APT ATTACK

Nguyen Hong Son

WHAT IS AN APT?

- The term **Advanced Persistent Threat** was created by analysts in the United States Air Force in 2006. It describes three aspects of attackers that represent their profile, intent, and structure:
  - ✓ Advanced: The attacker is fluent with cyber-intrusion methods and administrative techniques and is capable of crafting custom exploits and tools.
  - ✓ Persistent: The attacker has a long-term objective and works to achieve his or her goals without detection.
  - ✓ Threat: The attacker is organized, funded, motivated, and has ubiquitous opportunity.

Features (1/2)

- Attackers seek to remove obstacles
- Do not usually include sabotage
- Clean traces of their actions from system logs
- APT tools utilize normal everyday functions native within the operating system and hide in the file system “in plain sight.”
- Do not want to impede or interrupt the normal system operations of the hosts they compromise
- Practice low-profile attack, penetration, reconnaissance, lateral movement, administration, and data exfiltration techniques
- The most popular technique used by APT groups to gain access to target networks is spear-phishing
- Spear-phishing relies upon e-mail, may include malware that deliberately attempts to exploit software on the user’s computer

Features (2/2)

- Attackers generally utilize previously compromised networks of computers as “cutouts” to hide behind for proxied command and control communications
- Popular and common techniques observed in APT campaigns include SQL injection of target websites, “meta”-exploits of web server software, phishing, and exploits of social networking applications
- Common social engineering techniques such as impersonating users to help desk personnel, infected USB “drops,” infected hardware or software

Phases of APT

- Targeting
- Access
- Reconnaissance
- Lateral movement
- Data collection and exfiltration
- Administration and maintenance

Targeting phase

- Attackers collect information about the target from public or private sources
- Testing methods that may help permit access.This may include vulnerability scanning, social engineering, and spear-phishing.
- The target may be specific or may be an affiliate/partner that can provide collateral access through business networks.

Access phase

- Attackers gain access and determine the most efficient or effective methods of exploiting the information systems and security posture of the target organization.
- The compromised host's identifying data (IP address, DNS, enumerated NetBIOS shares, DNS/DHCP server addresses, OS, etc.) as well as collecting credentials or profile information where possible to facilitate additional compromises.
- Attackers may attempt to obfuscate their intentions by installing rogueware or other malware.

Reconnaissance phase

- Attackers enumerate network shares, discover the network architecture, name services, domain controllers, and test service and administrative rights to access other systems and applications.
- They may attempt to compromise Active Directory accounts or local administrative accounts with shared domain privileges.
- Attackers often attempt to hide activities by turning off antivirus and system logging

Lateral movement phase

- Once attackers have determined methods of traversing systems with suitable credentials and have identified targets, they will conduct lateral movement through the network to other hosts.
- Activities often do not involve the use of malware or tools other than those already supplied by the compromised host operating systems such as command shells, NetBIOS commands, Windows Terminal Services, VNC, or other similar tools utilized by network administrators.

Data collection and exfiltration phase

- Attackers often establish collection points and exfiltrate the data via proxied network cut-outs, or utilize custom encryption techniques (and malware) to obfuscate the data files and related exfiltration communications.
- In many cases, attackers have utilized existing backup software or other administrative tools used by the compromised organization’s own network and systems administrators.
- The exfiltration of data may be “drip fed” or “fire hosed” out, the technique depending on the attackers’ perception of the organization’s ability to recognize the data loss or the attackers’ need to exfiltrate the data quickly.

Administration and maintenance phase

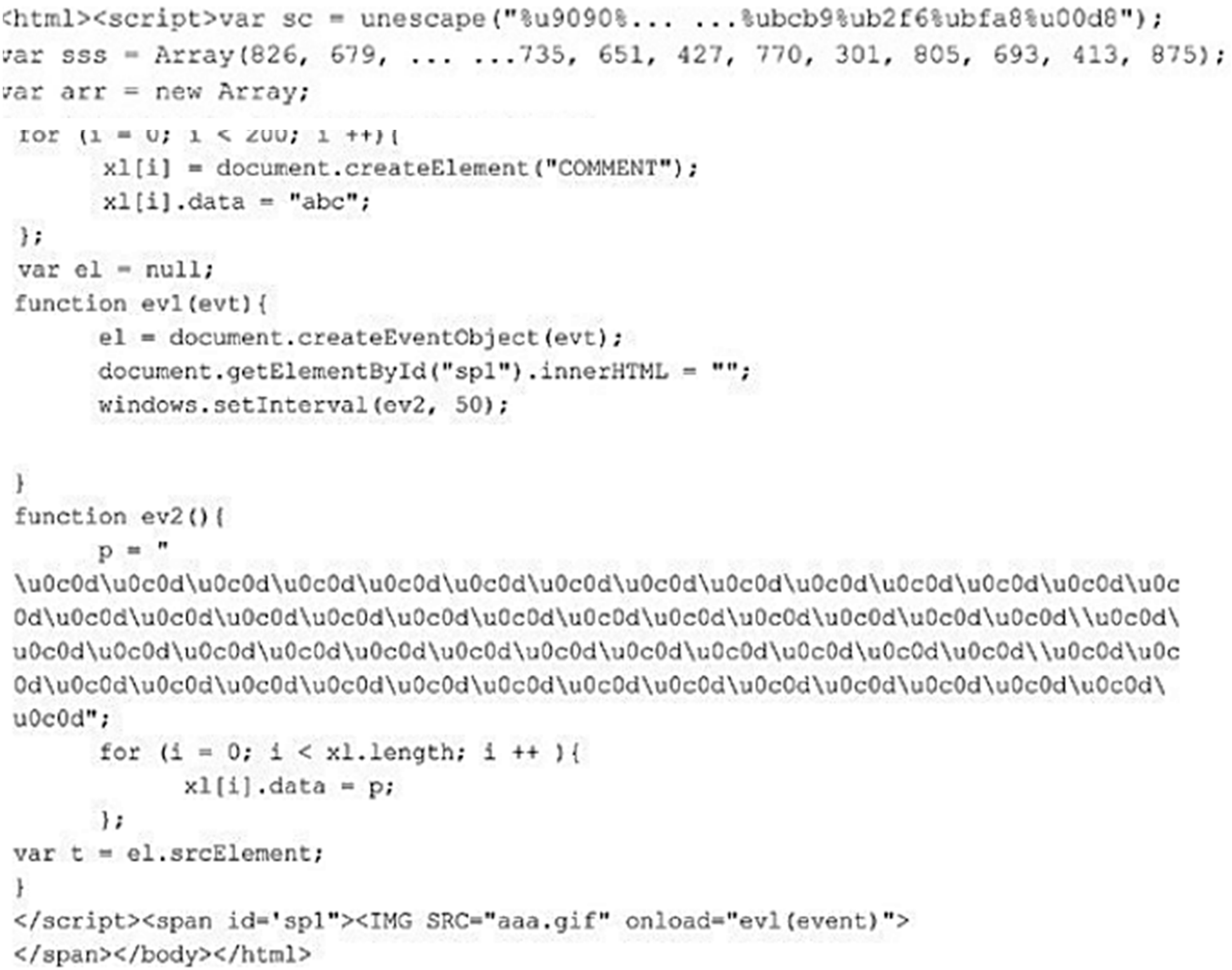
- Another goal of an APT is to maintain access over time. This requires administration and maintenance of tools and credentials.
- Attackers will establish multiple methods of accessing the network of compromised hosts remotely and build flags or triggers to alert them of changes to their compromised architecture, so they can perform maintenance actions
- Attackers usually attempt to advance their access methods to most closely reflect standard user profiles, rather than continuing to rely upon select tools or malware.

