FORENSICS Case Study

12 December 2007

How Nation States Are Attacking the US Industrial Base

IATAC

Ron Ritchey
Chief Scientist
703/377.6704
Ritchey_ronald@bah.com

Agenda

- Case Study 1
- Case Study 2
- Trends In Foreign Organized Data Mining Intrusions

Case Study 1: Victim Organization Profile

A major U.S. defense contractor (Rev $48B 06) with 100,000+ users deployed on multiple continents

- The organization had an impressive security policy
  - Annual enterprise Vulnerability Assessments
  - Monthly vulnerability scanning
  - Perimeter and internal networks protected by firewalls
  - 24-hour IDS monitoring (HIDS & NIDS)
  - Comprehensive patching and anti-virus program
  - DMZ (single tier) for Internet facing servers
  - VPN required for remote access
  - Well trained internal security team
- What went wrong?

Initial Response & Investigation

Responded after a Windows 2000 server repeatedly Blue Screen of Death (BSOD) for no obvious reason

- Microsoft initially diagnosed the issue as a .NET problem
  - Identified a sophisticated kernel-mode rootkit
  - Conducted an incident triage consisting of domain configuration, compromised account review, forensic analysis, and a custom developed rootkit detection utility
- Initial assessment indicated the attackers established multiple covert channels on the network
  - Initially found 13 DMZ and 7 internal servers that were compromised several months earlier
  - Initial assessment indicated the attackers compromised the network almost three years earlier
  - Conflicting rootkits were causing the BSOD
- **Not identified via existing security device**

Response & Investigation

By the time Team arrived, the attackers had a established fault tolerant covert channels, obtained privileged user credentials, and were data mining the network

- Several DMZ's and internal systems were compromised
  - Variety of previously unknown malicious code
  - User and kernel mode rootkits & data mining tools
  - Hostile ASP pages deployed
- Desktop systems of key users were compromised
- Key loggers were widely and strategically deployed
- Corporate executives & key users directly targeted
- VPN access via home and laptop systems

How The Attackers Compromised Systems

- **FrontPage & WebDAV mis-configuration**
  - Both run over port 80/443
  - Both rely on NTFS ACLs for security - content managers usually don’t realize this and change directory ACLs to fix a file share or script issue
  - This opens the server up to modification from the Internet
  - ASP rootkits frequently followed these mis-configurations
- **Application attacks**
  - SQL injection
  - Variable manipulation
- **System Vulnerabilities**
  - Unpatched systems, known vulnerabilities
- **Undocumented vulnerabilities**
  - When the attackers could not compromise a system any other way, they used non-public vulnerabilities
  - There is no shortage of these vulnerabilities for our adversaries to choose from

Incident Response Techniques

Traditional incident response techniques were not effective

- *Standard volatile data collection and live response techniques yielded no useful information*
- Sophisticated kernel-mode malicious code utilized hooking and patching to hide files, registry entries, processes, services, network connections, etc. from standard user-mode programs like net stat, pslist, fport, and others
- This led the parent organization to believe the system was not compromised
- Existing malicious code detection tools were unable to identify the rootkits on live systems
- Team developed our own utility that compared processes in the kernel v. viewable processes
- Utilizing IR tools that work from physical memory and disk was critical

Incident Response Techniques

We Had to Work Faster!

Team had to modify IR techniques so we could detect our adversary and capture malicious code

- We moved traditional back-end forensic lab work to the field for faster results
- We imaged the process and physical memory on suspected compromised systems
- We automated the collection of system binaries, log files, packed files, and analyzed them offline
- We developed a live response utility that would scan the system and identify well-hidden malicious code

Incident Response Techniques

Developed host and network malicious code identification techniques - driven by malicious code functional analysis

- File scanning Windows administrative shares (C$, D$) from clean systems was effective at identifying malicious files
- Creative techniques were effective
  - Creating and monitoring special accounts and services
  - DNS blackhole/pass-through to identify malicious code
  - System surveillance countermeasures
- Host solutions effective, but depended on prior malicious code analysis – minor malicious code changes were sufficient to thwart several of our host-based solutions
- NIDS was often thwarted by the use of encryption, and not practical when the attackers used standard Windows binaries like net use, terminal services, remote desktop, etc.

