Evaluating the APT Armor

Benedikt Tröster
btroester@ernw.de
ERNW GmbH

- IT-Security Service Provider
- Vendor-independent
- Based in Heidelberg
- Founded in 2001
- 40 Employees

- Troopers (www.troopers.de)
  - We invite you to come to Heidelberg ;)

23.04.2015 | Old Attacks meet Modern Technologies
Agenda

- What is APT
- Defining attack primitives
- Evaluate attack primitives
- Bypassing
Shout Outs

- **Research:**
  - Matthias Luft, Felix Wilhelm

- **Special Thanks:**
  - Hendrik Schmidt
  - Oliver Matula
  - Dirk Zurawski
  - Dominik Phillips
  - Bernd Euler
5-Minute Workout: Triple Your Workout Results

14-DAY AMAZING ABS challenge
Real-Time protections – The IPS Software Blade is constantly updated with new defenses against emerging threats. Many of the IPS protections are pre-emptive, providing defenses before vulnerabilities are discovered or exploits are even created.
Complete protection — Today, antivirus alone isn’t enough to defend against sophisticated, stealthy malware and attacks. The highest scoring vendor in an NSS Labs comparative test of current defenses against evasion attacks, McAfee finds, fixes, and freezes malware fast with multiple layers of protection. And strong encryption secures your vital confidential data and prevents unauthorized access to PCs, Macs, laptops, and removable media — transparently and without slowing system performance. Behavior and reputation systems integrate with the cloud-based McAfee Global Threat Intelligence to protect against emerging cyberthreats across all vectors — file, web, message, and network.
Products

FireEye cyber security products combat today's advanced persistent threats (APTs). As an integral piece of an Adaptive Defense strategy, our state-of-the-art network security offerings protect against cyber attacks that bypass traditional signature-based tools such as antivirus software, next-generation firewalls, and sandbox tools. View the FireEye Corporate Brochure to learn more about our offerings.
APT Protection*?

* or Advanced/Next-Generation malware detection/protection – or one of the other terms. We will define it later.
APT?
APT

Bejtlich, 2010
What APT is (and what it isn’t)

- **Advanced** means the adversary can operate in the full spectrum of computer intrusion.
- **Persistent** means the adversary is formally tasked to accomplish a mission. They are not opportunistic intruders.
- **Threat** means the adversary is not a piece of mindless code.

In another source: US Air Force invented the term "advanced persistent threat" around 2006, not Mandiant.
In other words, human attackers with some skills and not automated malware.

First observation:
- It is an interesting assumption to prevent a threat which is \textit{not} caused by automated software with automated software.
Evaluation

1) Model APT scenarios
2) Derive attack patterns
   1) ...and then, attack primitives
3) Evaluate detection rate
Define APT Scenarios

- What we see
- What is described in incident reports
- What is shared by other researchers
What we see

1) Compromise Webapp
2) Dump Credentials
3) Spread
Incident Reports

- Analysis of 20 breaches
  - More than 10 mio breached data records
  - Within the last three years
  - Only two technical incident reports available

- 39 incidents in February 2015
  - 1 technical analysis available

- Further prominent cases of the last three years
  - LinkedIn, AOL, Snapchat, Hetzner, Operation Arid Viper, Desert Falcons
  - 3 technical analyses available
Incident Reports

What can be deducted

- JP Morgan, ms-hydraulic.com, most likely Zappos, and many smaller incidents compromise
  - Attack scheme described above

- Operation Arid Viper, Desert Falcon, Ebay, some governments:
  - Spear phishing
Research shared by others

- Ange Albertini, 44con, typical attack vectors:
  - (Spear) phishing, link to/attached pdf/office/exe
- Mandiant APT1
  - Spear phishing
What we see

1) Spear phishing
2) Dump Credentials
3) Spread
Attack Phases

- Infect
  - User-based or
  - Server-based

- Persist

- Loot

- Exfiltrate

- Spread (repeat)
Detection?
Detection?
Scope

- Experiences with FireEye and zScaler
- Available in many customer environments
- Typical deployment: Web and Mail Analysis/Filtering
  - Can only/mainly detect User-based attacks!
Infect

- **User-/File-based**
  - Java, MS Office, PDF, Flash, Browser, plain exe in email, ...
  - Wireshark, Photoshop, IDA?

