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 ;)

ERNW
providing security.

Agenda

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

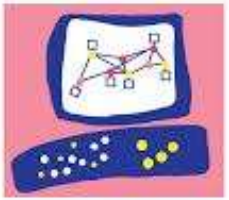
ERNW
providing security.

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


MMA 2
ACCELERATION
12 WEEK PROGRAM
BEFORE
AFTER



Check Point®
SOFTWARE TECHNOLOGIES LTD.

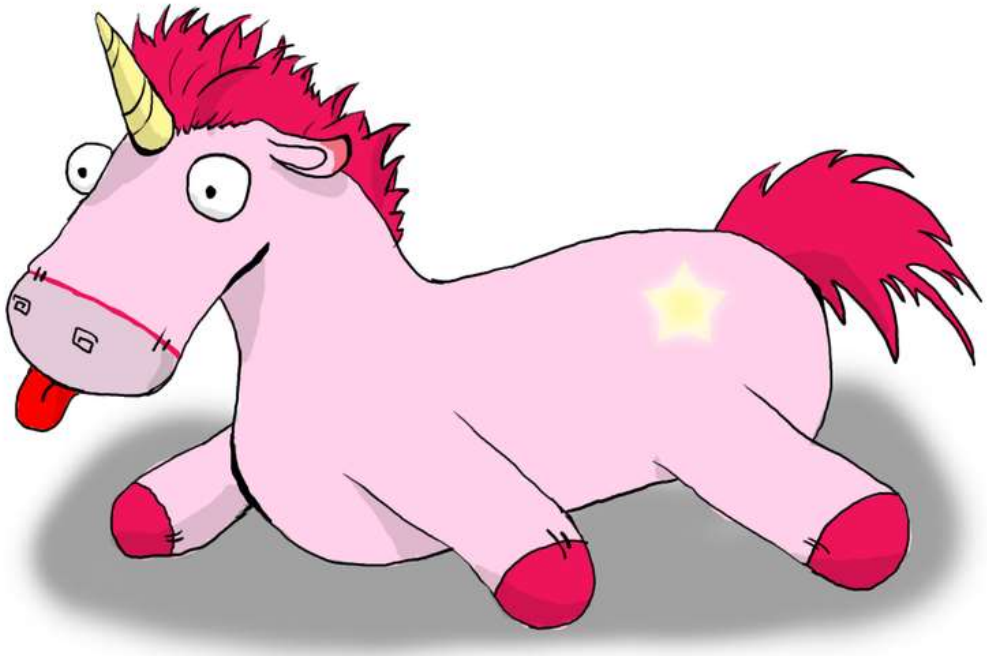
- **Real-Time protections** – The IPS Software Blade is constantly updated with new defenses against emerging threats. Many of the IPS protections are pre-emptive, providing defenses before vulnerabilities are discovered or exploits are even created.

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?

© Suckerpunch

APT

- Bejtlich, 2010
  What APT is (and what it isn't)
  - *A*dvanced means the adversary can operate in the full spectrum of computer intrusion.
  - *P*ersistent means the adversary is formally tasked to accomplish a mission. They are not opportunistic intruders.
  - *T*hreat 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.

APT

- 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 *not* caused by automated software with automated software.

ERNW
providing security.

