



# Attacker Ghost Stories



Mostly free defenses that give attackers nightmares

# About me...

Mubix “Rob” Fuller

- Father
- Husband
- NoVA Hacker
- Marine



**Why are we here?**





# EMET (Enhanced Mitigation Experience Toolkit)



## What is EMET?

- <http://www.microsoft.com/emet>
- Think of it like a big bouncer that protects any kind of memory funny business, but only for things you tell it to protect
- Deployable by GPO
- Logs
- **FREE**





# What about EMET bypasses?

A movie poster for 'Bypassing All of the Things' featuring Aaron Portnoy. The background shows a man in a green cardigan looking up at a large, complex, metallic structure. The title 'BYPASSING ALL OF THE THINGS' is written in large, white, outlined letters. Below the title, the name 'Aaron Portnoy' is listed, followed by his title 'VP of Research' and company 'Exodus Intelligence'. Social media and contact information are provided at the bottom right of the poster. The Exodus Intelligence logo is in the bottom left corner.

**BYPASSING  
ALL OF THE THINGS**

Aaron Portnoy  
VP of Research  
Exodus Intelligence

Twitter: @aaronportnoy  
E-Mail: aaron @exodusintel.com

**EXODUS  
INTELLIGENCE**



<http://goo.gl/QrJZdd>

# Another good resource about EMET

<http://goo.gl/ELIBSi>



EMET 4.1 Uncovered 0xdabbad00

---

## EMET 4.1 Uncovered

@0xdabbad00 (Dabbadoo)



[0xdabbad00.com](http://0xdabbad00.com)  
2013-11-18

<b>Introduction</b>	<b>2</b>
Limitations of this paper . . . . .	2
Download . . . . .	2
History . . . . .	2
<b>General notes</b>	<b>3</b>
Design of the . . . . .	3





# Block Java UA at the Proxy

- Java apps (exploits) require the use of Java, which uses it's own User-Agent

## STEP 1



# Internet Explorer User Agent

Mozilla/4.0 (compatible; MSIE 8.0;  
Windows NT 6.1; WOW64;  
Trident/4.0; SLCC2; .NET CLR  
2.0.50727; .NET CLR 3.5.30729;  
.NET CLR 3.0.30729; Media Center  
PC 6.0; MS-RTC LM 8; InfoPath.3;  
.NET4.0C; .NET4.0E)  
chrome/8.0.552.224



# Block Java UA at the Proxy

Examples:

JNLP/6.0 **javaws**/1.6.0\_29

**Java**/1.6.0\_26

Mozilla/4.0 (Windows 7 6.1)

**Java**/1.7.0\_45



# Block Java UA at the Proxy

- Java apps (exploits) require the use of Java, which uses its own User-Agent

## STEP 2

Follow TCP Stream

Stream Content

```
GET /forum/links/column.php?yf=1j:1h:2w:1g:1k&xe=2v:1k:1m:32:33:  
User-Agent: Mozilla/4.0 (Windows 7 6.1) Java/1.7.0_10  
Host: demoralization.ru:8080  
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2  
Connection: keep-alive
```

# Block Java UA at the Proxy

○ Java apps (exploits) require the use of Java, which uses its own User-Agent

## STEP 3

This never happens if they can't pull the code!



# Block Java UA at the Proxy

- Java apps (exploits) require the use of Java, which uses it's own User-Agent
- Pull a report of every domain your users went to using the Java User-Agent. Parse the list and make them the exclusions.
- **FREE**
- Stops java exploits loaded by a browser.
- Attacker cannot modify UA pre-exploit

