The Darkside of ~~Red~~ Blue-Teaming?

Common Traps & Pitfalls

In Recent ~~Red~~ Blue-Teaming Part II

Content

- Whoami /group
- Introduction
- Preparation
- Scenario 1 – Firewalls
- Scenario 2 – Payloads
- Scenario 3 – Logging
- Post incident activities
- Technical expertise
  - Shellcode
  - ToR

Red-Side

Andy Davies

Old skool pentester from circa 2000

Developer of some popular scripts & hardware

Professional experience in infosec consulting +15 yrs

Track day addict

This Photo by Unknown Author is licensed under CC BY-SA

Blue-Side

Reseverd for guest speaker

VS

http://rvb.wikia.com/wiki/File:Red_Team_Jersey.jpg
http://gamebattles.majorleaguegaming.com/xboxone/halo-5-guardians/team/blue-team-na-ot-5

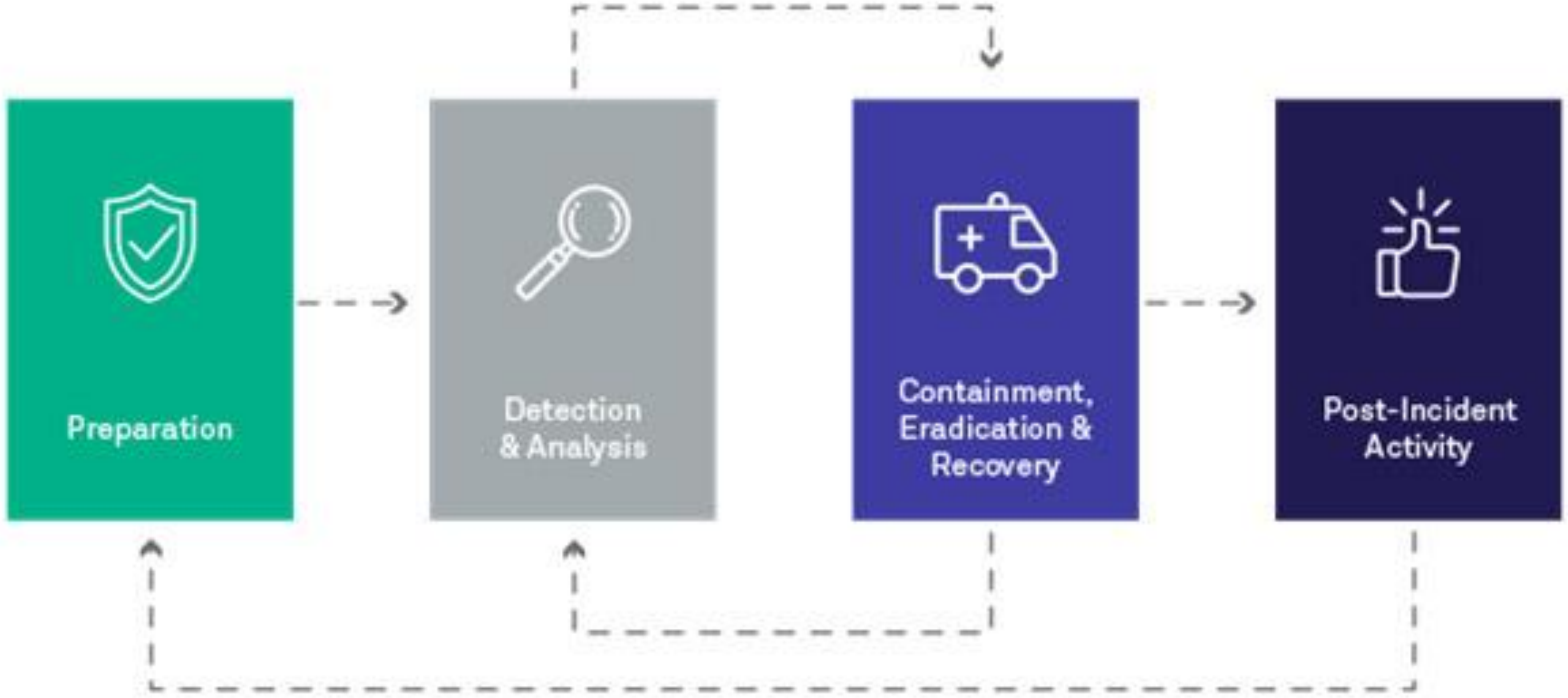
VS

http://rvb.wikia.com/wiki/File:Red_Team_Jersey.jpg
http://gamebattles.majorleaguegaming.com/xboxone/halo-5-guardians/team/blue-team-na-ot-5

VS

http://rvb.wikia.com/wiki/File:Red_Team_Jersey.jpg
http://gamebattles.majorleaguegaming.com/xboxone/halo-5-guardians/team/blue-team-na-ot-5

Introduction:
Typical 4-Step Response Process



https://www.moi.gov.sa/wps/portal/ncsc/home/services/incidentresponse/!ut/p/z0/04_Sj9CPykssy0xPLMnMz0vMAfIjo8ziDQ1dLDyM3A183MMszQwcjYPMXcOCXI293Yz1g1Pz9AuyHRUBS2nzmQ!!/

Preparation

- Host based IDS
- Log collection
- Network based IDS
- Firewalls
- Network Management & Segregation
- Anti Virus
- Data Loss Prevention