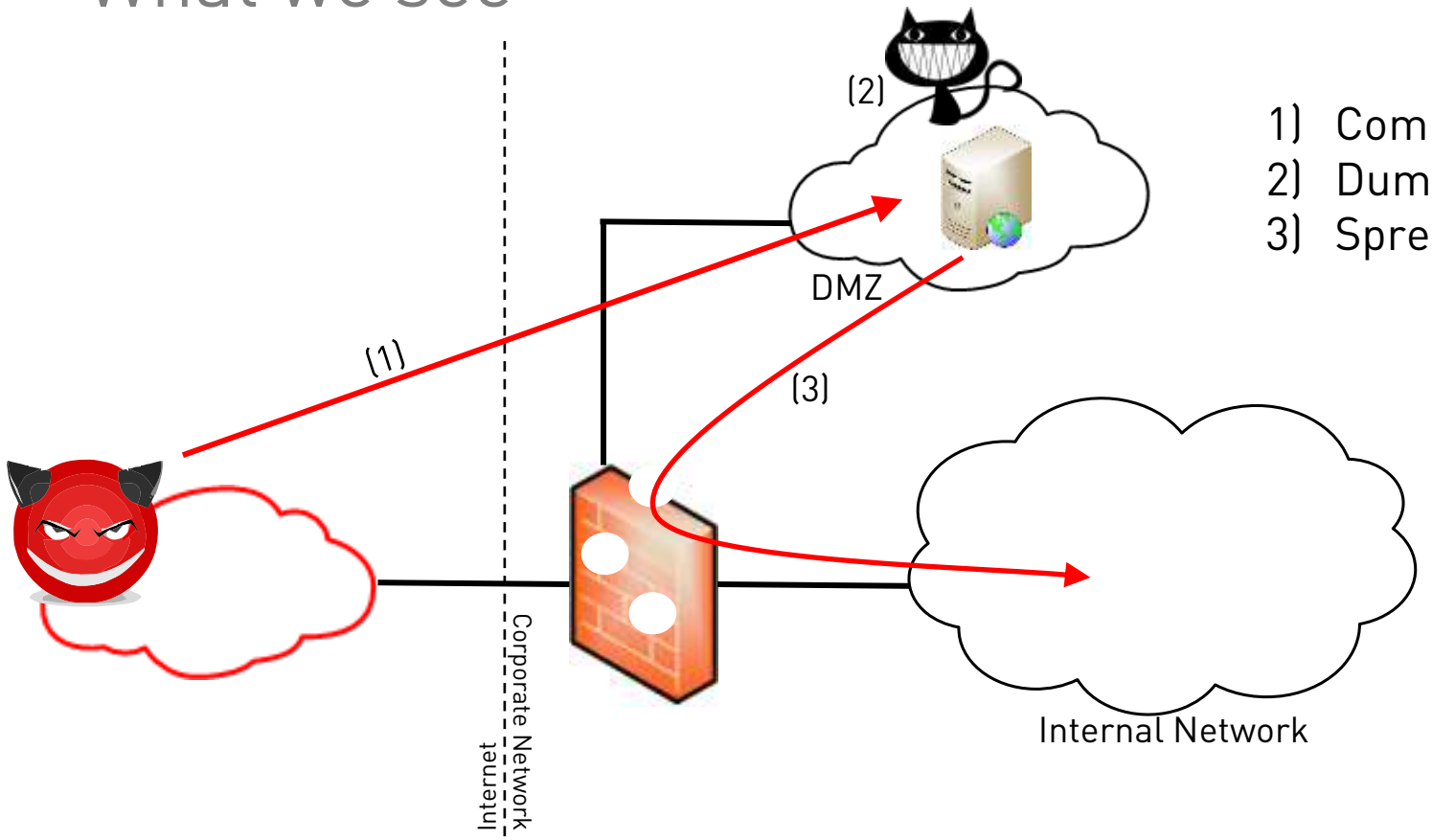
Evaluation

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 10mio 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