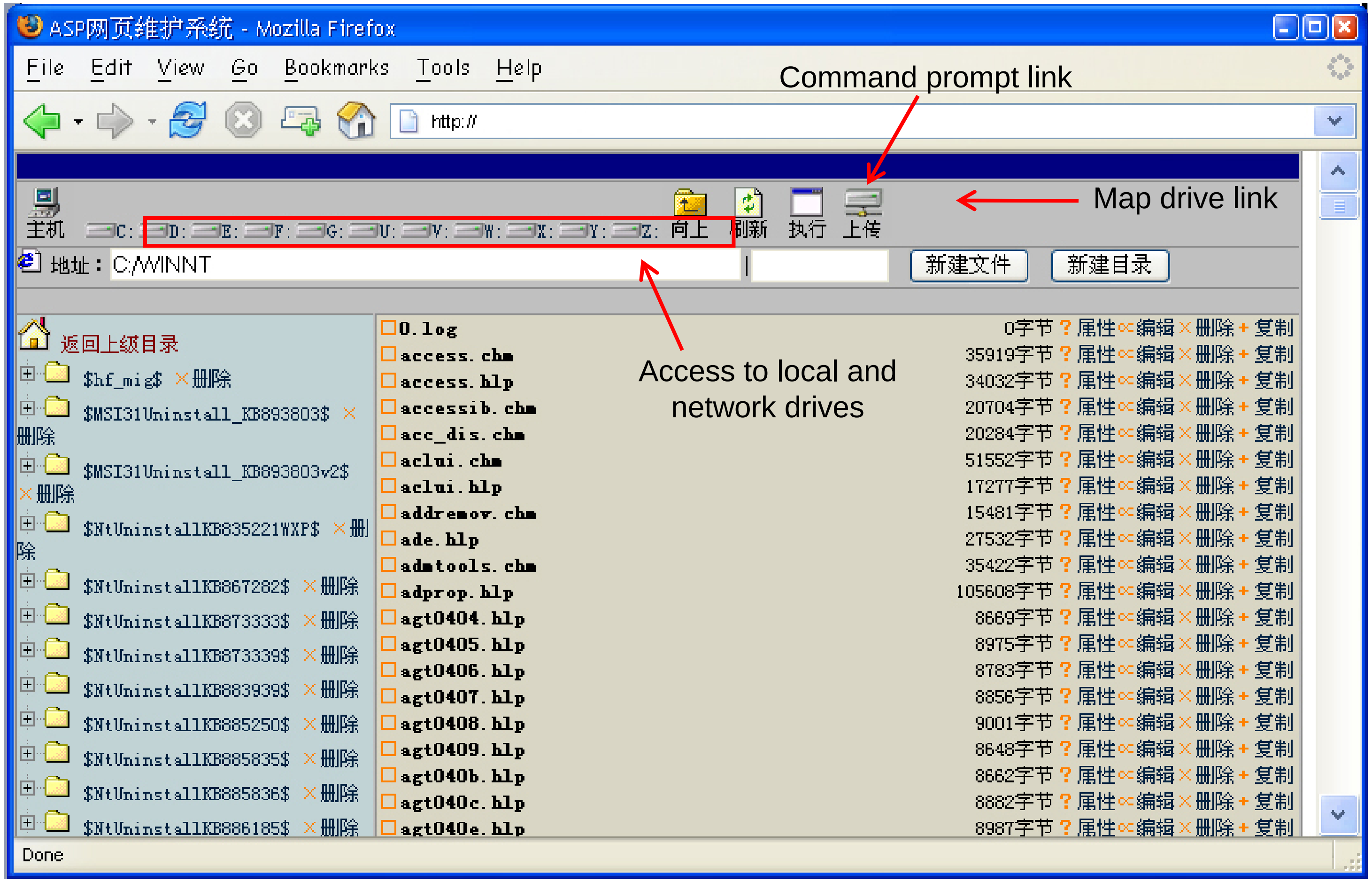
Captured ASP Rootkit from the Adversary

The attackers utilized several ASP “rootkits” to maintain system access and bypass the firewall, NIDS, and HIDS