Typical APT campaigns

- Several APT attacks, code-named by investigators : Aurora, Nitro, ShadyRAT, Lurid, Night Dragon, Stuxnet, DuQu
- Each involved operational activities, including access, reconnaissance, lateral movement, manipulation of information systems, and exfiltration of private or protected information

Example: Aurora

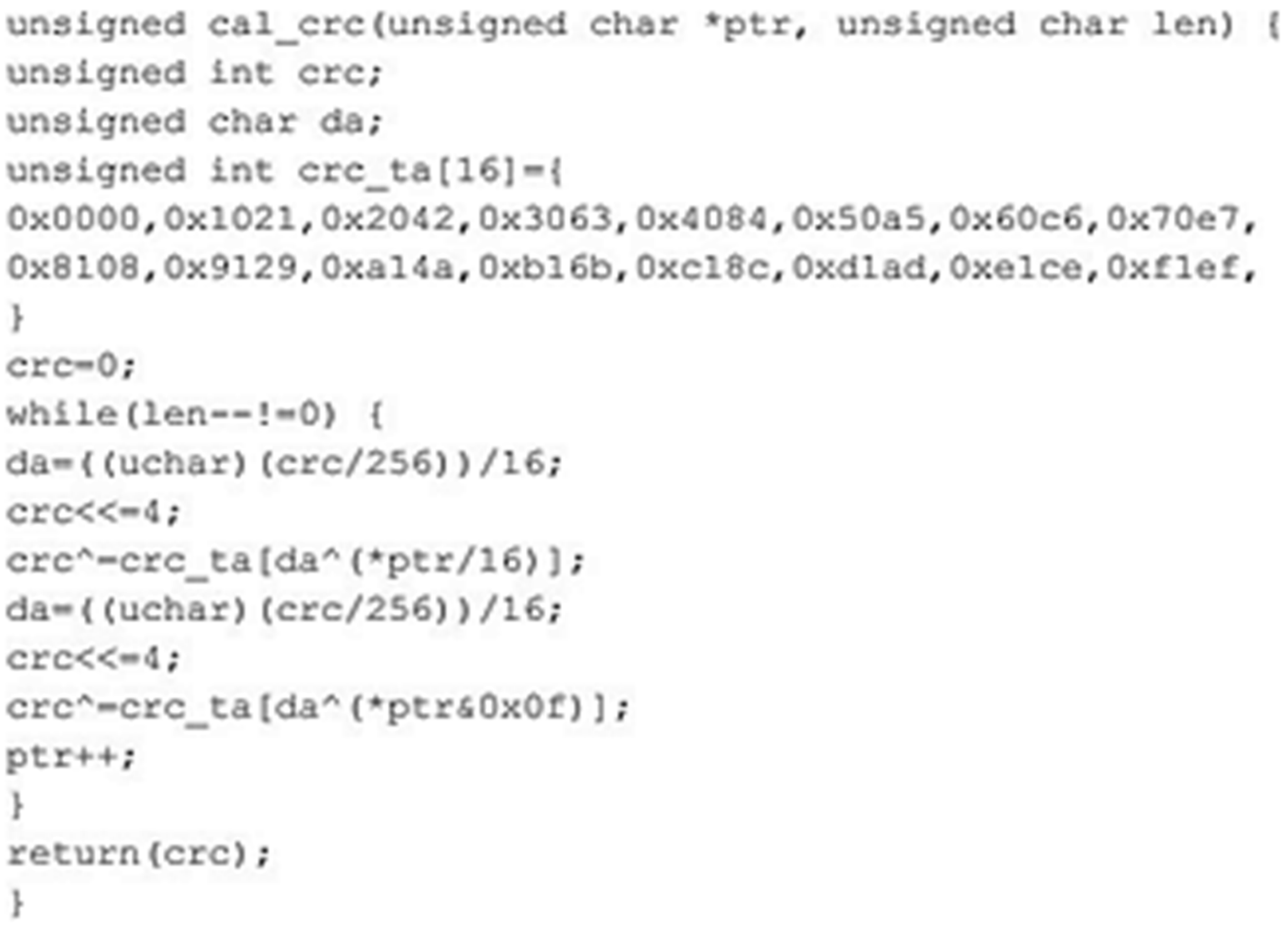
- The attackers gained access to victims' networks by using targeted spear-phishing e-mails sent to company employees.
- The e-mail contained a link to a Taiwanese website that hosted a malicious JavaScript.
- When the e-mail recipient clicked the link and accessed the website, the JavaScript exploited an Internet Explorer vulnerability that allowed remote code execution.
- The malicious JavaScript was undetected by antivirus signatures. It functioned by injecting shell code with the following code:



```
<html><script>var sc = unescape("%u9090%... ...%ubcb9%ub2f6%ubfa8%u00d8");
var sss = Array(826, 679, ... ...735, 651, 427, 770, 301, 805, 693, 413, 875);
var arr = new Array;
 for (i = 0; i < 200; i ++){
        xl[i] = document.createElement("COMMENT");
        xl[i].data = "abc";
 };
 var el = null;
 function ev1(evt){
        el = document.createEventObject(evt);
        document.getElementById("sp1").innerHTML = "";
        windows.setInterval(ev2, 50);


 }
 function ev2(){
        p = "
\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c
0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\\u0c0d\
u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\\u0c0d\u0c
0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\
u0c0d";
        for (i = 0; i < xl.length; i ++ ){
               xl[i].data = p;
        };
 var t = el.srcElement;
 }
 </script><span id='sp1"><IMG SRC="aaa.gif" onload="ev1(event)">
 </span></body></html>
```

