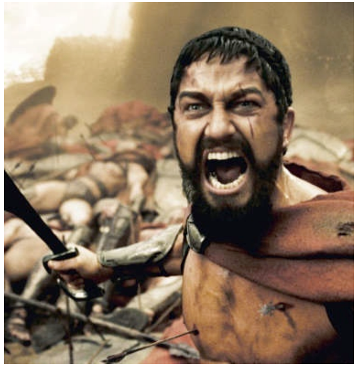
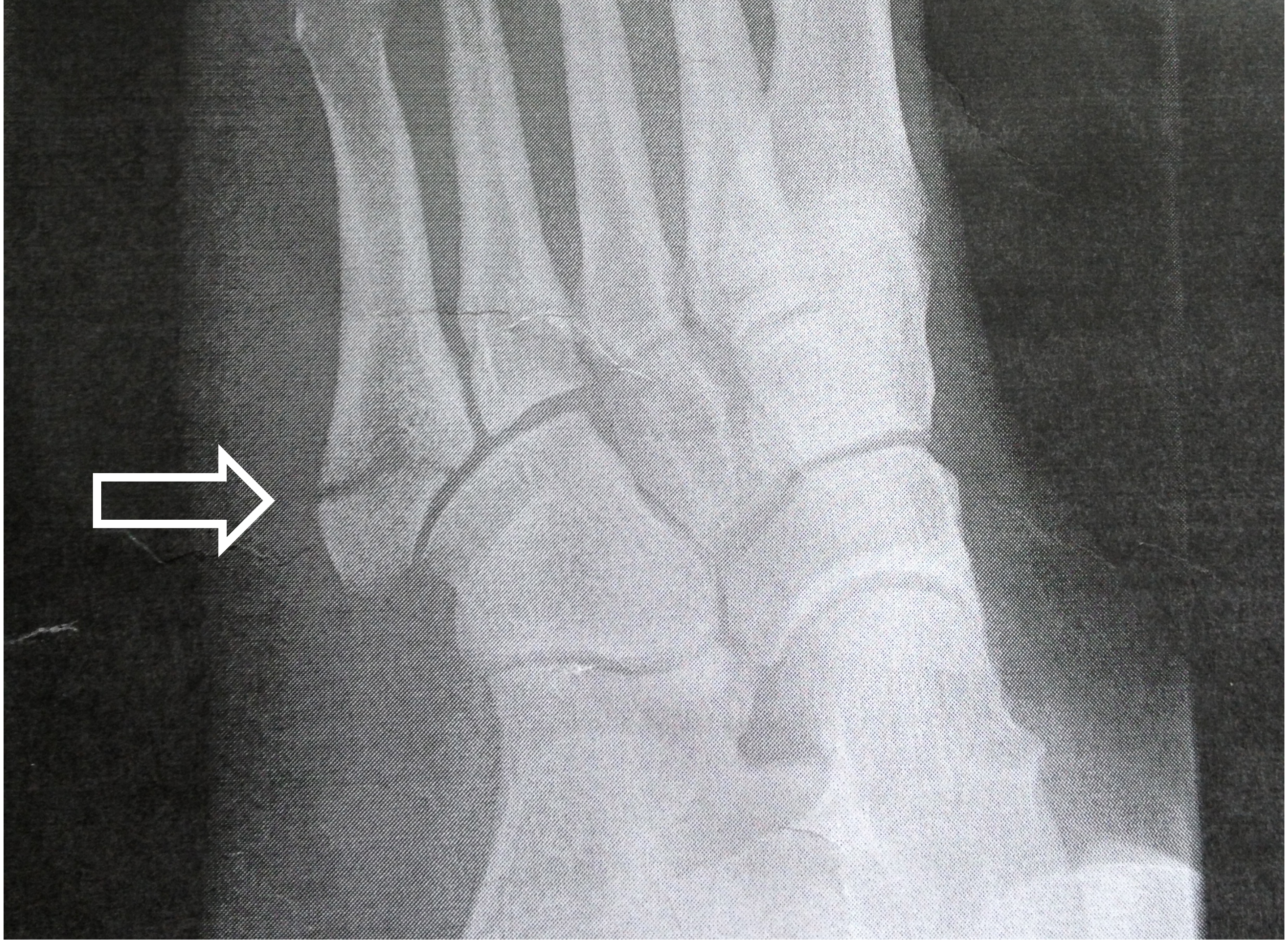
Evaluating the APT Armor

Matthias Luft & Felix Wilhelm
{fwilhelm, mluft}@ernw.de

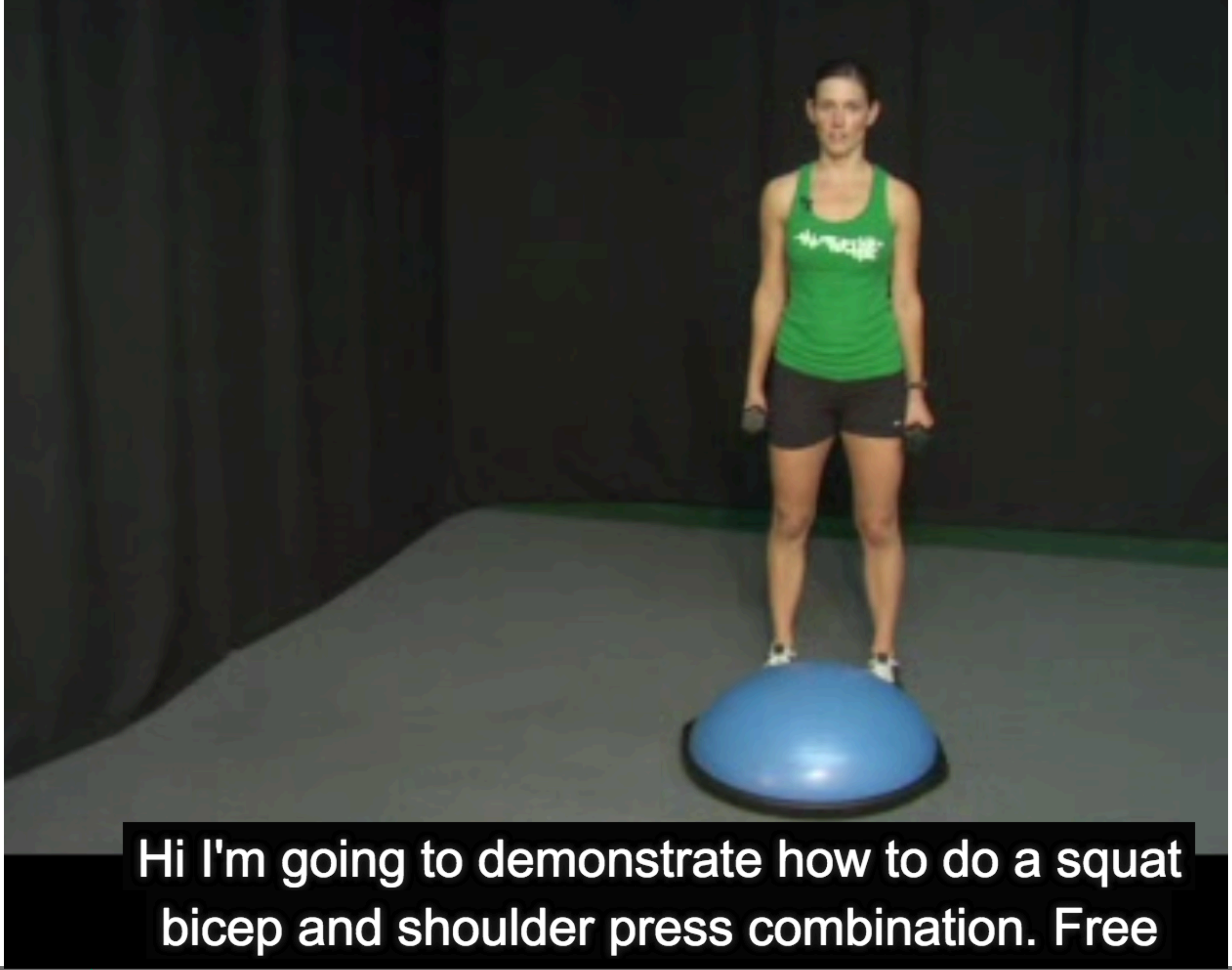
Shout Outs



- Hendrik Schmidt
- Oliver Matula
- Dirk Zurawski
- Dominik Phillips
- Bernd Euler
- Florian Horsch