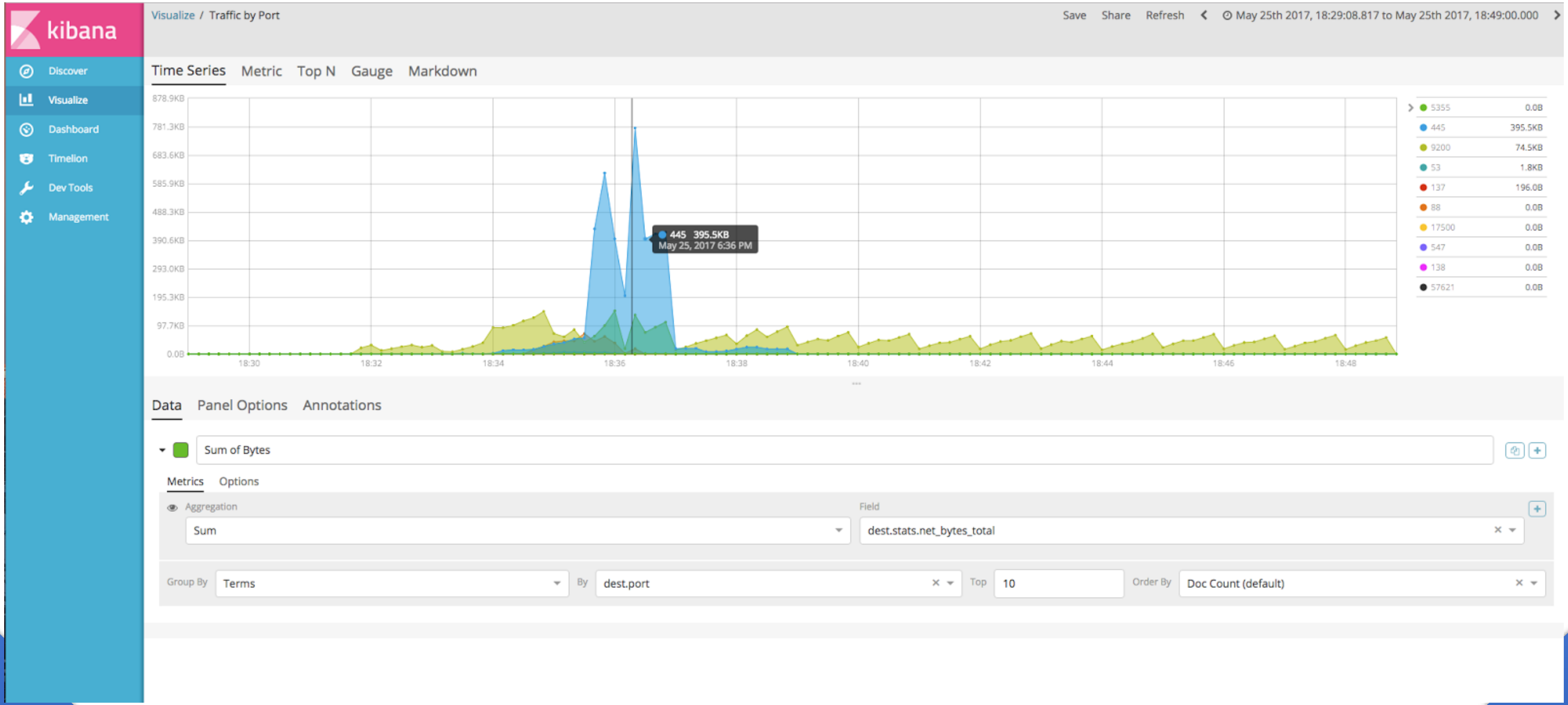
Detection

- Arcsight
- Qradar
- Splunk
- *ELK
- BRO
- Securicata
- SNORT
- OSSEC & Wazhu
- Sensu & Uichqa

Our Blue-Teams First Simple Mistake…

Scenario 1

Detecting Suspicious IPs / Traffic



Sum of Bytes

Aggregation: Sum

Field: dest.stats.net_bytes_total

Group By: Terms

By: dest.port

Top: 10

Order By: Doc Count (default)

©2018 Netscylla

Blocking the Offending IP on the Firewall?

https://pixabay.com/en/firewall-security-internet-web-29940/

Containment / Recovery Success?

Business Internet Fail

Yep – They blocked their corporate Gateway

https://pixabay.com/en/firewall-security-internet-web-29940/

Feeling Dumb…

BUT I SAW AN ATTACK PATTERN...
YOU BLOCKED MY INTERNET ACCESS
imgflip.com

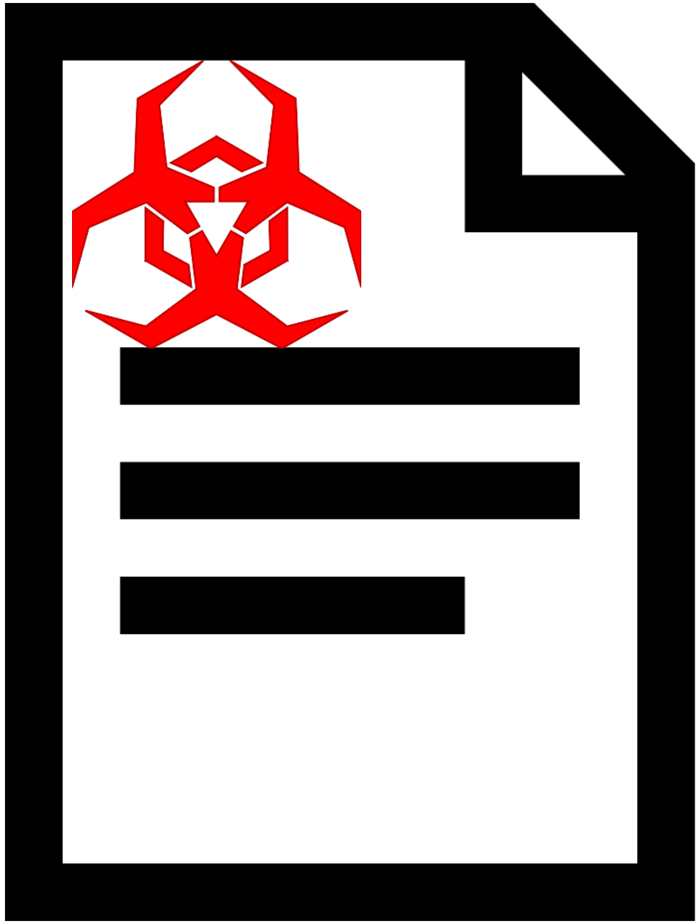
Blocking IPs – Lessons Learnt

- Check that the IP is not the corporate load-balancer or internal proxy
- Check that the IP is not part of the corporate range
    - Might be easier if you can record and track the businesses IP space
- Check that the IP is not a subsidiary or another business unit, with its own Internet connection.
    - Again change-control and connection tracking required.

Another Common Blue-Team Mistake…

Scenario 2

Payloads & Suspicious Docs



Payloads & Suspicious Docs

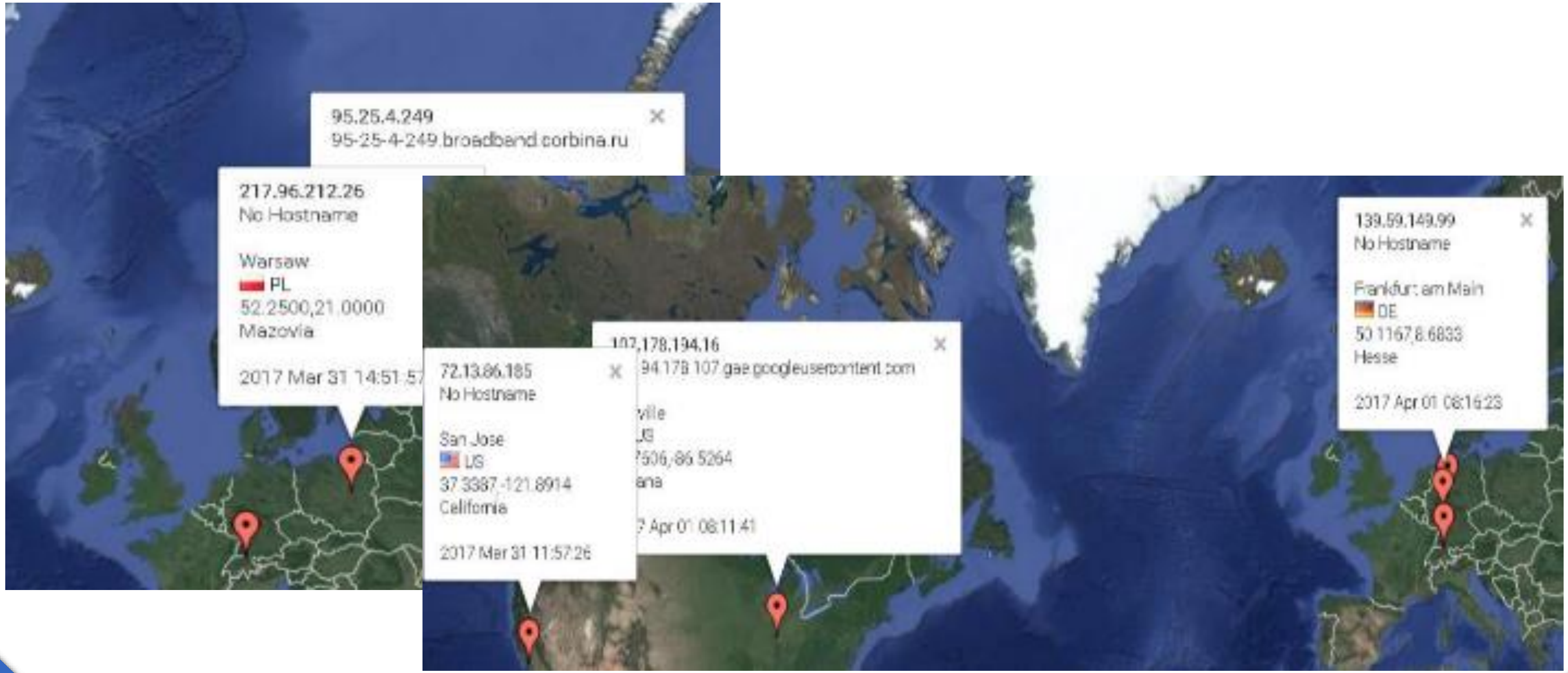
What is the first think new blue-teamers do with a sample?

