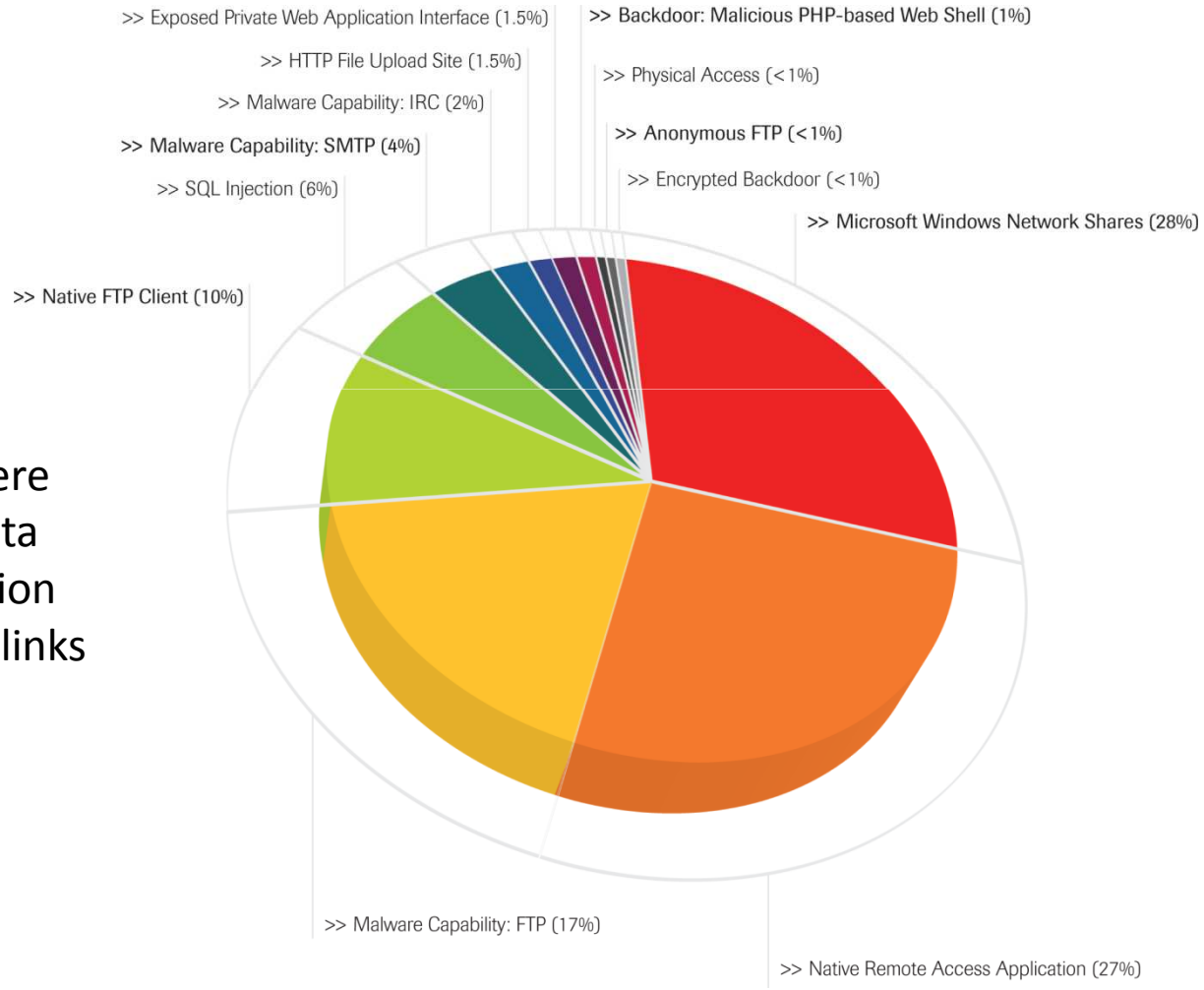
Top Methods of Harvesting (using Malware):



In 54% of our case, attackers used Malware to harvest data in transit.