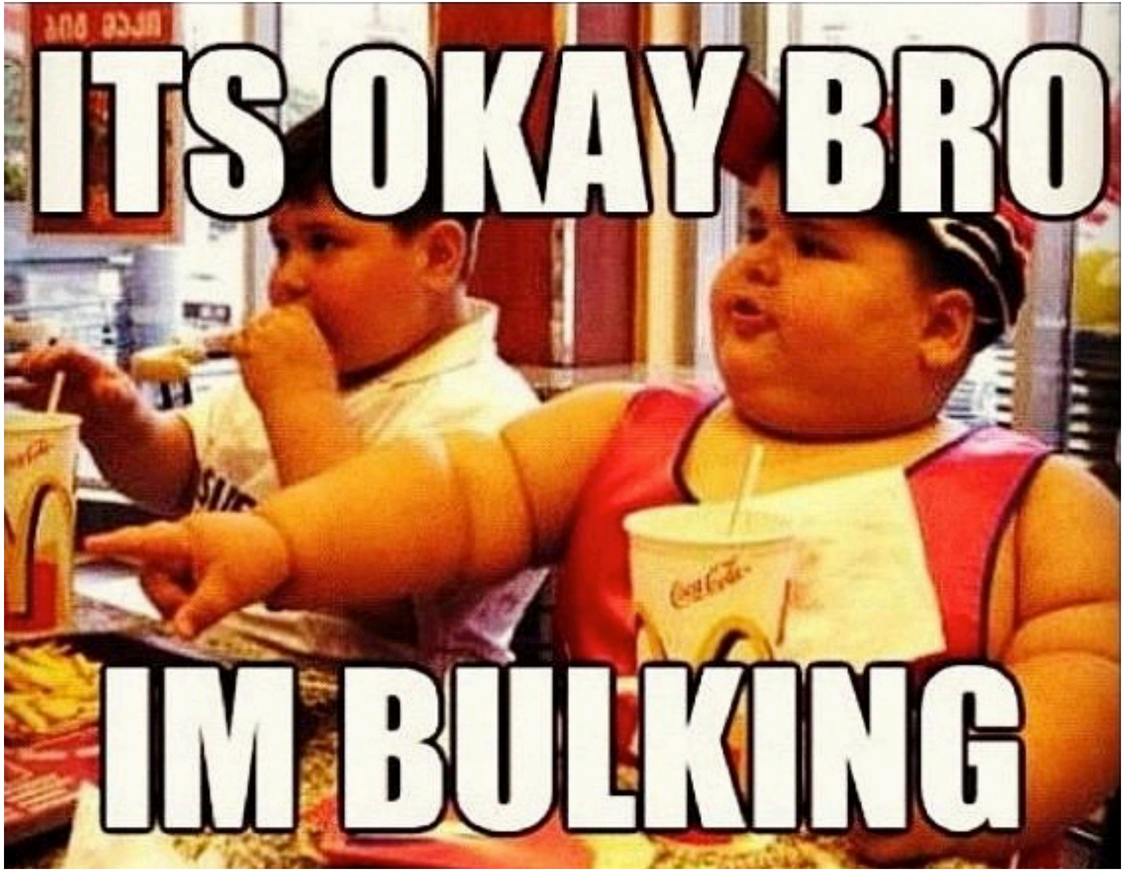


MMA 2
ACCELERATION
12 WEEK PROGRAM
BEFORE
AFTER



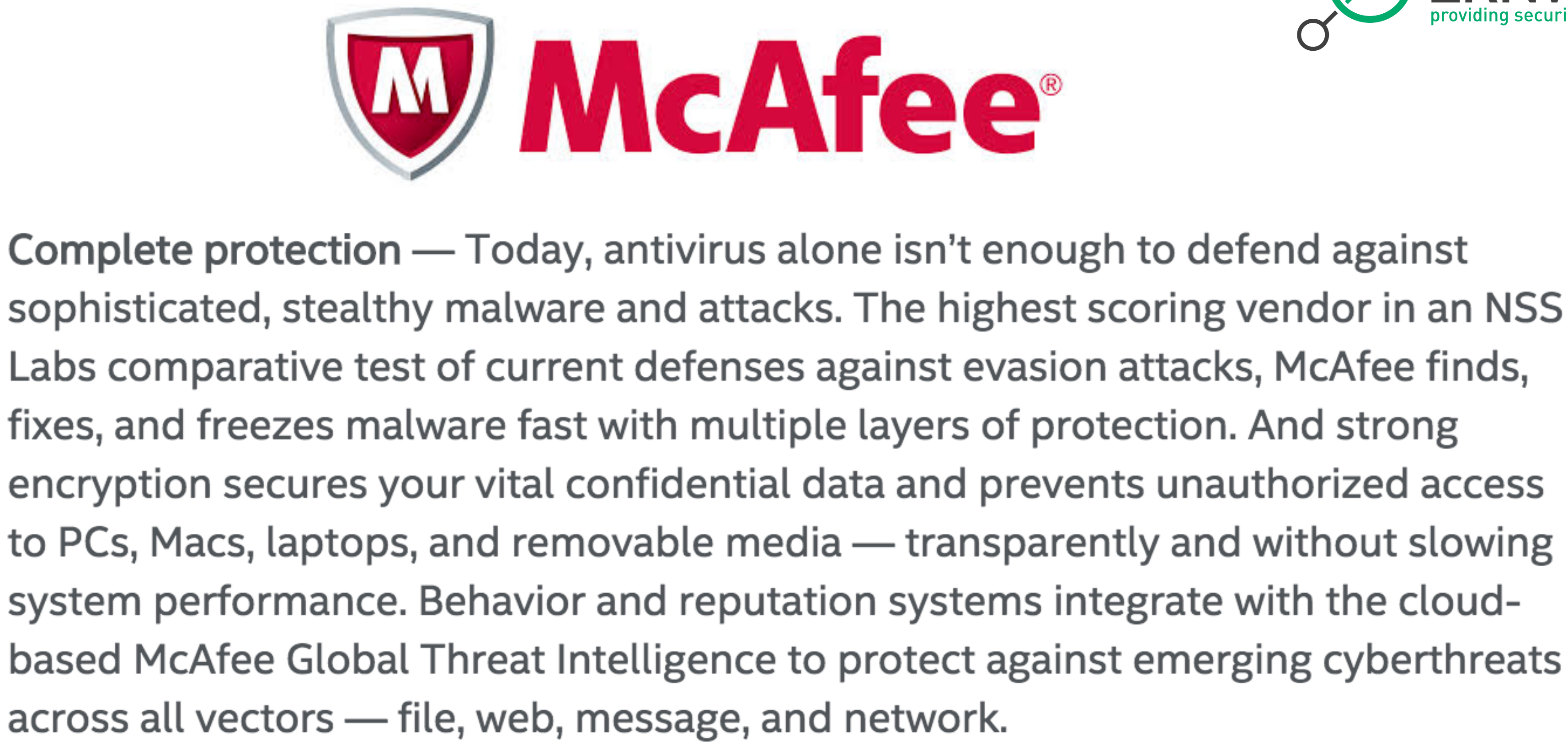
Hi I'm going to demonstrate how to do a squat bicep and shoulder press combination. Free