Payloads & Suspicious Docs

https://upload.wikimedia.org/wikipedia/commons/e/e0/Virustotal_logo_pixelalign.png

Payloads – Tracking

VirusTotal will share your payloads!



https://github.com/yt0ng/SAS/blob/master/MNeis_dont_push_the_button_SAS2017_PUBLIC.pdf

Payloads – Tracking

Other Privateers/Researchers:

- 176.24.96.80
- 213.254.241.7
- 95.211.95.129 (Tor Exit Node – Intro Later…)
- 193.226.177.0/24
- 66.102.0.0/20

Payloads – Reversing

What if the document you uploaded contains corporate Intellectual Property?

The Blue-Team Breach!

https://www.teachprivacy.com/wp-content/uploads/Module-Data-Security-Data-Breach-031.jpg

Payloads – Reversing

What if the payload comes back clean?

Payloads – Reversing

How did you collect the sample?

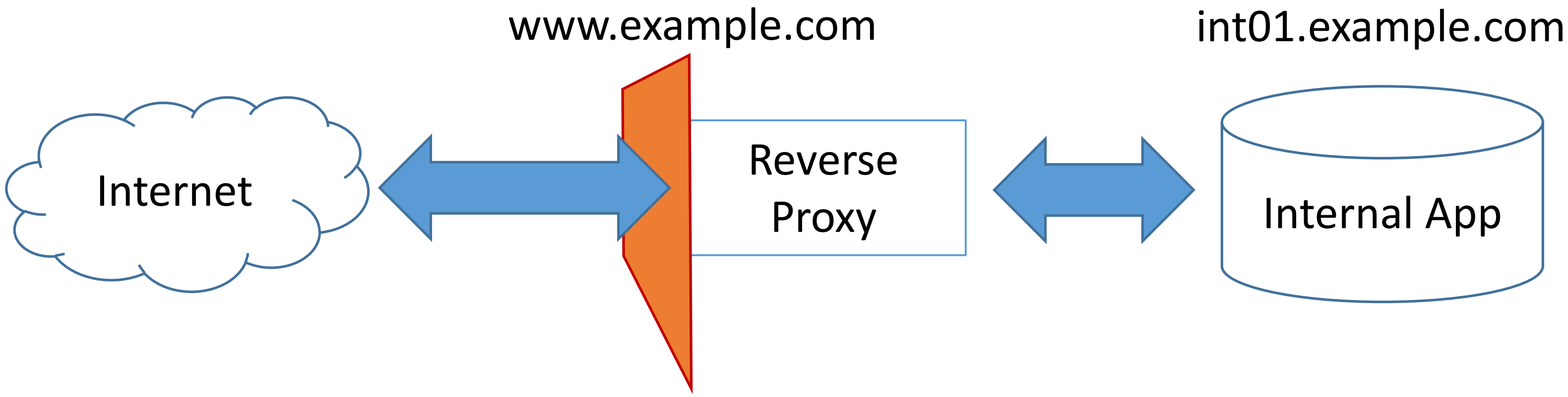
Red vs Blue

The Red-Team could be messing with you…

Reverse Proxies

What is a reverse proxy?

Unlike the traditional proxy that may be the gateway to the internet, it is an application that works (you guessed it) in reverse, it provides a gateway for the internet to access your application (or internal application).



Nginx Reverse Proxy (Not Complete)

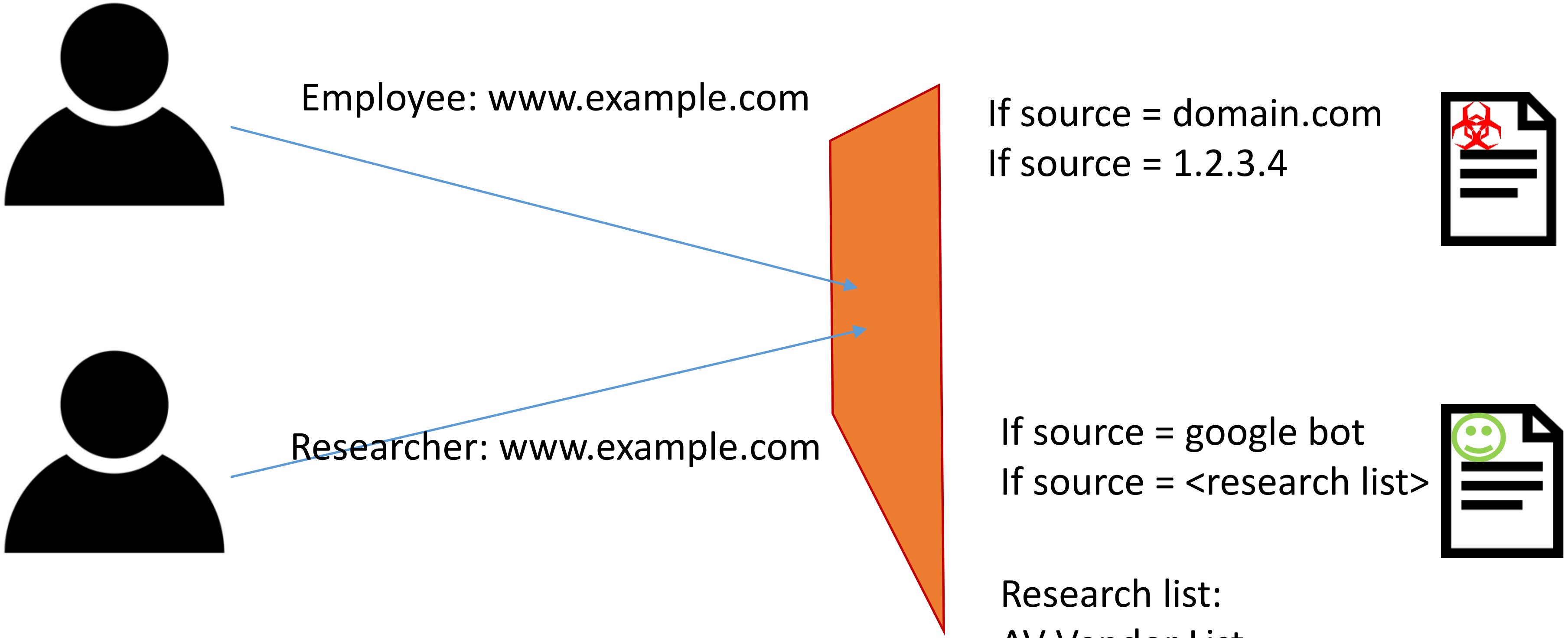
```
server {
        location / {
                proxy_set_header        Accept-Encoding   "";
                proxy_set_header        Host              $http_host;
                proxy_set_header        X-Forwarded-By    $server_addr:$server_port;
                proxy_set_header        X-Forwarded-For   $remote_addr;
                proxy_set_header        X-Forwarded-Proto $scheme;
                proxy_set_header        X-Real-IP         $remote_addr;
                ## default backend
                proxy_pass  http://cleanserver;
                ## send traffic to malicious backend if ip is 1.2.3.4 ##
                if ( $remote_addr ~* 1.2.3.4 ) {
                        proxy_pass http://dirtyserver;
                }
                proxy_next_upstream error timeout invalid_header http_500 http_502 http_503 http_504;
        }
```