Anatomy of a Data Breach – Exfiltration

Top Methods of Data Exfiltration:



Network Shares were used to transfer data between organization that had “trusted” links with each other.

Penetration Tests – About the Sample Set

In 2009, SpiderLabs performed 1,894 penetration tests in 51 countries

Most tests were performed remotely by the SpiderLabs team.

Australia
Argentina
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Croatia
Denmark
Dominican Republic
Ecuador
Egypt
France
Georgia
Germany
Greece
Hungary
Hong Kong
India
Japan
Iceland
Ireland
Lithuania
Luxembourg
Macedonia
Malaysia
Malta
Mexico
Moldova
Netherlands
Nigeria
Rep. of Cape Verde
Romania
Russian Federation
Saudi Arabia
Singapore
South Africa
Sri Lanka
Sweden
Switzerland
Taiwan
Turkey
Ukraine
United Arab Emirates
United Kingdom
United States

Trustwave® SpiderLabs℠

Penetration Tests – Top 10 – Internal Network

Rank	Vulnerability Name	Circa	Attack Difficulty
1	Address Resolution Protocol (ARP) Cache Poisoning	1999	Medium
2	Microsoft SQL Server with Weak Creds for Admin	1979	Trivial
3	Weak Password for Admin Level System Account	1979	Trivial
4	Client Sends LM Response for NTLM Authentication	1997	Medium
5	Crypto Keys Stored Alongside Encrypted Data	1974	Easy
6	Cached Domain Credentials Enabled on Hosts	1999	Easy
7	NFS Export Share Unprotected	1989	Medium
8	Sensitive Information Transmitted Unencrypted	1991	Trivial
9	Sensitive Info Stored Outside Secured Zone	1993	Trivial
10	VNC Authentication Bypass	2006	Trivial

Penetration Tests – Top 10 – Application

Rank	Vulnerability Name	Circa	Attack Difficulty	OWASP (2010)
1	SQL Injection	1998	Medium	A1
2	Logic Flaw	1985	Easy	None
3	Authorization Bypass	1997	Easy	A3
4	Authentication Bypass	1960	Easy	A4/A7
5	Session Handling	1997	Medium	A3
6	Cross-Site Scripting (XXS)	2000	Hard	A2
7	Vulnerable Third-Party Software	1960	Medium	A6
8	Cross-Site Request Forgery (CSRF)	1988	Hard	A5
9	Browser Cache-Related Flaws	1998	Medium	None
10	Verbose Errors	1980	Medium	None

The Global Remediation Plan – The Plan

Rank	Strategic Initiative
1	Perform and Maintain a Complete Asset Inventory; Decommission Old Systems
2	Monitor Third Party Relationships
3	Perform Internal Segmentation
4	Rethink Wireless
5	Encrypt Your Data
6	Investigate Anomalies
7	Educate Your Staff
8	Implement and Follow a Software Development Life Cycle (SDLC)
9	Lock Down User Access
10	Use Multifactor Authentication Every Where Possible

Take Aways

- Attackers are using old vulnerabilities
- Organizations do not know what they own or how their data flows
- Blind trust in 3rd parties is a huge liability
- Fixing new/buzz issues, but not fixing basic/old issues
- In 2010, take a step back before moving forward

Malware Landscape Today: 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.

