amtso

Anti-Malware Testing Standards Organization

Effectively Testing APT Defences

Simon Edwards (simon_edwards@dennis.co.uk)
Richard Ford (rford@se.fit.edu)
Gabor Szappanos (gabor.szappanos@sophos.com)

What is an APT?

A targeted attack is an infection scenario executed against a limited and pre-selected set of high-value assets or physical systems with the explicit purpose of data exfiltration or damage.

TLTR; Software **YOU** don't want, sent specifically to **YOUR** systems, to steal or damage **YOUR** stuff.

Is it possible to test anti-APT?

- Yes (it's 'just' hacking)
- Probably (within the scope you define)
- No (if the vendor doesn't want you to)

EULA

Do not conduct any benchmarking, comparative study or analysis for any reason.

(Exception: you can ensure the kit works with your existing network.)

But even then, don't talk about your findings.

6.1.
Intel ...bles,
Doc ...d its
licer

(iii) ...any
benc ...e
Mat ...he
limit
Proc ...al
com
Benchmarking or any other information related thereto…

Source: https://www.fireeye.com/company/legal.html

Other EULAs

Palo Alto

1.3 License Restrictions

End User… shall not… (d) disclose, publish or otherwise make publicly available any benchmark, performance or comparison tests that End User runs (or has run on its behalf by a third party) on the Products…

https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/datasheets/support/EULA-PANW-END-USER-LICENSE-AGREEMENT.pdf

Fortinet

2. Limitations on Use

Nothing related to comparative tests.

http://www.fortinet.com/doc/legal/EULA.pdf

EFF on EULAs

EULAs that ban public criticism of products:

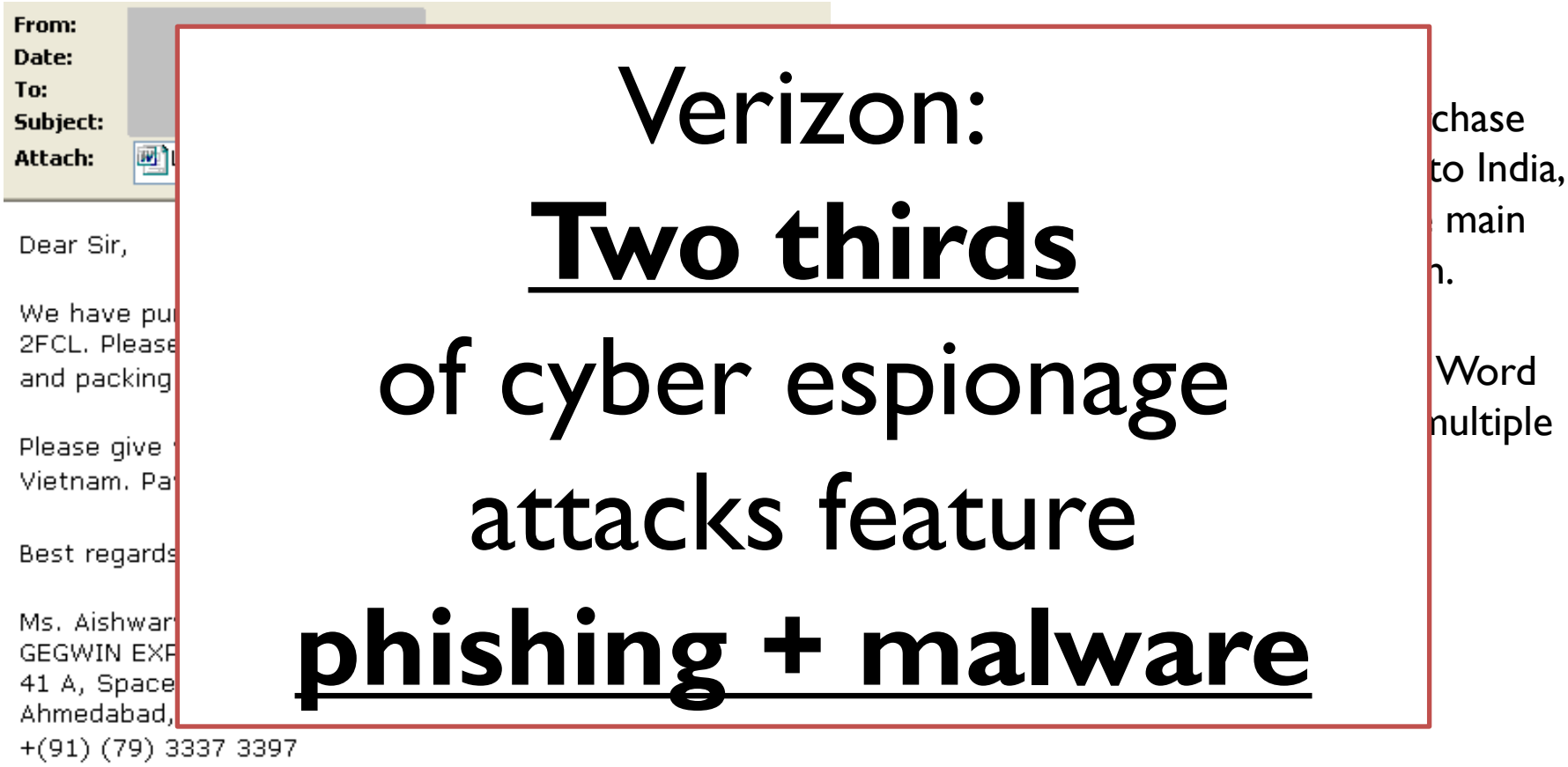
- Curtails free speech.
- Makes it difficult to make an informed buying decision.
- Damages fair competition.
- McAfee sanctioned in 2003 for such wording.

