Cyber Security Organized Crime
The Advanced Persistent Threat

Shawn W. Rabourn, Sr.
Microsoft Corporation
ACE Services

- Microsoft IT (MSIT) Information Security (InfoSec) ACE Infrastructure Services
  - Assessment, Consulting, Engineering
  - Reports to CISO
- Security-focused
- Available to Internal (MS) and External Customers
- External Customers engaged via Premier/MCS/Custom DoS
- Bringing MSIT Best Practices to the Field
  - Bringing Field Best Practices to MSIT
ACE Services (cont.)

- 35+ Unique Offerings
- Security Assessment Offerings
  - Application/Infrastructure
  - Active Directory, PKI, Azure, Mobile, Host, ISO 27001, Venture Integration, Application Privacy
- Custom consulting engagements
About Shawn

Experience
- Directory Services/Security Support
- Premier Field Engineering
  - Windows Server
  - Scarce Skills
- ACE Services

Specializations
- PKI, Identity Management (FIM/ILM/MIIS), Active Directory

Contact: shawnrabb@microsoft.com or @shawnrabourn
Session Agenda

- What Makes APT’s Different?
- Real World Examples
- A Plan For Dealing With APT’s
Advanced Persistent Threat (APT) attackers have compromised a large percentage of Fortune 1000 companies, governmental agencies, finance industry, infrastructure entities, and military sites.

Attackers gain access using client-side exploits, and quickly compromise all passwords, servers, and data.

Often get a copy of all data, including updates.

Often reading email of C-level executives and IT workers.

Stealing so much data they have to pick and choose.
It has been going on for many years, but is only now being recognized and publicized more frequently. Is one of the biggest threats any organization can face. Because entire IT system is compromised, most clients don’t know where to start when trying to eradicate.
How Is It Different From “Regular” Hackers?

- Attackers intend to remain permanently
- Dozens of compromises and exploits
- Social engineering, malware, and tools
- Total ownership of environment
- Complete password compromise is a given
- Objective is often stealing victim’s Intellectual Property (IP) over the long-term
- Home is often a “safe harbor” country
How Is It Different?
(cont.)

Defining Characteristic

- Organizational sophistication
- Think team approach with project managers
- Hackers work “9-5” shifts on a larger team
  - It is hacker’s full-time day job
- Victims will often get a “break” when foreign country has a major holiday
How Is It Different?
(cont.)

- APT does not panic when detected
  - What is the victim going to do?
  - There is little chance that attacker will suffer any sort of penalty
How Is It Different?
(cont.)

- Initial compromise is often from client-side attack sent via email to C-level executive
- Email often contains proprietary information that is not normally known outside a small group of team members
- Use normal, publically available hacking tools and malware, and custom tools (i.e. not always Advanced)
- Data collected and sent out using port 443 & AES
Real World Examples
Real World Examples

- In several instances, used patching/configuration servers to compromise all clients, and to push out malware updates.
- Sometimes APT services get built into victim’s “gold builds”.
- APT service has masqueraded as the intrusion detection product installed to detect it.
- Compromise PKI and issue certs.
Real World Examples (cont.)

- Installed services that detected every new file, folder, and email created, and sent a copy to attacker
- Often uses the information for bidding purposes
  - Used by competitor to beat prices
  - Used by “trusted” partner to make sure they were getting a fair deal
Real World Examples (cont.)

- Often compromises VoIP systems, turns on microphones in conference rooms, computers, and data projectors
- Often APT is “trusted” employees of foreign subsidiary
- APT uses learned IP to produce clone product cheaper and faster
Advanced Persistent Threat (APT) Fighting Back
Attacker is organized and strategic, so it requires an organized and strategic response.
Challenges

Biggest Problems

Victim is so:

- Thoroughly compromised that they realize that everything must be fixed at once in order to be completely successfully
- Big, hard to know where to begin
- Not even sure who they can trust
- Usually doesn’t know legitimate programs from malicious ones
Challenges

What We Want To Do – The Perfect Plan

1. Unplug client network from outside
2. Rebuild AD and change all logon credentials
3. Rebuild all hosts from scratch
   • Updated all software, defenses, policies
4. Restore data and legitimate applications
5. Educate end-users
6. Turn everything back on
Challenges

Business Interruption vs. Removing APT

- Company is more worried about business interruption than attackers
- IT staff is more likely to be disciplined for disrupting business than for attacker staying in environment
- Most entities just accept that APT will never be completely gone (i.e. “crime in the big city”)

Challenges

Living With Plan B

- Client cannot handle the downtime involved with the perfect solution
- We are always left implementing “Plan B”
Actions

General Remediation Plan Types

- Rebuild Everything and Migrate
- Big “Remediation Day\Week”
- Remediation Cycles Moving Outward
  - Push Bad Guys Out Starting With Crown Jewels and Moving Out
- Fixing Problems One-At-A-Time
- Hybrid combination
A. Define How Bad Compromise Is
B. Define Data “Crown Jewels” and/or Mission-Critical Apps
C. Fix Problems
  - Updated Software, Better Policies, New Defenses, End-User Education
D. Plans are timed in years versus weeks or months
   (Each tactic only takes days to weeks, but overall, deploying all tactics takes months to years)
Actions

Suppose You Rebuild Everything?

