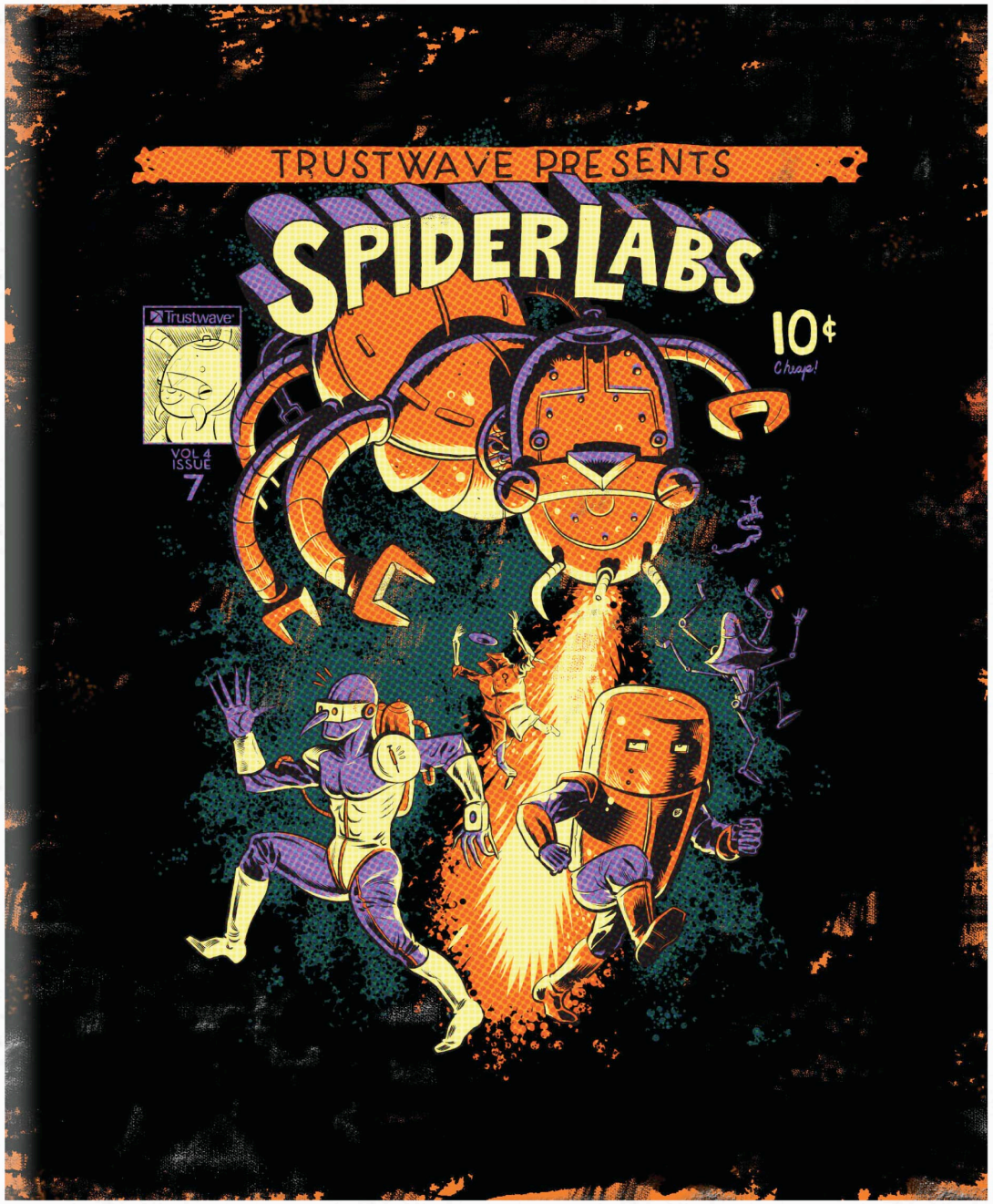


Malware freakshow DEFCON 17

Trustwave®

Nicholas J. Percoco
Jibran Ilyas
Trustwave's SpiderLabs

Agenda

- About Us
- How did we get the malware?
- Analysis Outline
- Sample A – Casino Club in Las Vegas
- Sample B – Hotel in New York
- Sample C – Video Poker in Lake Tahoe
- Sample D – Restaurant in Michigan
- Conclusions
- Tools We Like
- Contacts





About Us

Nicholas J. Percoco, Head of SpiderLabs @ Trustwave - 14 Yrs

Jibran Ilyas, Senior Forensic Analyst @ Trustwave - 5 Yrs

SpiderLabs is the advance security team at Trustwave responsible for **incident response, penetration testing and application security tests** for Trustwave's clients.

SpiderLabs has responded to **hundreds** of security incidents, performed **thousands** of penetration tests and security tested **hundreds** of business applications for Fortune 500 organizations.

How did we get the Malware?

In 2008, we visited **150 different environments** that were compromised via a number of different methods. Specifically, we saw a huge increase in **Malware** (targeted or mainstream) based attacks.

The basic method of acquisition was visit the location**, live analysis, memory dumps, and disk imaging.**

After we had a copy of the sample, it was taken back to SpiderLabs for further analysis. SpiderLabs has two physical laboratories - **Chicago** and **London**.

The contents of this talk is a walk through of what found to be some of more interesting samples we have in our collection going from simple and common to rare and complex.

Analysis Outline

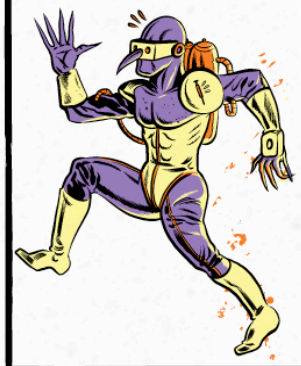
During this presentation we are going to present each case in the following way:

- **Architecture and Problems**
  - What did the Target Environment look like?
- **Tools Found**
  - What did the attackers leave behind?
- **Installation Vector**
  - How did it end up in the Target Environment?
- **Static Analysis / Dynamic Analysis**
  - A deeper look at the Malware with and without executing it.
- **Data Exfiltration / Propagation**
  - What damage did it do?
- **Live Demo**
  - The malware in action - live in a VM environment.