https://www.eff.org/wp/dangerous-terms-users-guide-eulas

Attack phases

- Reconnaissance
- Initial compromise
- Establish Foothold
- Escalate Privileges
- Internal Reconnaissance
- Move Laterally
- Maintain Presence
- Complete Mission

Step 1: Phishing email



Verizon:

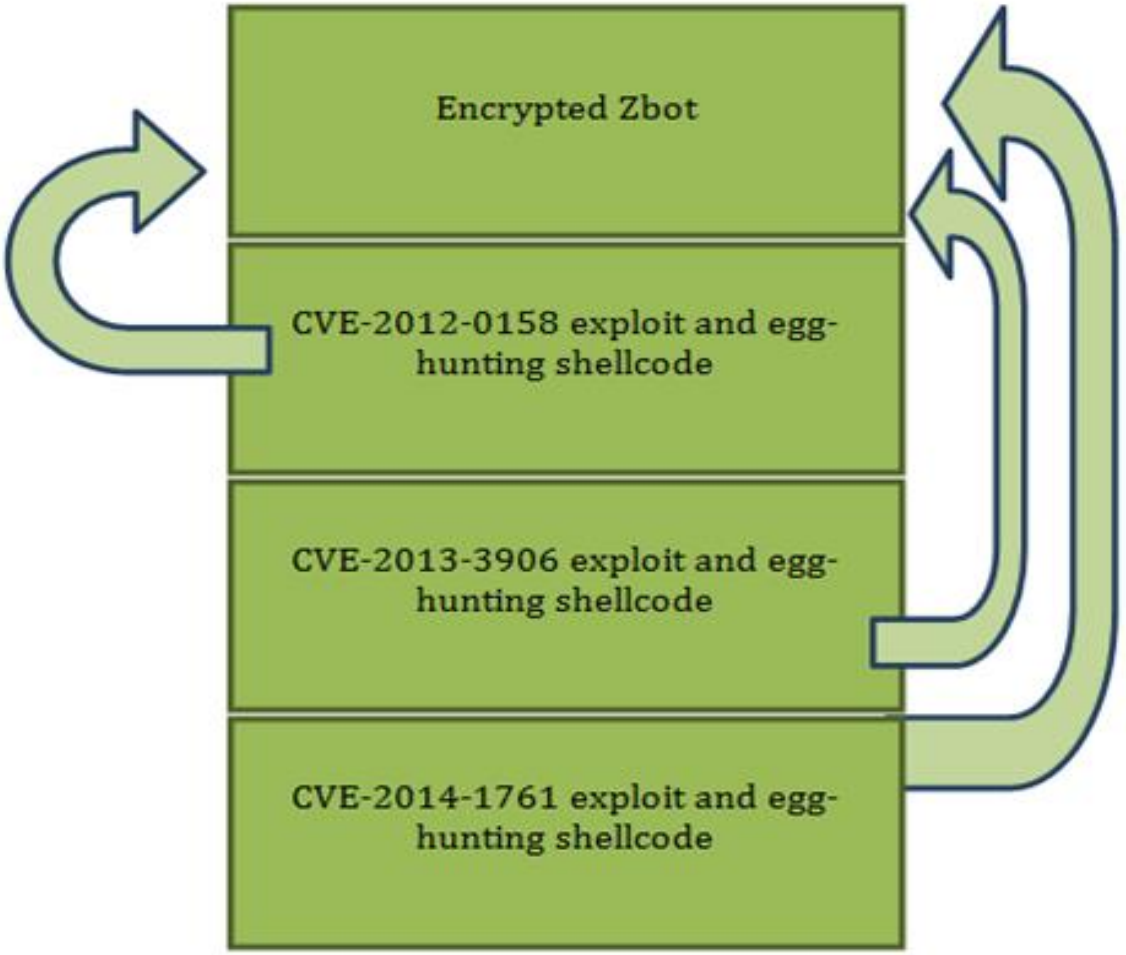
Two thirds

of cyber espionage attacks feature

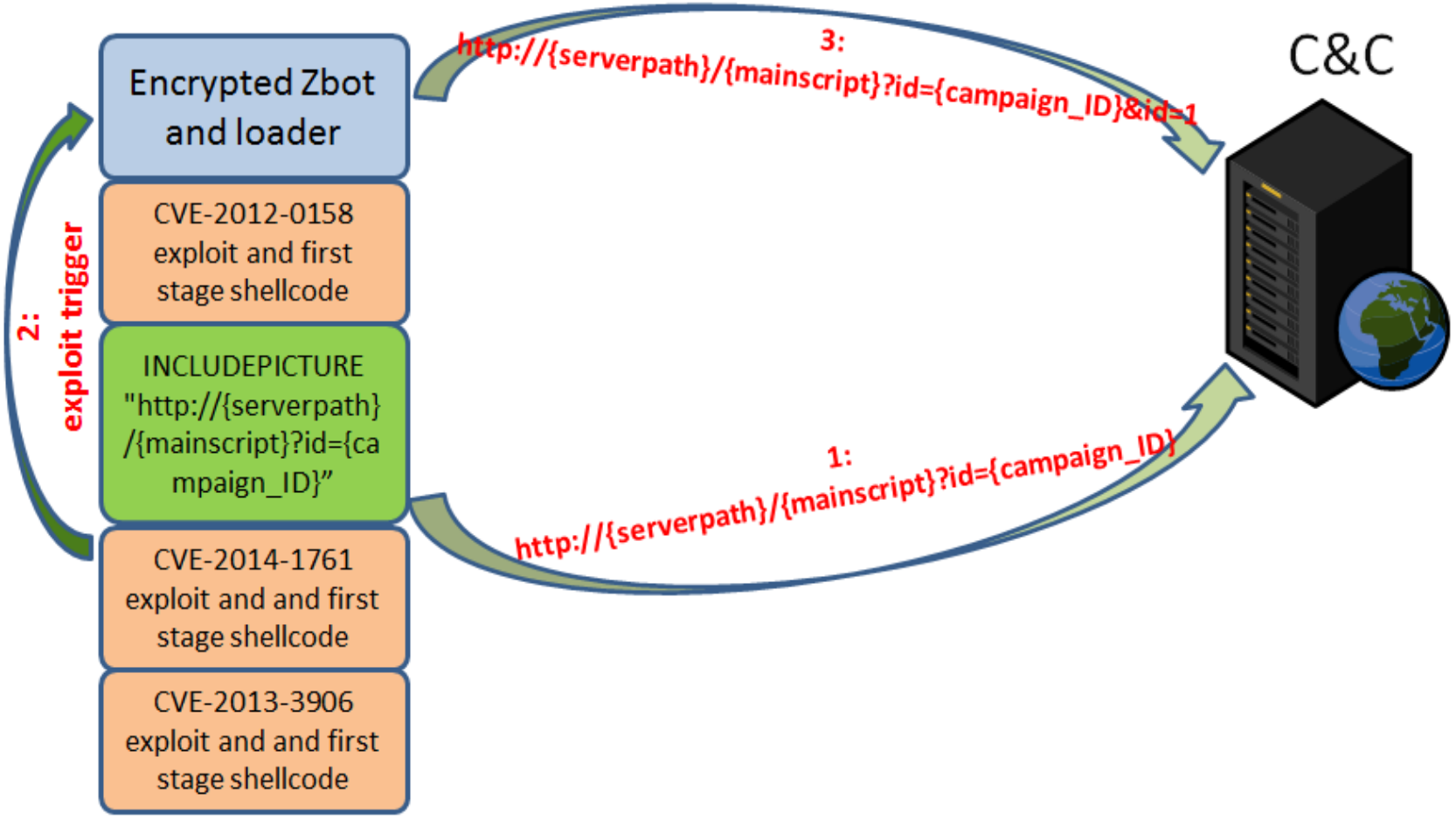
phishing + malware

Step 2: Exploitation

- The exploited document was generated by Microsoft Word Intruder
- Exploits three different Word vulnerabilities
- Installs HawkEye keylogger as the payload



Step 3: C&C communication



Step 4: data exfiltration

HaykEye collects clipboard data, raw keystrokes and user credentials for numerous applications and services:

- Firefox, Internet Explorer, Google Chrome
- Chrome Canary, CoolNovo, Opera, Safari
- Flock, SeaMonkey, SRWare Iron Browse
- Comodo Dragon Browser
- Microsoft Outlook Express
- Microsoft Outlook 2002/2003/2007/2010/2013
- Mozilla Thunderbird, Windows Live Mail 2012
- IncrediMail, Foxmail v6.x – v7.x