Blue Screen of Jeff

If you are more comfortable with Apache; a short shout out to Bluescreenofjeff (www.blackhillsinfosec.com) who already covered this:

https://bluescreenofjeff.com/2016-03-22-strengthen-your-phishing-with-apache-mod_rewrite-and-mobile-user-redirection/

Why Attackers Love Reverse Proxies



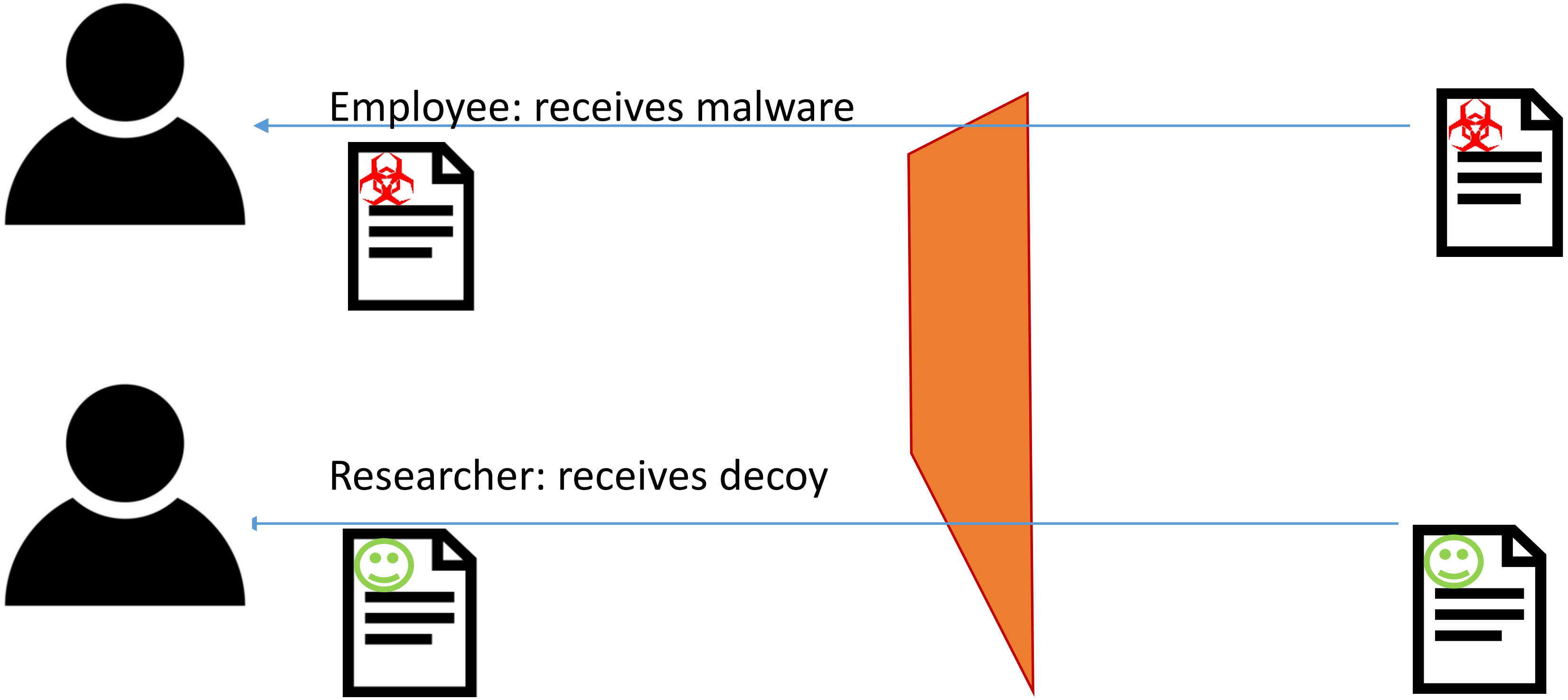
Employee: www.example.com

Researcher: www.example.com

If source = domain.com
If source = 1.2.3.4

If source = google bot
If source = <research list>

Research list:
AV Vendor List
Virus Total IP Space
Etc …

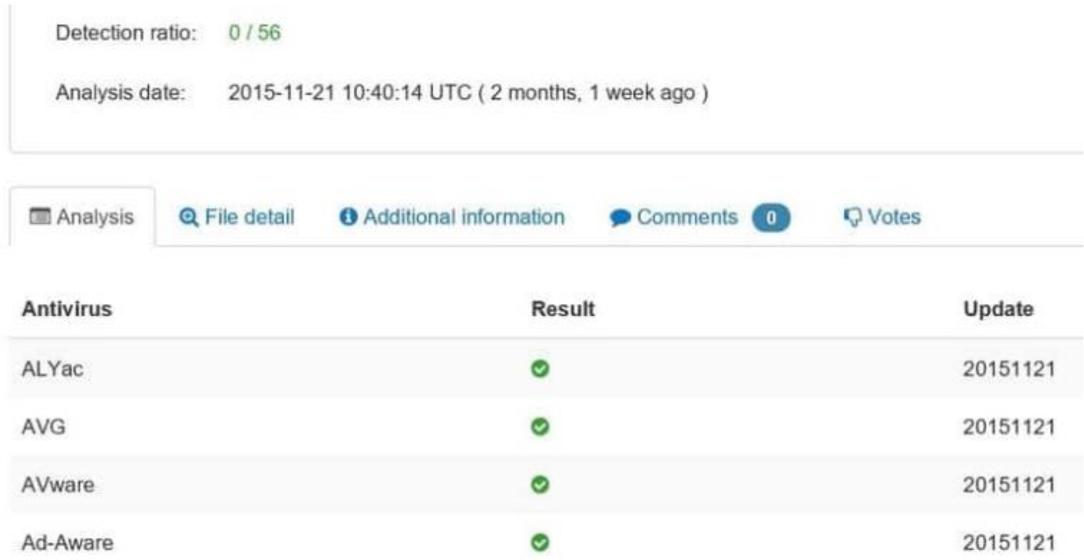


Employee: receives malware

Researcher: receives decoy

You could have analysed the wrong sample?

Clean Sample

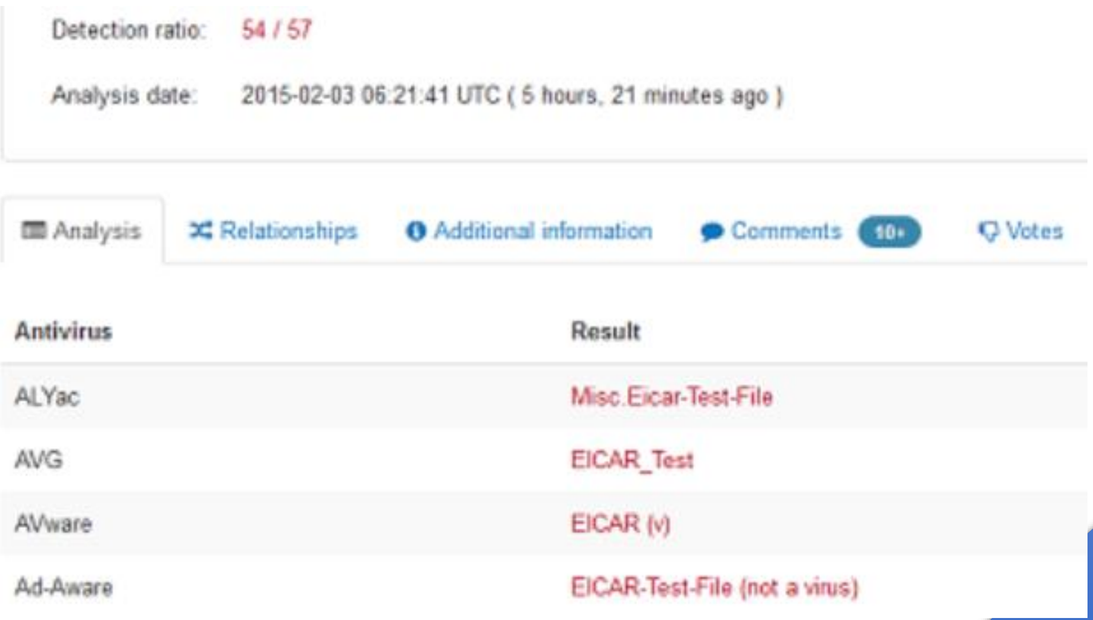


Detection ratio: 0 / 56

Analysis date: 2015-11-21 10:40:14 UTC (2 months, 1 week ago)