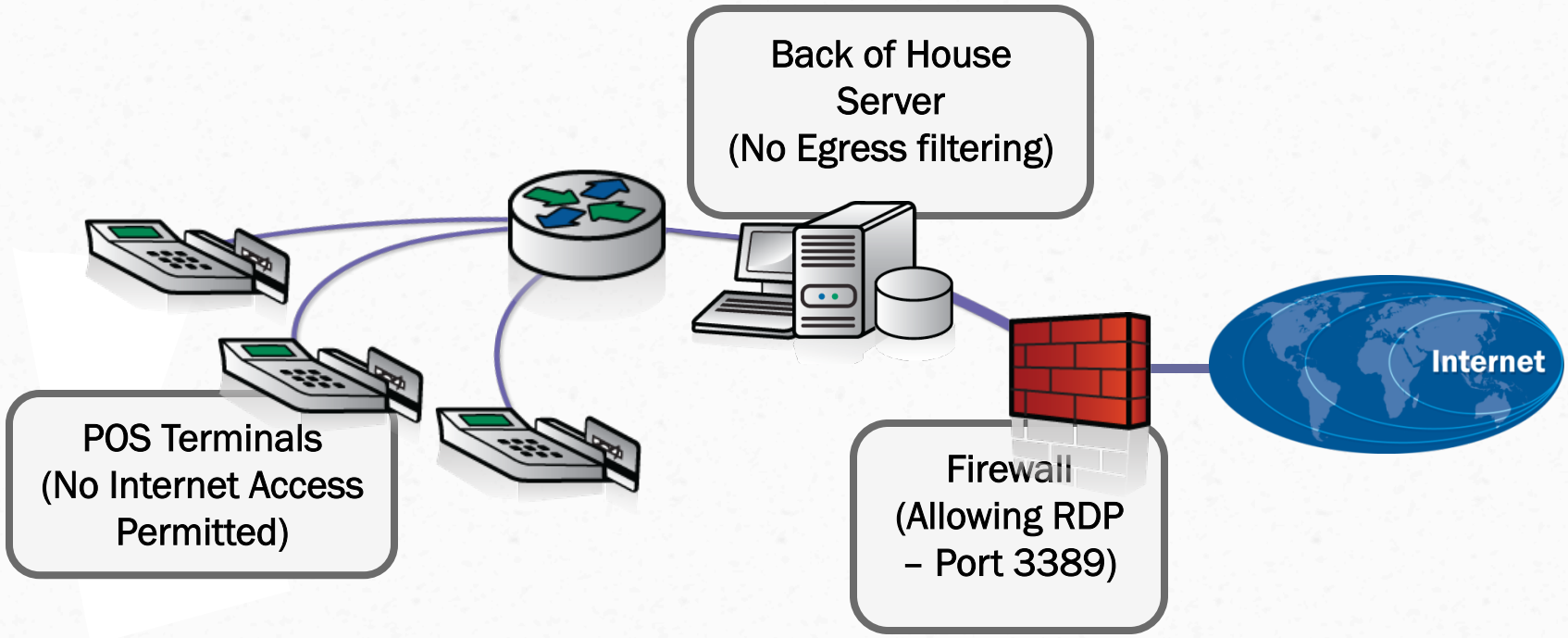
Sample A:

Casino Club in Las Vegas



Trustwave®

Sample A - Architecture



Sample A – Problems

- Remote Desktop allowed from Internet to Club POS Server
- Weak / Common passwords
  - E.g. <pos name> : <pos name>
    <pos name user> : <pos name user>
  - Beauty of life lies in simplicity
- Antivirus had not been updated since last POS software upgrade i.e. 8 months
- Customer data carried from two previous owners of the systems.
  - Data was not wiped between owners!!!!
- Casino's network was very flat and lacked "physical" network security controls.

Sample A – Tools Found

Name	Size	MD5 Hash	Description
XXX[1].EXE	680KB	7c0444811ef6a9ad8551215707cecfa9	Unprotected SFX archive containing Keylogger and Putty
PUTTY.EXE	444KB	9BB6826905965C13BE1C84CC0FF83F42	Putty (SSH Client)
XXX.EXE	**424KB**	**994FFAE187F4E567C6EFEE378AF66AD0**	**Main Keylogger executable**
A0045175.exe	**1,969KB**	**cd6d403474e7c94a7ea81ce652d8ccf8**	**SMTP Server (original name 1st.exe)**

Sample A – Installation Vector

- Entry via Remote Desktop from IP in United States (216.15.X.X)
  - Targeted account was "posuser"
- Downloaded an unprotected SFX archive from FTP site in United States (drugzseller.xxxxx.com)
- SFX Archive had Keylogger and Putty executable
- Purchased and Installed SMTP Server on Club POS server
  - Remember POS Terminals not allowed to access the Internet, thus Club POS server used as the outbound SMTP proxy
- Used VNC to get to POS Terminals and install Keylogger

Sample A – Installation Vector

Index of /

Name	Last modified	Size	Description
Parent Directory	14-Sep-2008 07:09	-	
1ST.exe	14-Sep-2008 07:27	3.9M	
71.tgz	29-Oct-2008 09:03	294k	
ACARET.exe	14-Sep-2008 07:27	665k	
MSVCP60.DLL	14-Sep-2008 07:27	392k	
Q.exe	24-Oct-2008 10:51	1.8M	
TOY.exe	14-Sep-2008 07:28	122k	
TS.exe	14-Sep-2008 07:28	168k	
UltraVNC-102-Setup.exe	14-Sep-2008 07:24	1.7M	
X.exe	28-Oct-2008 05:43	168k	
X1.exe	09-Oct-2008 12:40	168k	
X2.exe	26-Sep-2008 19:55	168k	
X3.exe	06-Oct-2008 22:54	168k	
XXX.exe	14-Sep-2008 07:24	472k	
rdp.tgz	14-Sep-2008 07:28	302k	
tmp/	02-Oct-2008 13:22	-	
wrar38b5.exe	14-Sep-2008 20:06	1.2M	

Attacker's server with tools

Trustwave®

Sample A – Installation Vector

The following is a summary of your order. Please review the details and then click on the *Complete Transaction* button to complete the checkout process.

Cardholder Details		Transaction Details	
Name :	Betty [redacted]	Card Number :	(*last 4 digits*) 0658
Company Name :		Expiry Date :	04 / 09
Street Address :	214[redacted]	Security Code :	***
		Issue Number :	
City :	Moneett		
State/Province :	MO	Card Type :	Visa
Zip/Postal Code :	65[redacted]	Order Number :	U30072404
Country :	United States		
E-Mail Address :	drugzseller2@[redacted]		
Alternative E-Mail :			

Product Code	Name	Comments	Price	License Pack	Quantity	Net Total
4507SMTP	1st SMTP Server	Single	US $69.00	1 - User License Keycode by email	1	US $69.00
					Net Total	US $69.00
					Grand Total	US $69.00

