/Rooted 2010

Fighting Advanced Persistent Threats (APT) with Open Source Tools

What is APT?

- The US Air Force invented the term in 2006
- APT refers to advanced techniques used to gain access to an intelligence objective to gather the needed information to execute specific objectives.

APT characteristics

- Advanced: The intruder can exploit publicly known vulnerabilities but the attackers also are highly skilled and well funded and can research and exploit new vulnerabilities.
- Persistent: the attacker wants to accomplish a mission that can take place over months.
- Threat: Dedicated organized groups are behind the attack motivated by political, economical or military reasons.

GhostNet

- Ghostnet: China VS Tibetan institutions
- 1295 computers in 103 countries

Aurora Attack

- Coordinated attack against Google, Adobe, Juniper and 30 other companies.
- Exploits a zero-day vulnerability in Microsoft Internet Explorer (CVE-2010-0249)
- Installs Trojan.Hydraq.

Trojan.Hydraq

- Standard Trojan, not too sophisticated.
- No anti-debugging, No anti-analysis tricks.
- Uses spaghetti code to make code analysis more difficult. (Easily analized with IDA)
- Previous versions of Trojan.Hydraq observed 6 month previous to Aurora Attack.

Trojan.Hydraq

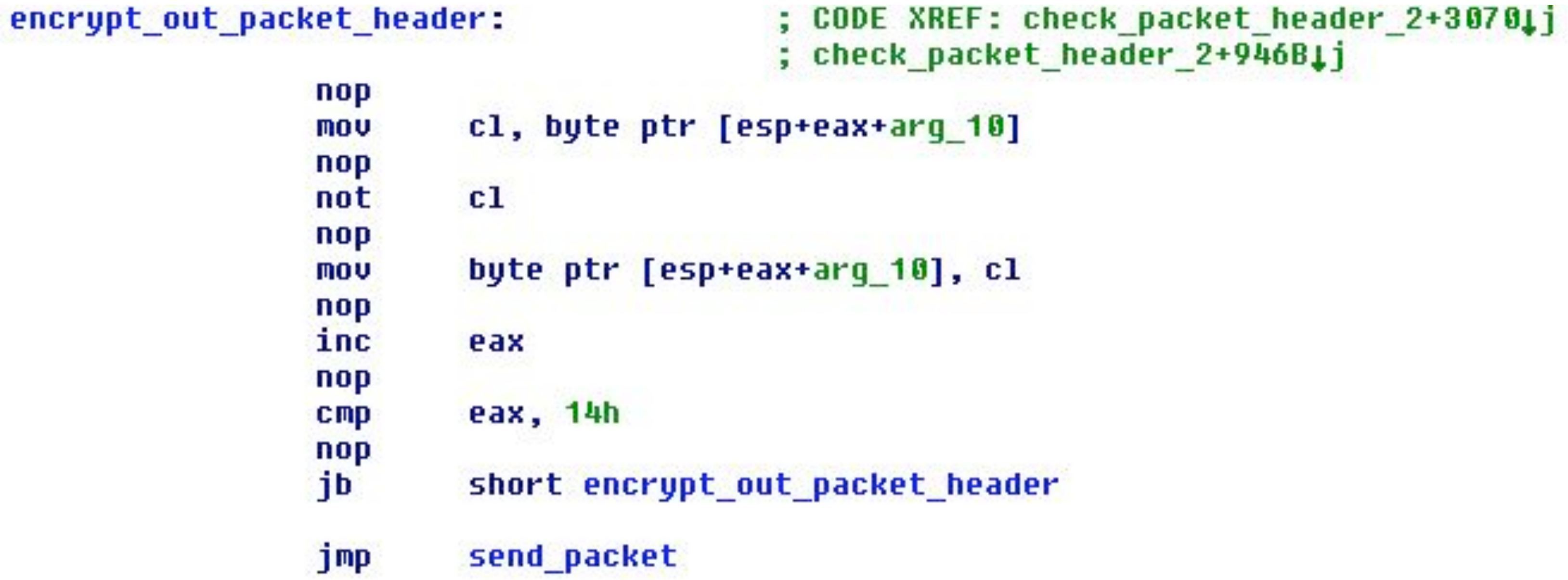
- Files:
  - %System%\[RANDOM].dll: Main backdoor registered as a service.
  - %System%\acelpvc.dll: Remote access capabilities (VNC).
  - %System%\VedioDriver.dll: Helps monitoring keyboard and mouse activity.