- Remote cmd.exe command shell via webpage
- File upload and download
- Network scanning and data mining
- Sometimes hidden in a virtual directory, with files physically hidden deep in the directory structure, outside of the webroot
- IIS guest account was sometimes found in the Administrators group, giving the ASP page privileged access
- All through port 80/443

Captured ASP Rootkit

Once the attackers logged in, they could upload/download/execute files, open a command shell, and data mine the system over HTTPS



Command prompt link

Map drive link

Access to local and network drives

地址： C:/WINNT

```
$hf_mig$  ×删除
$MSI31Uninstall_KB893803$  ×删除
$MSI31Uninstall_KB893803v2$  ×删除
$NtUninstallKB835221WXP$  ×删除
$NtUninstallKB867282$  ×删除
$NtUninstallKB873333$  ×删除
$NtUninstallKB873339$  ×删除
$NtUninstallKB883939$  ×删除
$NtUninstallKB885250$  ×删除
$NtUninstallKB885835$  ×删除
$NtUninstallKB885836$  ×删除
$NtUninstallKB886185$  ×删除
```

```
□0.log              0字节 ? 属性 ∝编辑 × 删除 + 复制
□access.chm     35919字节 ? 属性 ∝编辑 × 删除 + 复制
□access.hlp     34032字节 ? 属性 ∝编辑 × 删除 + 复制
□accessib.chm   20704字节 ? 属性 ∝编辑 × 删除 + 复制
□acc_dis.chm    20284字节 ? 属性 ∝编辑 × 删除 + 复制
□aclui.chm      51552字节 ? 属性 ∝编辑 × 删除 + 复制
□aclui.hlp      17277字节 ? 属性 ∝编辑 × 删除 + 复制
□addremov.chm   15481字节 ? 属性 ∝编辑 × 删除 + 复制
□ade.hlp        27532字节 ? 属性 ∝编辑 × 删除 + 复制
□admtools.chm   35422字节 ? 属性 ∝编辑 × 删除 + 复制
□adprop.hlp    105608字节 ? 属性 ∝编辑 × 删除 + 复制
□agt0404.hlp     8669字节 ? 属性 ∝编辑 × 删除 + 复制
□agt0405.hlp     8975字节 ? 属性 ∝编辑 × 删除 + 复制
□agt0406.hlp     8783字节 ? 属性 ∝编辑 × 删除 + 复制
□agt0407.hlp     8856字节 ? 属性 ∝编辑 × 删除 + 复制
□agt0408.hlp     9001字节 ? 属性 ∝编辑 × 删除 + 复制
□agt0409.hlp     8648字节 ? 属性 ∝编辑 × 删除 + 复制
□agt040b.hlp     8662字节 ? 属性 ∝编辑 × 删除 + 复制
□agt040c.hlp     8882字节 ? 属性 ∝编辑 × 删除 + 复制
□agt040e.hlp     8987字节 ? 属性 ∝编辑 × 删除 + 复制
```

Compiled Malicious Code Protected

- Compiled malicious code was well protected
  - UPX, FSG, aspack, Mew, NSpack, Petit, and other known programs were used to pack Windows binaries and known malicious code
  - **A proprietary packing utility was used for packing some proprietary software**
- Malicious code was written to prevent easy reverse engineering
  - Decompilers like IDA Pro, WinDBG, OllyDBG, and SoftICE have a hard time with well protected code
  - Most of the time a malicious code functionality test will provide you with enough information to develop host and network countermeasures
- Changing malicious code's MAC date and time stamp
  - The attackers used proprietary and open source tools to change malicious code file dates and times
  - Often changed dates to match other files in Windows/System32 directory
- Changing malicious code file names
  - Sometimes entire name was changed but often just a variant of original name – this may be a language issue