Complete Transaction

Attacker buying SMTP serverwhile on Club POS Server

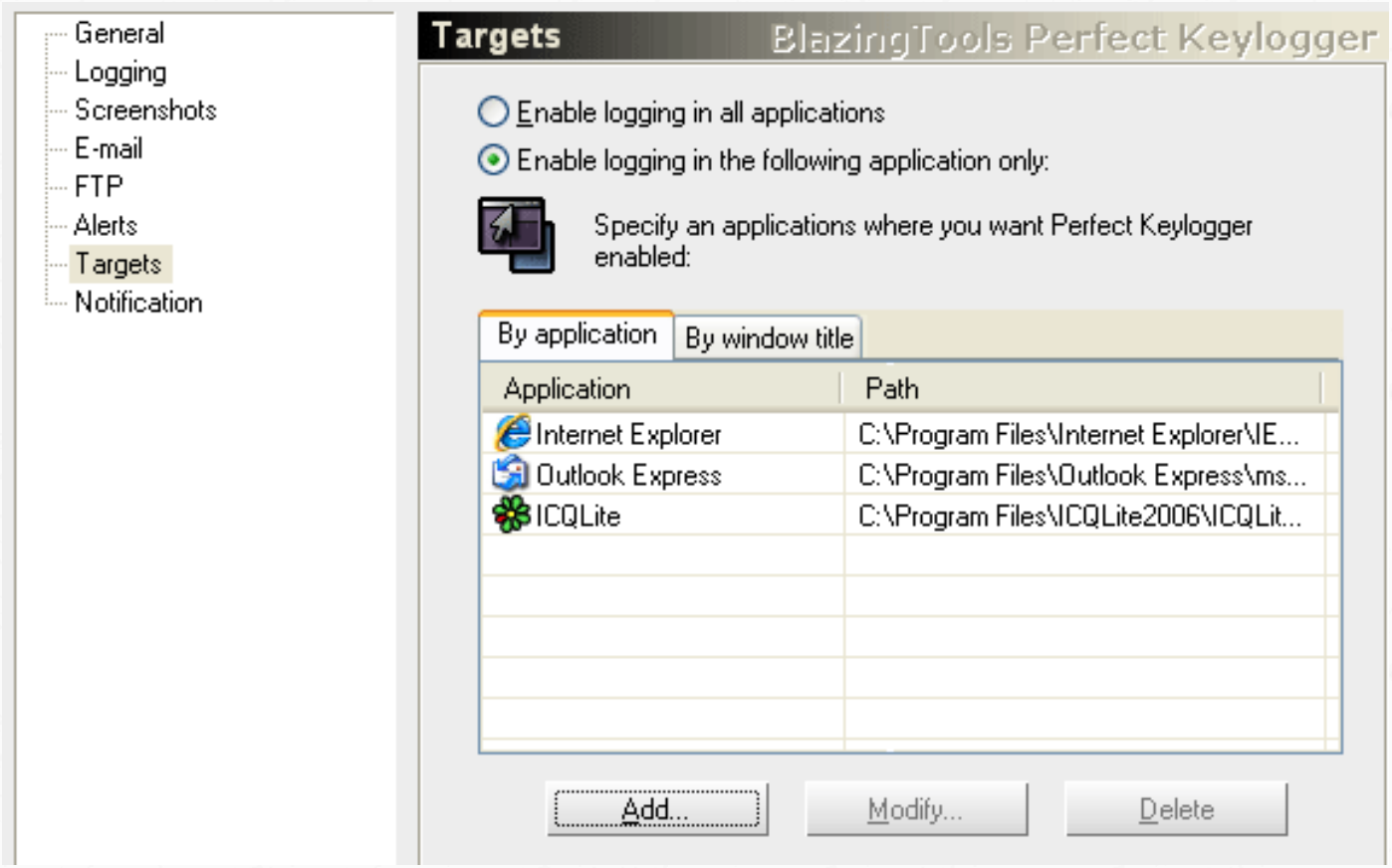
Sample A – Dynamic Analysis

XXX.EXE

- Installed in C:\Program Files\outlook folder of the system
  - Other possible locations include:
    - C:\Windows\Security
    - C:\Windows\System32
    - C:\Program Files\BPK
- Uses Keylogger's properties to hide from task manager, start menu and system tray ; uses a keyboard combination to unlock
- Creates a BPK.dat file which can be opened only by Keylogger's log viewer; contains full credit card track data
- Keylogger also takes screenshots of system at regular intervals; doesn't spare attacker activity either