Antivirus	Result	Update
ALYac	✓	20151121
AVG	✓	20151121
AVware	✓	20151121
Ad-Aware	✓	20151121

Dirty (Potential Malware)



Detection ratio: 54 / 57

Analysis date: 2015-02-03 06:21:41 UTC (5 hours, 21 minutes ago)

Antivirus	Result
ALYac	Misc.Eicar-Test-File
AVG	EICAR_Test
AVware	EICAR (v)
Ad-Aware	EICAR-Test-File (not a virus)

Moving on….

Enough about samples, what about logs

Scenario 3

Log / Event Retention

- What is your logging retention policy? 1 week, 1 month, 1 year? When the logs rotate at anytime?
- Where do you store your logs?
- Do you have a case management system?
- Do you log/store malware / potential malware?

Why is this important…

Average Detection Time for Malware?

89 – 294 Days

One time during an engagement (Detection)

A client asked us to help verify an anomaly in their user behavioural detection system.

We identified a malware beacon – but the customer responded with :

“That’s ok it’s a false positive, its always there, its expected traffic, we’re worried about X”

Turns out X was their business messaging system, and what we identified really was malware beaconing for 294 days!

How the incident was contained

- Logs contained IP address and hostname of the infected machine
- Asset log means we could track laptop to single member of staff
  - Member of staff had several laptops in their name (entire team) – but hey we can figure it out from this small pool of 5-10 laptops
  - Check all device serials against asset log to single out infected machine
- Using standard computer forensic practises, contain and image the machine
- Review image to find malicious process in start-process
- Review malware to discover that its custom malware written by a previous red-team 294 days previously!
- Why was the malware not removed, or laptop rebuilt?

Payloads – Lessons Learnt

- How many hours have been spent analyzing the wrong / completely clean malware?
- Incidents are often detected between 89 – 294 days after initial infection, could this detection time have been reduced?
- Was the malware from a red-team or real-world threat actor?
- Have you got enough logs to trace back to the original infection?

Payloads – Lessons Learnt

Always attempt to collect the sample from the original source/infected host.

Reporting….

Dealing with the Boss / Stakeholders.

Dealing with the Boss/Stakeholders can be tricky

Some of the questions asked and the mistakes we've heard:

Stakeholder (SH) : Is the situation contained are we safe?

Analyst: YES

or

You're safe

Dealing with the Boss/Stakeholders can be tricky

Some of the question ked and the istakes we've heard:

SH : Is the situation co fe?

Analyst: YES

or

You're safe

Dealing with the Boss/Stakeholders can be tricky

SH : Is the anything you have learnt from the incident or is there anything you would do differently in there near future.

Analyst: NO

Dealing with the Boss/Stakeholders can be tricky

SH : Is the anything [illegible] lea[illegible]he incident or is there anything you would d[illegible]e near future.

Analyst: NO

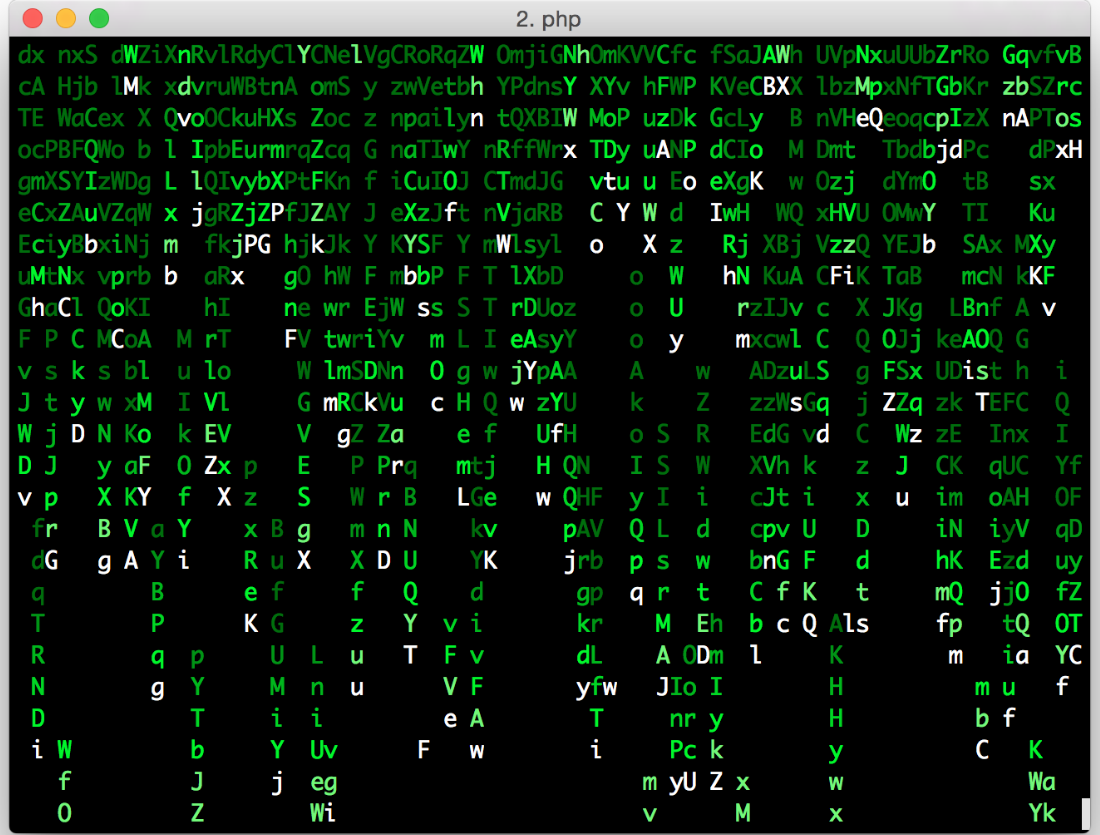
Dealing with the Boss/Stakeholders can be tricky

- Next question

Now for something more technical….