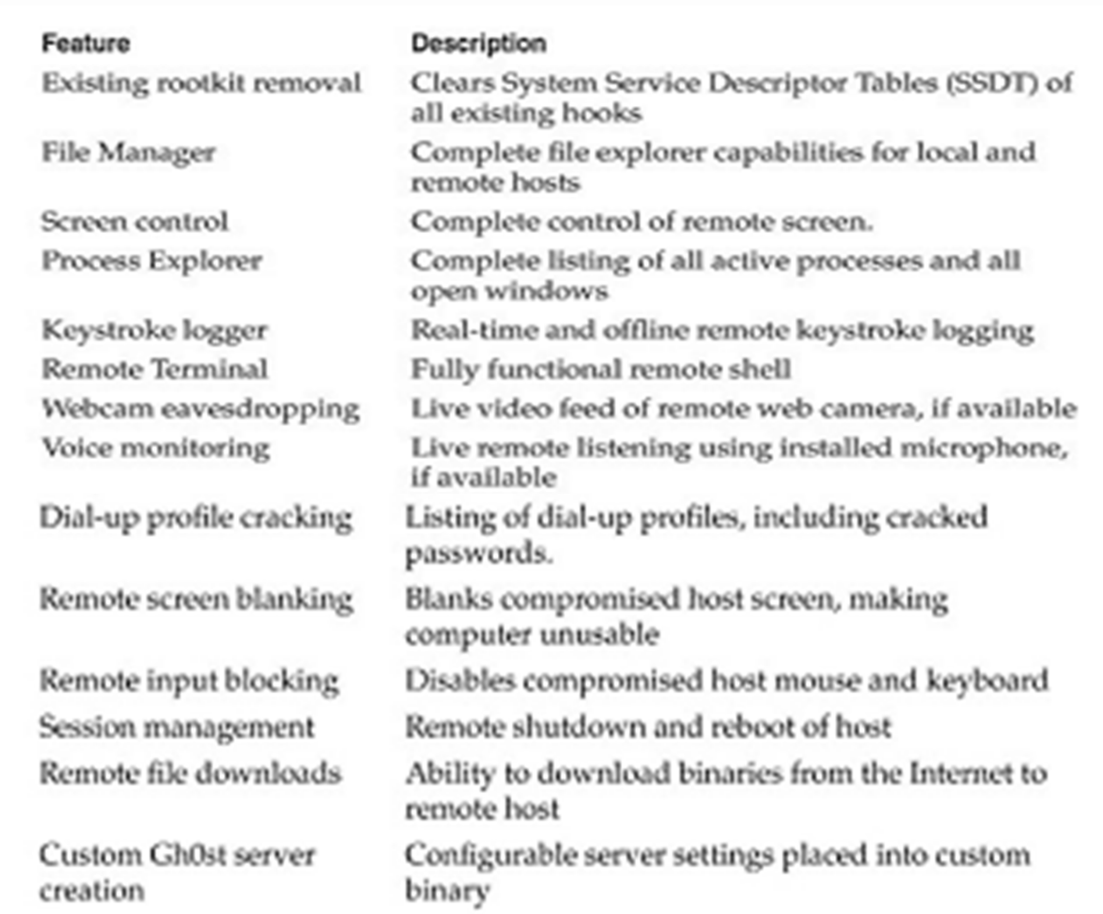
- In the JavaScript exploit, a simple cyclic redundancy checking (CRC) routine of 16 constants was used. The following code demonstrates the CRC method:



```
unsigned cal_crc(unsigned char *ptr, unsigned char len) {
unsigned int crc;
unsigned char da;
unsigned int crc_ta[16]={
0x0000,0x1021,0x2042,0x3063,0x4084,0x50a5,0x60c6,0x70e7,
0x8108,0x9129,0xa14a,0xb16b,0xc18c,0xd1ad,0xe1ce,0xf1ef,
}
crc=0;
while(len--!=0) {
da=((uchar)(crc/256))/16;
crc<<=4;
crc^=crc_ta[da^(*ptr/16)];
da=((uchar)(crc/256))/16;
crc<<=4;
crc^=crc_ta[da^(*ptr&0x0f)];
ptr++;
}
return(crc);
}
```

Popular APT Tools: Gh0st Attack

- It is a Remote Administration Tool (RAT)
- It is used in the "Gh0stnet" attacks in 2008–2010, as the example of malware used for APT attacks



Feature	Description
Existing rootkit removal	Clears System Service Descriptor Tables (SSDT) of all existing hooks
File Manager	Complete file explorer capabilities for local and remote hosts
Screen control	Complete control of remote screen.
Process Explorer	Complete listing of all active processes and all open windows
Keystroke logger	Real-time and offline remote keystroke logging
Remote Terminal	Fully functional remote shell
Webcam eavesdropping	Live video feed of remote web camera, if available
Voice monitoring	Live remote listening using installed microphone, if available
Dial-up profile cracking	Listing of dial-up profiles, including cracked passwords.
Remote screen blanking	Blanks compromised host screen, making computer unusable
Remote input blocking	Disables compromised host mouse and keyboard
Session management	Remote shutdown and reboot of host
Remote file downloads	Ability to download binaries from the Internet to remote host
Custom Gh0st server creation	Configurable server settings placed into custom binary

Other APT Tools

- DarkComet RAT
- PlasmaRAT
- NingaliNET
- Marble codes

Example: Malicious E-mail

From: Jessica Long
[mailto:administrateur@hacme.com]
Sent: Monday, 19 December 2011 09:36
To: US_ALL_FinDPT
Subject: Bank Transaction fault

This notice is mailed to you with regard to the Bank payment (ID: 012832113749) that was recently sent from your account.

The current status of the referred transfer is: ‘failed due to the technical fault’.