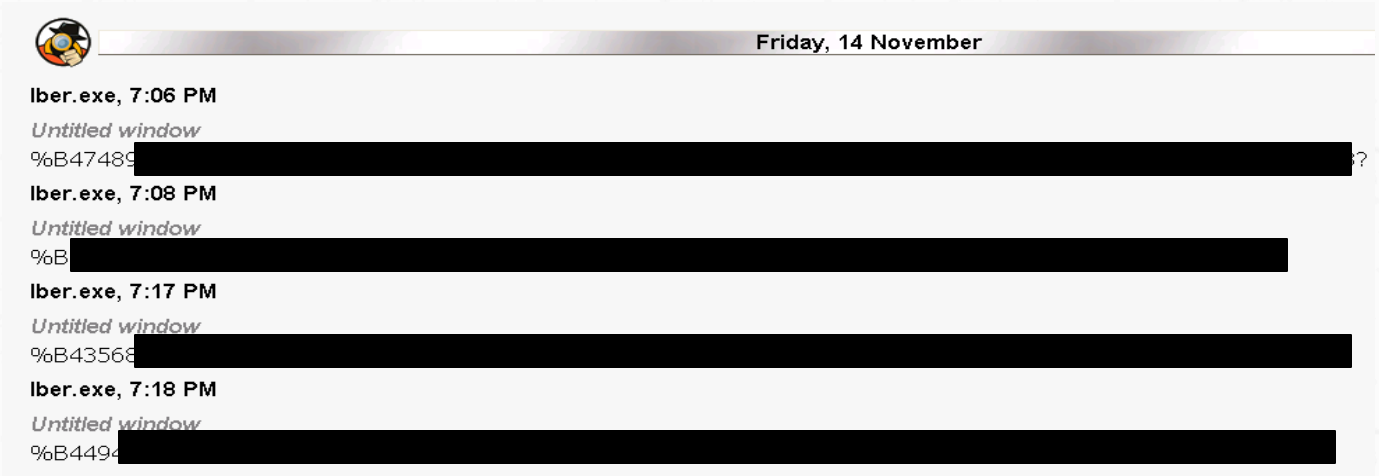
Sample A – Dynamic Analysis

XXX.EXE



Sample A – Data Exfiltration

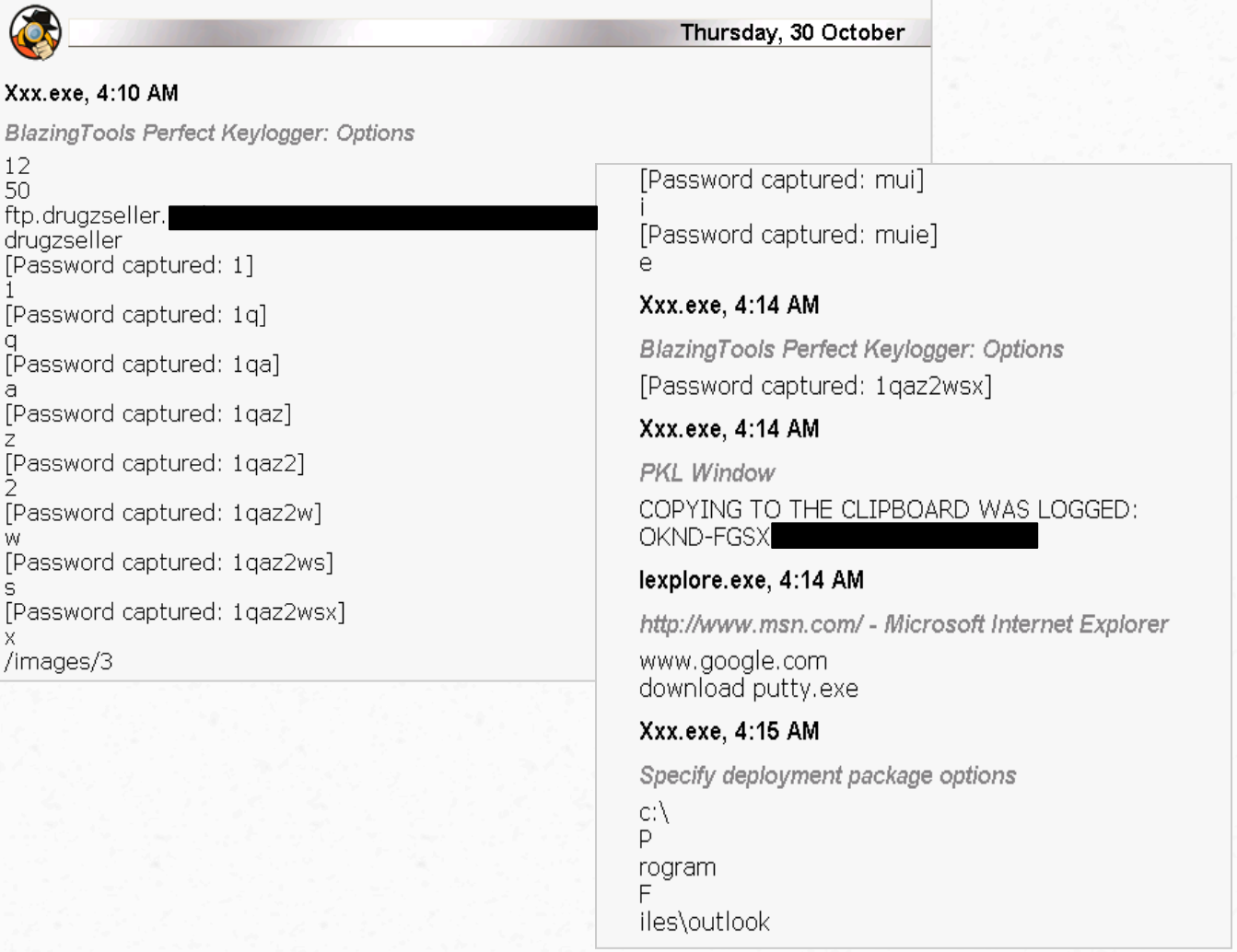
Data was collected in BPK.DAT file



Data was exported via SMTP server to montana2XXXXX@xxxx.com

Trustwave®

Sample A – Data Exfiltration



Thursday, 30 October

Xxx.exe, 4:10 AM

BlazingTools Perfect Keylogger: Options

12
50
ftp.drugzseller.[redacted]
drugzseller
[Password captured: 1]
1
[Password captured: 1q]
q
[Password captured: 1qa]
a
[Password captured: 1qaz]
z
[Password captured: 1qaz2]
2
[Password captured: 1qaz2w]
w
[Password captured: 1qaz2ws]
s
[Password captured: 1qaz2wsx]
x
/images/3
[Password captured: mui]
i
[Password captured: muie]
e

Xxx.exe, 4:14 AM

BlazingTools Perfect Keylogger: Options

[Password captured: 1qaz2wsx]

Xxx.exe, 4:14 AM

PKL Window

COPYING TO THE CLIPBOARD WAS LOGGED:
OKND-FGSX[redacted]

Iexplore.exe, 4:14 AM

http://www.msn.com/ - Microsoft Internet Explorer

www.google.com
download putty.exe

Xxx.exe, 4:15 AM

Specify deployment package options

c:\
P
rogram
F
iles\outlook

Trustwave®

Sample A – Propagation

- The attacker used VNC to get to the POS Terminals
  - Installed the Keylogger and configured settings to only capture keystrokes from a single process
  - Process was for POS credit card transactions
- Since there was no Internet Access allowed on POS Terminals, the data was sent via SMTP server installed on Club POS Server

```
{01/Oct/0108 09:16:19} [3392] [Debug] 192.168.9.102:4464|25 -> 201 Welcome to ESMTP Server
{01/Oct/0108 09:16:19} [3392] [Debug] 192.168.9.102:4464|25 <- HELO Term2
{01/Oct/0108 09:16:19} [3392] [Debug] 192.168.9.102:4464|25 -> 250 Hello and welcome
{01/Oct/0108 09:16:01} [3392] [Debug] 192.168.9.102:4464|25 <- QUIT
{01/Oct/0108 09:16:01} [3392] [Debug] 192.168.9.102:4464|25 -> 221 Signing Off
{01/Oct/0108 09:16:01} [3392] [Debug] 192.168.9.102:4464 Disconnected from us. Port: 25
{01/Oct/0108 09:17:19} [3392] [Debug] 192.168.9.102:4475 Connected to us on port 25
{01/Oct/0108 09:17:19} [3392] [Debug] 192.168.9.102:4475|25 -> 201 Welcome to ESMTP Server
{01/Oct/0108 09:17:19} [3392] [Debug] 192.168.9.102:4475|25 <- HELO Term2
{01/Oct/0108 09:17:19} [3392] [Debug] 192.168.9.102:4475|25 -> 250 Hello and welcome
{01/Oct/0108 09:17:01} [3392] [Debug] 192.168.9.102:4475|25 <- QUIT
{01/Oct/0108 09:17:01} [3392] [Debug] 192.168.9.102:4475|25 -> 221 Signing Off
```

```
{01/Oct/2008 09:20:54} [1668] [Info] Sending message C:\FkeySMTP\Queue\00002.msg to
monta[redacted] through relay number 0 out of 3. IP is [redacted]
{01/Oct/2008 09:20:54} [1668] [Debug] We are connected to [redacted]ort 1062
{01/Oct/2008 09:20:54} [1668] [Debug] [redacted] <- 220 mx.google.com ESMTP
j8si5161058gvb.1
{01/Oct/2008 09:20:54} [1668] [Debug] [redacted] -> EHLO [redacted]
[redacted]
{01/Oct/2008 09:20:55} [1668] [Debug] [redacted] <- 250-mx.google.com at your service,
[[redacted]ZE 35651584250-8BITMIME250 ENHANCEDSTATUSCODES
{01/Oct/2008 09:20:55} [1668] [Debug] [redacted] -> MAIL FROM:<montana2[redacted]
{01/Oct/2008 09:20:55} [1668] [Debug] [redacted] <- 250 2.1.0 OK j8si5161058gvb.1
{01/Oct/2008 09:20:55} [1668] [Debug] [redacted] -> RCPT TO:<montana2[redacted]
{01/Oct/2008 09:20:55} [1668] [Debug] [redacted] <- 250 2.1.5 OK j8si5161058gvb.1
{01/Oct/2008 09:20:55} [1668] [Debug] [redacted] -> DATA
{01/Oct/2008 09:20:55} [1668] [Debug] [redacted] <- 354  Go ahead j8si5161058gvb.1
{01/Oct/2008 09:20:55} [1668] [Debug] [redacted] -> .
{01/Oct/2008 09:20:56} [1668] [Debug] [redacted] <- 250 2.0.0 OK 1222871262
j8si5161058gvb.1
{01/Oct/2008 09:20:56} [1668] [Debug] [redacted] -> QUIT
```

