

# Commercial Cyber Systems

Anatomy of an APT Attack  
ISSA - LA 2011



**GENERAL DYNAMICS**



# Digital Forensics & Network Defense

## Anatomy of an APT Attack

# Agenda

- **Discuss APT attacks**
- **Examples of an APT attack**
- **What strategies are not working**
- **What strategies are working**
- **Anatomy of attack**
- **Potential Containment Strategies**

# What is APT?

- **The "Advanced Persistent Threat" (APT) refers to advanced and normally clandestine means to gain continual, persistent intelligence on an individual, or group of individuals such as a foreign nation state government. While the APT is more commonly thought of as being an article of the computer era, it has existed since the realization of the benefits of intelligence gathering and long before the invention of the computer or internet.**

Definition from Wikipedia: [http://en.wikipedia.org/wiki/Advanced\\_Persistent\\_Threat](http://en.wikipedia.org/wiki/Advanced_Persistent_Threat)

# What is with the APT hype?

- **Don't focus on the buzz with APT. Focus on the persistence of the attack for means of gathering confidential information: Espionage**
- **Espionage or spying involves an individual obtaining information that is considered secret or confidential without the permission of the holder of the information. Espionage is inherently clandestine, unless the legitimate holder of the information changes plans or takes other countermeasures once it is known that the information is in unauthorized hands.**

Definition from Wikipedia: <http://en.wikipedia.org/wiki/Espionage>

# Need to answer the question, Why?

- In this example, the attacks occur to gather information for business purposes
- The question is who or what are the targets and how will the information be used?

# Think Ninjas & Jason Bourne



# NINJAS

There are four of them in this picture.

# Who is attacking me?

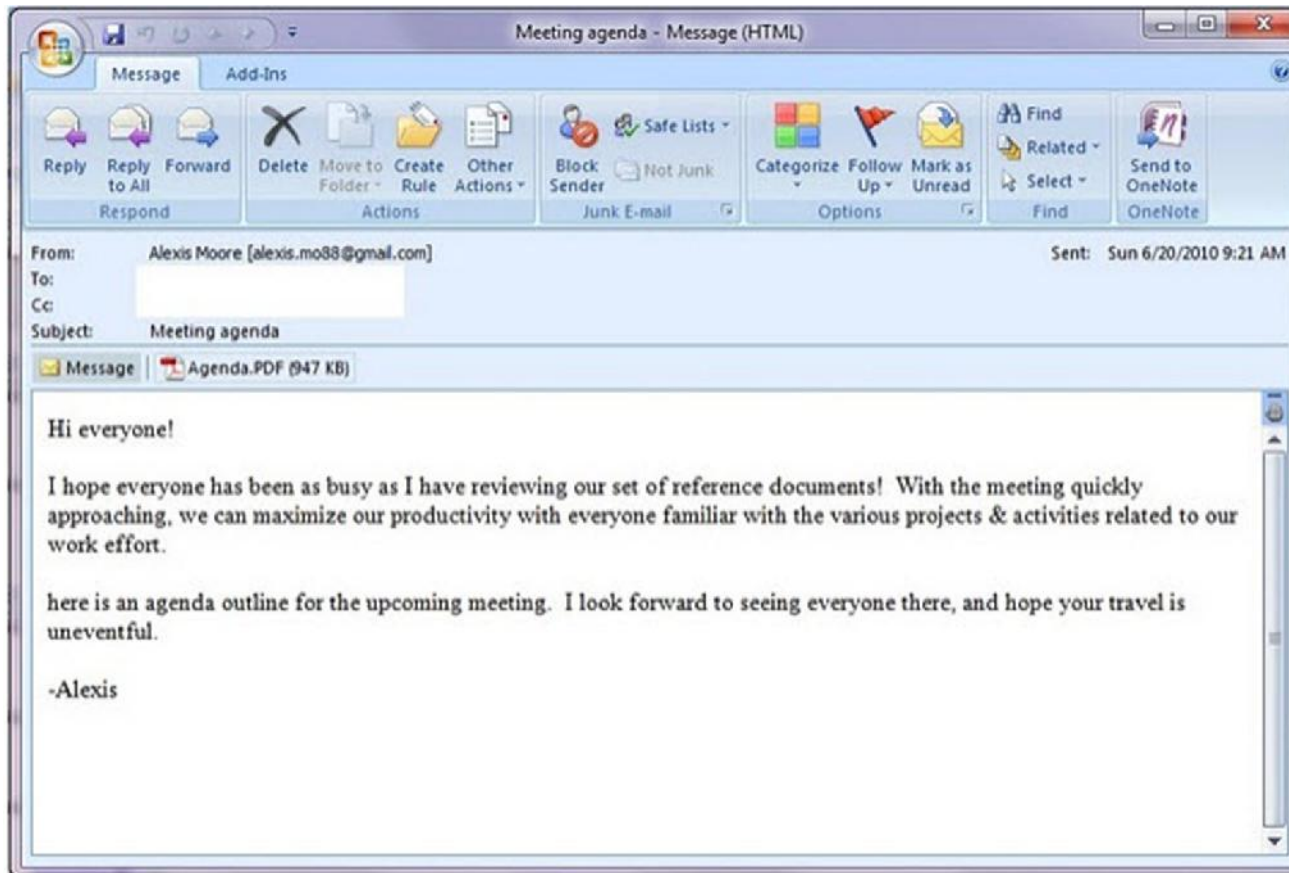
- **They are well funded**
- **Knowledgeable**
- **Sophisticated**
  - They have already anticipated your containment attempts, keep that in mind when you try to respond