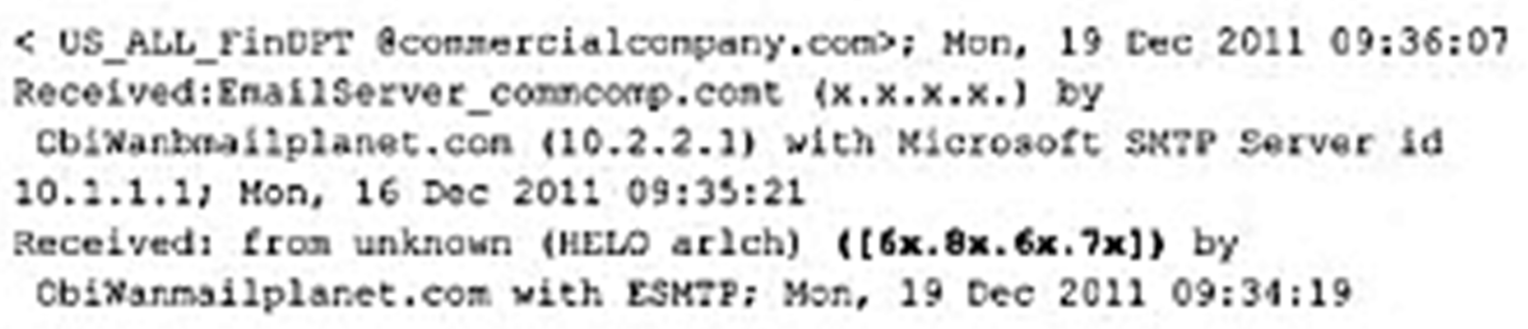
Please check the report below for more information:

http://finiancialservicesc0mpany.de/index.html

Kind regards,
Jessica Long
TEPA - The Electronic Payments
Association – securing your transactions

Example: Malicious E-mail

- The next step involved analyzing the e-mail headers for any leads:



```
< US_ALL_FinDPT @commercialcompany.com>; Mon, 19 Dec 2011 09:36:07
Received:EmailServer_commcomp.cont (x.x.x.x.) by
 CbiWanbmailplanet.com (10.2.2.1) with Microsoft SMTP Server id
10.1.1.1; Mon, 16 Dec 2011 09:35:21
Received: from unknown (HELO arlch) ([6x.8x.6x.7x]) by
 ObiWanmailplanet.com with ESMTP; Mon, 19 Dec 2011 09:34:19
```

- Using whois, robtex.com, phishtank.com, the investigator discovered that the IP address originated from Germany and was on several blacklists as being used in SPAM campaigns

Mechanisms for malware to survive a reboot

- Using various “Run” Registry keys
- Creating a service
- Hooking into an existing service
- Using a scheduled task
- Disguising communications as valid traffic
- Overwriting the master boot record
- Overwriting the system’s BIOS

RFC 3227: incident response procedures

- The correct way to perform incident response is by using the order of volatility described in RFC 3227
- The order in which evidence should be collected based upon the volatility of the data:
  - Memory
  - Page or swap file
  - Running process information
  - Network data such as listening ports or existing connections to other systems
  - System Registry (if applicable)
  - System or application log files
  - Forensic image of disk(s)
  - Backup media

The toolkit for APT investigation

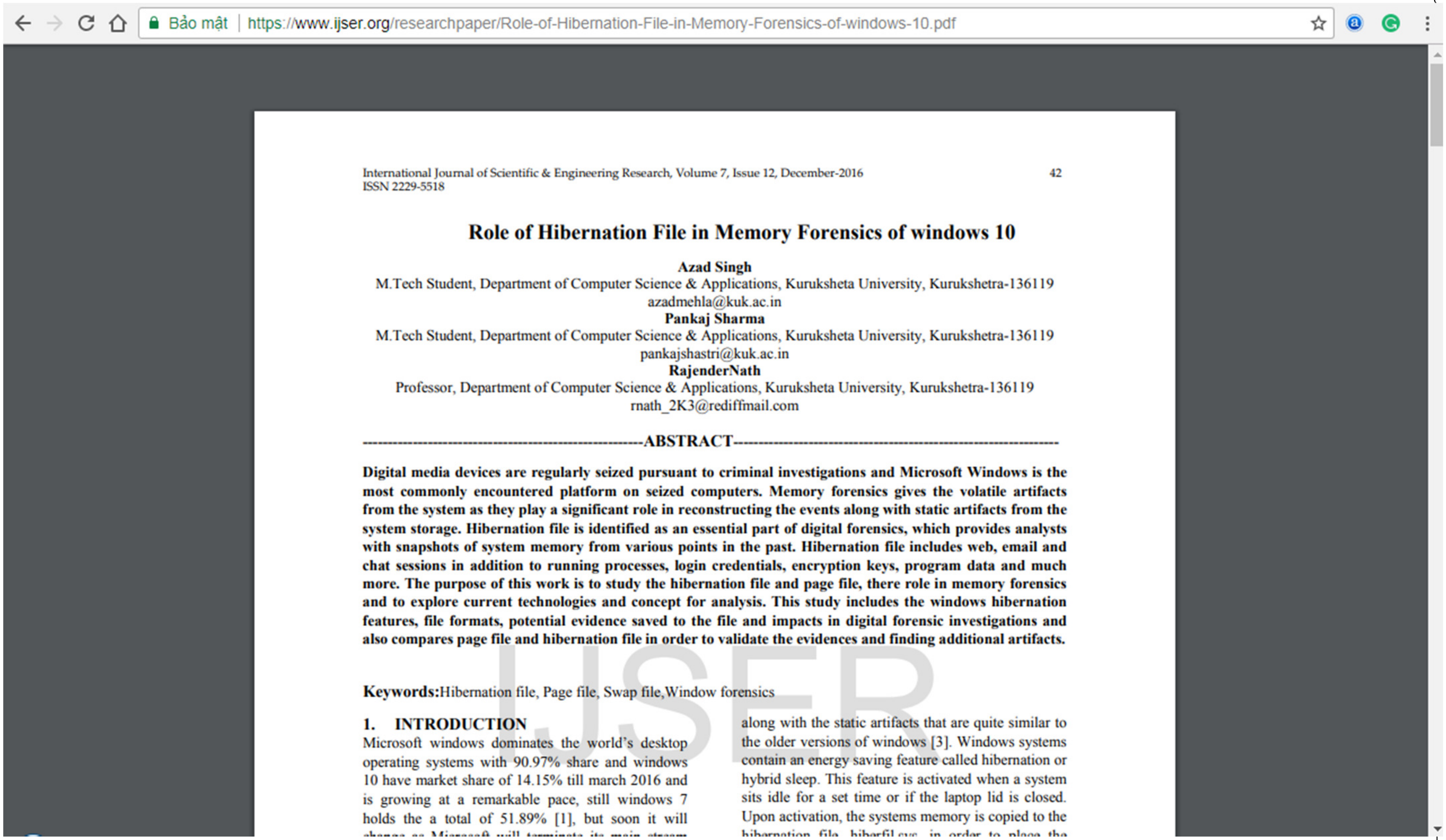
- Investigators used in this case consisted of a mix of Sysinternals and forensic tools:
  - AccessData FTK Imager
  - Sysinternals Autoruns
  - Sysinternals Process Explorer
  - Sysinternals Process Monitor
  - WinMerge
  - Currports
  - Sysinternals Vmmap

Memory Capture

- First perform a memory dump of the compromised computer
- This dump can be useful for analysis of related malware within the Volatility Framework Tool, for example FTK Imager.
- Several memory analysis tools are available including HBGary FDPro and Responder Pro, Mandiant Memoryze and The Volatility Framework
- Memory analysis is a crucial part of APT analysis as many tools or methods employed by attackers will involve process injection or other obfuscation techniques.