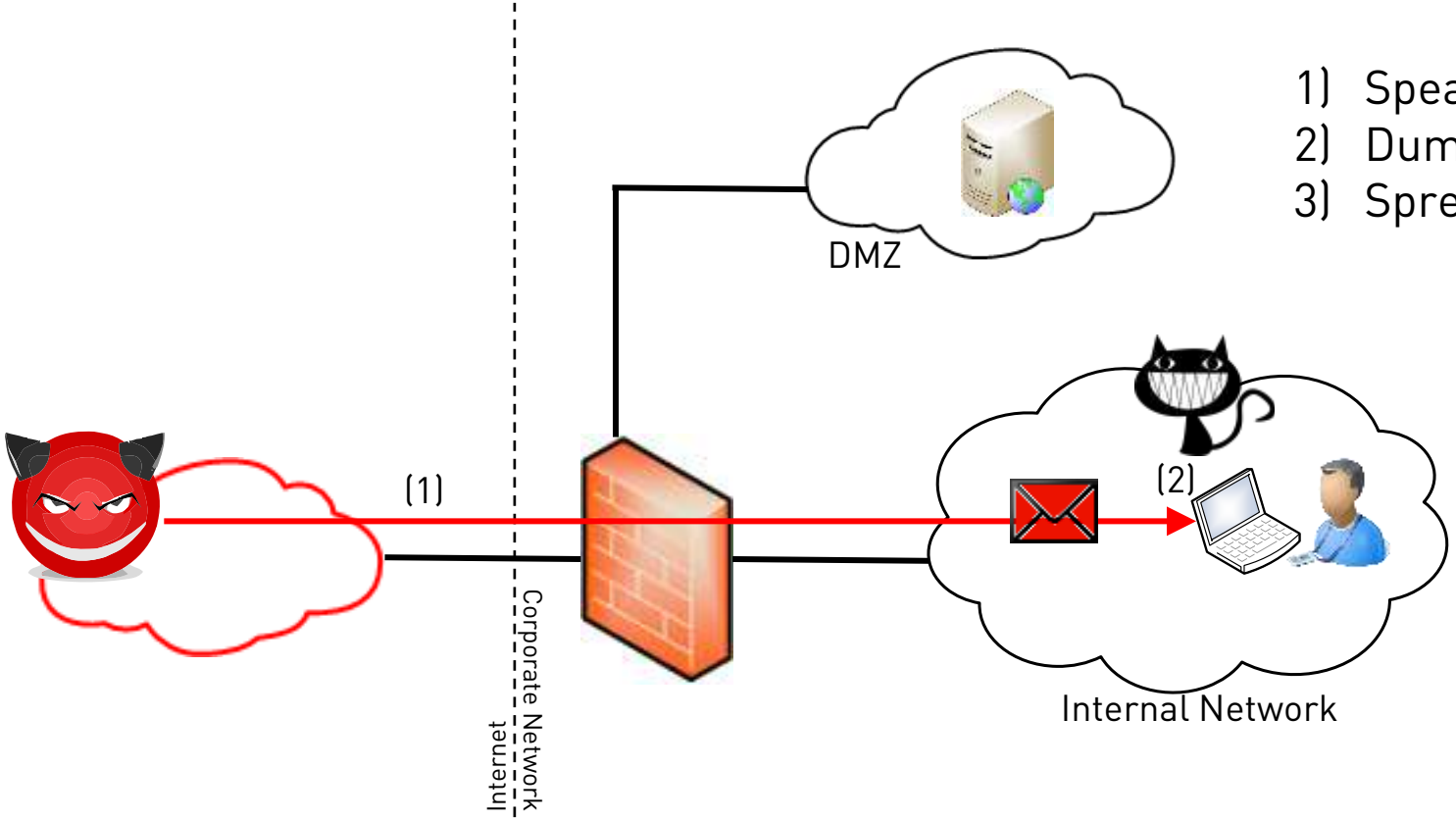
What can be deducted

- 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?


FireEye


ThreatGRID
Malware Threat Intelligence Platform


zscaler®


McAfee®


websense®
TRITON™


lastline

Detection?


FireEye


ThreatGRID
Malware Threat Intelligence Platform


zscaler®


McAfee®


websense®
TRITON™


lastline

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!

ERNW
providing security.