- Windows Live Messenger, MSN Messenger
- Google Talk, GMail Notifier, PaltalkScene IM
- …

Layered defence

- **Application Control**: block the execution of potentially unwanted/unauthorized applications
- **Anti-Spam**: block bulk e-mail
- **Scanner**: specific detection for known malware, generic detection for new malware
- **Firewall**: blocks outbound communication attempts and inbound attacks
- **IPS**: packet level filtering of network traffic
- **URL filtering**: reputation or blacklist based URL blocking
- **DLP:** prevents exfiltration of sensitive data
- **Exploit protection:** detect exploitation of application vulnerabilities
- **Behaviours based detection:** detect malware based on runtime activities in the system

Layered defence

Anti-Spa	• Blocks the initial phishing e-mail distribution
Scanner	• Detects the exploited document
Exploit protectio	• Detects the exploitation of Word
URL filtering	• Blocks the websites that host the intermediate and final trojan components
Scanner	• Detects the temporary dropper and downloader components
Scanner	• Detects the downloaded/dropped final payload
Behaviou detectio	• Detects the system activities of the dropper and the final payload
Firewall	• Detects outbound connection to the C&C server
DLP	• Detects data exfiltration

VirusTotal testing

- Anti-Spar: • Blocks the initial phishing e-mail distribution
- Scanner: • Detects the exploited document
- Exploit protectio: • Detects the exploitation of Word
- URL filtering: • Blocks the websites that host the intermediate and final trojan components
- Scanner: • Detects the temporary dropper and downloader components
- **Scanner: • Detects the downloaded/dropped final payload**
- Behaviou detectior: • Detects the system activities of the dropper and the final payload
- Firewall: • Detects outbound connection to the C&C server
- DLP: • Detects data exfiltration

Objections to testing

- Public disagreements between testers and vendors
- Security testing/testers are dishonest and/or incompetent
- The anti-APT market is quite sensitive to test results
- Resources to engage
- Tests are not ‘real world’

Who/what is an APT?