# Initial Infection Vector

- **Attacks can occur through a spear phishing attack on very targeted individuals**
- **If the attack does not succeed on the targeted individuals, attackers will find another way in**

# Malicious PDF



CVE-2010-1297 - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1297>

Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64; Adobe AIR before 2.0.2.12610; and Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted SWF content, related to authplay.dll and the Action Script Virtual Machine 2 (AVM2) new function instruction, as exploited in the wild in June 2010.

## Best solution, stop them from getting inside

- **Stop them from ever getting in!**
  - Implement security awareness training (last line of defense)
  - Implement proxy level tools that prevent phishing and web based attack vectors
- **Before you respond, anticipate their escalation!**

# What happens when they get in

- **Attacker establishes multiple backdoors on systems that may likely remain on all the time – DESKTOPS & SERVERS**
- **Where does the real information exchange happen in regards to business – E-MAIL**
- **Attacker performs recon to determine where the mail servers are and what system tools they need for their attack**

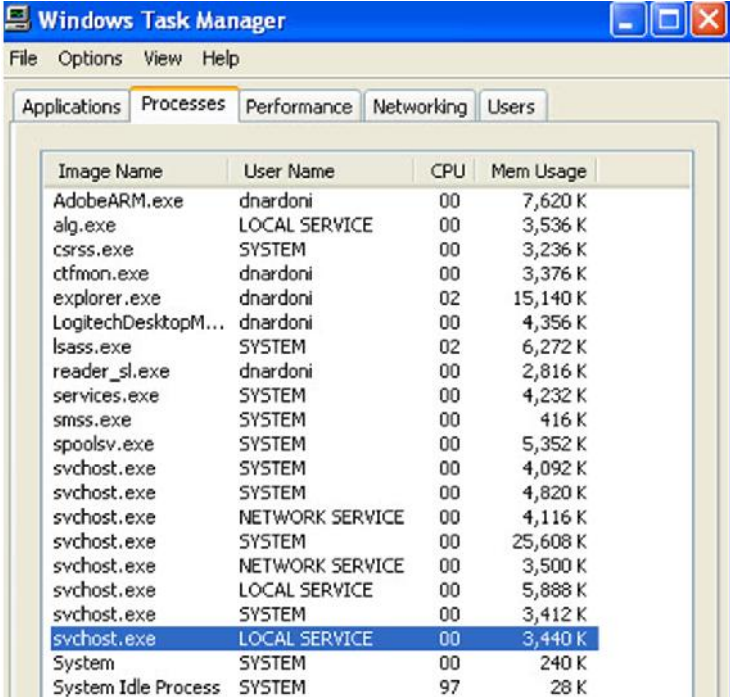
# The Example Malware (Tool set)

- **Pwdump.exe – Steal credentials**
- **Mapi.exe – Steal e-mail**
- **Rar.exe – Deploying tools and assist in exfiltration**
- **Wiam.exe – Passing the hash**
- **Various DLL and Exes – DLL's and exe's used as backdoor for attackers – often masking themselves as legitimate AV files**
- **Large dependency on windows based tools already present on systems (They have command line kung-fu!)**



# Maintaining Persistence

- **Run malicious DLL as legitimate service via svchost.exe**
  - Client Service for NetWare
  - RIP Listener Service
  - Portable Media Serial Number Service
  - Authentication Service



Windows Task Manager

File Options View Help

Applications Processes Performance Networking Users

Image Name	User Name	CPU	Mem Usage
AdobeARM.exe	dnardoni	00	7,620 K
alg.exe	LOCAL SERVICE	00	3,536 K
csrss.exe	SYSTEM	00	3,236 K
ctfmon.exe	dnardoni	00	3,376 K
explorer.exe	dnardoni	02	15,140 K
LogitechDesktopM...	dnardoni	00	4,356 K
lsass.exe	SYSTEM	02	6,272 K
reader_sl.exe	dnardoni	00	2,816 K
services.exe	SYSTEM	00	4,232 K
smss.exe	SYSTEM	00	416 K
spoolsv.exe	SYSTEM	00	5,352 K
svchost.exe	SYSTEM	00	4,092 K
svchost.exe	SYSTEM	00	4,820 K
svchost.exe	NETWORK SERVICE	00	4,116 K
svchost.exe	SYSTEM	00	25,608 K
svchost.exe	NETWORK SERVICE	00	3,500 K
svchost.exe	LOCAL SERVICE	00	5,888 K
svchost.exe	SYSTEM	00	3,412 K
svchost.exe	LOCAL SERVICE	00	3,440 K
System	SYSTEM	00	240 K
System Idle Process	SYSTEM	97	28 K