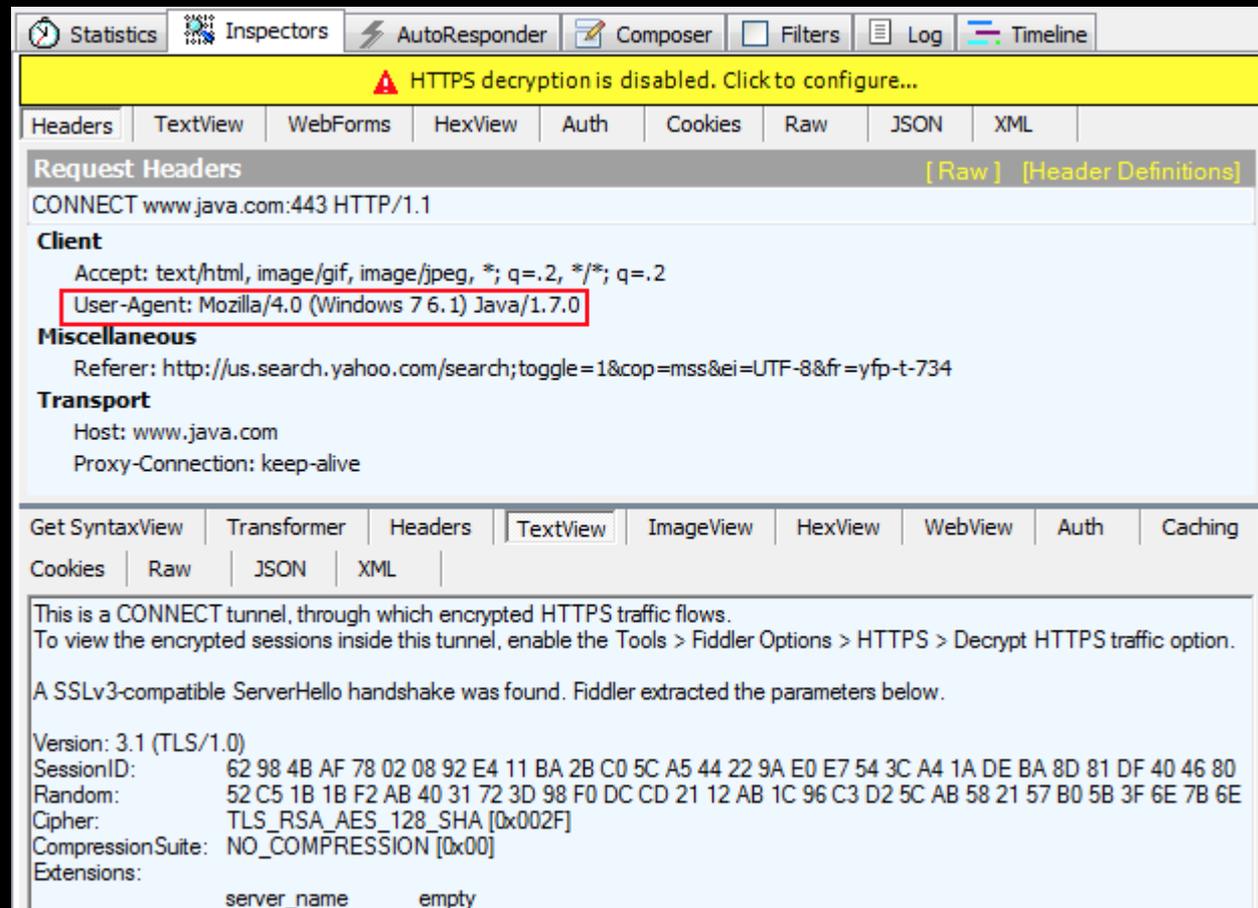


# Update: Block Java UA at the Proxy

And according to “Z” this works for SSL too



<http://goo.gl/4mtwqN>



Statistics Inspectors AutoResponder Composer Filters Log Timeline

⚠ HTTPS decryption is disabled. Click to configure...

Headers TextView WebForms HexView Auth Cookies Raw JSON XML

**Request Headers** [Raw] [Header Definitions]

CONNECT www.java.com:443 HTTP/1.1

**Client**

Accept: text/html, image/gif, image/jpeg, \*, q=.2, \*/\*; q=.2  
User-Agent: Mozilla/4.0 (Windows 7 6.1) Java/1.7.0

**Miscellaneous**

Referer: http://us.search.yahoo.com/search;toggle=1&cop=mss&ei=UTF-8&fr=yfp-t-734

**Transport**

Host: www.java.com  
Proxy-Connection: keep-alive

Get SyntaxView Transformer Headers TextView ImageView HexView WebView Auth Caching

Cookies Raw JSON XML

This is a CONNECT tunnel, through which encrypted HTTPS traffic flows.  
To view the encrypted sessions inside this tunnel, enable the Tools > Fiddler Options > HTTPS > Decrypt HTTPS traffic option.