- **Server-based**
  - SQLi, remote memory compromise, account compromise...
Persist

- Drop binary/executable
  - Obfuscation/Packing
  - VM/Debugger detection?
- Create user
- Open network port
- Persist to autorun (and other places)
- Hiding (= Hooking, obscure paths)
- Stalling
Loot

- Dump credentials
  - Windows
  - Mail
  - Browser
  - IM
  - Banking
  - ...

- Network sniffing/Traffic redirection
- Find company valuable information
Exfiltrate

- HTTP/S (potentially via proxy)
- IRC
- DNS
- SMTP
- TOR
- MSN/Jabber
- ...

Spread

- Often called *lateral movement*
- Compromising more hosts within the network
  - Using same infection technique or compromised accounts

- *Not covered in this presentation.*
Detection Methods

- In our case, solutions deployed as proxies/inspecting web traffic
  - Regular zScaler services incl. behavior-based analysis
  - FireEye NX 900
Deployment

Internet

Corporate Network

TAP

FireEye

Proxy

Internal Network
Detection Methods

- No specific details about detection available

- Typical approaches:
  - In-OS
    - API hooking
    - Register Filter Driver
  - Emulation
  - VM Introspection
    - VMX Trapping
    - EPT-/SLAT-based
Detection Methods

- Analysis approaches are used to create execution trace
  - Containing e.g. system calls, registry access, network activity.

- Heuristics to analyze execution trace and detect malicious behavior
  - Automating the traditional dynamic analysis mode...
  - API monitors, wireshark, regmon/procmon...
Evaluation Scope

- **Characteristics of the heuristics:**
  - Create a number of attack primitives, see what results in malicious classification
  - Understand how the solutions are working

- **NOT:**
  - Quality of detection methods
    - Emulation vs. hooking...
  - Mass testing of samples
  - Performance evaluation
## Samples – Data Infection

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2012-0754.pdf</td>
<td>PDF used in actual attack. Heap Spraying, ROP Chains, Dropper.</td>
</tr>
<tr>
<td>CVE-2014-2299.pcap</td>
<td>Wireshark wiretap/mpeg.c Stack Buffer Overflow, bind_shell</td>
</tr>
<tr>
<td>ms14_017.rtf</td>
<td>MSF MS14-017 RTF exploit, bind shell</td>
</tr>
<tr>
<td>2014-0515.swf</td>
<td>Metasploit module, reverse_shell</td>
</tr>
<tr>
<td>2013-3346.pdf</td>
<td>Metasploit module, bind_shell</td>
</tr>
<tr>
<td>CVE-2012-2052.dae</td>
<td>Photoshop File-based overflow, calc.exe</td>
</tr>
</tbody>
</table>
## Samples - Persistence

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateUser.exe/CreateUser 64.exe</td>
<td>Custom application creating a local user account.</td>
</tr>
<tr>
<td>msvc.exe</td>
<td>Meterpreter as windows service</td>
</tr>
<tr>
<td>mp_default.exe</td>
<td>Meterpreter bind shell TCP 4444</td>
</tr>
<tr>
<td>mpdflt.msi</td>
<td>Meterpreter bind shell TCP 4444, msi format</td>
</tr>
<tr>
<td>mp_reverse_http.exe</td>
<td>A flying unicorn</td>
</tr>
</tbody>
</table>
## Samples - Loot