Trojan.Hydraq

- Capabilities:
  - Command execution
  - Download additional files
  - System operations (halt, clean log files…)
  - Service, registry control.

Trojan.Hydraq

- C&C communication:
  - Encrypted protocol on port 443 (not SSL)
    [ff ff ff ff ff ff 00 00 fe ff ff ff ff ff ff ff ff ff 88 ff]



```
encrypt_out_packet_header:                ; CODE XREF: check_packet_header_2+3070↓j
                                          ; check_packet_header_2+946B↓j
                nop
                mov     cl, byte ptr [esp+eax+arg_10]
                nop
                not     cl
                nop
                mov     byte ptr [esp+eax+arg_10], cl
                nop
                inc     eax
                nop
                cmp     eax, 14h
                nop
                jb      short encrypt_out_packet_header

                jmp     send_packet
```

Source: McAfee Labs

Keys for Fighting APT

- An anti-APT solution doesn't exist~~s~~.
- Centralizing and correlating security data is the key (SIEM!!)
- Security is a continuous process.

Intrusion

- Examples:
  - An email with a PDF or Office document that exploits a vulnerability (Maybe 0-day).
- Countermeasures:
  - Patch Management and Auditing (Openvas + OVAL).
  - Policy Auditing (Openvas – Ossec checks).
    - Is Adobe Javascript support disabled?
    - Internet Explorer Security Configuration

Setting Up

- Examples:
  - – Backdoor and Rootkit installation, system modification, privilege escalation.
- Countermeasures:
  - – Log monitoring: Ossec, Snare.
  - – Integrity Monitoring: Ossec
    - Registry changes.
    - File creation/modifications
    - Service registration and process creation.

Network Activity

- Examples:
  - C&C communication, cover channels, updated downloads…

- Countermeasures:
  - IDS/IPS technology (Snort, Suricata). Ej: Packed binary download.
  - Deep Packet Inspection (OpenDPI). Ej: Non SSL traffic over port 443.

Network Activity

- Netflow Data : Nfdump + Nfsen (plugins).
  - AS and Country data.
    - Alert on suspicious AS's (reputation) – Fire project
      - http://www.maliciousnetworks.org/index.php
  - Identify traffic patterns:
    - Mutiple clients sending high amount of data to an external server.
    - Regurar~~ly~~ client connections to external servers (even after hours)

Advanced techniques

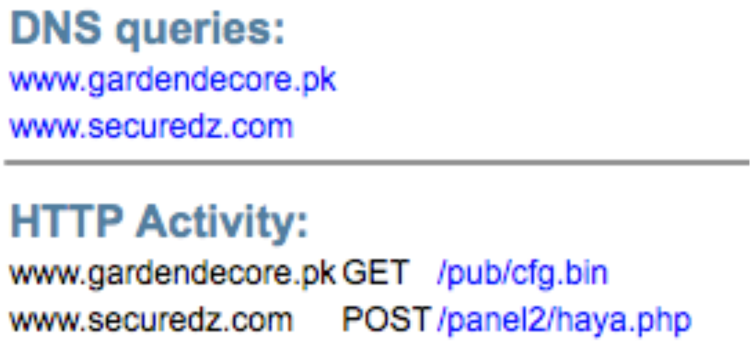
- Create an APT trap
  - Information Gathering
    - Collect suspicious content from Corporate Mail Server.
    - Create false accounts.
  - Automatic analysis framework
    - Analize obtained information
      - Check for exploits/javascript on .pdf, .xls, .doc files.
    - Extract the involved binary
    - Automatic sandbox/analysis environment.
    - Compare obtained patterns with your SIEM data.

Advanced techniques

- Analize obtained data
  - The goal is to identify malicious content an extract the involved binary.
  - Tools:
    - **Didier Stevens pdf tools**
    - SpiderMonkey
    - Libemu
    - JsUnpack
    - Malzilla
    - Wepawet

Advanced techniques

- Automatic sandbox/analysis environment
  - Once we have the binary we have to extract the information needed to build the Behaviour Matrix.
  - SandBox execution:
    - Qemu, VirtualBox, Bochs….
    - Dynamic pattern extraction:
      - Snare, Ossec, memoryze, Volatility…
    - Network behaviour pattern extraction:
      - Snort for IDS pattern detection
      - Scapy protocol parsers:
        - » DNS, HTTP, IRC, SMTP….