Pagefile/Swapfile

- The virtual memory used by the Windows operating systems is stored in a file called Pagefile.sys (Pagefile)
- The Pagefile can contain valuable information about malware infections or targeted attacks
- The Hyberfil.sys contains in-memory data stored while the system is in Hibernation mode and can offer additional data to examiners
- https://www.ijser.org/researchpaper/Role-of-Hibernation-File-in-Memory-Forensics-of-windows-10.pdf



Bảo mật | https://www.ijser.org/researchpaper/Role-of-Hibernation-File-in-Memory-Forensics-of-windows-10.pdf

Role of Hibernation File in Memory Forensics of windows 10

Azad Singh
M.Tech Student, Department of Computer Science & Applications, Kuruksheta University, Kurukshetra-136119
azadmehla@kuk.ac.in
Pankaj Sharma
M.Tech Student, Department of Computer Science & Applications, Kuruksheta University, Kurukshetra-136119
pankajshastri@kuk.ac.in
RajenderNath
Professor, Department of Computer Science & Applications, Kuruksheta University, Kurukshetra-136119
rnath_2K3@rediffmail.com

--**ABSTRACT**--

Digital media devices are regularly seized pursuant to criminal investigations and Microsoft Windows is the most commonly encountered platform on seized computers. Memory forensics gives the volatile artifacts from the system as they play a significant role in reconstructing the events along with static artifacts from the system storage. Hibernation file is identified as an essential part of digital forensics, which provides analysts with snapshots of system memory from various points in the past. Hibernation file includes web, email and chat sessions in addition to running processes, login credentials, encryption keys, program data and much more. The purpose of this work is to study the hibernation file and page file, there role in memory forensics and to explore current technologies and concept for analysis. This study includes the windows hibernation features, file formats, potential evidence saved to the file and impacts in digital forensic investigations and also compares page file and hibernation file in order to validate the evidences and finding additional artifacts.

Keywords: Hibernation file, Page file, Swap file,Window forensics

1. INTRODUCTION

Microsoft windows dominates the world's desktop operating systems with 90.97% share and windows 10 have market share of 14.15% till march 2016 and is growing at a remarkable pace, still windows 7 holds the a total of 51.89% [1], but soon it will change as Microsoft will terminate its main stream

along with the static artifacts that are quite similar to the older versions of windows [3]. Windows systems contain an energy saving feature called hibernation or hybrid sleep. This feature is activated when a system sits idle for a set time or if the laptop lid is closed. Upon activation, the systems memory is copied to the hibernation file, hiberfil.sys, in order to place the

Memory Analysis

- For analysis of the memory dump file, use the Volatility Framework Tool.
- First, start with image identification:

```
$ python vol.py –f  /home/imegaofmemdump.mem imageinfo
```

- Next, retrieve the processes:

```
$ python vol.py –f  /home/imegaofmemdump.mem pslist
```

- Next, check the network connections:

```
$ python vol.py –f  /home/imegaofmemdump.mem connscan
```

- For example: The other active connection to 192.168.6.128 over port 80 is using PID 1024. That PID is used by one of the svchost.exe processes. Let’s have a deeper look into the process with PID 1024:

```
$ python vol.py –f  /home/imegaofmemdump.mem dlllist –p 1024
```

Master File Table

- Each file on an NTFS volume is represented by a record in a special file called the Master File Table (MFT).
- This table is of great value in investigations. Filenames, timestamps, and many more “metadata” can be retrieved to provide insights into the incident through timeline correlations, filenames, file sizes, and other properties.
- For example, in malicious email as above mentioned, the MFT indicates that a Trojan Dropper (server.exe) was created in the %TEMP% directory of the Ch1n00k user profile at 9:43 am on 2/19/2011:

Network/Process/Registry

- For attackers in an APT, it is important to have connectivity to a couple of hosts and move throughout the network. Therefore, determining if there are any suspicious connections from the machine toward other (unknown) addresses is important.
- On the compromised computer, open a command prompt and enter the following command:

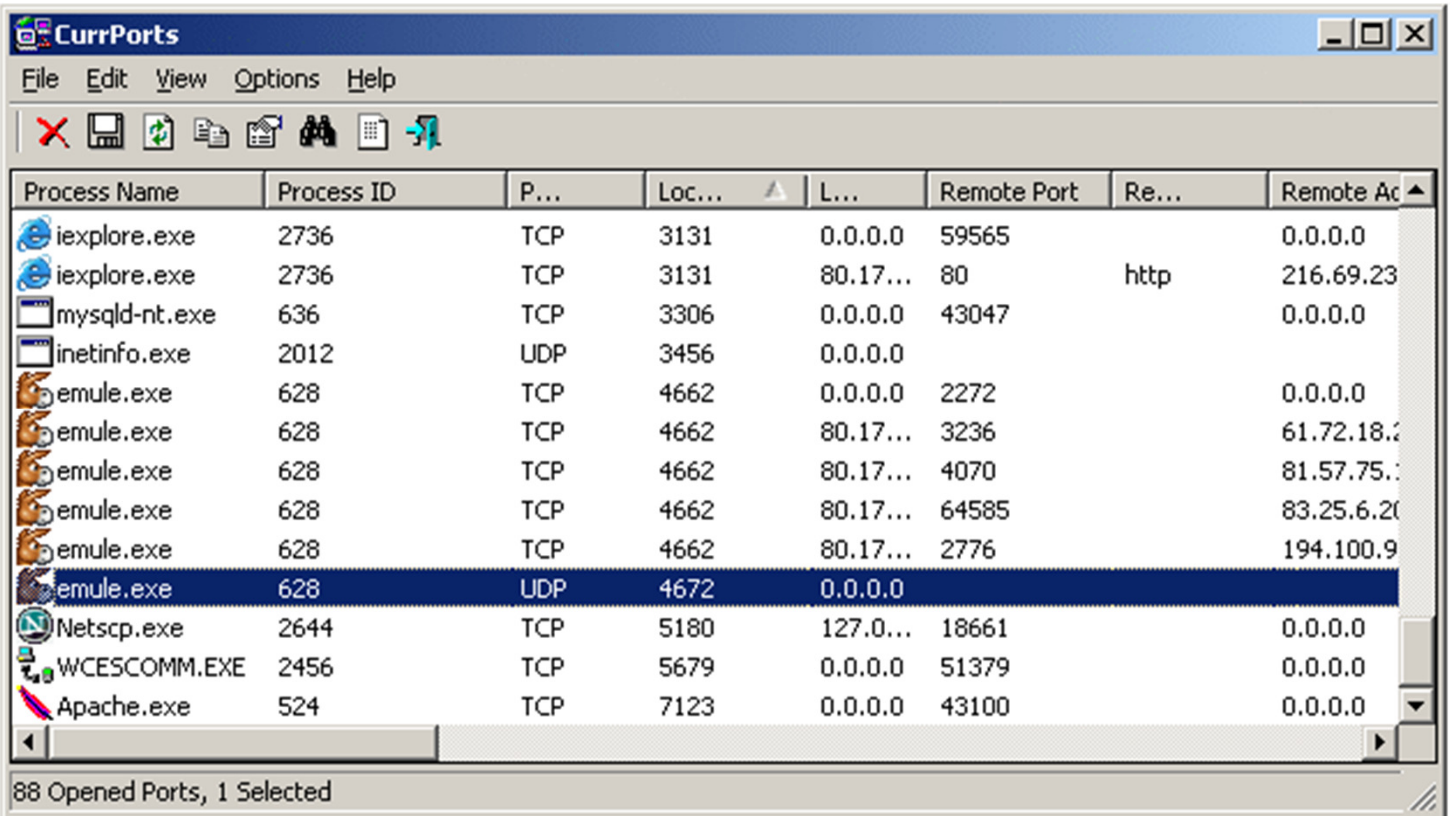
```
netstat -ano
```

Hosts File

- A quick check can be made of the system’s hosts file for changes.
- The original hosts file (/Windows/System32/drivers/etc) has a size of 734 bytes. Any increase in size is suspicious.

CurrPorts

- A useful tool for investigating active network sessions
- This tool graphically represents the sessions



Process Name	Process ID	P...	Loc...	L...	Remote Port	Re...	Remote Ac
iexplore.exe	2736	TCP	3131	0.0.0.0	59565		0.0.0.0
iexplore.exe	2736	TCP	3131	80.17...	80	http	216.69.23
mysqld-nt.exe	636	TCP	3306	0.0.0.0	43047		0.0.0.0
inetinfo.exe	2012	UDP	3456	0.0.0.0			
emule.exe	628	TCP	4662	0.0.0.0	2272		0.0.0.0
emule.exe	628	TCP	4662	80.17...	3236		61.72.18.2
emule.exe	628	TCP	4662	80.17...	4070		81.57.75.1
emule.exe	628	TCP	4662	80.17...	64585		83.25.6.20
emule.exe	628	TCP	4662	80.17...	2776		194.100.9
emule.exe	628	UDP	4672	0.0.0.0			
Netscp.exe	2644	TCP	5180	127.0...	18661		0.0.0.0
WCESCOMM.EXE	2456	TCP	5679	0.0.0.0	51379		0.0.0.0
Apache.exe	524	TCP	7123	0.0.0.0	43100		0.0.0.0

88 Opened Ports, 1 Selected

Process Explorer

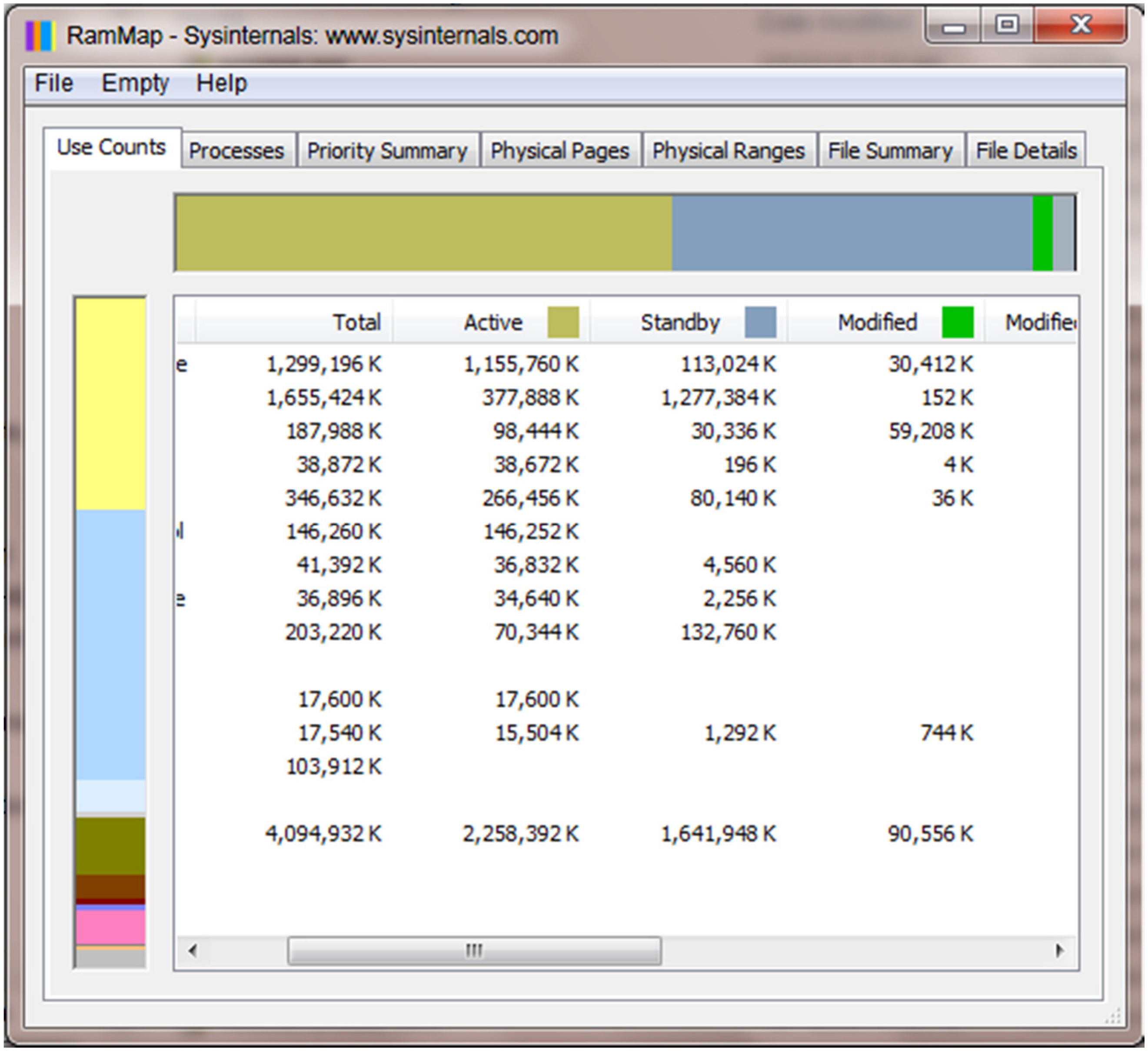
- In Process Explorer, look up the process with PID and right-click on the process and then select the Properties option
- The Strings tab gives detailed information about the printable strings that are present, both in the image and memory, regarding this process