5-Minute Workout: Triple Your Workout Results


ITS OKAY BRO
IM BULKING

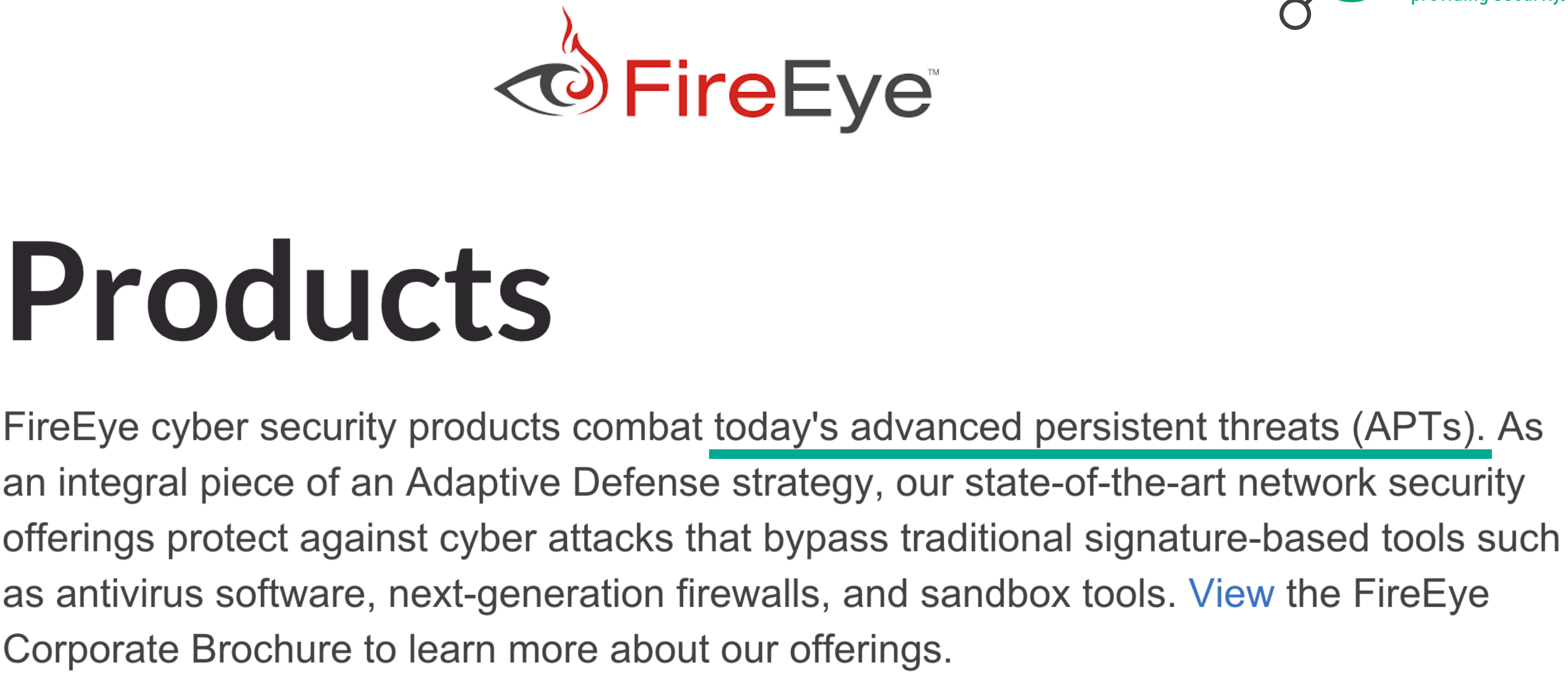
Check Point®
SOFTWARE TECHNOLOGIES LTD.

- **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.



McAfee®

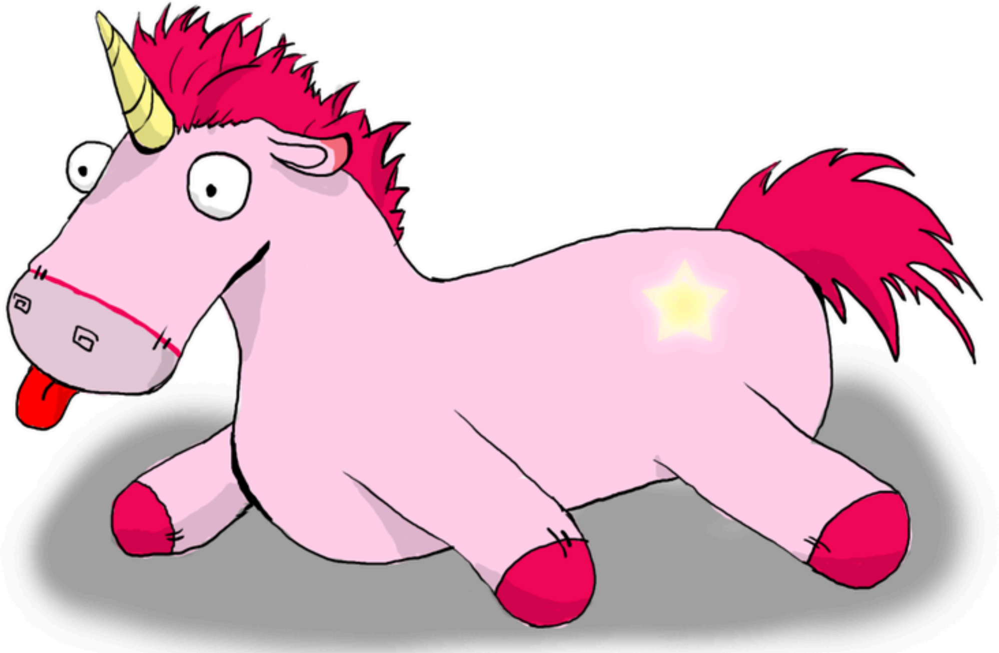
Complete protection — Today, antivirus alone isn't enough to defend against sophisticated, stealthy malware and attacks. The highest scoring vendor in an NSS Labs comparative test of current defenses against evasion attacks, McAfee finds, fixes, and freezes malware fast with multiple layers of protection. 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

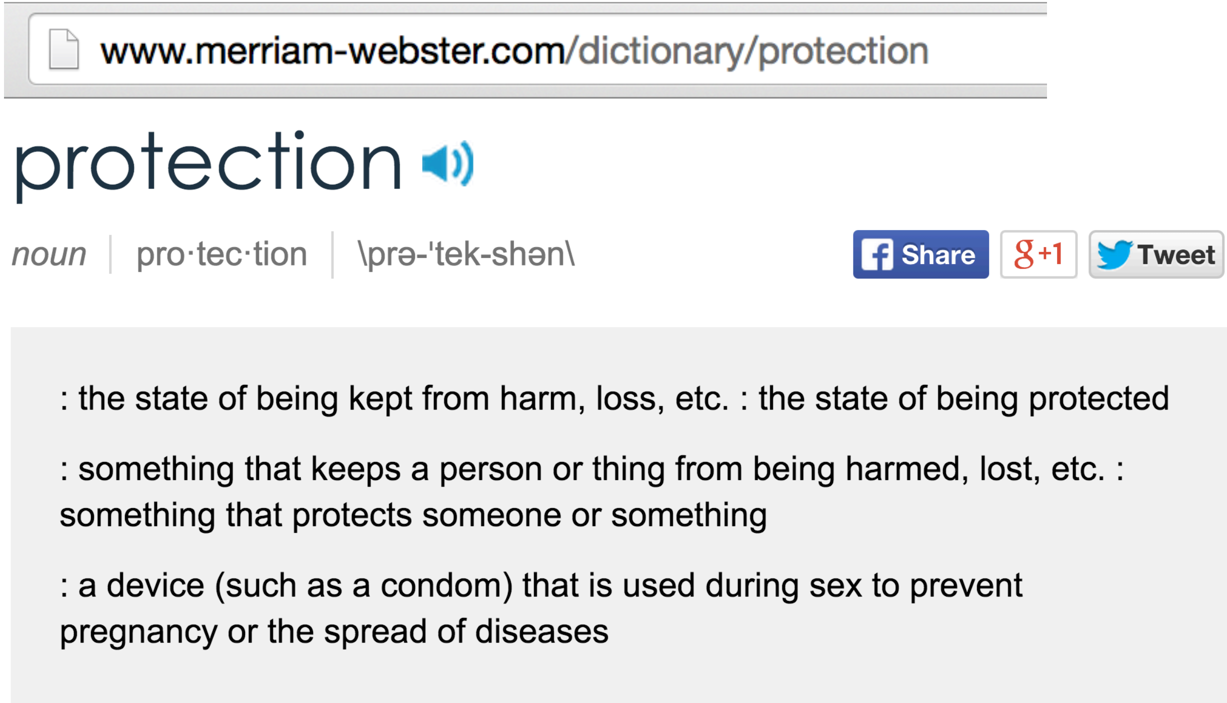
FireEye cyber security products combat today's advanced persistent threats (APTs). As an integral piece of an Adaptive Defense strategy, our state-of-the-art network security offerings protect against cyber attacks that bypass traditional signature-based tools such as antivirus software, next-generation 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.

Protection



www.merriam-webster.com/dictionary/protection

protection

noun | pro·tec·tion | \prə-'tek-shən\

: the state of being kept from harm, loss, etc. : the state of being protected

: something that keeps a person or thing from being harmed, lost, etc. : something that protects someone or something

: a device (such as a condom) that is used during sex to prevent pregnancy or the spread of diseases

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.

APT

- First observation:
  - It is an interesting assumption to prevent a threat which is *not* caused by automated software with automated software.
- Or, as Alex Stamos in *AppSec is Eating Security* said it:

"*You need to be an idiot to be a nation-state-level attacker and to use malware that FireEye catches*"

Beyond this statement…

"Capability evaluation of sandbox-/behavior-based malware detection to find out to what degree the solutions are suited to protect from common targeted/advanced attacks in the enterprise context"

Provide insight on some internals and the capabilities and limits of APT Protection Solutions.