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mimi32/mimi64.exe</td>
<td>Mimikatz clone.</td>
</tr>
<tr>
<td>autorun.exe</td>
<td>Writing a binary to autorun.</td>
</tr>
<tr>
<td>down-to-ar.exe</td>
<td>Downloading a python script and writing it to autorun.</td>
</tr>
<tr>
<td>sam_post.exe</td>
<td>Reading the backup SAM and HTTP POSTing it to a server.</td>
</tr>
<tr>
<td>keylog_post.ps1</td>
<td>Powershell keylogger HTTP POSTing the keys to a server.</td>
</tr>
<tr>
<td>Meterpreter reverse http</td>
<td>Meterpreter C2 traffic</td>
</tr>
<tr>
<td>traffic</td>
<td></td>
</tr>
<tr>
<td>shell.exe</td>
<td>Custom reverse shell.</td>
</tr>
</tbody>
</table>
fireeye.ernw.net # show workorders
Number of workorders pending = 0
Number of workorders running = 0
Number of workorders terminating = 0
Total number of traces submitted = 67
Total number of traces canceled due to no profile = 4
Total number of traces canceled due to other reasons = 0
Total number of workorders queued = 65
Total number of workorders scheduled = 65
Total number of workorders with anomaly = 16
Total number of workorders preempted = 0
Total number of workorders dropped = 0
Total number of workorders stopped = 0
Total number of workorders done by avc = 22
Total number of workorders done due to unknown reason = 0
Total number of workorders processed = 65
Max number of workorders pending at any time = 2
Number of Network Anomalies detected = 4
Number of OS Anomalies detected = 16
fireeye.ernw.net #
## Blackbox Assessment

<table>
<thead>
<tr>
<th>URL</th>
<th>Policy Action</th>
<th>URL Category</th>
<th>Page RL</th>
<th>Threat Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>54.145.222.132/</td>
<td>Allowed</td>
<td>Miscellaneous</td>
<td>--</td>
<td>None</td>
</tr>
<tr>
<td>54.145.222.132/favicon.ico</td>
<td>Allowed</td>
<td>Miscellaneous</td>
<td>--</td>
<td>None</td>
</tr>
<tr>
<td>54.145.222.132/favicon.ico</td>
<td>Allowed</td>
<td>Miscellaneous</td>
<td>--</td>
<td>None</td>
</tr>
<tr>
<td>54.145.222.132/corkamix.html</td>
<td>Allowed</td>
<td>Miscellaneous</td>
<td>--</td>
<td>None</td>
</tr>
<tr>
<td>54.145.222.132/</td>
<td>Allowed</td>
<td>Miscellaneous</td>
<td>--</td>
<td>None</td>
</tr>
<tr>
<td>54.145.222.132/</td>
<td>Allowed</td>
<td>Miscellaneous</td>
<td>5</td>
<td>None</td>
</tr>
<tr>
<td>54.145.222.132/icons/blank.gif</td>
<td>Allowed</td>
<td>Miscellaneous</td>
<td>--</td>
<td>None</td>
</tr>
<tr>
<td>54.145.222.132/icons/text.gif</td>
<td>Allowed</td>
<td>Miscellaneous</td>
<td>--</td>
<td>None</td>
</tr>
<tr>
<td>54.145.222.132/corkamix.html</td>
<td>Allowed</td>
<td>Miscellaneous</td>
<td>5</td>
<td>Sent for Analysis</td>
</tr>
</tbody>
</table>
Routine

File

AV

Filetype Check

Behavior-based Analysis

malicious

benign

benign

malicious

www.ernw.de
# Results

<table>
<thead>
<tr>
<th>ID</th>
<th>FireEye</th>
<th>zScaler</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2011-2462.pdf</td>
<td>AV</td>
<td>AV</td>
</tr>
<tr>
<td>CVE-2012-0754.pdf</td>
<td>AV</td>
<td>AV</td>
</tr>
<tr>
<td>CVE-2013-0640.pdf</td>
<td>AV</td>
<td>AV</td>
</tr>
<tr>
<td>CVE-2014-2299.pcap</td>
<td>Not analyzed</td>
<td>Not analyzed</td>
</tr>
<tr>
<td>ms14_017.rtf</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014-0515.swf</td>
<td>-</td>
<td>AV</td>
</tr>
<tr>
<td>2013-3346.pdf</td>
<td>Behavior, “Orange”</td>
<td>Behavior, 70%, suspicious</td>
</tr>
<tr>
<td>CVE-2012-2052.dae</td>
<td>Not analyzed</td>
<td>Not analyzed</td>
</tr>
</tbody>
</table>
## Results