DNS queries:

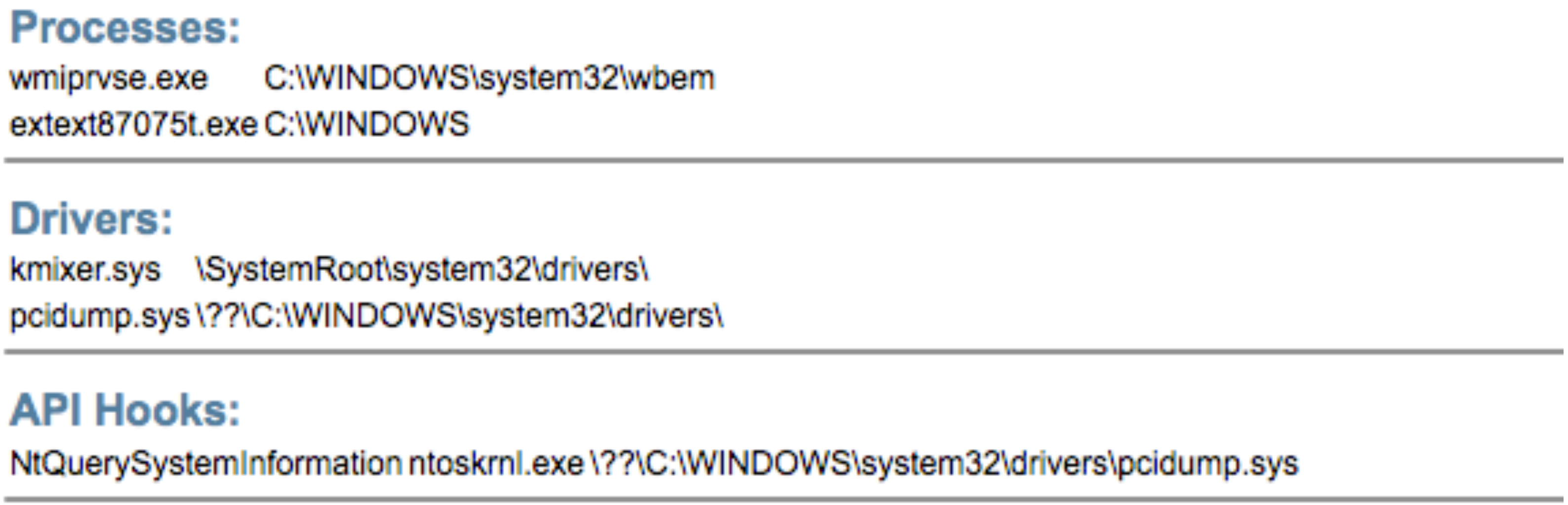
www.gardendecore.pk
www.securedz.com

HTTP Activity:

www.gardendecore.pk	GET	/pub/cfg.bin
www.securedz.com	POST	/panel2/haya.php

Advanced techniques

- Static analysis
  - Antivirus Coverage : VirusTotal
  - Packers : PeFile + PEID
  - Imports/Exports : PeFile
  - Antidebug/Virtual Machine Detection : Pyew



Processes:

wmiprvse.exe C:\WINDOWS\system32\wbem

extext87075t.exe C:\WINDOWS

Drivers:

kmixer.sys \SystemRoot\system32\drivers\

pcidump.sys \??\C:\WINDOWS\system32\drivers\

API Hooks:

NtQuerySystemInformation ntoskrnl.exe \??\C:\WINDOWS\system32\drivers\pcidump.sys

Advanced techniques

- Build the behaviour matrix, example:

[Process_Creation, test.exe]

[DNS_Query, www.securedz.com]