A SSLv3-compatible ServerHello handshake was found. Fiddler extracted the parameters below.

Version: 3.1 (TLS/1.0)  
SessionID: 62 98 4B AF 78 02 08 92 E4 11 BA 2B C0 5C A5 44 22 9A E0 E7 54 3C A4 1A DE BA 8D 81 DF 40 46 80  
Random: 52 C5 1B 1B F2 AB 40 31 72 3D 98 F0 DC CD 21 12 AB 1C 96 C3 D2 5C AB 58 21 57 B0 5B 3F 6E 7B 6E  
Cipher: TLS\_RSA\_AES\_128\_SHA [0x002F]  
CompressionSuite: NO\_COMPRESSION [0x00]  
Extensions:  
server\_name empty

# Block Java UA at the Proxy

Oh yea, it protects Macs too...





# Logging / Vuln Scanning / AV / HIPS

- **PWDump** removed on an internal **IIS** box doesn't mean the job is done.
- Logon alerting - **ADAudit Plus** (only product in this presentation simply because I can't find anyone else who does it) (**Netwrix?**)
- HIPS (enable the **prevention** part)
- Vuln Scanning is what a tool does. Lets start **Vuln Reporting**.
- Get your pentester/red team involved!





# Crowdsourcing Security

Security Incident / Phishing Incentive Program

- Reward “top” users for reporting malicious or “phishy” content.
- Make a big deal out of it (company / section wide emails)
- Every employee becomes an IDS
- Quarterly “Think Evil” games



# Crowdsourcing Security

## Internal Bug Bounty Program

- Developers Developers Developers ....
- Incorporate the entire company though, if anyone reports a bug in a system they don't own, they'll be entered in the bounty.
- Make it **EASY**
- Payout in gift cards instead of incident response and forensics





# Port-forwarding Honeypots

If you have public IP space, **use it.**

1. Spin up a VPS (Like Linode)
2. Add vulnerable looking software to the VPS
3. Install snort / other sensor on the VPS
4. Port forward 80, 1433, etc on your IP to the VPS via your firewall.
5. Watch as attacks roll in without endangering your infrastructure at all.

**Note:** Don't share passwords from real infrastructure to VPS.





# WPAD

My \_favorite\_ vulnerability:



# WPAD

- Make null routed (127.0.0.1) DNS entry for WPAD
- Make null routed (:::1) for DNS entry WPADWPADWPAD
- Disable NetBIOS resolution domain wide. Your DNS servers can handle it.
- It's also a privacy concern NetBIOS traffic is broadcasted to everyone
- **FREE**





# DNS

- There is no reason a user needs to resolve Google.com internally
- Let your web proxies do all the DNS
- **FREE**
- Turn off forward lookups on your internal DNS servers.
- Point your proxies at DNS servers that only they are allowed to use.





# Dump your own hashes!

Your passwords suck

- One of these passwords almost always works...

password[1]

Passw0rd[1]

Password[1]

\$Company[1-10]

Password123

\$Company123

welcome1

changeme123

welcome123

p@ssw0rd[1]

Username123

p@ssw0rd123

\$Season\$Year

Welcome\$YEAR



# Dump your own hashes!



## ○ Crackers

- John the Ripper
- Rockyou.txt

## ○ Dumpers

- Depends...
- Goes back to the, “don’t use code you don’t trust”.
- List by Bernardo Damele - <http://goo.gl/wDpJHc>
- Ask your Pentesters/Red Teamers to do the dump and maybe even the audit. They will jump at it.
  - (under supervision)





# Authenticated Splash Proxies

- Use a web form with fields other than “username=” and “password=”
- Block all “uncategorized”
- Splash page requirement (every domain is blocked every day, first person to go to the page is shown a big red button that says “approve this domain”) any automated C2 **will fail.**



# Authenticated Splash Proxies



THIS DOMAIN HAS BEEN BLOCKED!  
Don't worry, this could be the first time today  
someone is attempting to go there. Click on  
"UNBLOCK" to ALLOW THIS DOMAIN  
THROUGH

