Search and Destroy the Unknown

FROM MALWARE ANALYSIS TO INDICATIONS OF COMPROMISE

Who am I?

- Michael Boman, Malware Researcher
- Malware Research Institute
- Provide the community with knowledge and tools

Detecting the Unknown

- FBI: There are only two types of companies: those that have been hacked, and those that will be.
- Always assume that you have been compromised and look for signs to confirm the assumption

Where to look

- There is gold in those logfiles!
  - Firewall
  - IDS / IPS
  - Proxy
  - DNS
  - System logfiles
  - Netflow data

Firewall

- New sessions are enough, no need to log every packet
- Ingress (incoming) AND Egress (outgoing)
- Denied AND Permitted

IDS / IPS

- Detecting attacks are "nice", detecting compromises are "cool"
- You need **actionable** information from your IDS / IPS system
- Custom rules are the path to salvation

Proxy

- Detecting known bad sites
- Trace infections to source
- Detecting outliers

DNS

- Log queries
- Establish DNS query & response baseline
- Analyze NXDOMAIN responses
- Analyze successful DNS lookups
- Identify domain name abnormalities

Windows 7 regular expressions	SOURCE	EventID Number
.*APPCRASH.*	Application	1001
.*he protected system file.*	Application	64004
.*EMET_DLL Module logged the following event:.*	Application	2
.*your virus/spyware.*	Application	Depends
.*A new process has been created\..*	Security	4688
.*A service was installed in the system\..*	Security	4697
.*A scheduled task was created\..*	Security	4698
.*Logon Type:[\W]*(3|10).*	Security	4624, 4625
.*\\Software\\Microsoft\\Windows\\CurrentVersion\\Run.*	Security	4657
.*service terminated unexpectedly\..*	System	7034
.*service was successfully sent a.*	System	7035
.*service entered the.*	System	7036
.*service was changed from.*	System	7040

Netflow data

- WHO is talking to WHOM
- When doing incident response, being able to narrow down the scope is key

Aquire the sample

- Exctraction from network traffic
- File on disk
- Memory dump

Extracting from Network Traffic

- Wireshark
  - GUI
- Network Miner
  - GUI
- Foremost
  - foremost –v –i /path/to/pcap
- Dshell
  - DShell> decode –d rip-http --rip-output_dir=output/ /path/to/pcap

Extracting from Memory

- Creating the memory dump

PsExec.exe \\HOSTNAME_OR_IP -u DOMAIN\privileged_account -p passwd -c mdd_1.3.exe - -o C:\MEMORY.DMP

- Extracting the executable / DLL from the memory dump

volatility dlldump -f MEMORY.DMP -D dumps/

volatility procmemdump -f MEMORY.DMP -D dumps/

Analyze the sample

- Confirm the malicious nature of the suspected sample
- Identify behavior that can be used to identified infected machines

Confirming the sample

- Static analysis
- Dynamic analysis

Cuckoo Sandbox

- Uses DLL-injection techniques to intercept and log specific API calls
- Uses TCPDump to capture network traffic