Xxx.exe, 9:20 AM

BlazingTools Perfect Keylogger: Options

12
25
montana2[redacted]
gmail.com
192.168.9.100

Xxx.exe, 9:20 AM

Trustwave®

Sample A – Live Demo

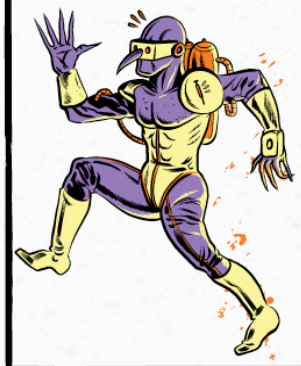
XXX.EXE

Sample A – Add'l Comments

- This attack vector was used for hundreds of bars/restaurants
  - Commonality was the accessibility of remote access programs and weak passwords
- These are not usually detected because there are no IT personal regularly monitoring the systems or alerts miss
- The Keylogger survived several upgrades and system audits as it was hidden from task manager, system tray and start menu
  - Also, the dat file was readable only by the Keylogger program
- Keyloggers are good; too good for even the attackers

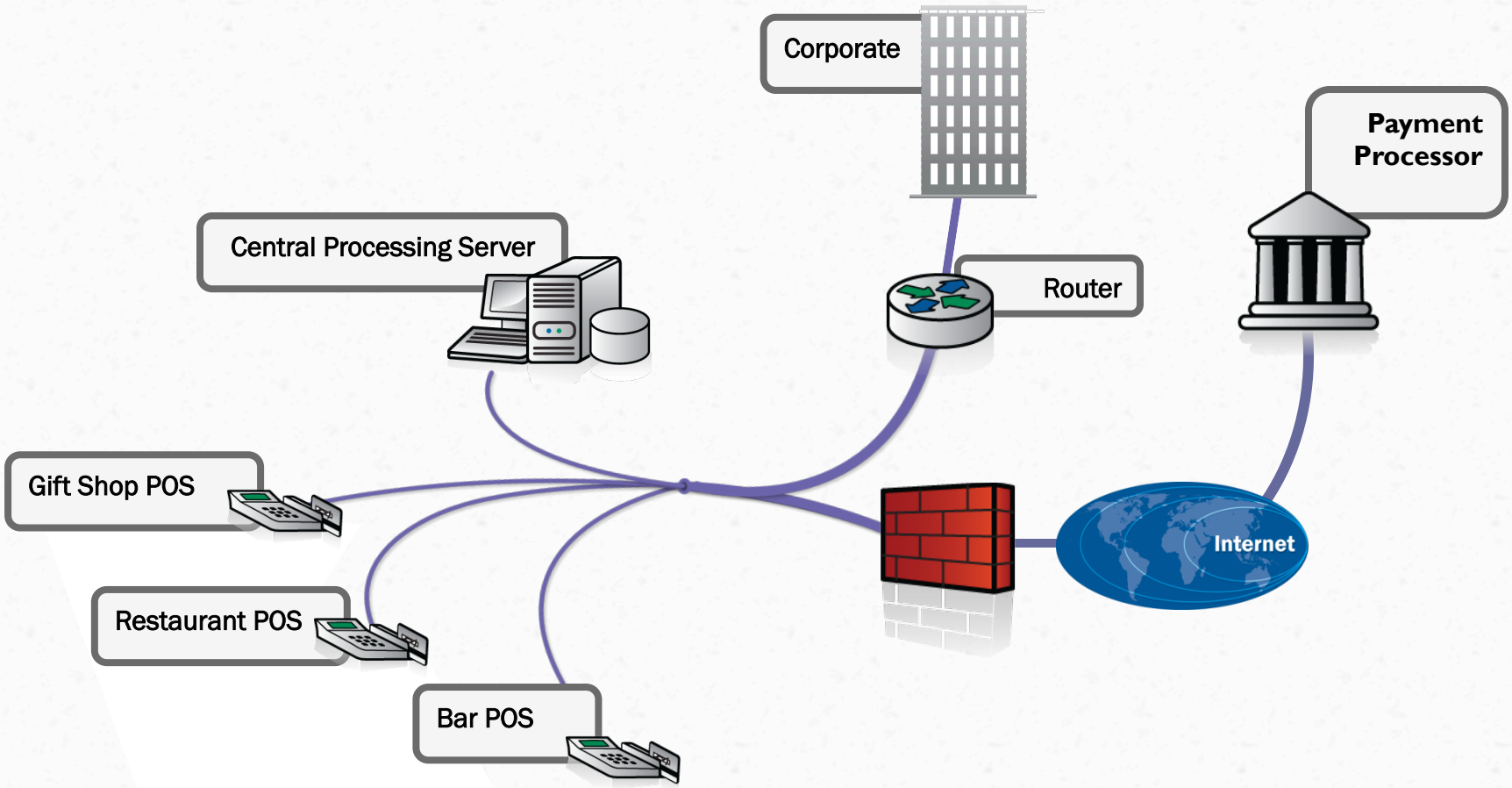
Sample B:

Hotel in New York



Trustwave®

Sample B – Architecture



Sample B – Problems

- The firewall was a consumer router – allowed RDP inbound to many systems.
- Hotel Management System and POS Terminals running Windows that had not been patched since their installation (2004 & 2006).
- Weak username and passwords (many BLANK) for local system and domain accounts including Administrator (password:nimda)
- No Anti-Virus or Anti-Malware on ANY of the systems in the environment.
- No network segmentation for any of the systems or networks in the hotel.