Shellcode and ToR

Shellcode



```
dx nxS dWZiXnRvlRdyClYCNelVgCRoRqZW OmjiGNhOmKVVCfc fSaJAWh UVpNxuUUbZrRo GqvfvB
cA Hjb lMk xdvruWBtnA omS y zwVetbh YPdnsY XYv hFWP KVeCBXX lbzMpxNfTGbKr zbSZrc
TE WaCex X QvoOCkuHXs Zoc z npailyn tQXBIW MoP uzDk GcLy  B nVHeQeoqcpIzX nAPTos
ocPBFQWo b l IpbEurmrqZcq G naTIwY nRffWrx TDy uANP dCIo  M Dmt  TbdbjdPc   dPxH
gmXSYIzWDg L lQIvybXPtFKn f iCuIOJ CTmdJG  vtu u Eo eXgK  w Ozj  dYmO  tB   sx
eCxZAuVZqW x jgRZjZPfJZAY J eXzJft nVjaRB  C Y W d  IwH  WQ xHVU OMwY  TI   Ku
EciyBbxiNj m  fkjPG hjkJk Y KYSF Y mWlsyl  o   X z   Rj XBj VzzQ YEJb  SAx MXy
uMtNx vprb b  aRx   gO hW F mbbP F T lXbD     o  W   hN KuA CFiK TaB   mcN kKF
GhaCl QoKI    hI    ne wr EjW ss S T rDUoz    o  U    rzIJv c  X JKg  LBnf A v
F P C MCoA  M rT    FV twriYv  m L I eAsyY    o  y    mxcwl C  Q OJj keAOQ G
v s k s bl  u lo     W lmSDNn  O g w jYpAA    A    w   ADzuLS  g FSx UDist h  i
J t y w xM  I Vl     G mRCkVu  c H Q w zYU    k    Z   zzWsGq  j ZZq zk TEFC  Q
W j D N Ko  k EV     V  gZ Za    e f   UfH    o S  R   EdG vd  C  Wz zE  Inx  I
D J   y aF  O Zx p   E   P Prq   mtj   H QN   I S  W   XVh k   z  J  CK  qUC  Yf
v p   X KY  f  X z   S   W r B   LGe   w QHF  y I  i   cJt i   x  u  im  oAH  OF
 fr   B V a Y    x B g   m n N    kv     pAV  Q L  d   cpv U   D     iN  iyV  qD
 dG   g A Y i    R u X   X D U    YK     jrb  p s  w   bnG F   d     hK  Ezd  uy
 q        B      e f     f   Q    d       gp  q r  t   C f K   t     mQ  jjO  fZ
 T        P      K G     z   Y  v i       kr    M  Eh  b c Q Als     fp   tQ  OT
 R        q  p     U  L  u   T  F v       dL    A ODm  l     K        m   ia  YC
 N        g  Y     M  n  u      V F       yfw   JIo I        H          m u   f
 D           T     i  i         e A        T     nr y        H          b f
 i W         b     Y  Uv      F   w        i     Pc k        y          C   K
   f         J     j  eg                       m yU Z x      w              Wa
   O         Z        Wi                       v      M      x              Yk
```

Shellcode

*In hacking, a **shellcode** is a small piece of code used as the payload in the exploitation of a software vulnerability. It is called "shellcode" because it typically starts a command shell from which the attacker can control the compromised machine, but any piece of code that performs a similar task can be called shellcode.*

-- Wikipedia

Shellcode – Simple Example

Shellcode

```
char code[] =
"\xe9\x1e\x00\x00\x00" // jmp 8048083 <MESSAGE>
"\xb8\x04\x00\x00\x00" // mov $0x4,%eax
"\xbb\x01\x00\x00\x00" // mov $0x1,%ebx
"\x59"                 // pop %ecx
"\xba\x0f\x00\x00\x00" // mov $0xf,%edx
"\xcd\x80"             // int $0x80
"\xb8\x01\x00\x00\x00" // mov $0x1,%eax
 "\xbb\x00\x00\x00\x00" // mov $0x0,%ebx
"\xcd\x80"              // int $0x80
"\xe8\xdd\xff\xff\xff"  // call 8048065 <GOBACK>
“\x22\x48\x65\x6c\x6c\x6f\x20\x77“
"\x6f\x72\x6c\x64\x21\x22\x0a"  // "Hello world!\n";
```

Execution

```
$ ./simple_helloworld
“Hello world!”
$
```

Shellcode

Blue-team analysts don’t necessarily understand:

- Shellcode
- File formats
- Encryption
- Encodings

Especially those level-1 analysts just starting out – they have a whole lot of learning and development ahead of them.

Cyber Chef – Cool new (and not so new) features

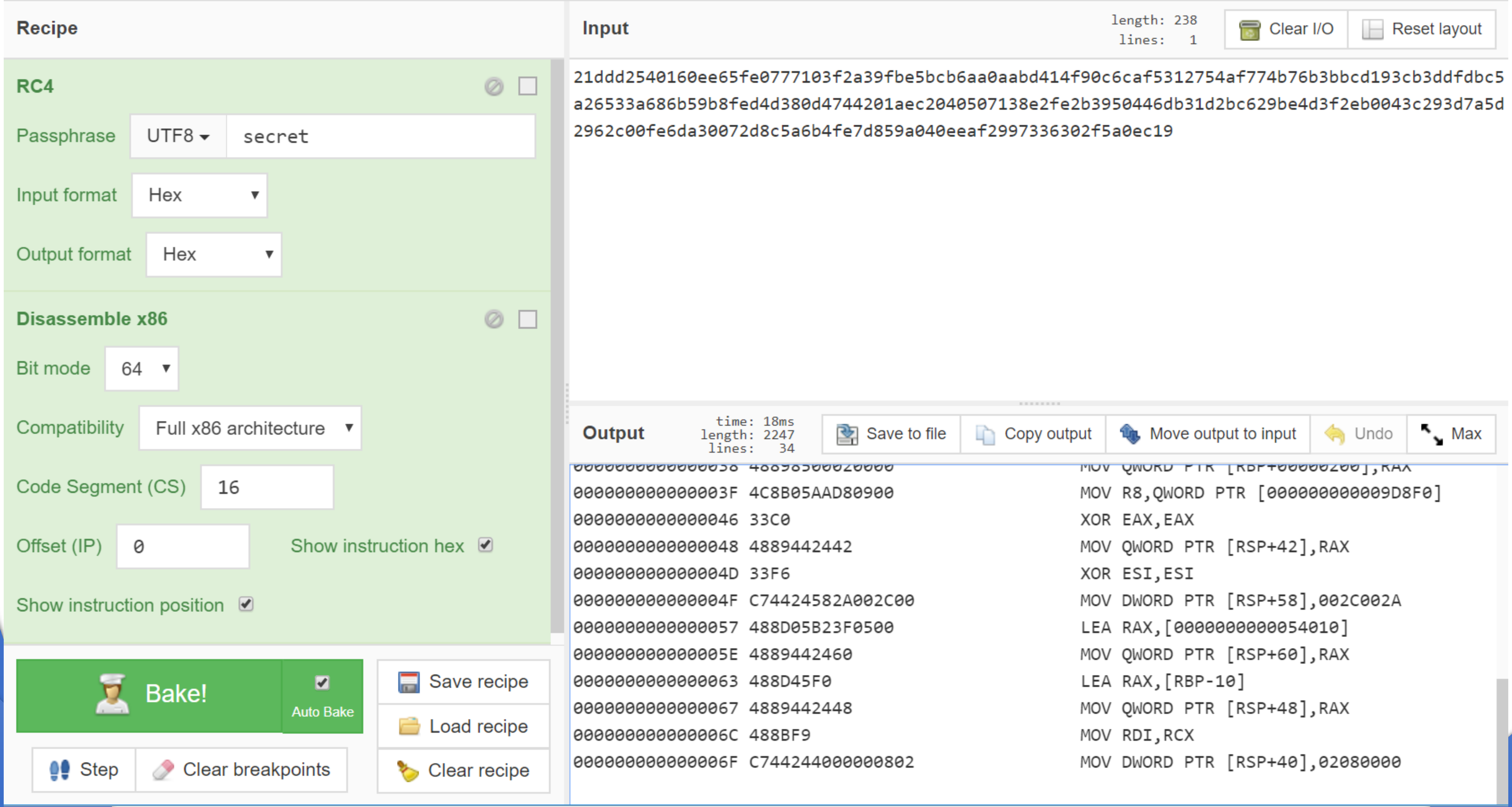
- Code tidy
- Encryption/Encoding
- Other -> Disassemble x86
- Other -> Scan for embedded files

Cyber Chef – Decoding & Disassembly

CyberChef should now have a number of operations, that enable you to build recipes to quickly decode and analyse (potential) malware.