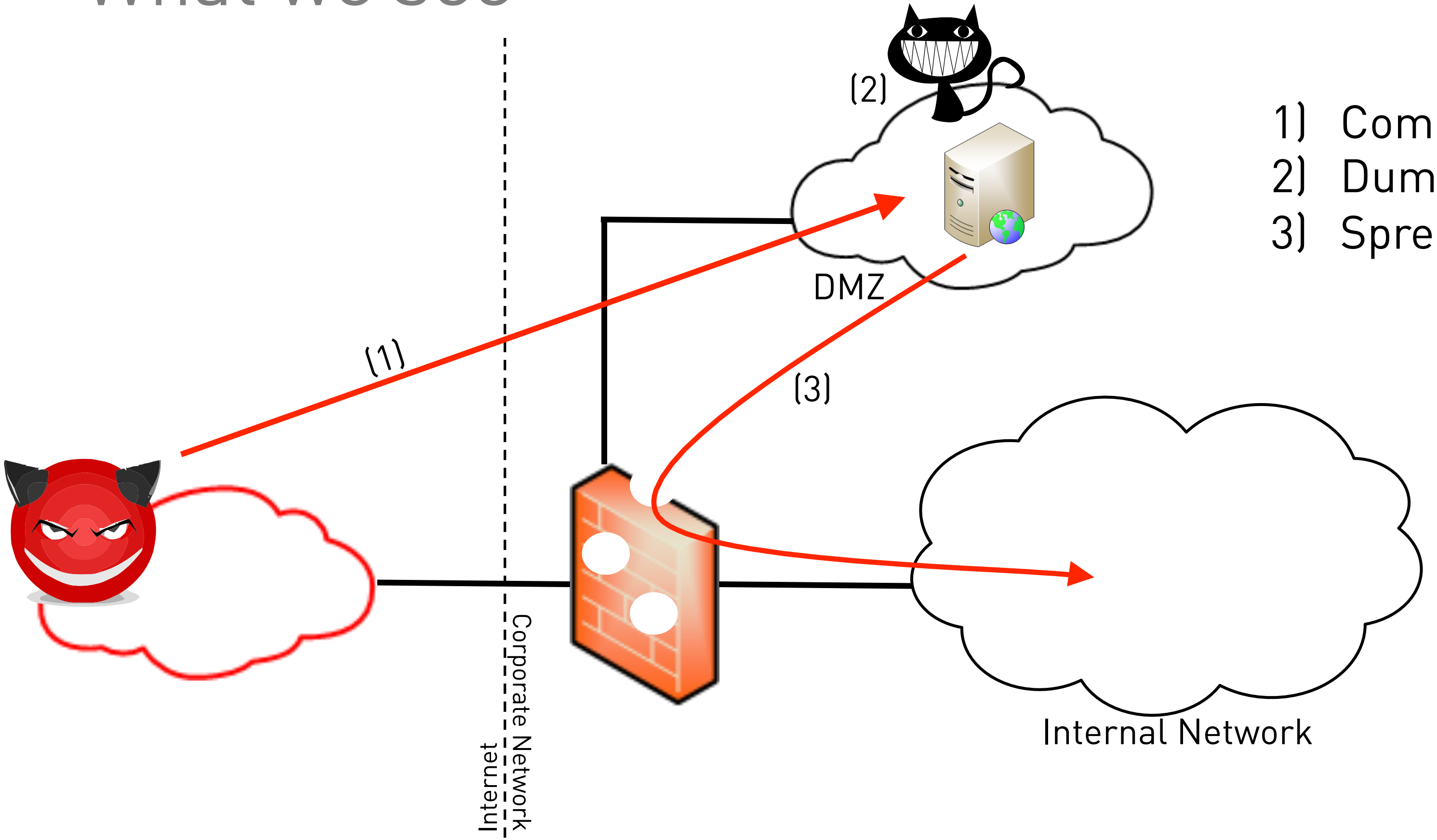
Evaluation

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

Define APT

- 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

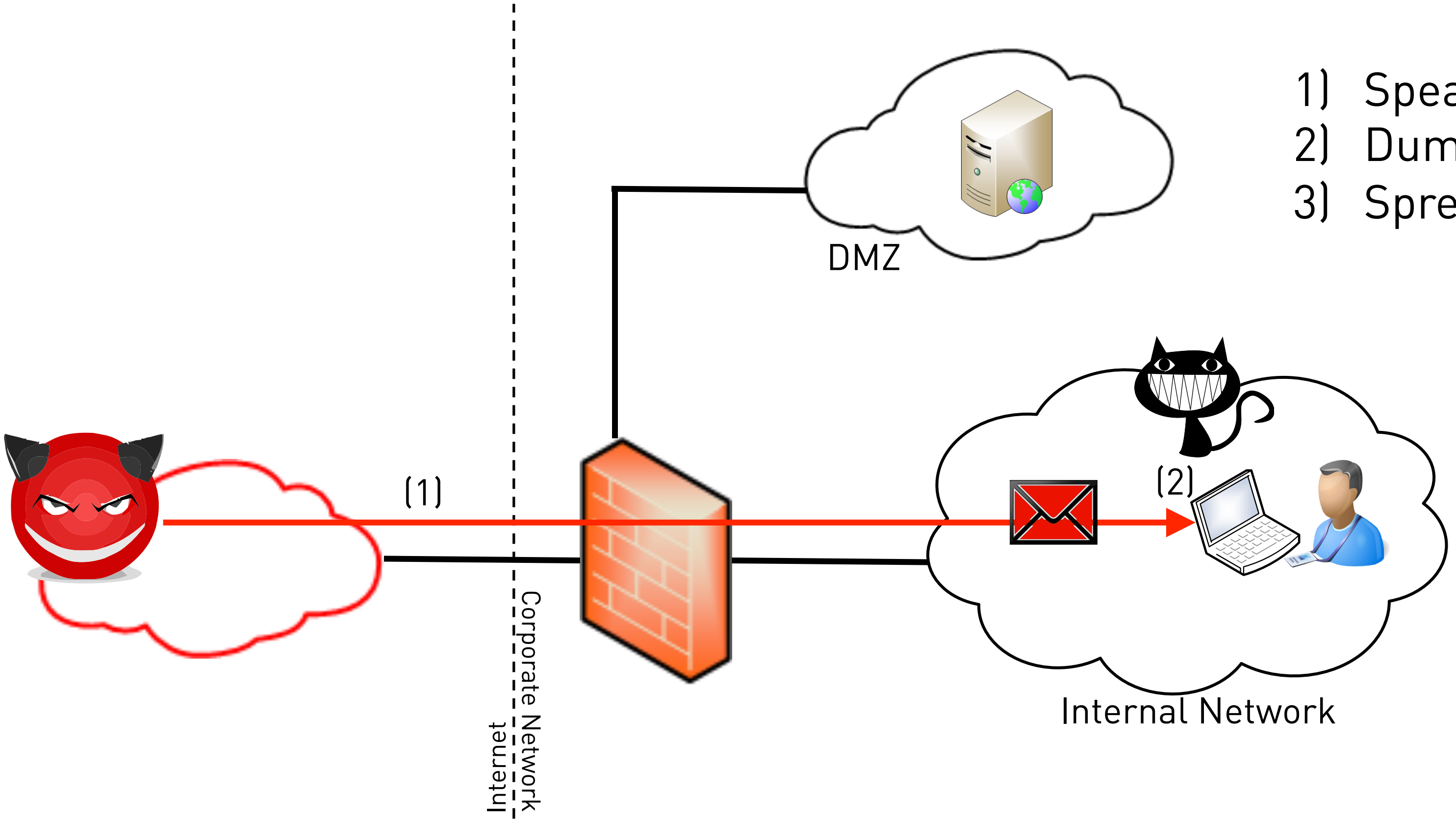
What can be deducted

- 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

Spear Phishing



1) Spear phishing
2) Dump Credentials
3) Spread

Attack Phases

- Infect
  - User-based or
  - Server-based
- Persist
- Loot
- Exfiltrate
- Spread

Detection?

ThreatGRID®
Malware Threat Intelligence Platform

FireEye™

zscaler®

McAfee®

websense®
TRITON™

lastline

Detection?

ThreatGRID
Malware Threat Intelligence Platform
FireEye™
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!

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...