- Nation state actors
  - Virtually unlimited technical resources (inc. exploits)
  - Virtually unlimited financial resources
- Organised criminals
  - May overlap with nation state actors…
  - Incentives to malicious developers:
    - Money
    - Violence
- Testers?

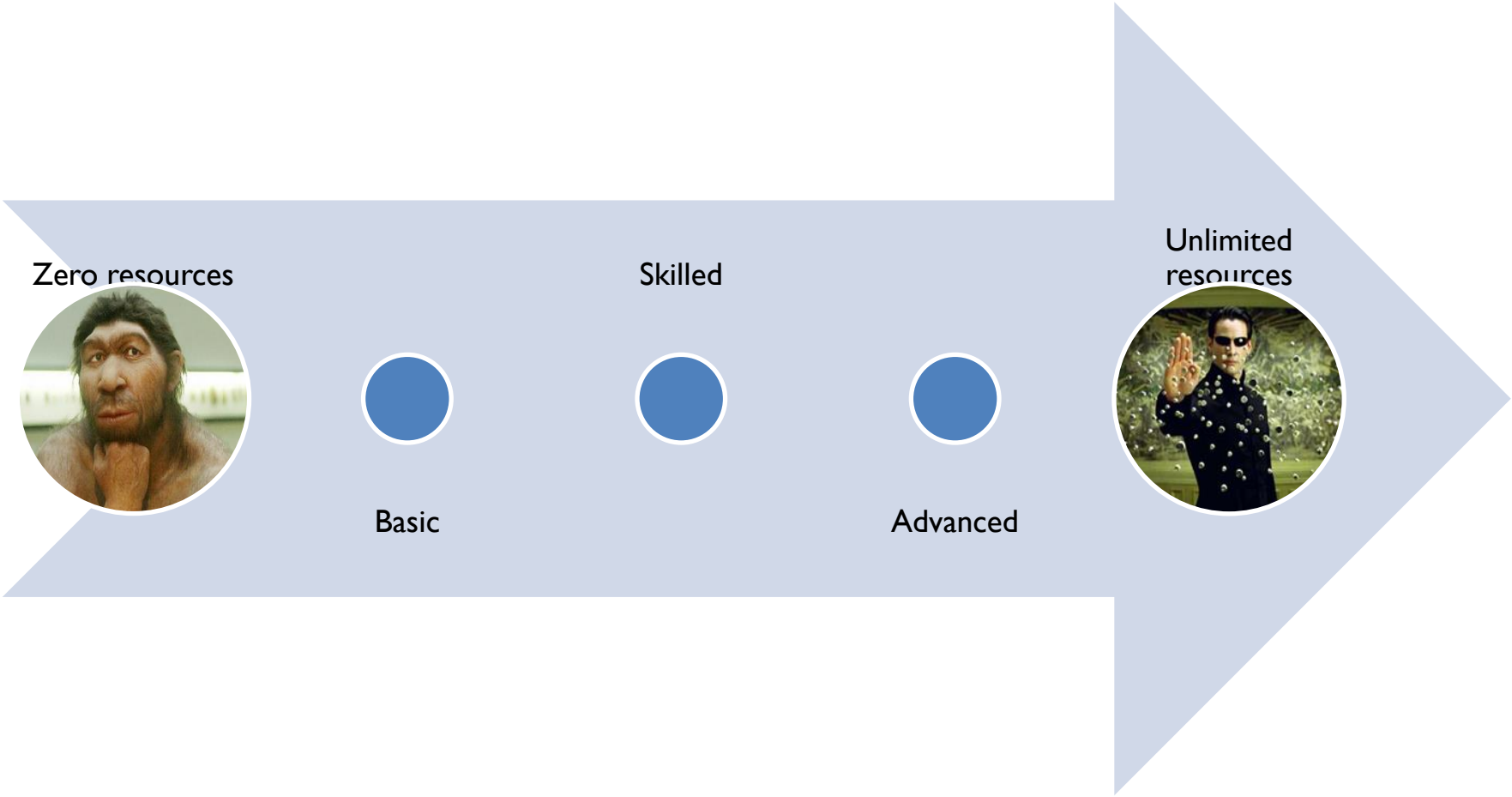
Tactics

Just because you can launch really sophisticated attacks doesn't mean you should!

- Not an ethical issue…

- Disavowal
- Confusion
- Misdirection

Zero to Neo



Tools, tactics and techniques

- **What *could* they use?** vs. **What *do* they use?**

- Freely-available penetration testing tools
- Well-known software bugs
- Social engineering techniques
- Exploit code based on known vulnerabilities
- Known 0 days – the exploits are out there but no patches
- Unknown 0 days – no general public knowledge

Threat levels

	Zero	Basic	Skilled	Advanced	A+	Neo
Spear-phishing (info gathering)	✓	✓	✓	✓	✗	✓
Commercial toolkits	✗	✓	✓	✓	✗	✓
Metasploit (default settings)	✗	✓	✓	✓	✗	✓
Customised Metasploit	✗	✗	✓	✓	✗	✓
Anti-malware evasion techniques	✗	✗	✓	✓	✓	✓
Non-metasploit tools	✗	✗	✗	✓	✓	✓
Original zero days	✗	✗	✗	✗	✗	✓

Possible results

	Zero	Basic	Skilled	Advanced	Neo
Product A	✓	✓	✓	✘	✘
Product B	✘	✓	✓	✘	✘
Product C	✓	✘	✓	✘	✘
Product D	✘	✓	✓	✓	✘
Products E	✓	✓	✘	✘	✘