Sample B – Tools Found

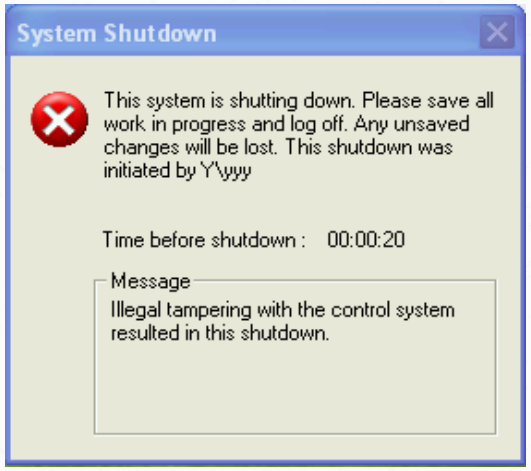
Name	Size	MD5 Hash	Description
FAR.EXE	573K	ee7d411f47b13fb204a188fc37e7fc61	FAR is a collection of productivity tools combining advanced find/replace, HTML Help 1.x & MS Help 2.x authoring, FTP, File and ZIP functions in a single interface.
ENT.EXE	350K	defd991b647811e8e8e5591365e3be41	ENT is a set of network scanning, security and admin tools useful in diagnosing networks and monitoring network connections.
GET2.EXE	48K	73ba6f159e752705ed2cde6953769a9b	GET2 Penetrator Version 1.9.9d - Windows Authentication information exfiltrator
SL.EXE	20K	3a97d9b6f17754dcd38ca7fc89caab04	Yep, Foundstone's ScanLine 1.01 tool.
SERVER.EXE	868K	e02d4cc6ec3b7907b35d9456ab092da3	This is obfuscated version of an application called REDIR.EXE, a proxy application used to redirect incoming connections.
SVCHOST.EXE	**596K**	**ee23d3c0de12c1644f0ed8abc818aca1**	**File transfer, anti-debugging**
WINMGMT.EXE	**65K**	**3e19ef9c9a217d242787a896cc4a5b03**	**Memory Dumper and Track Data Parser loader**
CSRSVC.EXE	**74K**	**1f9d0d200321ad6577554cc1d0bb6b69**	**Customized Memory Dumper**
DNSMGR.EXE	**1,135K**	**bf27e87187c045e402731cdaa8a62861**	**Track Data Parser**

Sample B – Installation Vector

- Initial entry via Remote Desktop
- Targeted accounts were Administrator (pwd =nimda) , Backup (pwd = veritas), SQLDebugger (pwd = user01)
- Download of Attacker toolkit (protected SFX archive)
- Malware was extracted on target computer and remote deployment via Microsoft's "psexec.exe" to other systems on local and corporate network.

Sample B – Static Analysis

SVCHOST.EXE



- Runs as a Windows Service
- Used to establish connection to remote server in South Korea over SSL
- Anti-Debugging Built In:
  - When run from Explorer it tries to…
    1. Lock the Workstation
    2. Perform a System Shutdown
    3. Terminate All Processes
    4. Close All Terminal Sessions
    5. Toss the Workstation in Standby Mode
- It checks to see if the Windows Service is running in a virtual environment such as VMWare, Virtual PC, Qemu, VirtualBox.
- If so, it executes the above shutdown / system kill processes
- All strings in the binary are encrypted

Sample B – Static Analysis

SVCHOST.EXE

Decrypted Strings also contain a Memo from the author…

> "A few years ago I began to teach myself about computer science at my residence. I was initially interested in networking and security, so I developed this program. **I do not currently know what I intend to do with this, but I have accepted the fact that I must do some limited experiments.**"

Sample B – Static Analysis

WINMGMT.EXE

- Normal Windows Binary; Not Obfuscated.
- Strings Analysis show:
  - The malware utilizes Windows Service Control Management
- References to Winsock API
- FTP Commands (USER, PASS, TYPE I, 331, 230, etc.)
- Regular Expressions for Track 1 and Track 2 data:

```
((b|B)[0-9]{13,19}\^[A-Za-z\s]{0,30}\/[A-Za-z\s]{0,30}\^(0[7-9]|1[0-5])((0[1-9])|(1[0-2]))[0-9\s]{3,50}[0-9]{1})
```

```
([0-9]{15,16}[D=](0[7-9]|1[0-5])((0[1-9])|(1[0-2]))[0-9]{8,30})
```

Sample B – Dynamic Analysis

WINMGMT.EXE

- Executing from command line or Explorer produces Error 1063.
- Using "/install" does the trick.
- It can run in debug mode
- **Once running it locates one of eight Point of Sale system process it is designed to monitor.**
- As cards are swiped on monitored processes, it creates process memory dump file in "memdump" folder and then calls a process called "dnsmgr.exe" which parses track data from dump files to an ASCII file "dirmon.chm"

Sample B – Data Exfiltration

- The attacker's created RAR archives created with WinRar and password protected them.
  - We obtained the passwords for these RAR files by searching RAM dumps from the compromised systems and parsing for interesting strings
  - Found "!SYSTEMNAME#623!" and it worked!
- Data exported via over SSL to a host in South Korea (211.232.XXX.X).

1368	TCP	1825	127.0.0.1	1149	127.0.0.1	ESTABLISHED	2009-03-25T19:06:20Z
1368	TCP	1149	127.0.0.1	1825	127.0.0.1	ESTABLISHED	
1368	TCP	1826	10.33.44.143	443	[redacted]	ESTABLISHED	2009-03-25T19:06:20Z

- Estimated that 350,000 (or more) credit cards were exported during the time the attackers were on the systems. This is based upon the contents of the RAR files.

Sample B – Propagation

- The attackers made connection using RDP to 35 other hotel locations via the corporate WAN.
- We visited many of the other locations and found the exact same sets of tools and large quantities of RAR files containing credit card data.

Sample B – Live Demo

WINMGMT.EXE

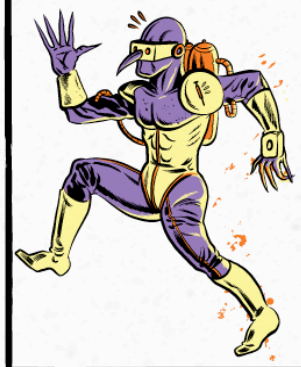
Sample B – Add'l Comments

Why isn't this malware caught?