Infect

- User-/File-based
  - Memory compromise
  - ASLR bypassing
  - ROP chains/stack pivoting
  - LoadLibrary techniques
  - Heap Spraying
  - Download further file

Persist

- Drop binary/executable
  - Packed?
  - VM/Debugger detection
  - Obfuscation
- Create user
- Open network port
- Persist to autorun
- Hooking/Hooking bypassing
- Stalling

Loot

- Dump credentials
  - Windows
  - Mail
  - Browser
  - IM
  - Banking
  - ...
- Network sniffing/Traffic redirection

Exfiltrate

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

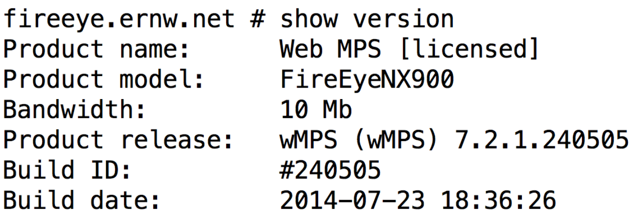
Spread

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

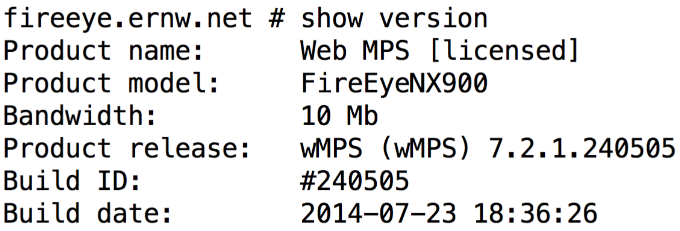
- *Not covered in this presentation.*

Detection Methods

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

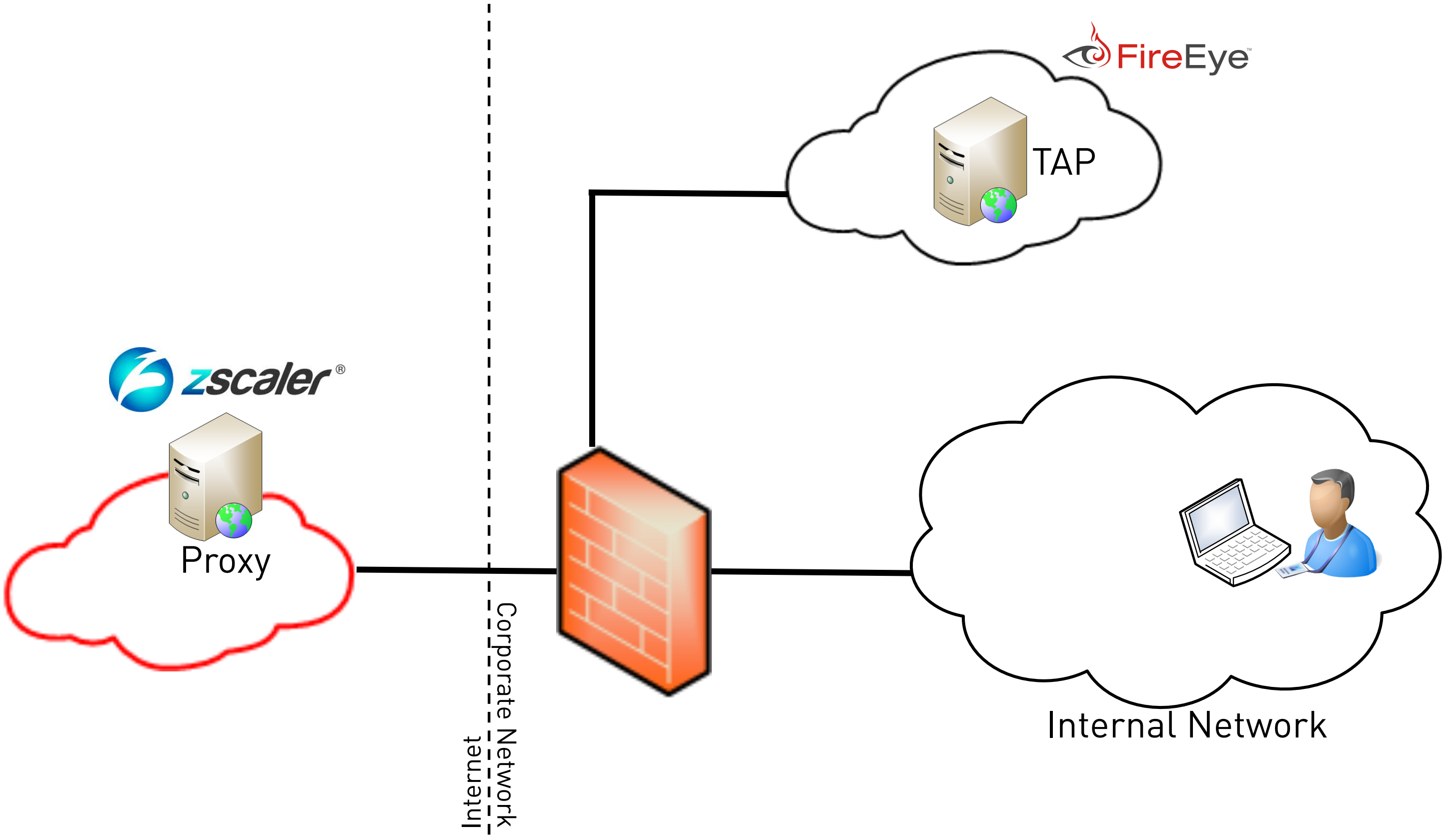


```
fireeye.ernw.net # show version
Product name:       Web MPS [licensed]
Product model:      FireEyeNX900
Bandwidth:          10 Mb
Product release:    wMPS (wMPS) 7.2.1.240505
Build ID:           #240505
Build date:         2014-07-23 18:36:26
```



```
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
```

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

- *NOT*:
  - Quality of detection methods
    - Emulation vs. hooking…
  - Mass testing of samples
  - Performance evaluation
- Characteristics of the heuristics:
  - Create a number of attack primitives, see what results in malicious classification
  - Understand how the solutions are working

Samples

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

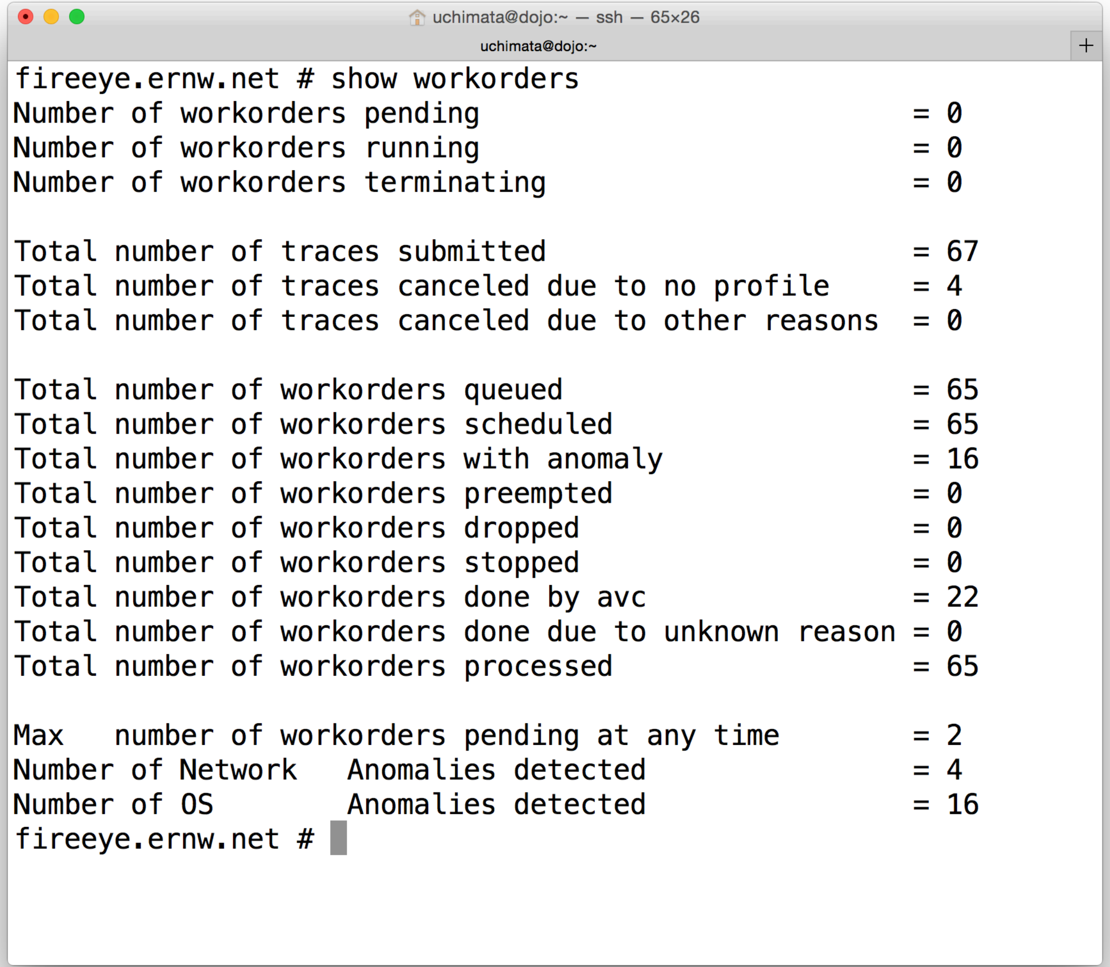
9381-7417-3831-2177-0307

Samples

ID	Description
CreateUser.exe/ CreateUser64.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