Auto disassemble X86 : { next slide }

Useful in decompiling suspect MSF payloads!



RC4

Passphrase: UTF8 secret

Input format: Hex

Output format: Hex

Disassemble x86

Bit mode: 64

Compatibility: Full x86 architecture

Code Segment (CS): 16

Offset (IP): 0

Show instruction hex ☑

Show instruction position ☑

☑ Auto Bake

Input — length: 238, lines: 1

```
21ddd2540160ee65fe0777103f2a39fbe5bcb6aa0aabd414f90c6caf5312754af774b76b3bbcd193cb3ddfdbc5
a26533a686b59b8fed4d380d4744201aec2040507138e2fe2b3950446db31d2bc629be4d3f2eb0043c293d7a5d
2962c00fe6da30072d8c5a6b4fe7d859a040eeaf2997336302f5a0ec19
```

Output — time: 18ms, length: 2247, lines: 34

```
0000000000000038 48898500020000                       MOV QWORD PTR [RBP+00000200],RAX
000000000000003F 4C8B05AAD80900                       MOV R8,QWORD PTR [00000000009D8F0]
0000000000000046 33C0                                 XOR EAX,EAX
0000000000000048 4889442442                           MOV QWORD PTR [RSP+42],RAX
000000000000004D 33F6                                 XOR ESI,ESI
000000000000004F C74424582A002C00                     MOV DWORD PTR [RSP+58],002C002A
0000000000000057 488D05B23F0500                       LEA RAX,[000000000054010]
000000000000005E 4889442460                           MOV QWORD PTR [RSP+60],RAX
0000000000000063 488D45F0                             LEA RAX,[RBP-10]
0000000000000067 4889442448                           MOV QWORD PTR [RSP+48],RAX
000000000000006C 488BF9                               MOV RDI,RCX
000000000000006F C744244000000802                     MOV DWORD PTR [RSP+40],02080000
```

Additional Skills Needed

- Multiple High-Level Program Languages
- Low-Level Programming knowledge
- Understanding of Cryptography
- Experience working with Cryptography
- Indepth knowledge of OS Internals
  - Defensive mechanisms
  - Stacks & Memory Layout
  - Processor architecture

Malicious URLs

We may receive malicious URLs delivered via:

- phishing emails
- social media
- other media (USB, CDROM)

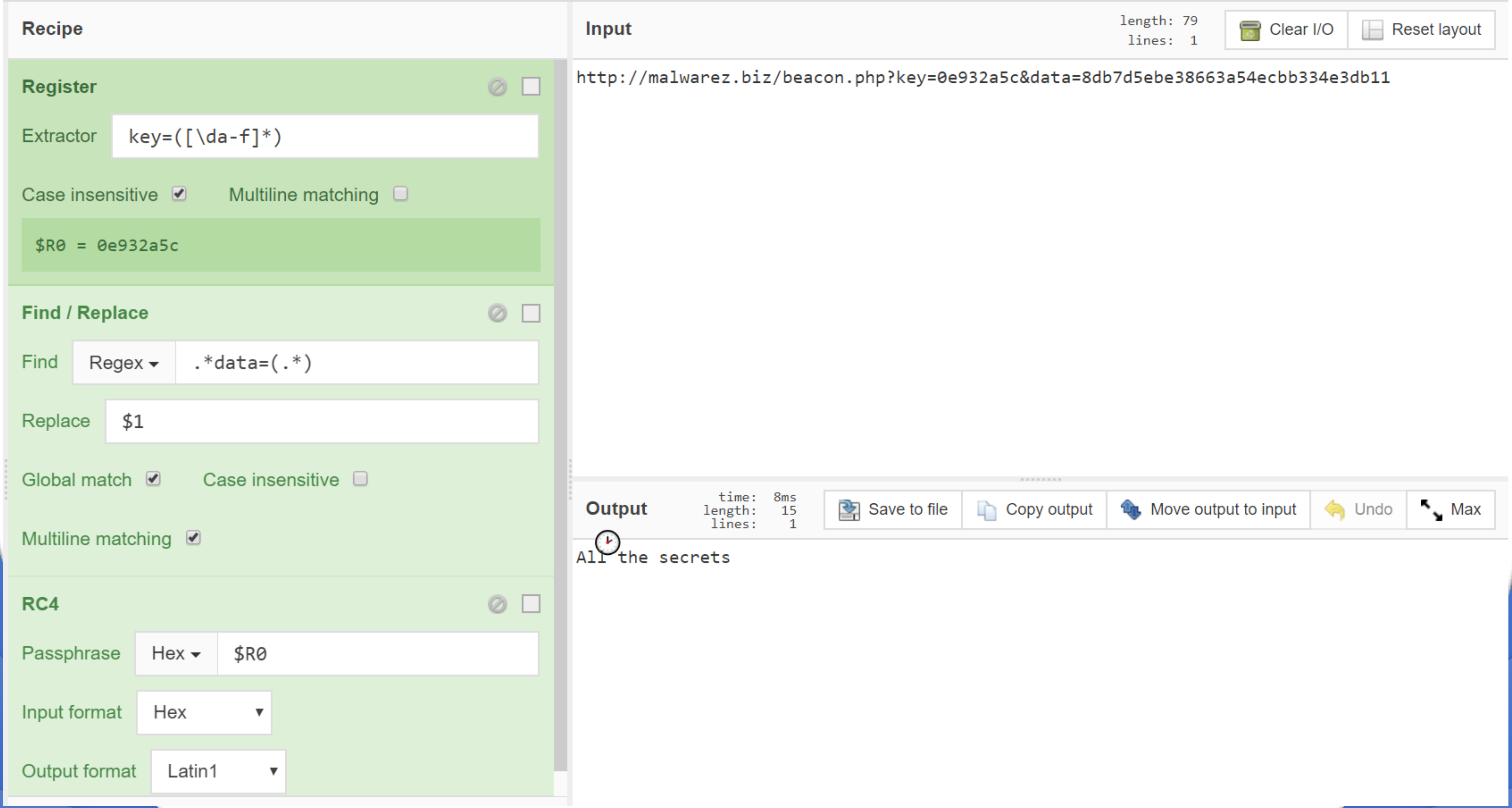
We may capture suspicious/malicious URLs via

- IDS/IPS events
- SOAR events
- Packet capture

Cyber Chef – Easy RC4 Decryption

CyberChef has some encryption transforms, and contains a very useful ‘register’ function, combine this with the regex function – for a useful recipe…

Auto-decrypt malware URLs: { next slide }



Recipe

Register

Extractor: `key=([\da-f]*)`

Case insensitive ☑ Multiline matching □

```
$R0 = 0e932a5c
```

Find / Replace

Find: Regex `.*data=(.*)`

Replace: `$1`

Global match ☑ Case insensitive □

Multiline matching ☑

RC4

Passphrase: Hex `$R0`

Input format: Hex

Output format: Latin1

Input

length: 79
lines: 1

```
http://malwarez.biz/beacon.php?key=0e932a5c&data=8db7d5ebe38663a54ecbb334e3db11
```

Output

time: 8ms
length: 15
lines: 1

```
All the secrets
```

Lessons Learnt

- Have a ticketing system to store malware, for further analysis later?
- Log and store Indicators of Compromise (IOCs), pass these onto the threat hunting team.
- Regularly update Anti-Virus, Anti-Malware controls on endpoint and perimeter devices.
- Attempt to bring sandbox technologies in-house to prevent accidental breaches.
- Train, train, and more training! You're always learning in infosec!

Other techniques that analysts may fall for?