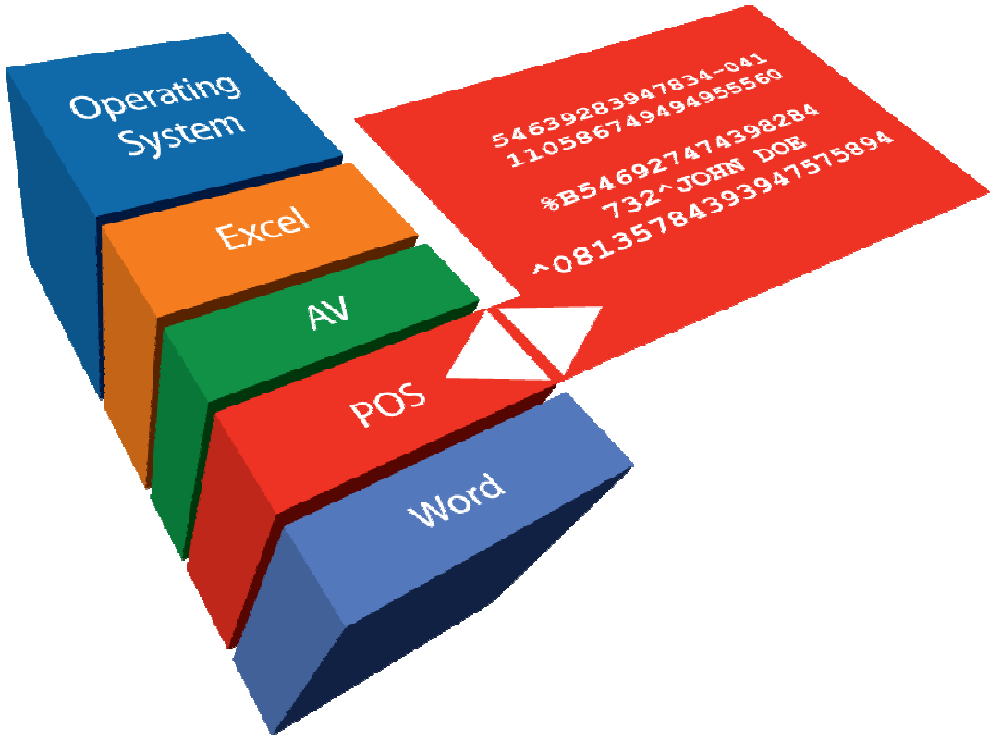
Covert

- 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.