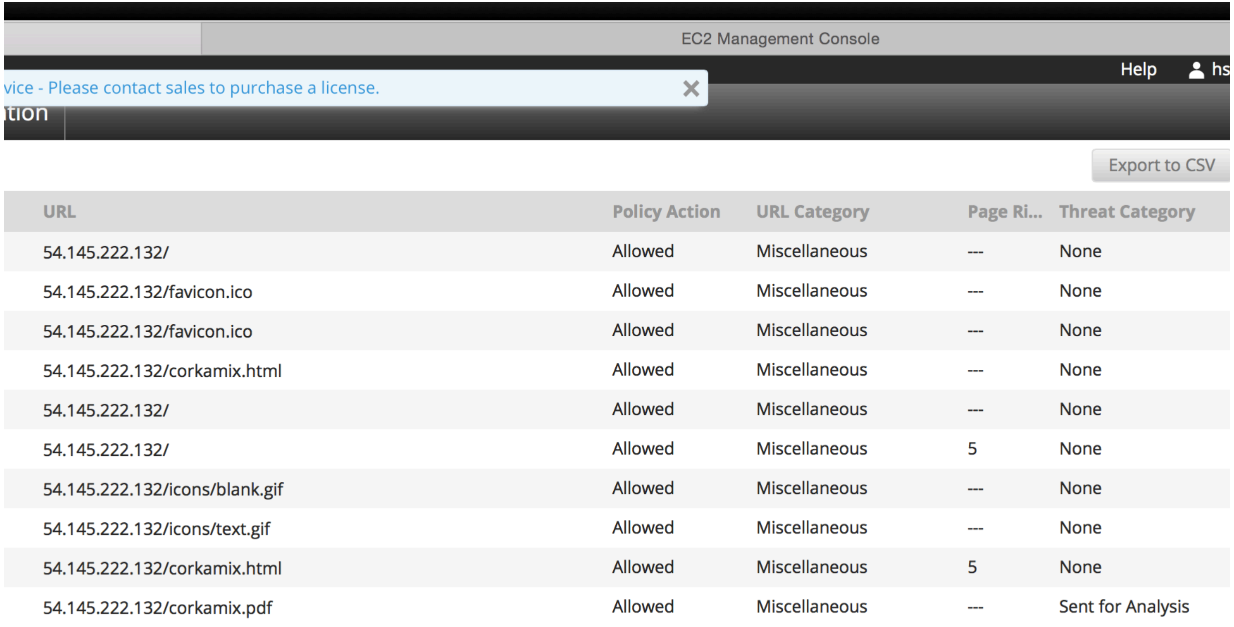
ID	Description
mimi32/mimi64.exe	Mimikatz clone.
autorun.exe	Writing a binary to autorun.
down-to-ar.exe	Downloading a python script and writing it to autorun.
sam_post.exe	Reading the backup SAM and HTTP POSTing it to a server.
keylog_post.ps1	Powershell keylogger HTTP POSTing the keys to a server.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



```
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 # 
```

ERNW
providing security.

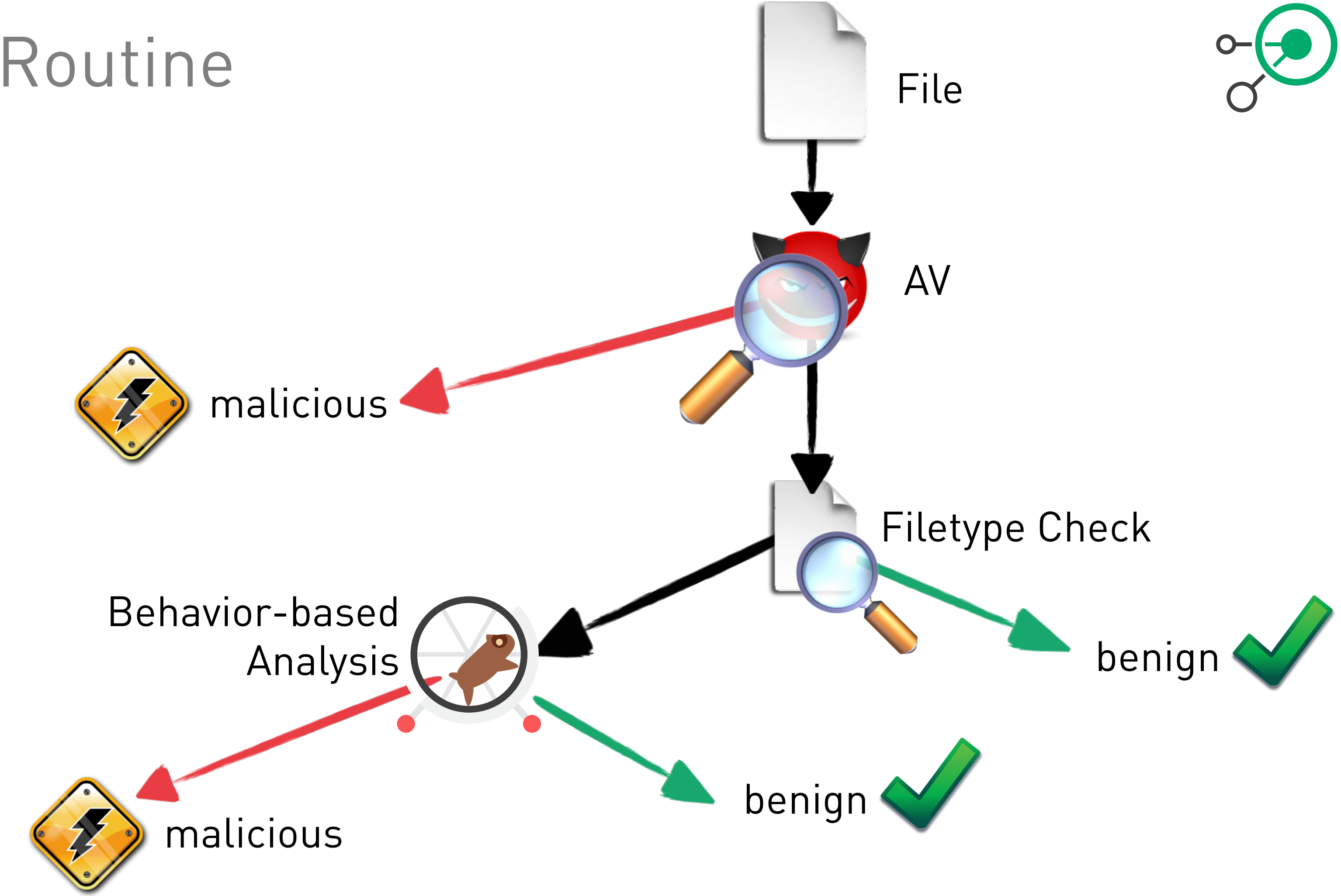
Blackbox Assessment



URL	Policy Action	URL Category	Page Ri...	Threat Category
54.145.222.132/	Allowed	Miscellaneous	---	None
54.145.222.132/favicon.ico	Allowed	Miscellaneous	---	None
54.145.222.132/favicon.ico	Allowed	Miscellaneous	---	None
54.145.222.132/corkamix.html	Allowed	Miscellaneous	---	None
54.145.222.132/	Allowed	Miscellaneous	---	None
54.145.222.132/	Allowed	Miscellaneous	5	None
54.145.222.132/icons/blank.gif	Allowed	Miscellaneous	---	None
54.145.222.132/icons/text.gif	Allowed	Miscellaneous	---	None
54.145.222.132/corkamix.html	Allowed	Miscellaneous	5	None
54.145.222.132/corkamix.pdf	Allowed	Miscellaneous	---	Sent for Analysis