<table>
<thead>
<tr>
<th>ID</th>
<th>FireEye</th>
<th>zScaler</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateUser.exe/CreateUser64.exe</td>
<td>Behavior, benign</td>
<td>Behavior, benign</td>
</tr>
<tr>
<td>msvc.exe</td>
<td>No results</td>
<td>AV</td>
</tr>
<tr>
<td>mp_default.exe</td>
<td>No results</td>
<td>AV</td>
</tr>
<tr>
<td>mpdflt.msi</td>
<td>No results</td>
<td>AV</td>
</tr>
<tr>
<td>mp_reverse_http.exe</td>
<td>No results</td>
<td>AV</td>
</tr>
<tr>
<td>ID</td>
<td>FireEye</td>
<td>zScaler</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>mimi32/mimi64.exe</td>
<td>behavior, suspicious, sleep</td>
<td>behavior, benign</td>
</tr>
<tr>
<td>autorun.exe</td>
<td>behavior, benign</td>
<td>AV, trojan</td>
</tr>
<tr>
<td>down-to-ar.exe</td>
<td>behavior, benign</td>
<td>AV, trojan</td>
</tr>
<tr>
<td>sam_post.exe</td>
<td>behavior, benign</td>
<td>behavior, benign</td>
</tr>
<tr>
<td>keylog_post.ps1</td>
<td>Not analyzed</td>
<td>Not analyzed</td>
</tr>
<tr>
<td>Meterpreter reverse http traffic</td>
<td>Detected</td>
<td>Not detected</td>
</tr>
<tr>
<td>shell.exe</td>
<td>Behavior based, Orange</td>
<td>Behavior based, benign</td>
</tr>
</tbody>
</table>
Some observations...
Some bypassing...

| 2013-3346.pdf | Behavior, “Orange” | Behaviour, 70%, suspicious |

**BEHAVIORAL ANALYSIS REPORT**
URL: 54.145.222.132/msf.pdf  
MD5: 647955a00a1d8268505fec8880540c2d

<table>
<thead>
<tr>
<th>Classification</th>
<th>Virus And Malware</th>
<th>Security Bypass</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspicious</td>
<td>No known Malware</td>
<td>Creates guard pages</td>
</tr>
</tbody>
</table>

**File Properties**

**File Type**
PDF Document
Some bypassing...

2013-3346.pdf  Behavior, “Orange”  Behaviour, 70%, suspicious

C:\Users\uchimata\Desktop>small.exe
go on...
C:\Users\uchimata\Desktop>

[uchimata@dojo ~/Desktop]$ cat small.exe msf.pdf > poly.pdf

File Properties

File Type
Windows Executable

thx @angealbertini
Some bypassing...

2013-3346.pdf | Behavior, “Orange” | Behaviour, 70%, suspicious

```
C:\Users\uchimata\Desktop>small.exe
go on...
C:\Users\uchimata\Desktop>

[uchimata@dojo ~/Desktop]$ cat small.exe msf.pdf > poly.pdf
```

Same result on FireEye!

thx @angealbertini
Conclusions

- Simple tricks can be used to get around these solutions
- Little context (add-user-bin from inet?)
- Good to complement traditional AV, but no silver bullet!
  - what a surprise ;)

4/23/2015
There’s never enough time...

THANK YOU...

...for yours!

@_fel1x
@uchi_mata

fwilhelm@ernw.de
mluft@ernw.de

Slides & further information: https://www.insinuator.net (..soon)
Disclaimer

All products, company names, brand names, trademarks and logos are the property of their respective owners!
Credits

Smiley by http://www.freepik.com
CC BY 3.0