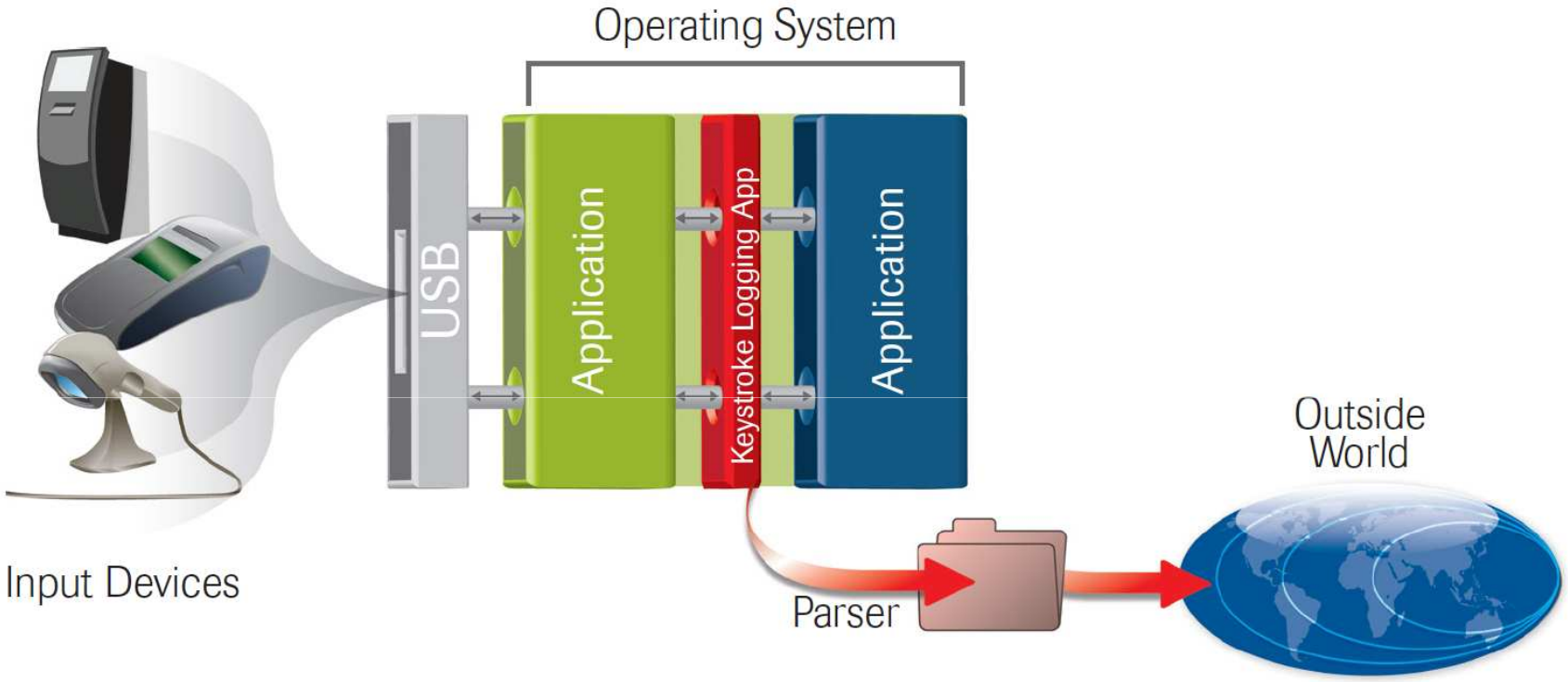
Targeted Malware: Memory Parser



- **Captures card data during computer processing**
- **Strength:** Targeted custom malware not easily detectable & can be installed anywhere in the processing chain
- **Weakness:** Seen on Windows platforms only