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

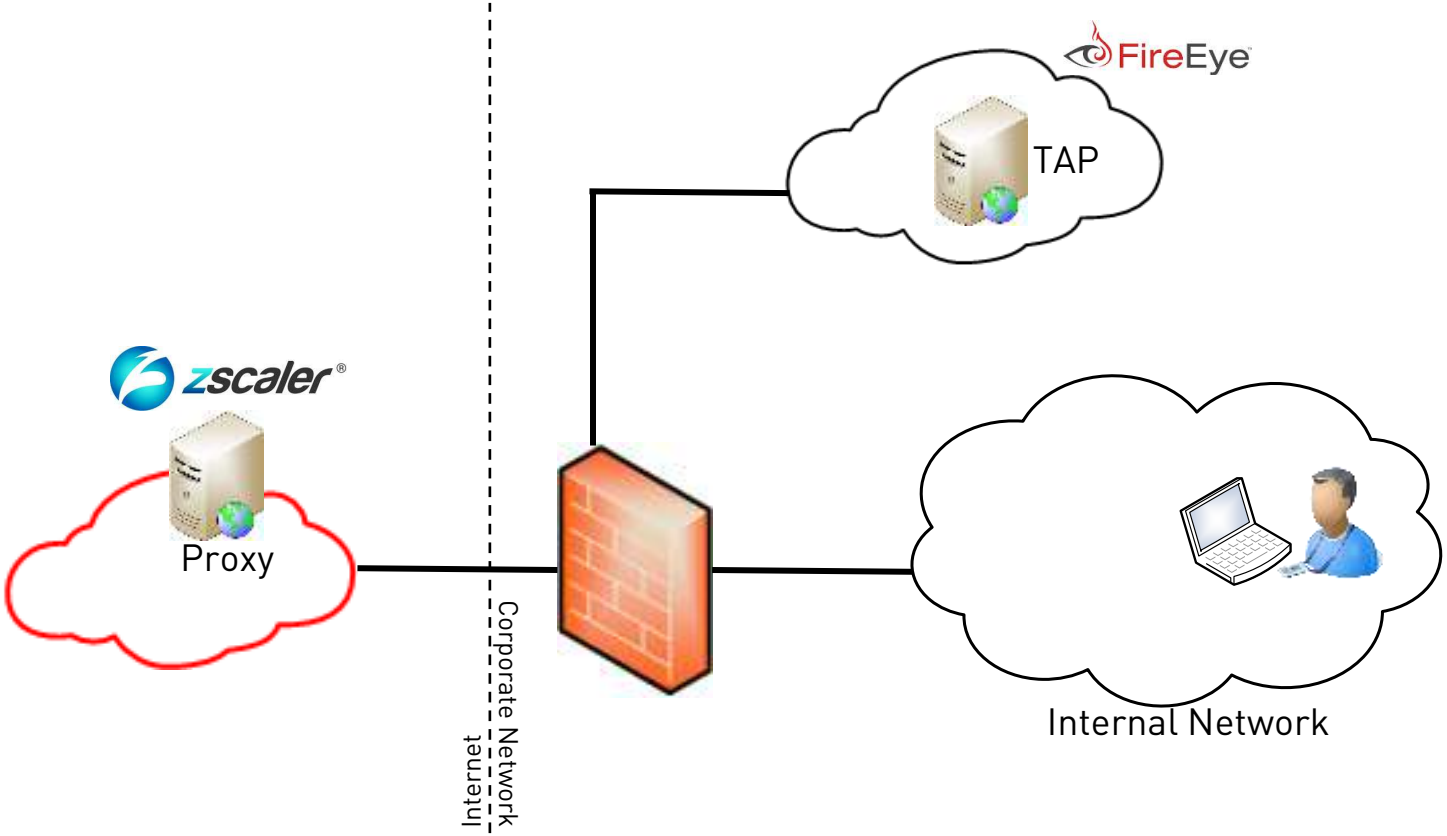
- Often called *lateral movement*
- Compromising more hosts within the network
  - Using same infection technique or compromised accounts
- *Not covered in this presentation.*

Detection Methods

```
fireeye.ernw.net # show version
Product name:       Web MPS [licensed]
Product model:      FireEyeNX900
Bandwidth:          10 Mb
Product release:    wMPS (wMPS) 7.2.1.240505
Build ID:           #240505
Build date:         2014-07-23 18:36:26
```

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

Deployment


FireEye
TAP
zscaler
Proxy
Internet
Corporate Network
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

ERNW
providing security.

ID	Description
CVE-2011-2462.pdf	PDF used in actual attack. Heap Spraying, ROP Chains, Dropper.
CVE-2012-0754.pdf	PDF used in actual attack. Heap Spraying, ROP Chains, Dropper.
CVE-2013-0640.pdf	PDF used in actual attack. Heap Spraying, ROP Chains, Dropper.
CVE-2014-2299.pcap	Wireshark wiretap/mpeg.c Stack Buffer Overflow, bind_shell
ms14_017.rtf	MSF MS14-017 RTF exploit, bind shell
2014-0515.swf	Metasploit module, reverse_shell
2013-3346.pdf	Metasploit module, bind_shell
CVE-2012-2052.dae	Photoshop File-based overflow, calc.exe