- Base64 encoded payloads
- Polygots
- Steganography
- Alternative Datastreams
- Code samples, that import malicious packages

Distraction Techniques / Broken Code

- Bad shellcode
  - Some analysts are unable to determine the difference between good and bad shellcode
  - Distract the analysts by supplying non-functional shellcode – trust me they could be distracted for hours – possibly days.
- Also possible that the attackers broke their code when using a new obfuscation technique.

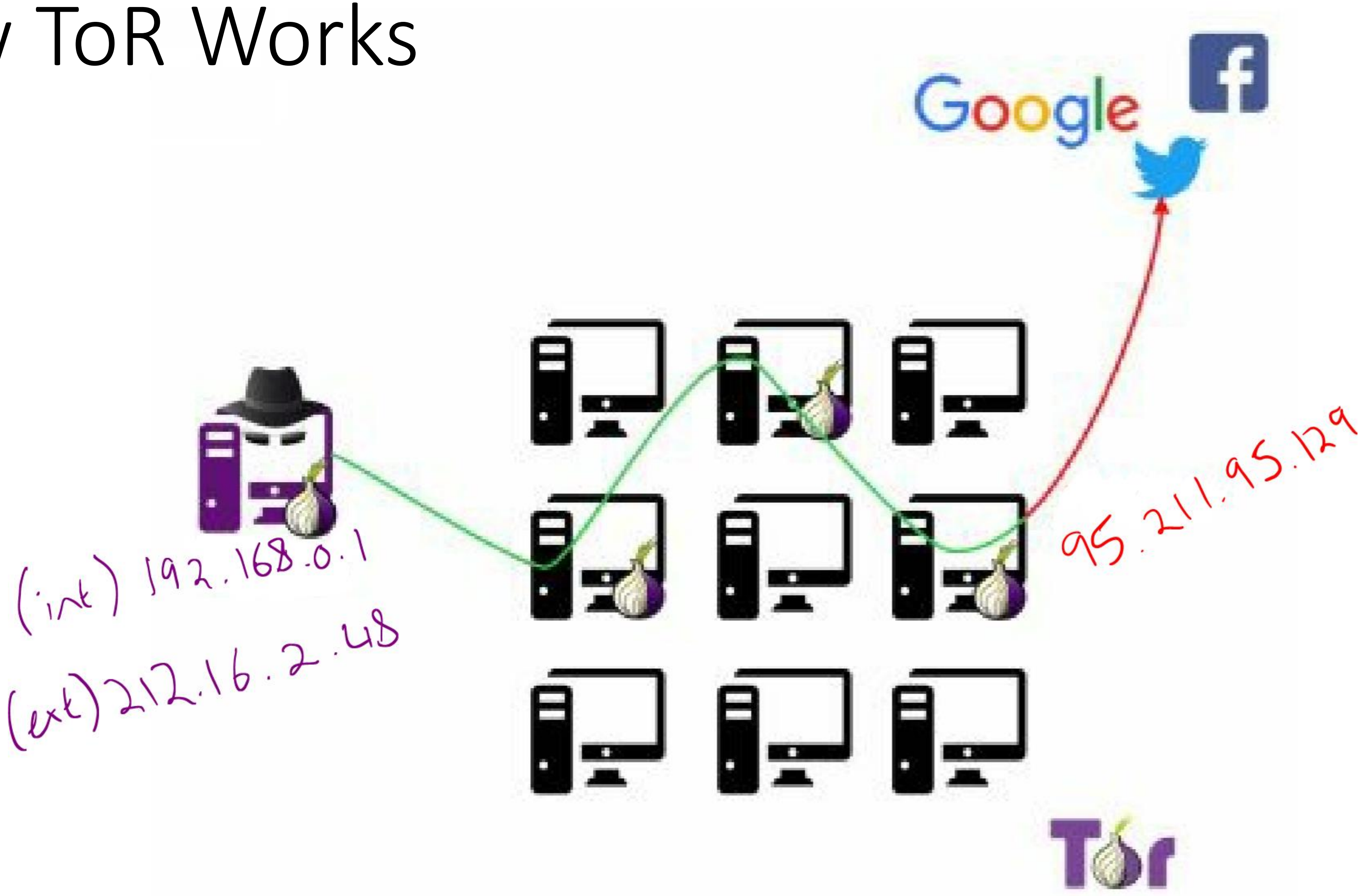
ToR – The Onion Routing

https://www.torproject.org/

Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.

-- *ToR*

How ToR Works



©2018 Netscylla

Advantages of an attacker/incident responder on ToR

Attacker/IR Perspective

- A factor of anonymity to mask their origin/identity when attacking an organisation.

Digital Defender Perspective

- A factor of anonymity when researching malware endpoints and C2.

Disadvantages of an attacker/incident responder on ToR

Attacker/IR Perspective

- A vulnerability or new technology can disclose origin IP outside of Tor.
- Misconfigured hidden services disclose other IP addresses
  - Apache /server-status
  - Tomcat /status
  - Nginx /status
- ToR is an anonymiser – not security provider.
- ToR is Slllooowwww……..

Digital Defender Perspective

- Easy to track/identify individual/organisation attacking through exploiting vulns.
- Vulnerabilities in services, disclose real Internet (External) IP
- Account information tallies to real identity in the real world.
  - SSL certs
  - Common username on forum
- Run a malicious Exit Node
  - Record all the things… but become a source of all thing

Tips on Navigating ToR/DarkWeb

It’s a sad, sad world, and unfortunately people* in addition to criminals use the ToR network (and other DarkWeb interfaces) to distribute illegal material.

- Use a console based browser: Lynx/Elinks
  - You don’t want certain graphics cached on your harddrive.
  - You don’t want certain graphics triggering ‘filters’ in your work place.
- Do not use your real personal info anyway!
  - Use proton email (or another provider) with a new custom PGP certificate!
- If you need to upload pictures/avatars/???? (why)
  - Scrub the meta-data first.

ToR and Anonymity

- ToR exit node IP addresses don’t necessarily mean your getting attacked!
- You may need to enable advanced logging procedures, to differentiate between attackers and legitimate legal ToR users.
- Some people value their privacy*, or a user might be unaware that they left ToR-proxy enabled?

Not All ToR Users Are BAD!

In Summary

- Blue Teaming doesn’t stop with the end of Red Teaming
- Blue Teaming is a never ending battle over 365 days a year
- Red Teaming – its easy to write (condemning?) report
- Blue Teaming – repeating exploit steps can be difficult? Also remediation and mitigation can be a difficult and challenging task.
- Purple Teaming - Don’t rely solely on Technology – encourage and grow the capabilities of your staff.
- False positives & false negatives sometimes happen!

Extra Time – Messing around

https://cdn.pixabay.com/photo/2017/08/13/05/08/deadline-stopwatch-2636259_960_720.jpg

Extra Time - Bonus Round

- Add to .bashrc or /etc/bashrc `sty s erase`
  - ‘s’ key now becomes backspace, just watch the chaos…
- Add to .bashrc alias=<common command>=‘echo’
  - `alias ls=‘echo’`
  - `alias cd=‘Directory not found’`
  - `alias vi=‘Could not allocate inode’`
- Download screengrab of ransomware lockscreen/wallpaper
  - Red-Team will stop in fear that you’re already infected, but be prepared for stakeholder panic!
- Containers, containers, everywhere.
  - When the red team thinks their progressing only to discover their stuck in a container? (Provided their configured correctly)
- If successfully reverse or implement their C2 comms/callback; Spoof calls, DoS their C2 endpoint, generate noise!

FIN

https://health.mil/~/media/Images/MHS/Photos/acoustics.ashx?h=428&la=en&mw=720&w=720