- Anti-Virus can't catch this
  - They only know what they know.
- Lack of Log Review
- No checks for storage of prohibited data; often a sign that someone is on the system doing something they shouldn't be
- Thanks to the IT Talent
  - On few of these cases, IT simply searched Google for the malware name. Needless to say the results.

Sample C:

Video Poker in Lake Tahoe



Note: This portion of the talk is based on actual cases we investigated where the use of "credentialed" malware was found. This portion of the presentation does not discuss or infer that any specific Video Poker system is vulnerable to this attack method.

Sample C – What is Credentialed Malware?

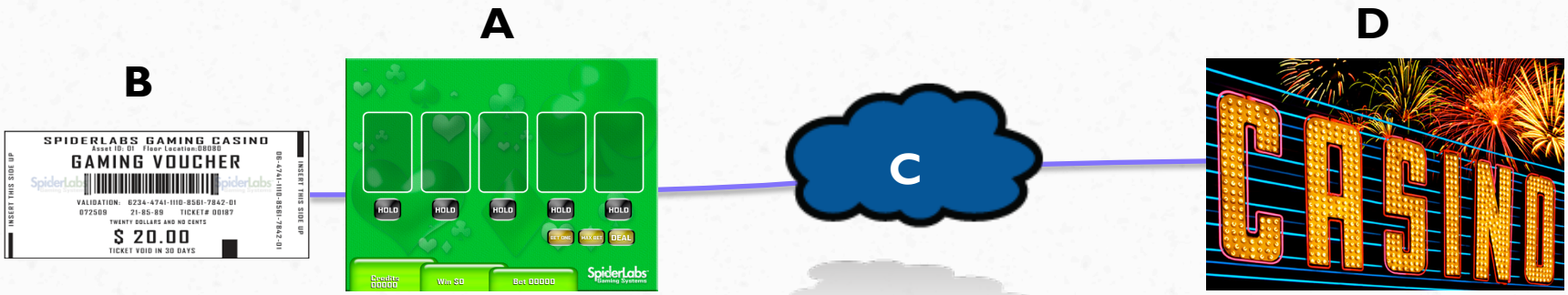
Credentialed Malware:

- A program that is specifically design to exploit functions of the target application that are not typically available to the normal end user.

- Access to the malware's functions are control by the developer using various forms of "authentication" tokens.

- Authentication Tokens could be sold or rented to criminals looking to illegally obtain what ever the target application is in the business of providing.

Sample C - Architecture



A – Video Poker Machine

B – Voucher Reader / Printer

C – Casino Network

D – The Casino

Trustwave®

Sample C – Common Problems

- Due to the number of machines and maintenance required, machines are constantly being worked on.
  - *Does the "Eye in the Sky" monitor repair personnel?*
- Unique passwords are difficult to manage.
- Do you need to run AV on Video Poker machines?
- Under the hardened case they are low end PCs and may have USB ports, etc.
- What OS are they running? How often are they patched?

Sample C – Installation Vector

Possible scenario:

- Attacker, dressed like casino repair staff, with a key walks up to the Video Poker Machine.
- They login using a default/common password (i.e. all Casino's machines have the same password)
- The Attacker inserts a USB key with the Malware on it
- The Attacker copies the dropper over to the local file system
- The Attacker executes the dropper file, removes the USB key, and locks up the machine

Another scenario:

- The malware is installed at the manufacture as a "backdoor"
- It is active on every single Video Poker machine deployed…

Sample C – Analysis

VIDEOPOKER.EXE



- While the malware is active it parsing for valid Vouchers, it is also looking for a User Voucher:
  - **Single Function** – activates a single function execution
  - **Multi-Function** – activates the malware interface window
- A User Voucher is identified by passing the value of the Voucher through a hashing algorithm and comparing the results to set values stored in the malware.
- If the malware does NOT see a User Voucher, it does nothing and passes the information over to the Video Poker software for adding credits to the game.

Sample C – Analysis

VIDEOPOKER.EXE

Key Value	Function	Description
Hold (1)	Uninstall	Deletes the malware service, puts the system logs back where they were before the malware was installed.
Hold (2)	Display Stats	Presents information on the number of User Vouchers uses (function 3 and 4) and malware version running on the machine.
Hold (3)	Odds Shift	Modifies the odds on the machine by increasing the face cards in 'deck'.
Hold (4)	Modify Credits	Prompts 'user' to enter value of credits (using 1,2,3,4,5 Hold keys), adds the value to the current game, and then can be cashed out.
Deal	Test Printer	Prints 'hello world' to the voucher printer.
Max Bet	Exit	Exits the malware and returns to normal game play. Also, used to enter a value to get to a sub-function.

Sample C – Propagation

- If the Video Poker machine is connected to the Casino network (and likely will be) a services based vulnerability would be needed.

- The attackers could check for successful propagation by walking up to random machines. Inserting a User Voucher that will either result in it being rejected or the activation of the Malware.