We Have "Anti" Anti-Forensics Techniques

We were able to utilize the attacker's anti-forensics techniques to help us identify malicious code that we may have otherwise may have missed

- **We wrote several programs and scripts to identify packed files**
  - We developed a network file scanning utility
  - We wrote an EnScript that identifies packed files
  - We developed HIDS and NIDS to check for packed files
- **We wrote a program that identifies files with changed date/time stamps**
  - Scans the MFT$ and identifies suspicious files
  - Recovers the file's original date/time stamps
  - Useful for identifying the earliest known unauthorized action
- **We developed a good malicious code functionality testing methodology**
  - We conducted a baseline functionality test and threat analysis
  - We need understand it and to develop a countermeasure for it
  - Full reverse engineering is usually not required

Adversary Countermeasures

We developed several countermeasures based on our forensic and malicious code analysis, however, the attackers countered our countermeasures quickly

- When we blocked ports and IP addresses
  - The attackers changed addresses and switched to new ports (2,400 unique IP addresses on 25+ networks used)
- When we scanned for malicious files by specific dates/times
  - The attackers started changing the create, modify, and last access dates/times (we eventually developed a utility to detect this)
- When we developed a HIDS signature for their malicious code
  - The attackers changed XOR or other values to bypass our signature
- When our vendors developed AV signatures
  - The attackers recompiled their malicious code in a manner which the existing AV signatures would not detect it
- When we blocked ICMP
  - The attackers utilized other protocols for exfiltration
- When we black holed their DNS zones
  - They used new domain names, and eventually switched to IP addresses – note: this increased their workload

What Did We Learn About This Adversary?

- Highly technically proficient, well-funded, organized professionals working in teams, and they never gave up
- Very familiar with the organization they compromised, and identified all relevant business units with a corporate LDAP dump of everyone in the organization, including job titles and workstation hostnames
- Traditional incident response and forensics techniques must be modified when investigating organized intrusions
- Traditional security measures like firewalls, intrusion detection, patch management, anti-virus, single tier DMZs, are not enough to stop professionals who bring their "A" game
- They got better as we got better

What Did We Learn About Our Adversary?

- Didn't always attempt to get root privileges - often after specific data
- Targeted
  - Military technology, especially weapons and aerospace technology
  - Export control, organizational data, and internal documents
  - Senior organization personnel
  - Engineering and research personnel
- Workstations and e-mail attacked
  - Covert channels, data mining tools, and key loggers
  - Used a variety of well-known attack and system administration tools
    - Pwdump, PSTools, Netcat, WinPcap
    - Hacker Defender
  - Variety of keystroke loggers
  - Standard Windows binaries (remote desktop, terminal services, cmd.exe, net use, net)

Remediation & Extraction

- Must be very well coordinated throughout the organization – don’t play whack-a-mole!
- Very disruptive, expensive, time consuming, and nearly impossible to do without everyone finding out about the incident
- If your remediation efforts are successful, you may buy your organization a couple of months before the attackers are back – and they will be back
- Don’t just protect the “technical” stuff, protect HR capital too
- **Spend your time preparing for real threats, not obscure scenarios where the sun, moon, and stars must line up for the attacker to be successful**

Agenda

- Case Study 1
- Case Study 2
- Trends In Foreign Organized Data Mining Intrusions

Victim Organization Profile

A U.S. defense contractor with 4,200 employees and contractors in the US, Europe, Middle & Far East

- The organization’s security policy did not reflect the organized adversary that eventually compromised the network
  - SSL VPN (weak authentication)
  - Windows LanManager password hashing enabled
  - All end-users have local administrative access
  - Large numbers of unmanaged systems and networks
  - Unproxied and unauthenticated outbound access
  - Domain controllers have Internet access
  - Well trained internal security team, but little experience in IR or forensics