Process Monitor

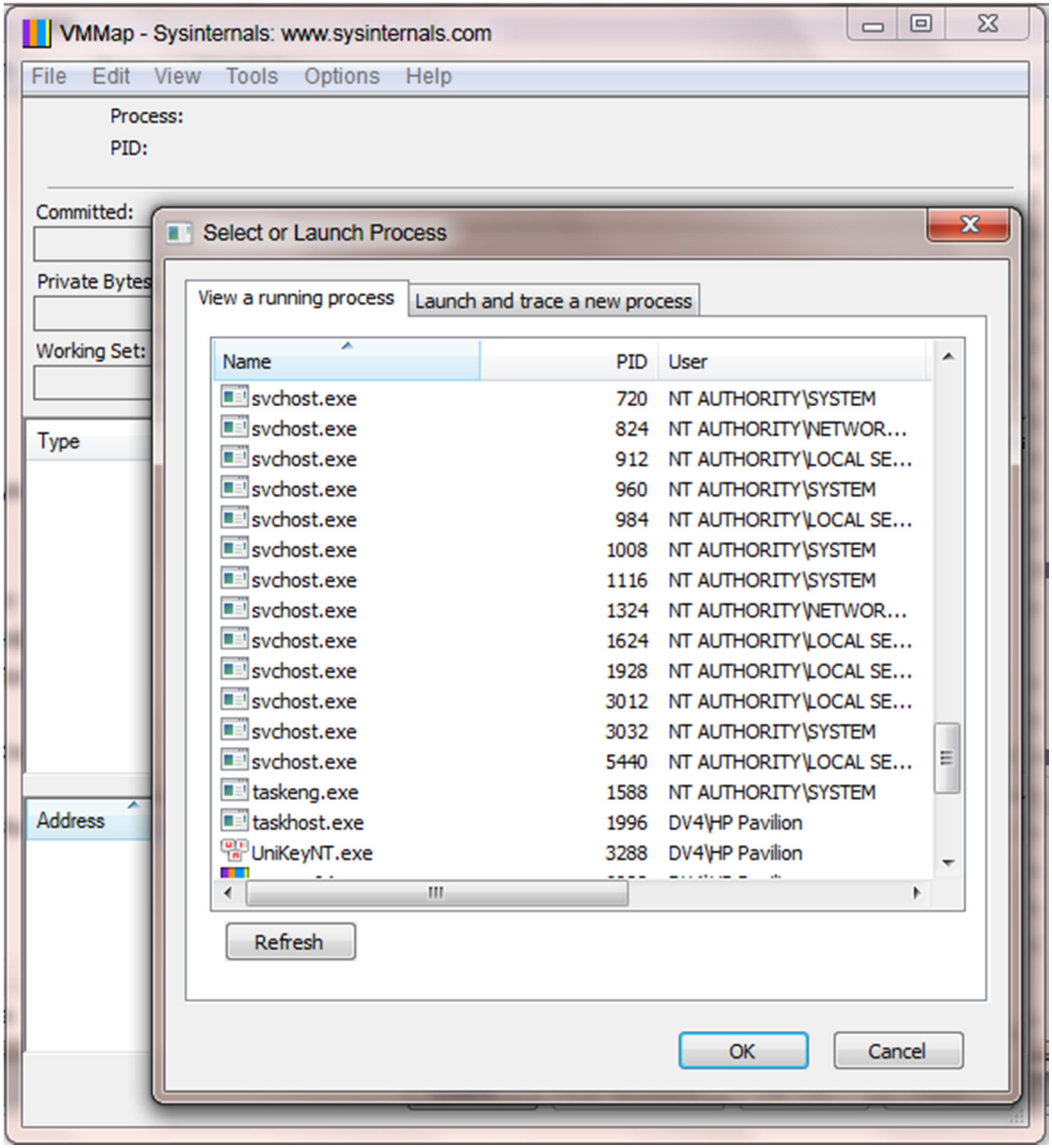
- Process Monitor allows us to view all kernel interactions that processes make with the file and operating systems
- This helps with understanding how malware modifies a compromised system and provides indicators of compromise that are useful for developing detection scripts and tools.

RamMap/VMMap

- RamMap is used to display system and process memory statistics and utilization
- VMMap is a process virtual and physical memory analysis utility.
- It shows a breakdown of a process’s committed virtual memory types as well as the amount of physical memory (working set) assigned by the operating system to those types.
- Besides graphical representations of memory usage, VMMap also shows summary information and a detailed process memory map.