Samples - Persistence

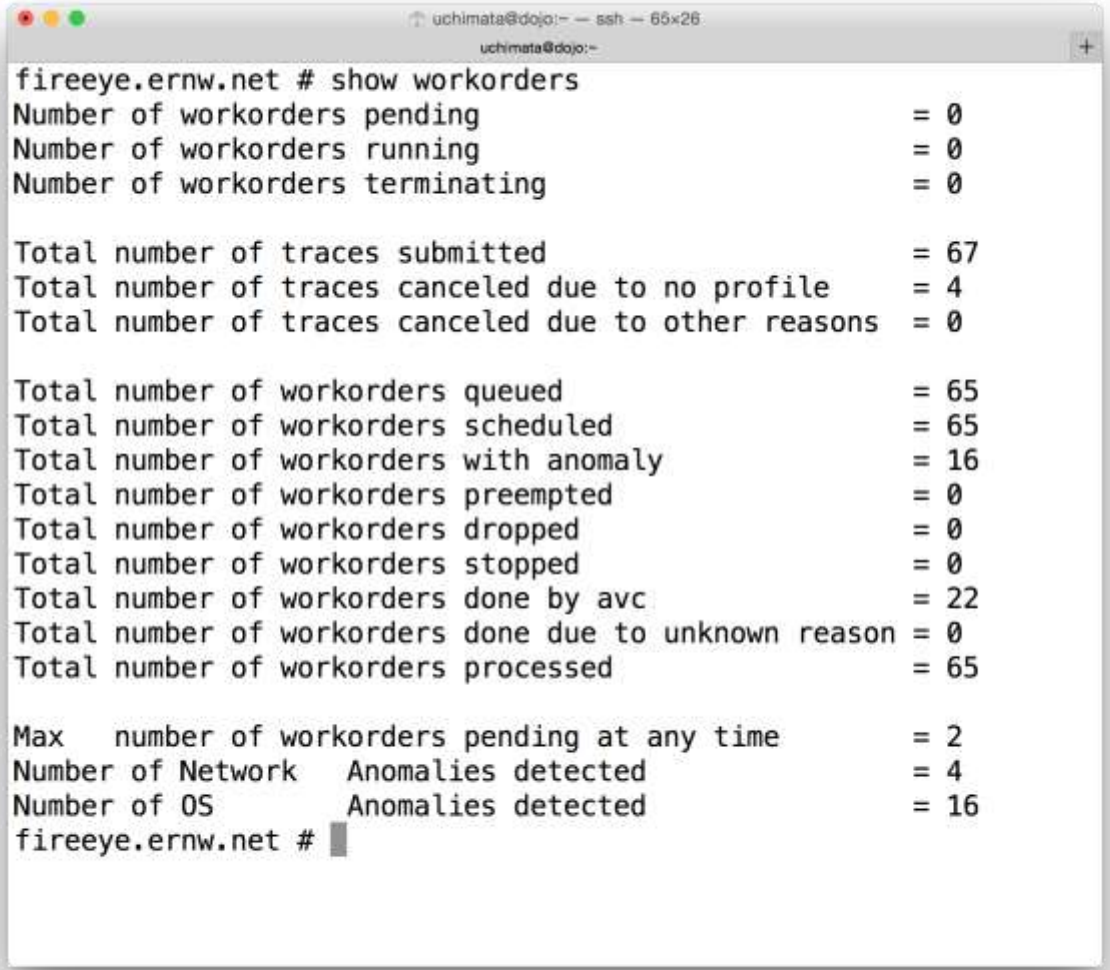
ERNW
providing security.

ID	Description
CreateUser.exe/CreateUser 64.exe	Custom application creating a local user account.
msvc.exe	Meterpreter as windows service
mp_default.exe	Meterpreter bind shell TCP 4444
mpdflt.msi	Meterpreter bind shell TCP 4444, msi format
mp_reverse_http.exe	A flying unicorn