Background

Security personnel noticed a large data transfer from an internal Internal servers to a foreign IP address

- On 6/19/2007, Client personnel noticed a large data transfer to a Korean IP address
- Approximately three gigabytes of compressed data was exfiltrated, which represents 6-12 gigabytes of actual data due to compression
- This is the equivalent of 1.5 – 3 million pages of printed paper
- The actual content that was exfiltrated is unknown
- Preliminary analysis of the system by Client personnel revealed malicious code that anti-virus and privileged users could not delete
- Analysis of known hostile IP address revealed additional systems that were also communicating with it

Preliminary Findings – Intrusion Scope

Booz Allen forensics personnel have analyzed over fifty systems, captured malicious code, and reviewed Client's network architecture

- 50+ servers and workstations have been compromised and re-compromised (several systems are in the forensics analysis queue)
- These systems are access points for our adversary - once they connect to an access point, they utilize Client employee and domain administrator credentials to navigate the network
- Many of the compromised systems are domain controllers located in office around the world
- These access points supplement our adversary's VPN access
- All domain user passwords are compromised
- **There are additional compromised systems and malicious code that we have not yet identified**

Preliminary Findings - Malicious Code

The adversary is utilizing a variety of malicious code to data mine and maintain a presence on the network

- We have recovered 15 unique rootkits
  - Hacker Defender widely deployed
  - 12 previously unknown rootkits
  - 6 kernel-mode, 8 user-mode
- We have also recovered the following
  - Three data mining programs
  - Four general purpose network utilities (network and system enumeration, proxy, etc.)
  - Six unique keyloggers
  - The adversary has developed tools that perform the same function as netcat, PS tools, pwdump, etc.
  - Most code is packed w/unknown packer

Preliminary Findings – Adversary Analysis

Client has been targeted by an organized adversary who is conducting a prolonged and sophisticated campaign against them

- The attackers have developed a Client-specific attack plan
- The attackers have utilized a variety of previously unknown malicious code to thwart anti-virus solutions and forensic analysis
- The attackers have re-compromised several systems hours after we eradicated malicious code from them
- The attackers are using extreme caution and utilizing countermeasures to prevent us from identifying the malicious code they are using, and the data they collect for exfiltration
  - They are utilizing multiple hostile IP addresses
  - They are using encryption to protect collected data
  - They are securely cleaning up after themselves
  - Their malicious code has built-in countermeasures
  - The use of multiple redundant covert channels on key systems

Preliminary Findings – Key Targets

Forensic analysis has revealed that the attackers are choosing their targets wisely, and the network has been compromised for months

- Client executives and key employees have been attacked with highly targeted and sophisticated spear-phishing attacks
- Spear-phishing attacks typically involve an attacker sending a seemingly benign and germane message between two known parties, compromising the recipient
- The attackers are collecting data from key technical users
- The attackers appear to focus on Client’s defense-related sites
- The Client corporate network has been fully compromised at least since Saturday, March 17th, 2007, although the attackers probably have been on the network for much longer

Evidence Of An Organized Adversary

There is compelling evidence that the Client has been targeted by a well-known organized adversary

- Client is the type of organization targeted by organized adversaries
- The adversary has performed intelligence gathering operations against Client (spear-phishing)
- The adversary has developed malicious code only recovered at the Client (often compiled the same day it's distributed)
- The adversary has identified, compromised, and re-compromised an unusually high volume of key internal systems and is focusing the attack on defense-related systems and key personnel
- The adversary is taking proactive countermeasures
- The adversary has been very quick to re-compromise systems and change techniques when we launch countermeasures
- The use of password protected RAR files
- The use of Asia-Pacific IP addresses
- The use of Asia-Pacific malicious code