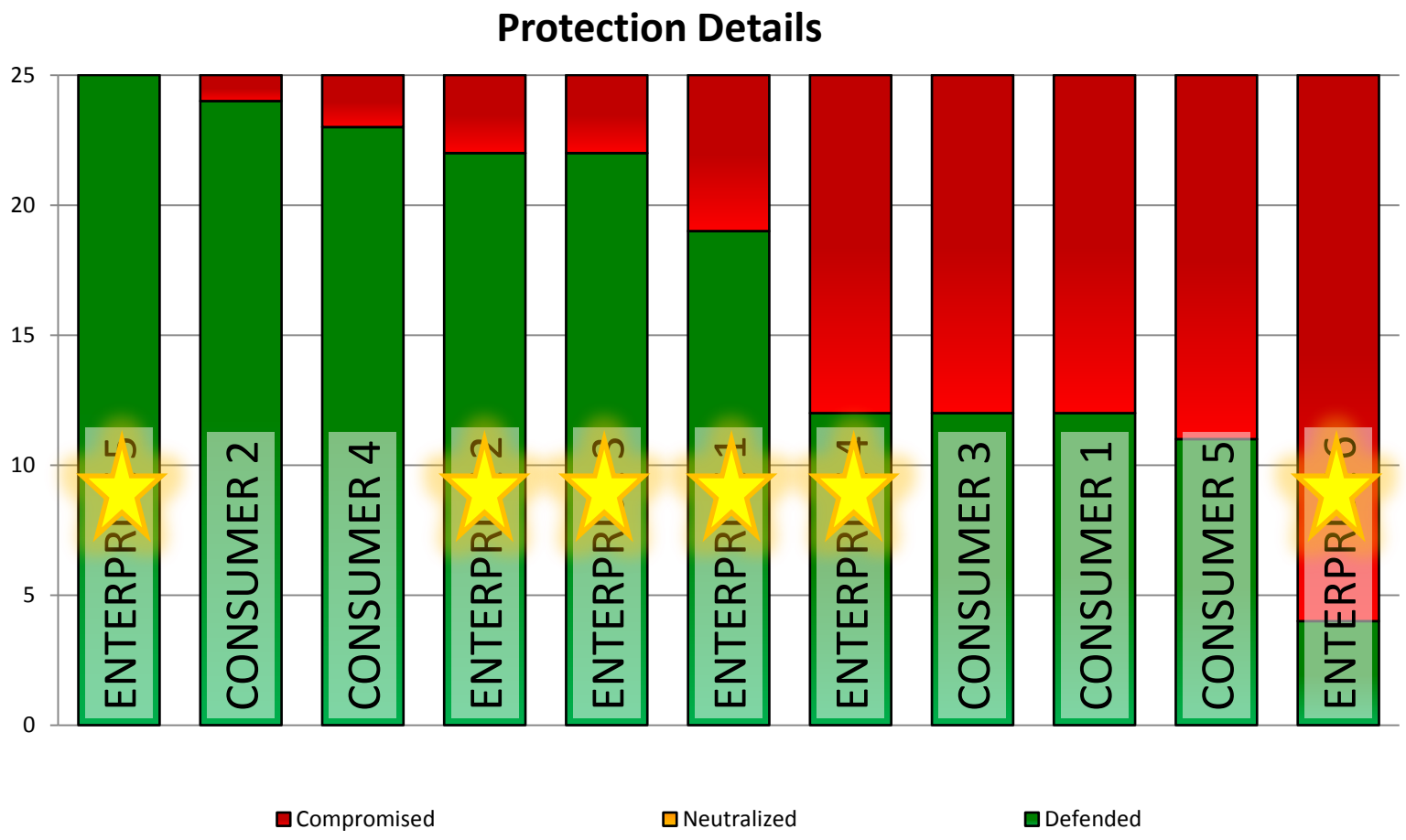
More objections to testing

- Tests require defender reactions
- Tests require unknown malware/exploits
- Tests require malware/exploits capable of bypassing other solutions

A basic test's results

- An almost laughably-basic anti-APT test…
- Using Metasploit…
- And not much else.
- Use no further tools
- Use no special encoding
- Do not attempt to proactively evade the anti-malware products
- Get a remote shell and admin privileges
- Not just calc.exe!