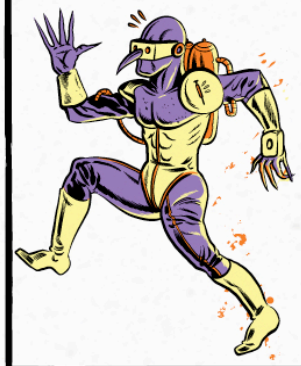
Sample C – Live Demo

VIDEOPOKER.EXE



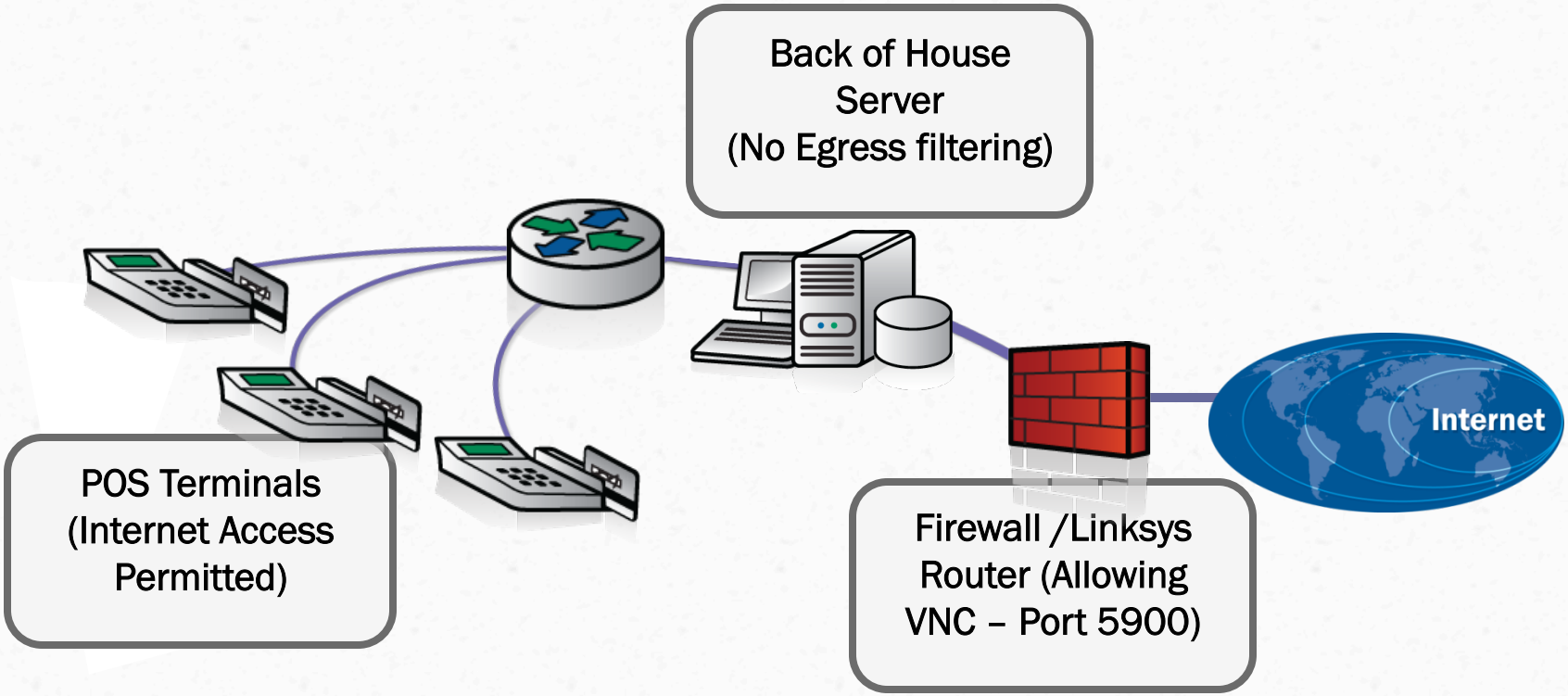
Sample D:

Restaurant in Michigan



Trustwave®

Sample A - Architecture



Sample D – Problems

- VNC allowed from Internet to Restaurant POS Server
- Weak / Common passwords
  - E.g. Admin: support
- POS Terminals were not running Anti Virus software
- Unrestricted Internet Access was allowed from all systems including POS Terminals
- POS Integrator used same passwords for all restaurants in the region

Sample D – Tools Found

Name	Size	MD5 Hash	Description
HOST32EDU.EXE	68KB	17c83eba9a436edbeb74a42a51b9087a	IRC Bot / Backdoor
X.BAT	2KB	N/A	Malware loader *contents of file found in Unallocated Clusters
REPZ.EXE	**65KB**	**6c9e01933aa88894f476d690666dc403**	**IRC Bot / Backdoor**
PACKETSNIFFER.EXE	**57KB**	**10e5a2813d51c547346173290a0ae53b**	**Packet Sniffer**

Sample D – Installation Vector

- Entry via VNC on POS Server
  - VNC password was "support"
- Downloaded malware files
  - IRC Bot
  - X.bat (Malware loader)
  - Custom Packet Sniffer
- Malware kills all security software in Windows
- Microsoft .Net framework version 2.0 was downloaded as Packet Sniffer was written in .Net and needs the framework to run properly.
- IRC Bot downloads the configuration (tcp ports, output file location, etc.) for the system based on POS software installed
- Sniffed files are placed in C:\Export folder and then uploaded to FTP server.

Sample D – Dynamic Analysis

PACKETSNIFFER.EXE

- Installed in C:\Windows\Temp folder of the system
- Uses Microsoft .Net Framework v2.0 to run properly
- Uses a configuration file, which is created based on POS software
- Sniffs TCP traffic on ports 5101,5010,5011,5100
- Stores the sniffed output in C:\Export folder
  - Filenames are <ip address>.SEND.cap and <ip address>.READ.cap
- Data is uploaded to an IP based in Munich, Germany

Sample D – Live Demo

PACKETSNIFFER.EXE

Sample D – Add'l Comments

- The destination FTP server for sniffed output files contained several other folders; all of which had sniffer output files.
- Upon analysis of FTP server, it was concluded that 9 other restaurants were affected by the same sniffer and they were all sending the data regularly to the FTP server
- 6 of the restaurants were all are based in Michigan; all restaurants are serviced by same POS Integrator.

Conclusions

- Malware is dominating
- Computer Memory is the target to extract sensitive data
- Companies are still not getting segmentation, passwords, firewalls right!! Easy Entry.
- Attackers are taking the time to learn, even obscure business applications before creating targeted Malware.
- Once Malware use has proved successful, similar businesses and environments are targeted quickly.

Tools We Like

Name	URL	Description
Dependency Walker	http://www.dependencywalker.com	Lists the imported and exported functions of an executable file
Encase	http://www.guidancesoftware.com	Forensic Analysis and Case Management
FastDumpPro	http://www.hbgary.com/products-services/fastdump-pro	Memory Acquisition Tool
FTK Imager Lite	http://www.accessdata.com/	Acquires Windows Images Live
GMER	http://www.gmer.net	Detect hidden processes and rootkits
Hex Workshop	http://www.hexworkshop.com	Analyze, edit, cut, copy, paste, insert, fill and delete binary data
IDA Pro	http://www.hex-rays.com/idapro	Disassembler and Debugger
NMAP	http://www.nmap.org	Network Port Scanner
Process Monitor	http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx	Tracks file, registry and network activity of a given process
RegRipper	http://regripper.net	Registry Analysis
Regshot	http://sourceforge.net/projects/regshot	Acquires and Compares registry snapshot
Sigcheck	http://technet.microsoft.com/en-us/sysinternals/bb897441.aspx	Checks for Digital Signatures of files on system
Volatility	https://www.volatilesystems.com/default/volatility	Memory Analysis
Win32dd	http://win32dd.msuiche.net	Memory Acquisition Tool
Wireshark	http://www.wireshark.org	Network Protocol Analyzer



Contact Us

Contacts:

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

Jibran Ilyas <jilyas@trustwave.om>

www.trustwave.com/spiderlabs/ @SpiderLabs

Special Thanks:
Adam, Stephen, Colin, Chris, Ferns, Brandon, and Nathan.