Evidence Of An Organized Adversary

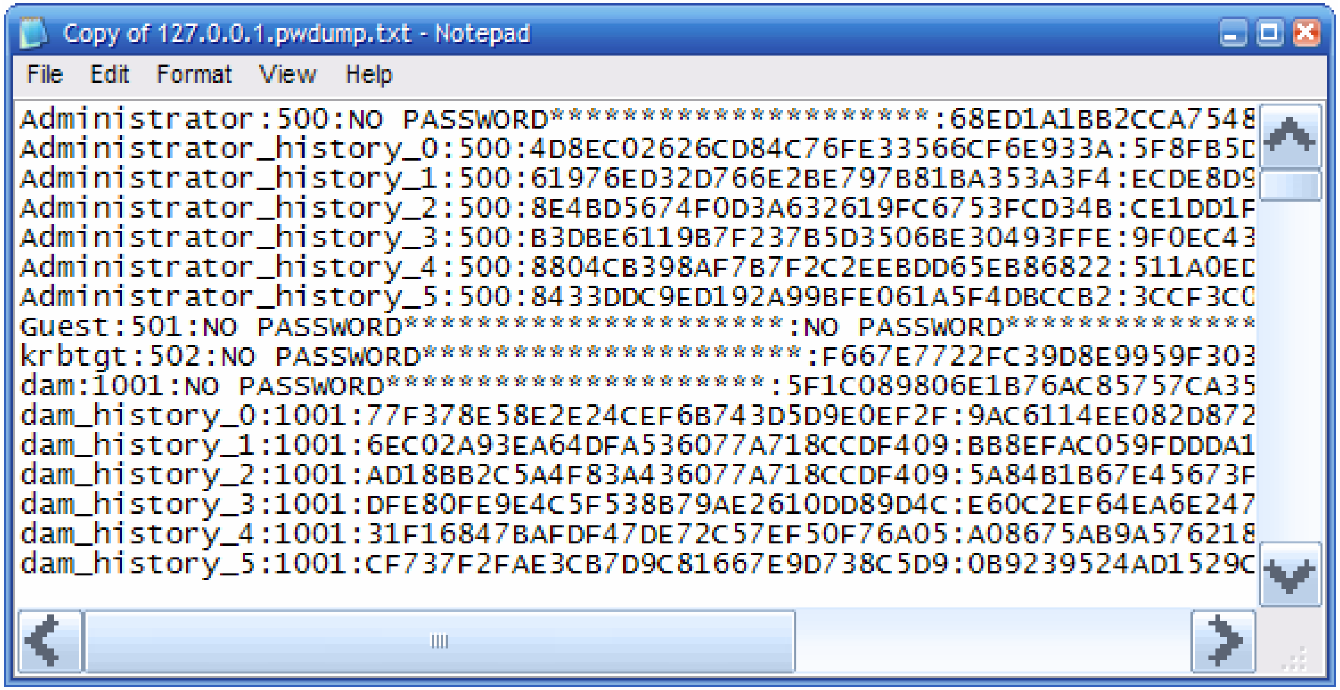
The attackers are responding in near real-time

- The attackers are modifying their techniques as we launch countermeasures (forensics metrics)
  - We block Internet from domain controllers – they proxy
  - We identify rootkits w/certain tools – they stop hiding the rootkit
  - We identify known rootkits – they start using unknown rootkits
  - We change the passwords – they continue to use the accounts
- Anti-virus solutions don't work against sophisticated malicious code
  - AV generally can't see the malicious files
  - AV is signature based, so it won't identify code it doesn't know
  - Compromised systems generally require manual cleaning
- Compromised systems have to be identified manually

Evidence Of An Organized Adversary

The attackers collected the password history for every employee and contractor on the Client network