Blackbox Assessment

Routine


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

Results

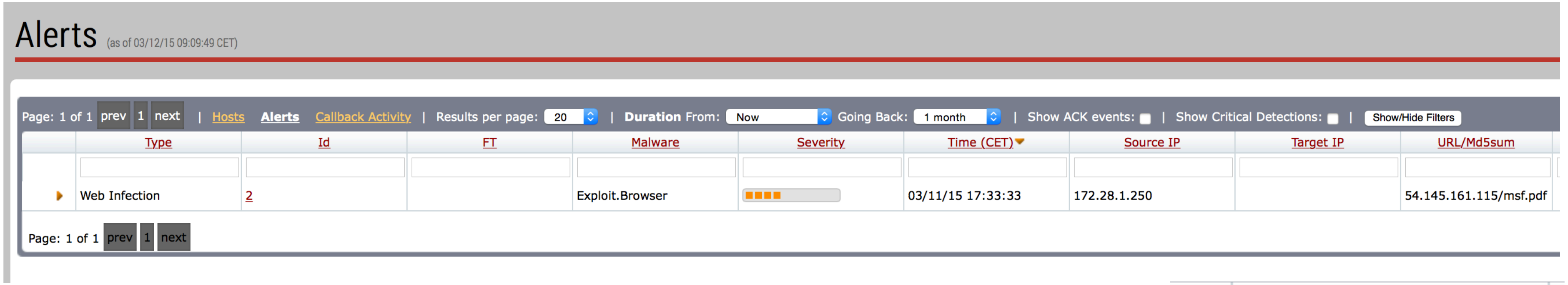
ID	FireEye	zScaler
CVE-2011-2462.pdf	🔍 ⚡	🔍 ⚡
CVE-2012-0754.pdf	🔍 ⚡	🔍 ⚡
CVE-2013-0640.pdf	🔍 ⚡	🔍 ⚡
CVE-2014-2299.pcap	Not analyzed ✓	Not analyzed ✓
ms14_017.rtf	🐞 ⚡	Not analyzed ✓
2014-0515.swf	Not analyzed ✓	🔍 ⚡
2013-3346.pdf	🐞 ⚡	🐞 ⚡
CVE-2012-2052.dae	Not analyzed ✓	Not analyzed ✓

Results

ID	FireEye	zScaler
CreateUser.exe/ CreateUser64.exe	🐹 ✓	🐹 ✓
msvc.exe	Not analyzed ✓	🔍 ⚡
mp_default.exe	Not analyzed ✓	🔍 ⚡
mpdflt.msi	Not analyzed ✓	🔍 ⚡
mp_reverse_http.exe	Not analyzed ✓	🔍 ⚡

Results

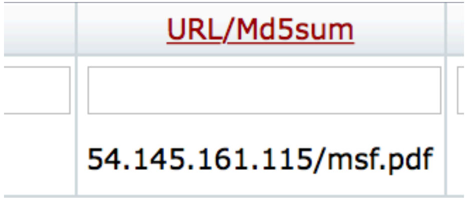
ID	FireEye	zScaler
mimi32/mimi64.exe	🐹 ⚠	🐹 ⚠
autorun.exe	🐹 ✓	🔍 ⚠
down-to-ar.exe	🐹 ✓	🔍 ⚠
sam_post.exe	🐹 ✓	🐹 ✓
keylog_post.ps1	🐹 ✓	Not analyzed ✓
Meterpreter reverse http traffic	⚠	✓



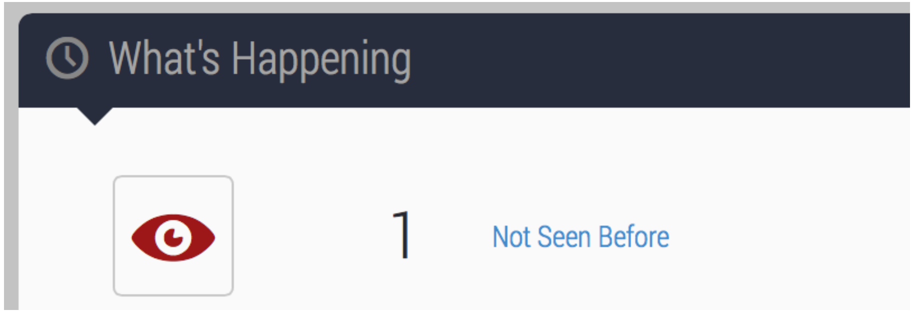
Alerts (as of 03/12/15 09:09:49 CET)

Results per page: 20 | Duration From: Now Going Back: 1 month | Show ACK events: □ | Show Critical Detections: □ |

	Type	Id	FT	Malware	Severity	Time (CET)	Source IP	Target IP	URL/Md5sum
▸	Web Infection	2		Exploit.Browser	■■■■	03/11/15 17:33:33	172.28.1.250		54.145.161.115/msf.pdf



URL/Md5sum
54.145.161.115/msf.pdf



What's Happening

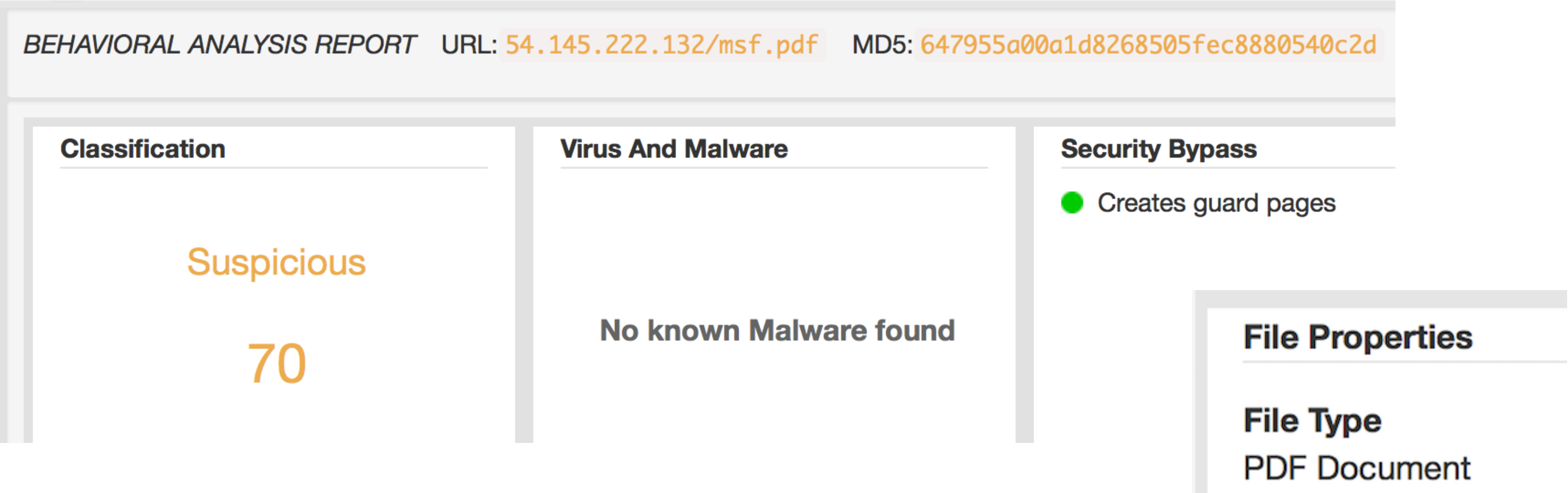
1 Not Seen Before

Some observations…

Some bypassing…

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

↓



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

Classification

Suspicious

70

Virus And Malware

No known Malware found

Security Bypass

● Creates guard pages

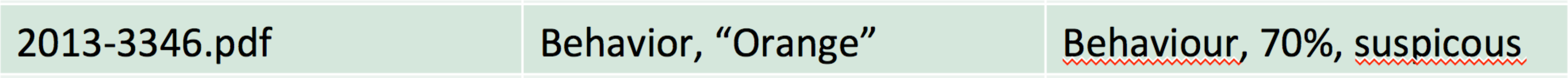
File Properties

File Type

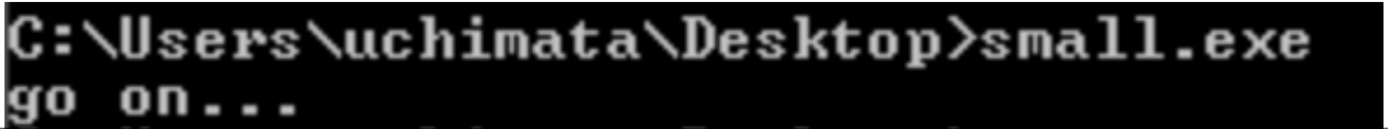
PDF Document

thx @angealbertini

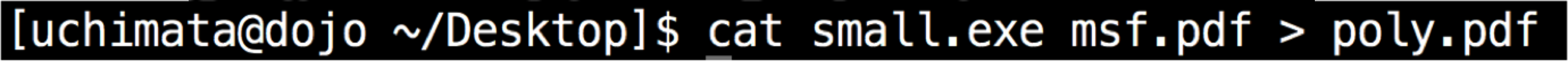
Some bypassing…



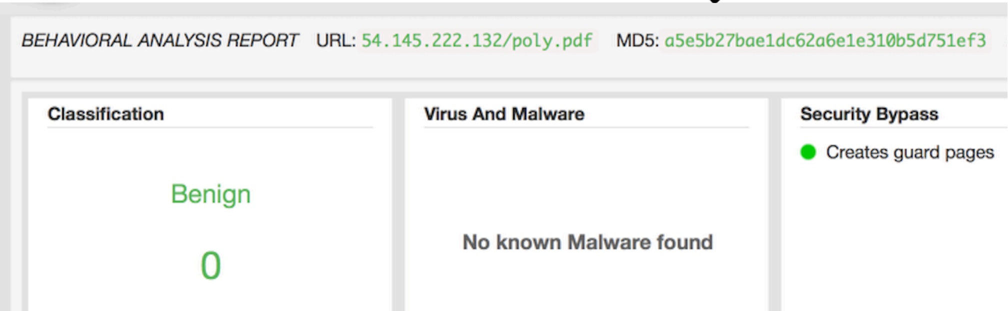
2013-3346.pdf	Behavior, “Orange”	Behaviour, 70%, suspicous