UNBLOCK

BLOCK





# Evil Canaries

- Domain User called “DomainAdmin\_Temp” with password in the description, and actually in Domain Admins group. Logon hours was 0. **CAUGHT**
- Public share called “Password Audit 2014”, EXLS docs about 4 MB, but “Everyone:Deny” permission. **CAUGHT**
- Computer called BACKUPDB, with out of date version of MySQL on Windows. **CAUGHT**



# Evil Canaries

- Web developer made .htaccess file forward common scanner (ala /nikto.html) requests to custom 402 (Payment Required) page, correlated hits and alerted. **CAUGHT**
- Credit card database:  
<http://www.getcreditcardnumbers.com/>  
**CAUGHT**
- VPN main page edited to include “default” credentials in HTML source. **CAUGHT**



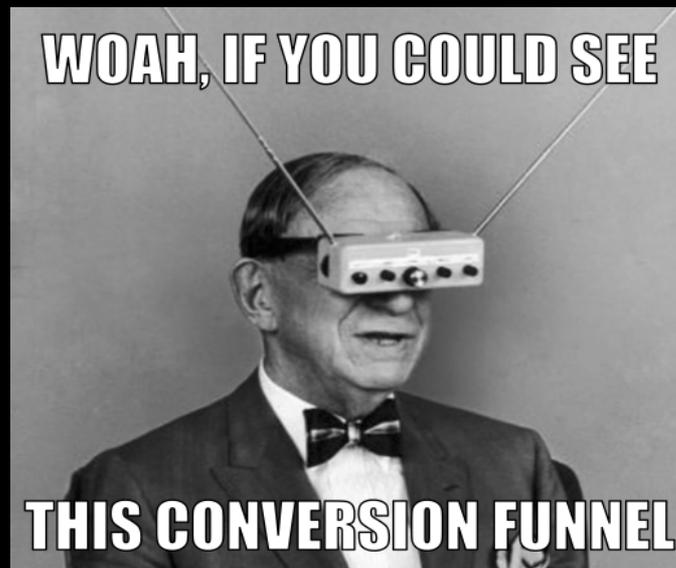
# Evil Canaries

- Web server had /admin/login.html and supposedly tied to AD which always returned “SUCCESS” but didn’t do anything except, report what creds were used, browser and IP information. **CAUGHT**
- Machine that does absolutely nothing, saw traffic to port 23 (not listening). **CAUGHT**



# Tell your helpdesk!

- Most of your actionable security alerts go through your helpdesk.
- Stop leaving them out of the loop.





# Thank you

- The countless people who listened to me practice this talk ahead of time in prep for today.



# Contact Me

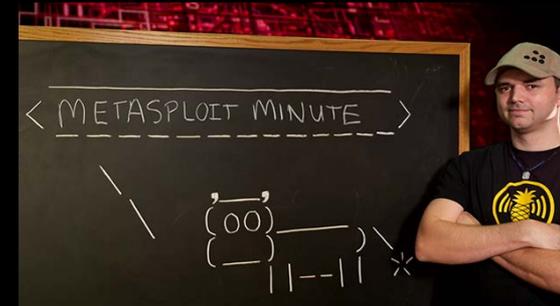
Rob Fuller

@mubix

Blog - <http://www.room362.com/>

Wiki - <http://pwnwiki.io/>

Email - [mubix@hak5.org](mailto:mubix@hak5.org)



# Appendix I - Psychology

The attacker is on your turf. Hackers freeze when they think they are caught. Nation states have “visibility assessment protocols” that take time. The more you can cause a visibility score to go up either by perceived or actual detection will cause more intelligence opportunities on the defence side.



# Appendix II - Other free wins

- Monitor anything that is tied to AD and is accessible from the Internet. OWA / MDM / SharePoint / VPN, or your web site.
- Baseline internal network traffic. Spider patterns mean scanning.
- MAC addresses that aren't in the same OUI class should be investigated.  
(DELL/HP/Wewei)



## Appendix II - Other free wins

- Allow users a way to specify when they are on vacation. Or integrate your vacation system with the authentication alerting system. If the user isn't there, there shouldn't be authenticating to anything be email and maybe the VPN for you workaholics.