Samples - Loot

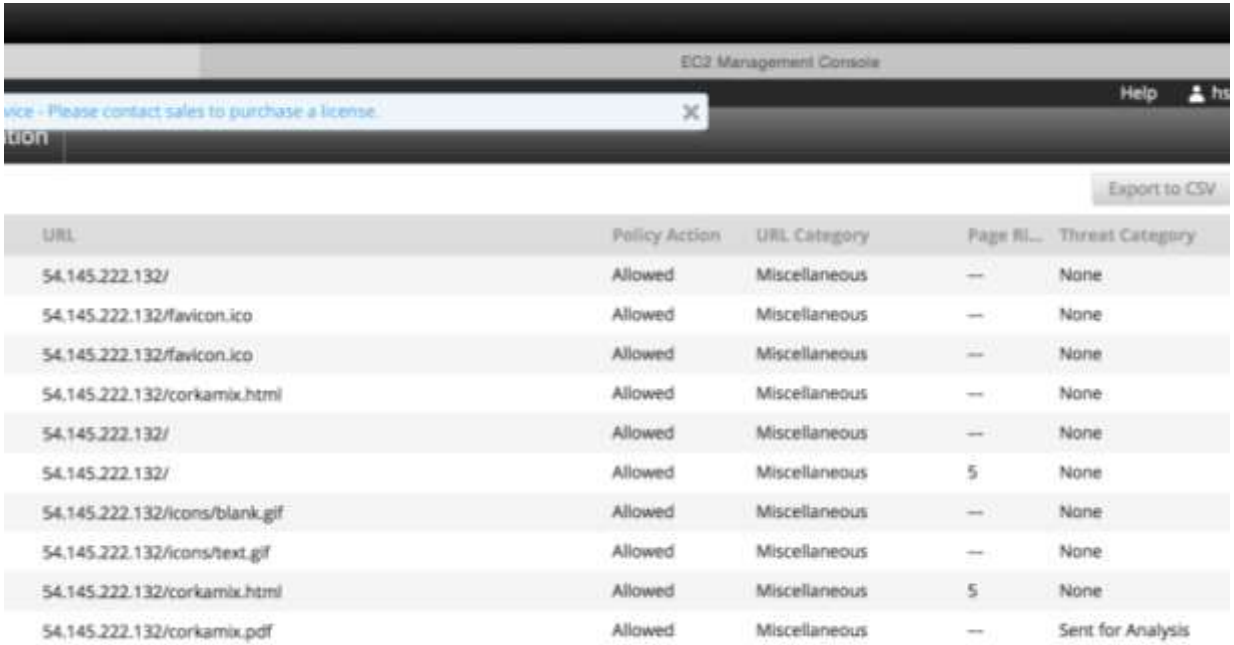
ERNW
providing security.

ID	Description
mimi32/mimi64.exe	Mimikatz clone.
autorun.exe	Writing a binary to autorun.
down-to-ar.exe	Downloading a python script and writing it to autorun.
sam_post.exe	Reading the backup SAM and HTTP POSTing it to a server.
keylog_post.ps1	Powershell keylogger HTTP POSTing the keys to a server.
Meterpreter reverse http traffic	Meterpreter C2 traffic
shell.exe	Custom reverse shell.