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



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



BEHAVIORAL ANALYSIS REPORT URL: 54.145.222.132/poly.pdf MD5: a5e5b27bae1dc62a6e1e310b5d751ef3

Classification

Benign

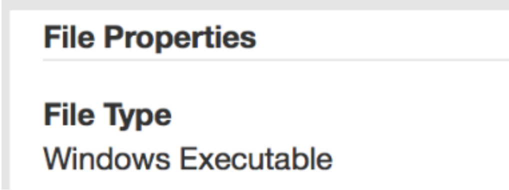
0

Virus And Malware

No known Malware found

Security Bypass

● Creates guard pages



File Properties

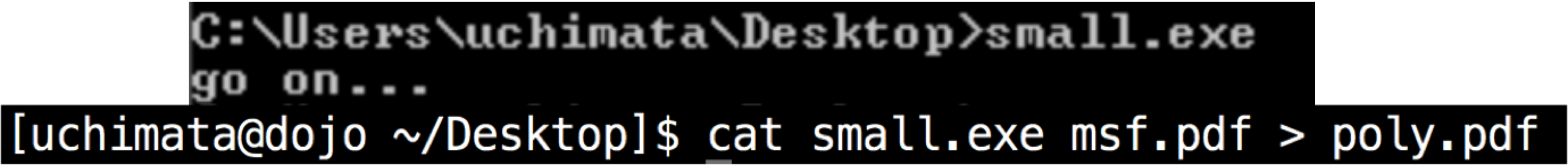
File Type

Windows Executable

thx @angealbertini

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
```

Same result on FireEye!

thx @angealbertini

Conclusions

- What was detected?
  - “Complete” attack paths
  - Certain exfiltration methods
  - (Some) Traditional MW behavior

Conclusions

- Little context-awareness.
  - E.g. binary that adds a local user which is downloaded from the Internet...
- Complementing AV, but no silver bullet.
  - What a surprise ;)
- Bypassing possible

Conclusions

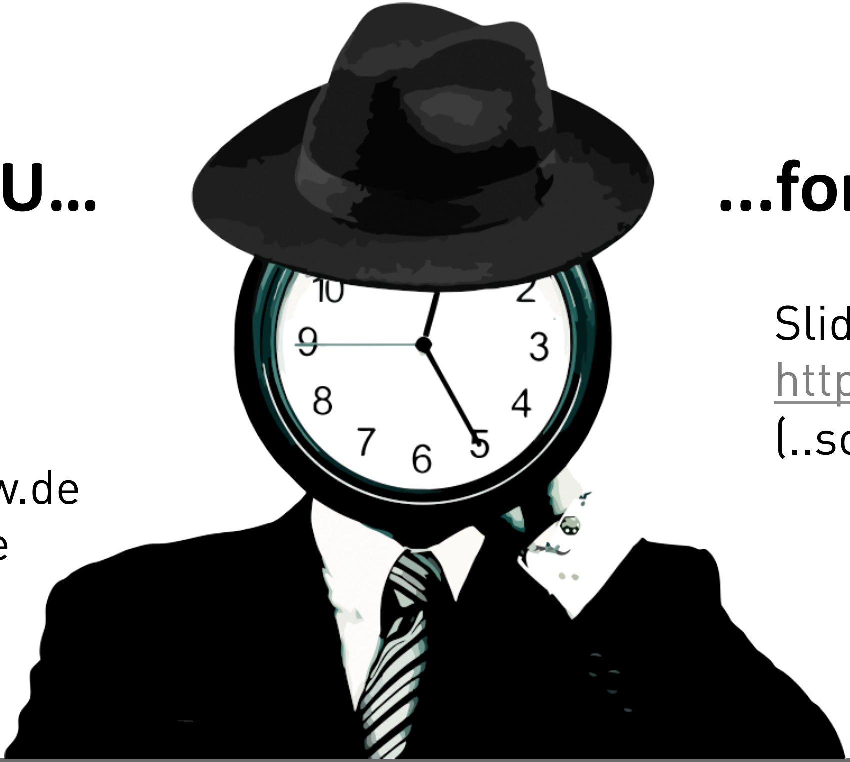
- Build solutions, don’t buy them.
- If you buy, you *must* implement the supporting processes.
  - Incl. potential MW analysis and incident response.

Conclusions

- Evaluate benefit of 100k/year subscription vs. additional administrator/$sec_person…
  - …o r vs. proper Email configuration
    - Plenty of large organizations we communicate with do not comply with simple SPF settings.
    - .exe attachments still allowed (or even file exchange methods for additional file types could be possible).
  - … or client hardening incl. EMET
  - … or $configuration_or_operational_control

There's never enough time...

THANK YOU...



...for yours!

@_fel1x
@uchi_mata

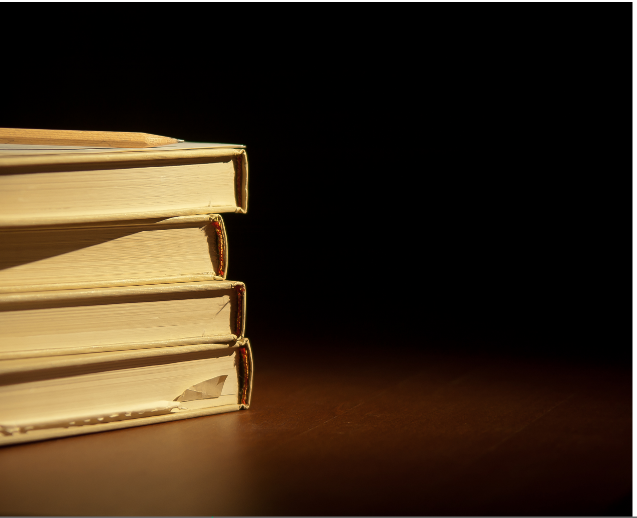
fwilhelm@ernw.de
mluft@ernw.de

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

Disclaimer

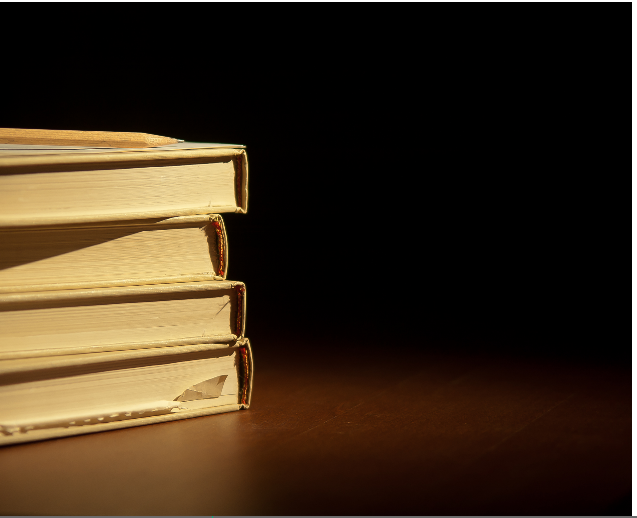
All products, company names, brand names, trademarks and logos are the property of their respective owners!

Sources



- Ange Albertini, 44Con, Evading Identification and Detection by Messing with Binary Formats
- Verizon Data Breach Report
- Mandiant APT 1

Sources



- https://apt.securelist.com/
- https://github.com/kbandla/APTnotes
- Rodrigo Branco, Prevalent Characteristics in Modern Malware/Scientific but Not Academical Overview of Malware Anti-Debugging, Anti-Disassembly and Anti-VM Technologies