# Anti-forensics Activities

- **Making it more difficult to find them**
  - **Dates and times are changed on dll's and exe's**
- **Covering their tracks**
  - **Files used for collection are securely wiped – Sdelete**
    - Original file called dave.doc becomes AAAA.AAA with hex 00 in every sector
  - **Overflow event logs with junk – fictitious logon entries**

# Detection methods

## ➤ Detection methods

- Review dates and times in \$MFT
  - Compare file name attributes to standard information attributes
- Frequent audit log review

## ➤ Countermeasures

- Increase log sizes and/or move to centrally managed archive with read-only access
- Implement HIPS tools to log network and/or increased access to systems
- AV and HIPS logs are quite often detecting malicious activity, but not blocking it

File Write	C:\WINDOWS\system32\cmd.exe	C:\WINDOWS\system32\rar.exe
File Write	C:\WINDOWS\system32\cmd.exe	C:\WINDOWS\system32\rar.exe
File Write	C:\WINDOWS\system32\cmd.exe	C:\WINDOWS\system32\p.rar



# Obtaining the Password Hash

- **Authenticates via command line to the remote victim system**
- **Copy's a password hash dumping tool onto the remote system via administrative network share**
- **Executes the hash dumping tool via scheduled tasks and dumps hashes to a file**
  - Little or no AV alerts
  - Log entries are more difficult to track down
  - Leaves few indicators

# Obtaining the Password Hash

- **The contents of the hash log is reviewed**
  - Targeted user and hash is possibly identified
  - Accounts with admin privileges identified
- **The hashing tool and log is deleted**
  
- **Now they have your hashes! What is your initial reaction?**

# Hash Dumping Tool Marks

- **The executable must be run from on the local system to retrieve the hashes**
- **We have only been able to get to tool work from a scheduled task.**
  - Remember scheduled tasks run as SYSTEM
- **The scheduled task log records the action of the job executing. (AT(x).job)**
  - Use this as part of your timeline
- **The scheduled task also appears in the security event log.**

# Attack Overview

- From a foothold in the network, the Net.exe is used to authenticate to the victim system
- Attacker verifies username and access permissions using net.exe
- A reverse shell is established over Port 443 to an IP on the internet for exfiltration
- Deploys rar.exe
- Tool set contained within [evil].rar file is deployed to victim system

# Mail Retrieval and Exfiltration

- The compressed archive containing tools are extracted
- One of the tools extracted from the compressed archive is used to retrieve mail from exchange servers (m.exe) legitimate name [MAPIGET.exe]
- Mail retrieval is executed via passing the hash to m.exe.

```
wiam -h  
[USERNAME]:[DOMAINNAME]:ADRED435B51404EEAAD3B435  
B5147466:DREFDE7D0DEEB31A80F134CEA7427466 -r "m -  
s:[EMAILSERVER] -u:[USERNAME] -t:2010-01-05-01 -  
o:c:\windows\system32\t\mail"
```

# Mail Retrieval and Exfiltration

- **The individual mail messages are stored as text files in a directory structure for the given user**
  - C:\windows\system32\t\mail\dnardoni
- **Any attachments associated with the individual mail messages are exported**
- **Once the mail retrieval process is completed, any files with the extension jpg, gif or png are deleted to minimize file size of archive to be exfiltrated**

# Mail Retrieval and Exfiltrated

- **The contents of the mail directories are compressed into an encrypted archive**
- **The retrieved mail files are then deleted**
- **(The compressed, encrypted archive is exfiltrated over the reverse shell)**
- **All of the tools and archives are deleted**
- **The reverse shell is shut down and deleted as the at(x).job completes**

**Whole process takes about 45 min (volume of email) from deployment of tools, gathering email, exfiltration and clean up**

# So what does that leave us to examine?

- **Prefetch**
- **Memory/Pagefile analysis**
- **Deleted files**
- **Registry (services running as dlls)**
- **Scheduled tasks At[x.]job files**
- **Event logs (sometimes)**
- **AV/HIPS logs attackers overlooked**
- **Network monitoring if in place?**
- **Any centralized logging**
- **Firewall/Router logs**



# Summary

## ➤ What works

- Be diligent, attackers make mistakes, things do not always go as planned
- Anticipate their response to your containment
- Have a tiered response that can easily give you information you need to answer the question

# Summary

- **What does not work**
  - Thinking attackers will just go away
  - Shutting the door they entered; they already have other ways in
  - Your internal team can not fight them in their spare time
- **You know you are making progress when you have made it harder for them to get what they want!**