- Evaluation of the password file reveals many employees who have not recently changed their domain password
- Evaluation of the password file reveals that many employees only change the last character or two when changing passwords



```
Administrator:500:NO PASSWORD*********************:68ED1A1BB2CCA7548
Administrator_history_0:500:4D8EC02626CD84C76FE33566CF6E933A:5F8FB5D
Administrator_history_1:500:61976ED32D766E2BE797B81BA353A3F4:ECDE8D9
Administrator_history_2:500:8E4BD5674F0D3A632619FC6753FCD34B:CE1DD1F
Administrator_history_3:500:B3DBE6119B7F237B5D3506BE30493FFE:9F0EC43
Administrator_history_4:500:8804CB398AF7B7F2C2EEBDD65EB86822:511A0ED
Administrator_history_5:500:8433DDC9ED192A99BFE061A5F4DBCCB2:3CCF3C0
Guest:501:NO PASSWORD*********************:NO PASSWORD**************
krbtgt:502:NO PASSWORD*********************:F667E7722FC39D8E9959F303
dam:1001:NO PASSWORD*********************:5F1C089806E1B76AC85757CA35
dam_history_0:1001:77F378E58E2E24CEF6B743D5D9E0EF2F:9AC6114EE082D872
dam_history_1:1001:6EC02A93EA64DFA536077A718CCDF409:BB8EFAC059FDDDA1
dam_history_2:1001:AD18BB2C5A4F83A436077A718CCDF409:5A84B1B67E45673F
dam_history_3:1001:DFE80FE9E4C5F538B79AE2610DD89D4C:E60C2EF64EA6E247
dam_history_4:1001:31F16847BAFDF47DE72C57EF50F76A05:A08675AB9A576218
dam_history_5:1001:CF737F2FAE3CB7D9C81667E9D738C5D9:0B9239524AD1529C
```

IATAC

What Are The Adversary’s Goals?

Client’s adversary has several well-planned objectives, and needs this network to accomplish them

- The attackers want to systematically data mine Client’s network
  - Collect organizational information
  - Collect customer’s data
  - Military/defense information
  - For Official Use Only (FOUO) documents
  - Engineering and other technical documents
  - ITAR/export control documents
  - Read/pilfer email
- The attackers want to use Client’s network, email addresses, and other information to attack customers
  - Military and government customers are at particular risk
  - Easy spear-phishing targets
- The attackers want to identify internal network connections to Client customer sites and attack those networks directly

Potential Stolen Data

- Briefings for government clients working in network security
- The names of classified projects
- Lists of staff including clearance levels, ssns, addresses, etc.
- ITAR documents
- NIPRnet documentation
- FOUO briefings
- Government internal organization charts
- Visit request authorization forms (includes PIV data)
- Resumes
- Client databases

Agenda

- Case Study 1
- Case Study 2
- Trends In Foreign Organized Data Mining Intrusions

Foreign Organized Hacking Trends Overview

Organized data mining attacks are increasing in quantity, scope, and sophistication

- There are a few common trends…
  - Originate from Chinese, Korean, and Taiwanese IPs
  - Eastern Europe and Brazil are improving their skills
  - Last several months to several years
  - Average 20-60 previously unknown pieces of malicious code per attack
  - Tens to hundreds of unique IP addresses per attack
  - Each incident contains multiple systems compromised with multiple covert channels each
  - Smart use of encryption for data at rest, covert channels, and data exfiltration
- Accurate statistics are not available
  - Many organizations reluctant to report

Organized Attack Threat Trends

Listed in the approximate order which we encounter them

- **Spear-phishing (growing threat)**
  - Increasing in sophistication and effectiveness over time
  - Multi-faceted attack including ease of use (for attackers), data collection from the end user, VPN like network access, etc.
- **Application attacks (growing threat)**
  - Few developers are skilled and developing secure online applications
- **Microsoft Internet Services mis-configuration (plateau threat)**
  - Slowly being mitigated over time due to improvements in Microsoft Windows, IIS, default configurations, and user knowledge
- **Browser attacks (growing threat)**
  - Increase in use of adult porn and other malicious websites
  - MS Internet Explorer is the most frequently targeted browser
- **Unpatched systems**
  - 0-Day exploits
- **Undocumented vulnerabilities**
  - Hardest vulnerability to negate, likely to remain the last resort

What Are They After When They’re In?