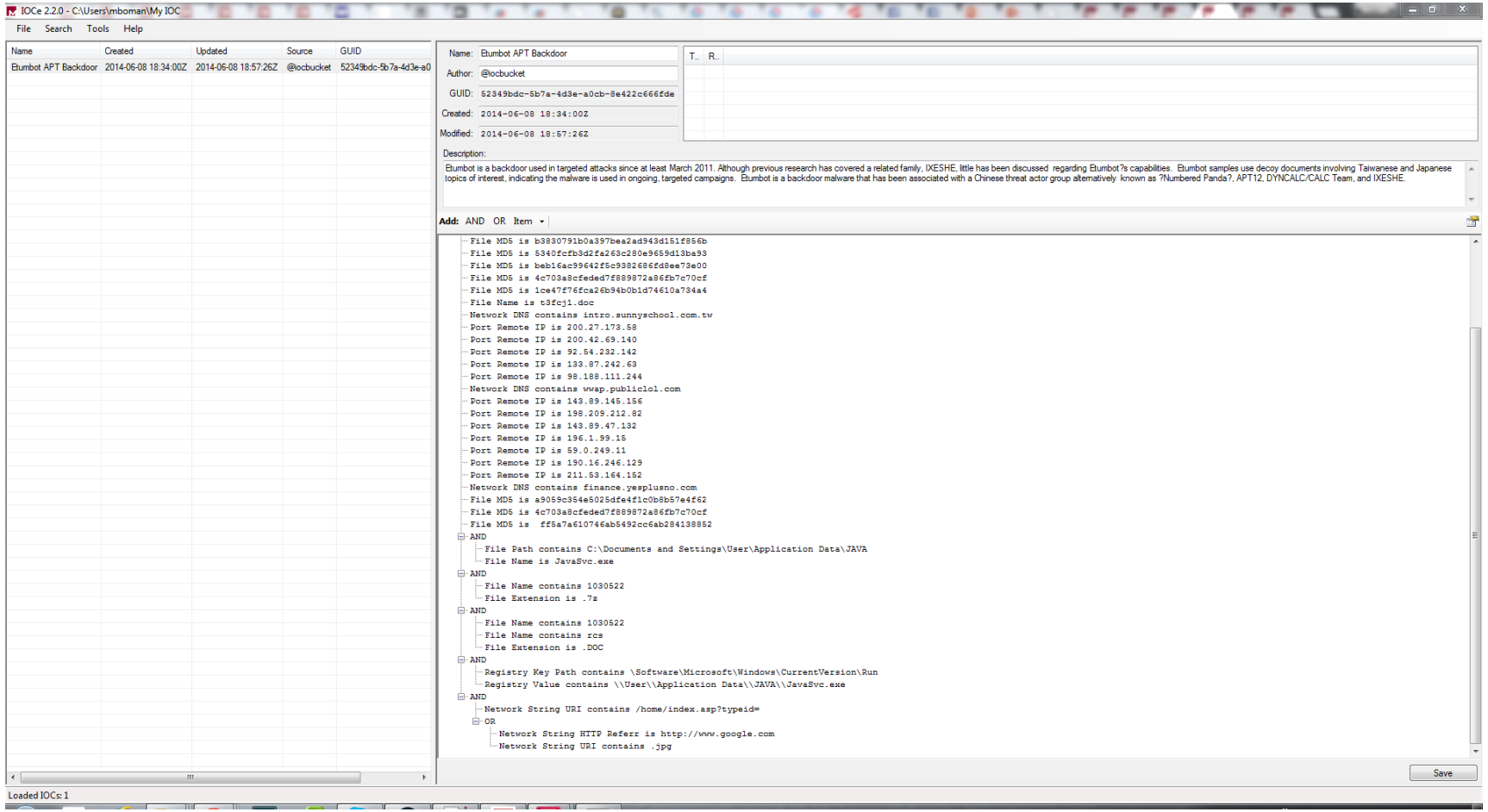
Minibis

- Uses Microsoft ProcMon inside the instrumented environment
- Uses TCPDump to capture network trafic
- ProcDOT can be used to analyze / visualize the execution process

Identify IOCs

- Identifiable patterns in the sample
- Created files
- Created / Modified registry keys
- Network traffic
- Memory patterns

Mandiant IOC Editor



Yara

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        thread_level = 3
        in_the_wild = true
    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"
    condition:
        $a and $b and $c
}
```

Snort

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 443 ( \
    content: "|6A 40 68 00 30 00 00 6A 14 8D 91|"; \
    content: "|8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9|"; \
    content: " UVODFRYSIHLNWPEJXQZAKCBGMT"; \
    msg: " silent_banker : banker C2 Traffic"; \
)
```

Finds unknown C2 servers

Mandiant IOC Finder

Collecting:

mandiant_ioc_finder collect [-o output_dir] [[-d drive]...] [-q] [-v] [-h]

Reporting:

mandiant_ioc_finder report [[-i input_iocs]...] [-s source_data] [-t html | doc]

[-o output_folder (html) or file (doc)] [-q] [-v] [-h] [-w verbose | summary | off]

Searching Network Traffic

- Firewall
  - Detection, Block specific communication
- IDS / IPS
  - Create signatures to Detect and Prevent C2 communication, additional infections
- Proxy
  - Detection, Block specific communication
- DNS
  - Detection, Block communication to sites

Conclusion

Contact information

- Website: blog.malwareresearch.institute
- Twitter: @mboman
- Email: michael@michaelboman.org

Tools mentioned

Snort, DaemonLogger, PassiveDNS, SANCP, Wireshark, Network Miner, Xplico, Dshell, PsExec, MDD, Volatility, Cuckoo Sandbox, Minibis, ProcDot, Mandiant OpenIOC Editor, Yara, Mandiant IOC Finder, Mandiant Redline