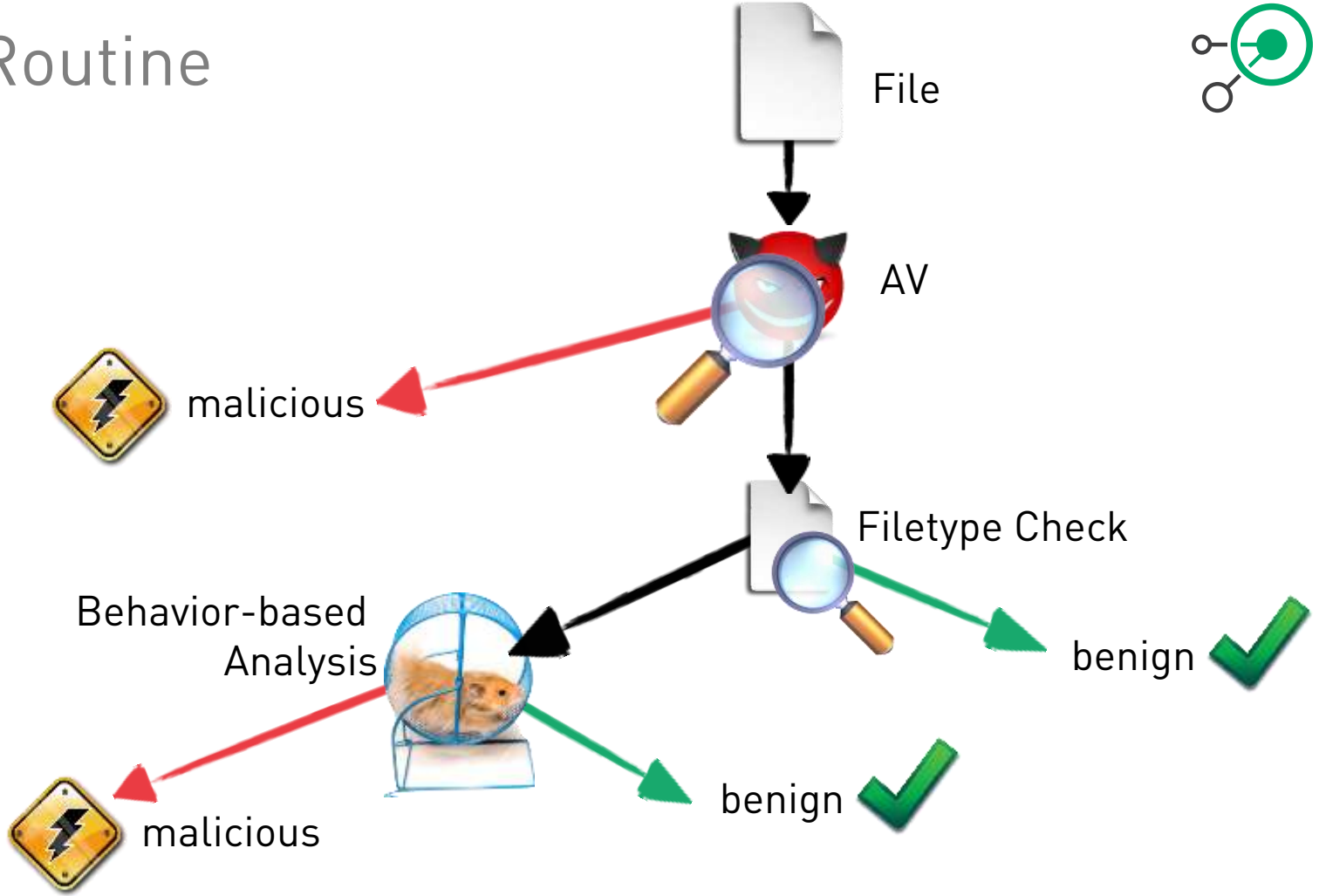
ERNW
providing security.

Blackbox Assessment



Blackbox Assessment

Routine


File
AV
malicious
Filetype Check
benign
Behavior-based
Analysis
benign
malicious

Results

ERNW
providing security.

ID	FireEye	zScaler
CVE-2011-2462.pdf	AV	AV
CVE-2012-0754.pdf	AV	AV
CVE-2013-0640.pdf	AV	AV
CVE-2014-2299.pcap	Not analyzed	Not analyzed
ms14_017.rtf		
2014-0515.swf	-	AV
2013-3346.pdf	Behavior, “Orange”	Behavior, 70%, suspicious
CVE-2012-2052.dae	Not analyzed	Not analyzed