- Even if everything is new, if old processes, policies, and end-user habits don’t change, APT is just right back in
- It is impossible to rebuild everything new at once in a very large company with tens of thousands of employees, hundreds of sites, and dozens of foreign entities and partners
Actions
Changing Passwords

- Often “just” changing all passwords is usually not acceptable
- Clients are too afraid of what applications they will break
- Clients aren’t even sure who owns what or what will break if passwords are reset
- More afraid of causing business problems than getting rid of APT
A Defense Plan
Communications

- Victim needs to notify senior management
  - Sr. Mgmt often notifies BOD
- IT should communicate as little as possible, at first
- Let Sr. Mgmt determine communication’s plan
- Often a specialized communication team is put into place
A Defense Plan
Communications (con’t)

- APT and Remediation event needs a “code word”
  - Boring, normal (e.g. Picnic event, Insurance Renewal, etc.)
- No one writes without using code word
- Consider air-gapped network and devices
- Additional people are told of APT only as needed
- Lots of manual and written communication
A Defense Plan
How Bad Is Problem?

- Need to get “eyes” into environment
- Log management
  - Process Tracking, Logon, Object Access, etc.
- Heavily monitor DCs and other major infrastructure, data servers, email servers, etc.
- NIDS\HIDS on everything
A Defense Plan
Review Policies

- What led to compromise?
  - Threat Model\Risk Management

- Best indicator of future behavior is past behavior
  - Applies to both victim and attacker

- What policies need to change?

- What software does client need to buy\upgrade?
  - Excellent opportunity to push refreshes
A Defense Plan

Identify “Crown Jewels”

- Instead of cleaning up everything at once (which is impossible anyway), start by strengthening crown jewels
- Crown Jewels = Very Important Data
  - Top secret, patents, new business, HBI, PCI, HIPAA, etc.
- Clean up crown jewel assets and networks and work your way out
Identify “Crown Jewels” (cont.)

- Inventory all apps and data
  - Identify owners
  - Identify AAA, needed groups, service accounts, permissions, etc.
  - Classify data
- Identify mission-critical apps
- Identify mission-critical partners and vendors
- Ask app owners and business unit managers to determine costs of downtime
A Defense Plan

Risk Acceptance

- Tell Sr. Mgmt that business interruption must be expected during fix phases
- Ask Sr. Mgmt to set “no-go” levels
  - Management must decide on what is allowed and accepted
  - Ex: “Late Financial Statements Are Unacceptable”
- Communicate to management that it is unlikely that APT will ever be fully gone forever, if at all
A Defense Plan

Protecting Data

- Improve Defenses
- Better Desktop and Server Policies
- Automate Security\Workflows
- Improved Authentication
- Software Refresh
- Server\Domain Isolation
A Defense Plan
Protecting Data (cont.)

- RMS, Encryption
- Better Patching for all Software
- RBAC, AD Delegation
- App-V, Med-V, VDI
- Forefront, Threat Management Gateway, etc.
- Improved End-User Education
A Defense Plan
Object Lifecycle Management

- Inventory all objects
  - Users, Groups, Service Accounts, GPOs, sites, entry points, elevated accounts, servers, etc.
- Get rid of what you don’t need
- Secure What You Have Left
A Defense Plan

Object Lifecycle Management (cont.)

Create policies and procedures to manage the lifecycle of all AD objects

Object Lifecycle Management Components

1. Acquisition/Provisioning/Creation/Approval
2. Assigning Ownership/Accountability
3. Changes/Renaming/Copies/Moves/Transfers
4. Disable/Deletion/De-Provisioning
5. Confirmation of Change
6. Auditing/Alerting/Monitoring
A Defense Plan
After Remediation Day

- Continue to improve policies
- Look for Future APT
  - Log Management
  - NIDS\HIDS, Honeypots
  - Look for hacker tools, tarballs, etc.
  - Unusual traffic patterns
In Review: Session Objectives and Takeaways

- APT is after Intellectual Property (IP) over the long-term
- Probably going to be a big problem for many years

Helping Clients
- Identify and Better Protect Crown Jewels
- Object Lifecycle Management
- Harden Servers, Clients, and Networks
- Refresh Software ("newest software is most secure")
- Better Monitoring
- End-User Education