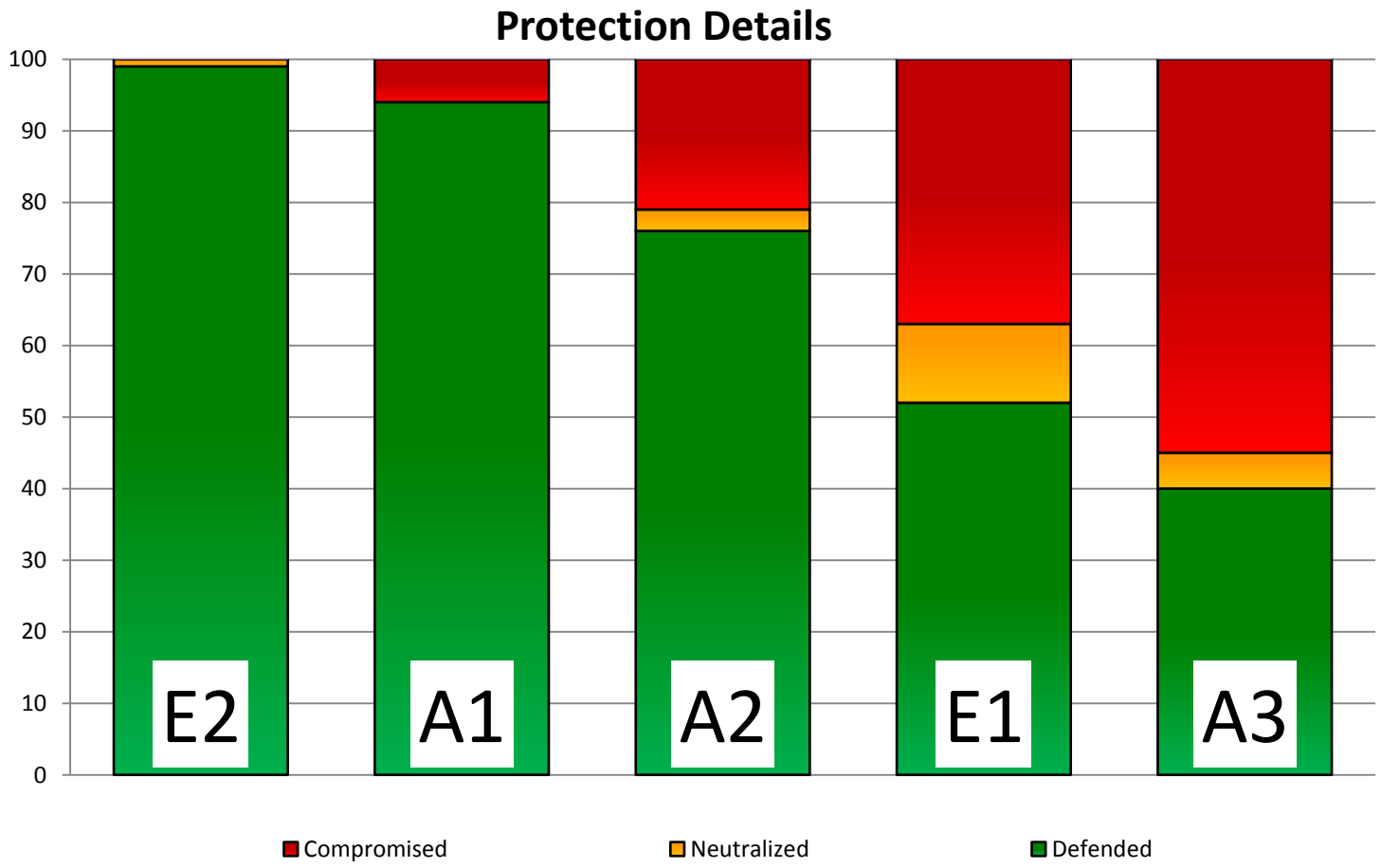
Boom….


Protection Details
25
20
15
10
5
0
CONSUMER 2
CONSUMER 4
CONSUMER 3
CONSUMER 1
CONSUMER 5
Compromised
Neutralized
Defended

Breach Response Test (BRT)

- Combination of endpoint and appliance products
- Web-based threats
  - 75% 'general' – live infected websites
  - 25% 'targeted' – tester selects exploits
- Baseline?
  - Prevalent threats
  - No special evasion; public exploits

BRT Results



BRT scoring

	Defended	Neutralized	Compromised	Protected
E2	99	1	**0**	**100**
A1	94	0	**6**	**94**
A2	76	3	**21**	**79**
E1	52	11	**37**	**63**
A3	40	5	**55**	**45**

- Classic scoring = protection/classification
- New methods need to factor in:
  - Attack provenance (Where did it **come from**?)
  - Progress of attack (Where did it **go**?)
  - Other **investigatory** details

Are all detections equal?

- AV detection/protection = blocked = ☺
- AV classification = W32/Something = 😐
- Breach detection:

Classification	Value
"Exploit kit"	😐
"Webpage has bad reputation"	😐
"Exploit Kit ABC"	☺
"Trojan/Generic.A"	☹
"Stuxnet"	WTF!

Testing advice

- Be clear on test's purpose! A basic test still has worth.
- Be clear on whether the threat is Zero, Neo or in-between
- Be clear on whether this is a test of a layer or test of a suite
- Any APT test must examine exfiltration

Questions?

Twitter: @SPGEdwards

Email: si@hak.me