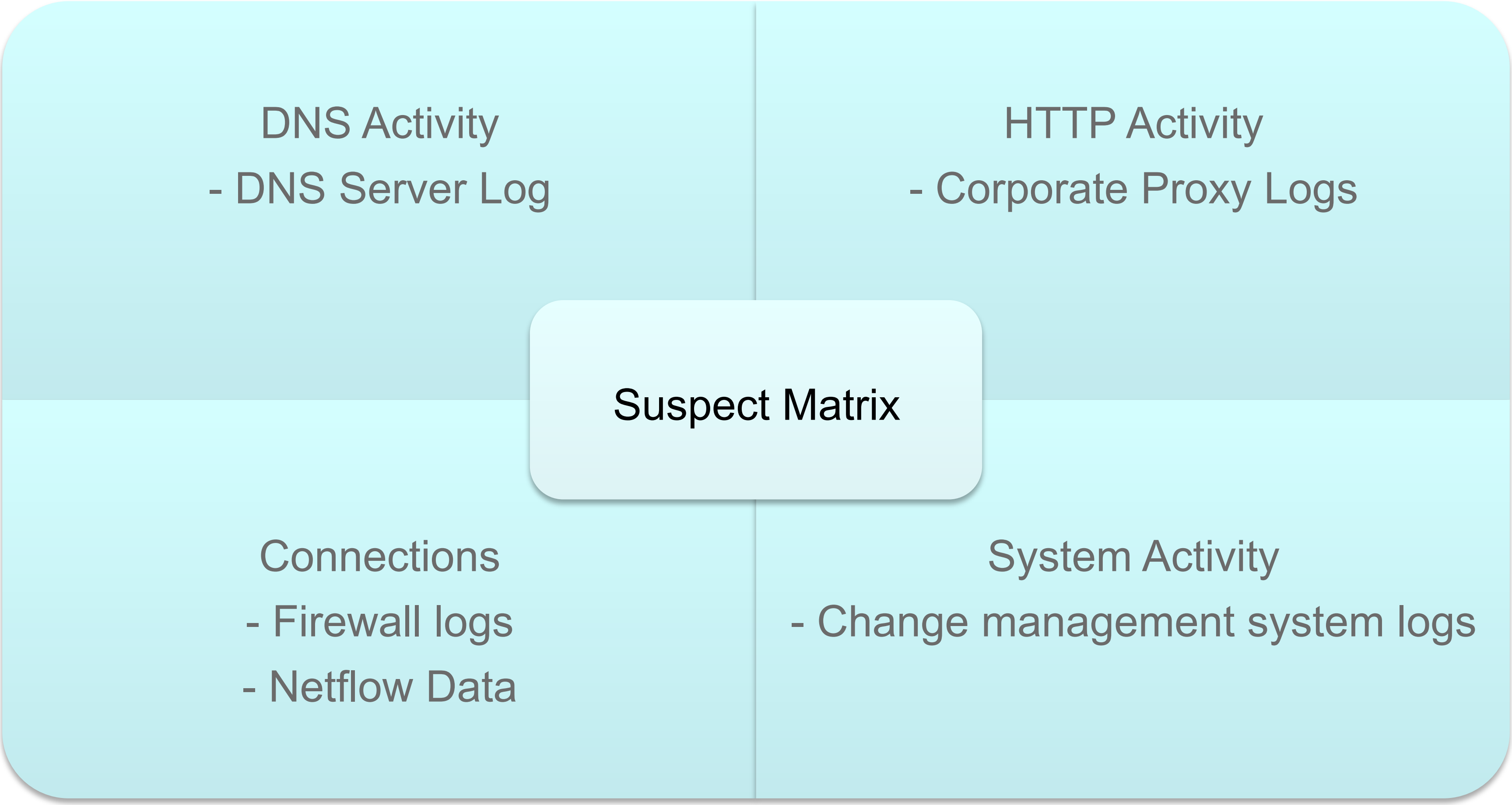
[HTTP_Request, POST, /panel2/haya.php]

[Driver_Loaded, wowsub.sys]

[IDS_Pattern, Snort, 200857

Advanced techniques

- Once you have the behaviour matrix:



DNS Activity
- DNS Server Log

HTTP Activity
- Corporate Proxy Logs

Suspect Matrix

Connections
- Firewall logs
- Netflow Data

System Activity
- Change management system logs

Jaime Blasco

jaime.blasco@alienvault.com

http://twitter.com/jaimeblascob