Results

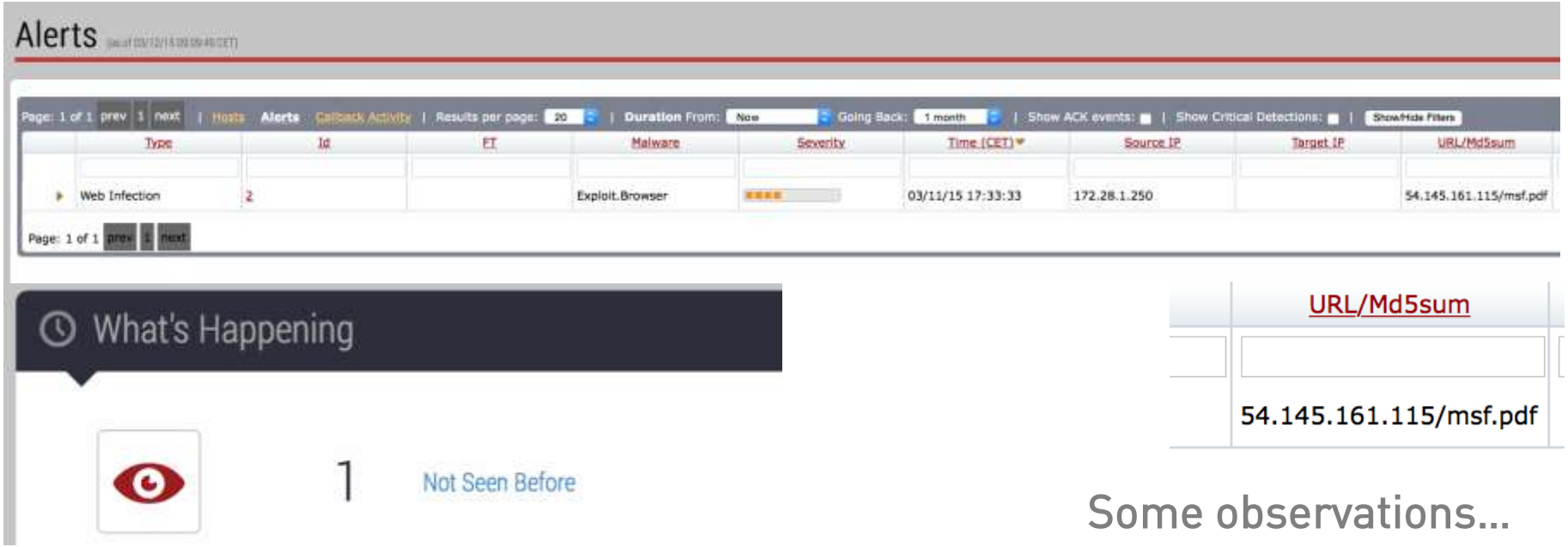
ERNW
providing security.

ID	FireEye	zScaler
CreateUser.exe/CreateUser64.exe	Behavior, benign	Behavior, benign
msvc.exe	No results	AV
mp_default.exe	No results	AV
mpdflt.msi	No results	AV
mp_reverse_http.exe	No results	AV

Results

ERNW
providing security.

ID	FireEye	zScaler
mimi32/mimi64.exe	behavior, suspicious, sleep	behavior, benign
autorun.exe	behavior, benign	AV, trojan
down-to-ar.exe	behavior, benign	AV, trojan
sam_post.exe	behavior, benign	behavior, benign
keylog_post.ps1	Not analyzed	Not analyzed
Meterpreter reverse http traffic	Detected	Not detected
shell.exe	Behavior based, Orange	Behavior based, benign



Some observations...

Some bypassing…

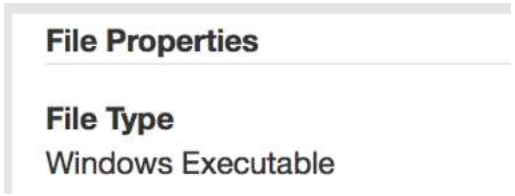
2013-3346.pdf	Behavior, “Orange”	Behaviour, 70%, suspicous

Some bypassing…

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

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

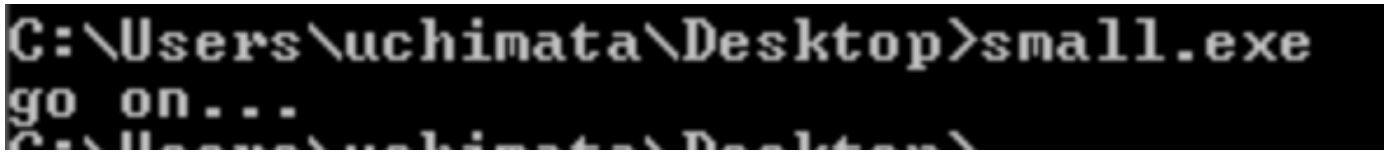
```
[uchimata@dojo ~/Desktop]$ cat small.exe msf.pdf > poly.pdf
```



thx @angealbertini

Some bypassing…

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




```
[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 ;)

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)

ERNW
providing security.

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