Once the adversaries redundant presence is established on the network, certain information is targeted

- Network connections to government and military networks
- Information that will assist in spear-phishing attacks
- Weapons Systems
  - Ground and air weapons systems
- Organizational Information
- Keyword searches (Microsoft Index Server)
  - Sensitive But Unclassified (SBU)
  - For Official Use Only (FOUO)
  - Employee Names
  - Export Control (ITAR, EAR)
  - Proprietary

How Are The Attackers Exfiltrating Data?

- Wide variety of covert channels
  - Collected internally and uploaded to Internet-facing web servers (HTTP/SSL)
  - ICMP channels often used where firewall rules permit
  - NetCat, HackerDefender, other rootkits
  - Via employee email accounts
- Typically over the weekend, holidays, evening hours (USA)
- Government and contractor data often exfiltrated via each other’s networks
- Extensive use of encryption, so we don’t always know what was exfiltrated

Why Do Our Adversaries Choose HACKINT?

Digital data mining, with proper encryption, is relatively easy, inexpensive, safe, hard to investigate, and extremely effective

Reporter: “Why do you rob banks?”
Willie Sutton: “Because that’s where the money is.”

- Recent foreign exfiltration example
  - A minimum of 89 650MB encrypted/compressed RAR files
  - This equals from 59,238 - 148,096 reams of paper
  - Roughly 29,619,000 – 74,048,000 pages of printed paper, depending on the compression ratio (2x-5x)
  - It would take 4 to 8 semi-trucks to move that much paper
  - Information was ITAR/export control
  - **<u>This was only one of several significant exfiltrations at this organization</u>**

IATAC

Looking Forward – Our Adversaries

This is what we think we can expect from our organized adversaries in the next three years

- **Increasingly sophisticated malicious code**
  - Non-persistent rootkits (memory based) increasingly used
  - Increased use of undocumented exploits
  - MS Vista kernel-mode rootkits
  - More advanced user-mode code “hiding in plain sight”
  - Browser attacks will increase in sophistication
  - Possibly hardware virtualization rootkits (Blue Pill type code)
- **Anti-detection and anti-forensic techniques will improve**
  - New malicious code anti-detection techniques emerge
  - More proprietary Windows PE packing utilities
  - Increased use of undocumented exploits
- **Spear-phishing and browser attacks will increase**
  - The benefits of these techniques easily justify the investment in developing them

Looking Forward – Incident Responders

We need to *immediately* respond to our adversaries increasing sophistication

- Current situation…
  - The worse this problem gets, the quieter and less likely it is that we'll identify it or have a successful remediation
  - U.S. defense industry merger mania = non-remediation friendly networks
  - Current detection tools will not identify next generation rootkits
  - Few IR teams are skilled at quickly developing and deploying countermeasures, or providing an organized response

- What does the IR community need to do?
  - Develop training & tools that reflect organized intrusion trends
  - Develop better identification techniques
  - Develop better live response techniques
  - Move the battle from the forensics lab to the field
  - Develop memory analysis skills

Next Generation Vulnerability Assessments

Organizations who are targeted by an organized adversary must change the way risk is evaluated on their networks

- Current risk assessments
  - We are still evaluating the risk to targeted networks with the same techniques that we used in 2000
  - The "snapshot in time" produced from a vulnerability scanner on a well-patched and well-maintained network will not provide the assessor with sufficient information to determine the organization's risk
  - Organized threats require new techniques and methodologies to recover sufficient information to make a risk determination
- Next Generation Vulnerability Assessments
  - Combination of traditional VA techniques with cutting edge incident response, forensics, and investigative techniques
  - Identifies currently *and* previously vulnerable systems
  - Identifies previously attacked systems
  - Identifies kernel and user-mode malicious code
  - Identified malicious DNS activity

Questions?