Trustwave® SpiderLabs℠

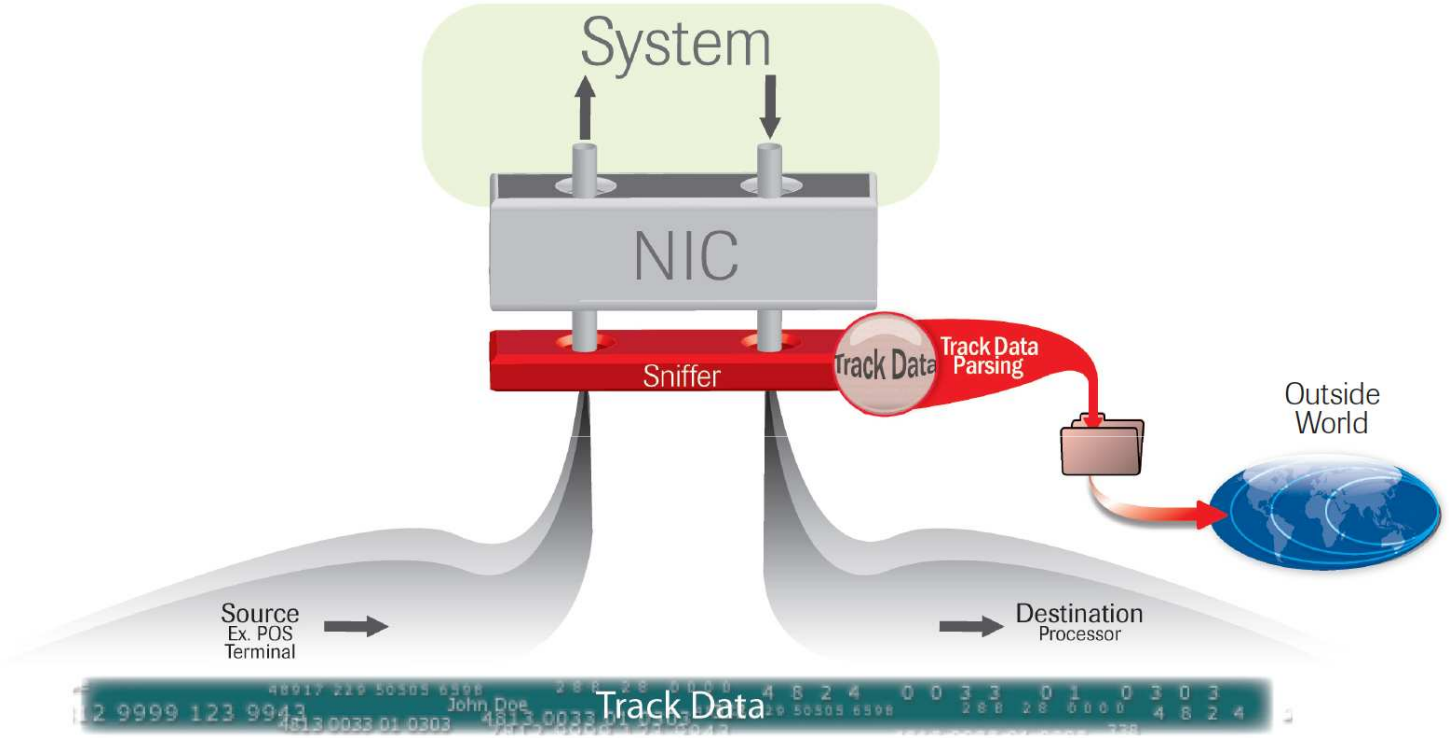
Targeted Malware: Keystroke Logger



- **Captures card data during swipe**
- **Strength:** Publicly Available, Output encryption, & upload capability
- **Weakness:** Easily detectable by AV & must be installed at point of swipe

Trustwave® SpiderLabs℠

Targeted Malware: Network Sniffer



- **Captures card data during network transmission**
- **Strength:** Multi-platform & highly customizable for environment
- **Weakness:** Must listen at a point of (unencrypted) data aggregation to be effective

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.

Sample SL2010-018 – Windows Credential Stealer

Vitals	**Code Name:**	Don't Call Me Gina
	Filename:	fsgina.dll
	File Type:	Win32 Dynamic Link Library
	Target Platform:	Windows
Key Features	• Loads with Winlogon.exe process • Changes Windows Authentication screen to a "Domain login" screen. • Stores stolen credentials in ASCII file on system • Only stores successful logins • Attempts exporting logins via SMTP to an email address.	
Victim	**Online Adult Toy Store** • A 100 person company on the West Coast of USA. • Outsourced website hosting and dev to a low cost provider • Admin page allows uploads of files • Database stores card data for 10 minutes post transaction	

Sample SL2010-018 – Windows Credential Stealer

Demo!

Sample SL2009-143 – Network Sniffer Rootkit

Vitals	**Code Name:**	Clandestine Transit Authority
	Filename:	winsrv32.exe
	File Type:	PE 32-bit
	Target Platform:	Windows
Key Features	• Components of malware embedded inside it - Ngrep, RAR tool and Config file • Uses rootkit to hide malware from Task Manager • Ngrep options contains Track Data regular expression • At the end of the day, it RARs and password protects the temporary output file and creates new file for next day. • Exports compressed and password protected data via FTP	
Victim	**International VoIP Provider** • Seven person company (~80,000 active customers) • 2 methods of payment: website or kiosk • Data Center was in barn; was home to 20 farm cats • Payment Switch support outsourced to 3rd party	

Sample SL2009-143 – Network Sniffer Rootkit

Demo #2!

Sample SL2010-007 – Client-Side PDF Attack

Vitals	**Code Name:**	**Dwight's Duper**
	Filename:	Announcement.pdf
	File Type:	Portable Document Format
	Target Platform:	Windows
Key Features	• Malware attached in targeted email looks to be normal PDF • PDF contains 0day exploit (in January it was). • Shell code executes upon PDF launch • Shell code calls a batch file which steals all *.docx, xlsx, pptx and txt files from user's My Documents folder • Stolen files are compressed, password protected and sent to FTP over TCP port 443	
Victim	**US Defense Contractor** • Provides analytics service to US Military • No inbound access allowed from the Internet without VPN • Egress filtering set to only allow TCP ports 80 and 443 • Extremely secure environment compared to previous 3	

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 SecTor, the techniques have improved significantly.

Trustwave®

SpiderLabs℠

Questions?

Trustwave®

SpiderLabs℠

Contact Info:

Jibran Ilyas
Senior Incident Response Consultant
Phone: +1 312 873-7473
Email: jilyas@trustwave.com
Twitter: @jibranilyas