	Total	Active 🟨	Standby 🟦	Modified 🟩	Modifie
e	1,299,196 K	1,155,760 K	113,024 K	30,412 K	
	1,655,424 K	377,888 K	1,277,384 K	152 K	
	187,988 K	98,444 K	30,336 K	59,208 K	
	38,872 K	38,672 K	196 K	4 K	
	346,632 K	266,456 K	80,140 K	36 K	
l	146,260 K	146,252 K			
	41,392 K	36,832 K	4,560 K		
e	36,896 K	34,640 K	2,256 K		
	203,220 K	70,344 K	132,760 K		
	17,600 K	17,600 K			
	17,540 K	15,504 K	1,292 K	744 K	
	103,912 K				
	4,094,932 K	2,258,392 K	1,641,948 K	90,556 K	



Name	PID	User
svchost.exe	720	NT AUTHORITY\SYSTEM
svchost.exe	824	NT AUTHORITY\NETWOR...
svchost.exe	912	NT AUTHORITY\LOCAL SE...
svchost.exe	960	NT AUTHORITY\SYSTEM
svchost.exe	984	NT AUTHORITY\LOCAL SE...
svchost.exe	1008	NT AUTHORITY\SYSTEM
svchost.exe	1116	NT AUTHORITY\SYSTEM
svchost.exe	1324	NT AUTHORITY\NETWOR...
svchost.exe	1624	NT AUTHORITY\LOCAL SE...
svchost.exe	1928	NT AUTHORITY\LOCAL SE...
svchost.exe	3012	NT AUTHORITY\LOCAL SE...
svchost.exe	3032	NT AUTHORITY\SYSTEM
svchost.exe	5440	NT AUTHORITY\LOCAL SE...
taskeng.exe	1588	NT AUTHORITY\SYSTEM
taskhost.exe	1996	DV4\HP Pavilion
UniKeyNT.exe	3288	DV4\HP Pavilion

DNS Cache

- To determine the infection vector, it can be useful to dump the cached DNS requests that the suspicious host has made
- Execute the following

```
ipconfig /displaydns > [evidencegatheringdrive]\displaydnsoutput.txt
```

COMMON APTS INDICATORS (1/2)

- Network communications utilizing SSL or private encryption methods, or sending and receiving base64-encoded strings
- Services registered to Windows NETSVCS keys and corresponding to files in the %SYSTEM% folder with DLL or EXE extensions and similar filenames as valid Windows files
- Copies of CMD.EXE as SVCHOST.EXE or other filenames in the %TEMP% folder
- LNK files referencing executable files that no longer exist
- RDP files referencing external IP addresses
- Windows Security Event Log entries of Types 3, 8, and 10 logons with external IP addresses or computer names that do not match organizational naming conventions

COMMON APTS INDICATORS (2/2)

- Windows Application Event Log entries of antivirus and firewall stop and restart
- Web server error and HTTP log entries of services starting/stopping, administrative or local host logons, file transfers, and connection patterns with select addresses
- Antivirus/system logs of C:\, C:\TEMP, or other protected areas of attempted file creations
- Generic Downloader, or Generic Dropper antivirus detections
- Anomalous .bash_history,/var/logs, and service configuration entries
- Inconsistent file system timestamps for operating system binaries

The most common method of attack: step 1,2 and 3

- A spear-phishing e-mail is delivered to address(es) in the organization
- A user opens the e-mail and clicks a link that opens the web browser or another application, such as Adobe Reader, Microsoft Word, Microsoft Excel, or Outlook Calendar. The link is redirected to a hidden address, with a base64-encoding key.
- The hidden address refers to a “dropsite,” which assesses the browser agent type for known vulnerabilities and returns a Trojan downloader. The Trojan downloader is usually temporarily located in c:\documents and settings\<user>\local settings\temp and automatically executes.

Step 4

- Upon execution, the downloader conveys a base64-encoded instruction to a different dropsite from which a Trojan dropper is delivered. The Trojan dropper is used to install a Trojan backdoor that is either:
  - a. Packaged into the dropper and then deletes itself, and the Trojan backdoor begins beaconing out to the C&C server programmed into its binary or
  - b. Requested from a dropsite (can be the same), according to system configuration details that the dropper communicates to the dropsite. Then the dropper deletes itself and the Trojan backdoor begins beaconing out to the C&C server programmed into its binary.

Step 5, 6

- The Trojan dropper usually installs the Trojan backdoor to c:\windows\system32 and registers the DLL or EXE in the HKLM\System\<Controlset>\Services portion of the registry,– usually as a svchost.exe netsvcs -k enabled service key (to run as a service and survive reboot).
- The Trojan backdoor typically uses a filename that is similar to, but slightly different from, Windows filenames.

Step 7, 8

- The Trojan backdoor uses SSL encryption for communications with its C&C server via a “cutout” or proxy server. Often several proxies are used in transit to mask the path to the actual C&C server. The beacon is usually periodic, such as every five minutes or hours.
- The attacker interacts with the Trojan backdoor via the proxy network, or occasionally directly from a C&C server. Communications are usually SSL encrypted, even if using nonstandard ports.

Step 9, 10

- The attacker typically begins with Computer name and User accounts listings to gain an understanding of the naming conventions used and then uses a pass-the-hash or security dump tool (often HOOKMSGINA tools or GSECDUMP) to harvest local and active directory account information.
- The attacker often uses service privilege escalation for initial reconnaissance to gain lateral movement in the network. For example, if an attacker exploits a vulnerable application (IE etc.) to gain local privileges, he or she often uses Scheduled Tasks to instantiate a command shell with administrative or service permissions. This is a known vulnerability in all Windows versions except Win 7 and commonly used; therefore, Scheduled Tasks are also important to review.

Step 11, 12

- The attacker cracks the passwords offline and uses the credentials to perform reconnaissance of the compromised network via the Trojan backdoor, including network scans, shares, and services enumerations using DOS. This helps the attacker determine lateral access availability.
- Once the lateral access across the network is determined, the attacker reverts to Windows administrative utilities such as MSTSC (RDP), SC, NET commands, and so on. If lateralaccess is impeded by network segmentation, the attacker often employs NAT proxy utilities

Step 13, 14

- When network lateral movement and reconnaissance activities have been completed, the attacker moves to a second stage and installs additional backdoor Trojans and reverse proxy utilities (such as HTRAN) to enable more direct access and establish egress points.
- The egress points are used to collect and steal targeted proprietary information, usually in encrypted ZIP or RAR packages, often renamed as GIF files

APTs Detection

- The easiest method is a simple administrative procedure.For example, a logon script that creates a file system index (c:\dir/a/s/TC>\index\%computername%_%date%.txt) can be used for auditing changes made to the file system
- SMS rules that alert administrative logons (local and domain) to workstations and servers can help to define a pattern of activity or reveal useful information for investigating these incidents
- Firewall or IDS rules that monitor for inbound RDP/VNC/CMD.EXE or administrative and key IT accounts can also be indicators of suspicious activity
- Key detection technologies: Endpoint security products, including antivirus, HIPS, and file system integrity checking

The End