Suricon:
EKs and Cuckoo and things

Will (Not a Rockstar) Metcalf
Emerging Threats
Introduction

• What I'm not...
  – A rockstar. (tks Kelly)
  – A good public speaker. I'm unsure why they keep inviting me back.

• What I am...

  – An analyst who writes NIDS, Cuckoo, ClamAV, Yara sigs, main focus on exploit kits. We employee Kafeine, I’m Alfred to his Batman.

  – OISF Co-founder? I was there in the beginning anyway :)

  – ET Research team ornament. Pretty sure they just keep me around because I'm pretty …
Emerging Threats

- Acquired by ProofPoint in 2015.
- Longtime open source (BSD license) and commercial IDS rule feeds for Snort® and Suricata.
- Commercial IP rep and Intel feed and query products.
- Malware sample exchange/research portal for vetted companies/researchers.
- Shared zombie infrastructure for small community of exploit kit researchers.
- Awesome community of contributors/researchers
- Purveyors of fine Twitter imagery @ET_Labs
- Join the fight here: http://lists.emergingthreats.net/mailman/listinfo/emerging-sigs
Exploit Kit Basics

- Generally take advantage of known/patched bugs in browser and plugins. Sometimes 0-days, as observed in Sednit EK (APT28) recently.
- Most end users won't notice they are pwn'd unless ransomware is dropped.
- Exploit kits are reached via malvertising, spam campaigns, compromised web servers, watering holes, and clickbots, to name a few.
- Various RATS, Trojans, Ransomware are dropped by exploit kits
http://www.kahusecurity.com/2016/wild-wild-west-112016/
Exploit Kit History

› Many have entered and exited the scene over the years... Few remain today.
› For a few years it seemed like there was a never-ending supply of fresh exploits in Internet Explorer and its plug-ins, Flash, Java, Silverlight, etc.
› Most challenging adversary in my tenure has been Angler. Fresh exploits, innovation in delivery/encoding. Targeting/break rate was good. One-offs such as HanJuan/Angler VIP EK etc.
› There have been other innovators in the past.
Exploit Kits Today

• Lurk arrests were the end of Angler and its variants. The ecosystem has struggled to recover. Definite lack of quality/innovation/freshness.
• Angler absence seems to have forced innovation and one-offs in other kits that historically had little movement. All that is old is new again.
• Lack of fresh exploits. Recycled/ripped exploits. No honor among thieves.
• Today: DNS Changer, KaiXin, Neutrino-v, RIG (and variants), SunDown (and variants), Astrum, Sednit, Magnitude (and variants).
Exploit Kits Future

- Browsers and underlying operating systems are becoming harder to exploit. Generally no longer a single exploit but a chain of them to elevate priv's, escape sandbox, etc. required.
- Historically vulnerable plug-ins are also getting better or are dying off, Java/Silverlight, etc. Lack of new exploits entering the ecosystem.
- Breakrate for existing exploits continues to decline as AV catches up. Recycled exploits in mem and addition of fancy anti-exploit feature sets to commodity AV.
- As things get harder to exploit I wonder if we will see a major shift to massive social engineering click-to-pwn campaigns commonly used by Maldocs/Adware/Crapware today.
- Move to SSL/TLS. With Let's Encrypt it's SSL for everybody. You can even DGA a bit as Let's Encrypt supports SAN’s and treats some DynDNS's second levels as TLD's :(.}
Why so much effort in sigging EKs instead of just vulns?

- Browser bugs that can be triggered via JS and DOM are easy to hide and hard to detect on the wire.
- Java/Silverlight vulns are generally exploited via zips containing MSIL/Java bytecode inside of class files/dll's, i.e., byte soup from the wire. (Don’t know if a single live EK using Java Exploits these days)
- Adobe Reader/Flash also have access to JS and compression within the file format itself, i.e., compressed flash/encryption/flash inside of flash. Reader with various encodings/compression JS objects.
- New droppers, Trojans, 0-days. Kaf and I found CVE-2016-3298 this way.
- Dealing with some of these issues using Suricata+Lua. If compression or structure iteration is involved, detection can be unreliable due to nature of sliding window inspection

https://github.com/EmergingThreats/et-luajit-scripts
Why Do we want to study Eks in a Sandbox.

- IDS hits may be from non-vulnerable clients. But there is always the weakest gazelle in the herd. (Patching is hard.)
- Plug-in Detect used to identify software on target so you get different exploits depending on software and version or none at all.
- Avoidance of trying to infect systems running common AV suites, EMET, or that lack common software stacks.
- Host introspection, Hooking of key browser functions.
- Select Your Geo.
- Kill chain from start to finish.
Solution: Cuckoo Sandbox

- Native functions and Windows API calls traces
- Copies of files created and deleted from the filesystem
- Dump of the memory of the selected process
- Full/Process memory dump of the analysis machine.
- Screen shots of the desktop during the execution of the malware analysis
- Network dump generated by the machine used for the analysis

Highlights above quoted from:
http://www.cuckoosandbox.org/
Cuckoo Cocktail for Suricata Sig Writers

https://github.com/spender-sandbox/cuckoo-modified
https://github.com/spender-sandbox/community-modified
https://github.com/wmetcalf/buildcuckoo-trusty
Problems we face using Cuckoo for analysis

- A majority of Trojans/Droppers have anti-* checks
- Exploit kit anti-analysis: IP connection limits/black listing, GeoIP targeting.
- Finding exploit kits to analyze -> sig
Anti-* Checks

• Malvertisers/EKs attempt to use information disclosure vulnerabilities in IE to determine the presence of local files. Many of the payloads will also perform anti-* checks once dropped/executed.


• VMCloak
  • [http://vmcloak.org/](http://vmcloak.org/)

• Use the scripts included with my Cuckoo builder.
  • [https://github.com/wmetcalf/buildcuckoo-trusty/blob/master/createVBox*.py](https://github.com/wmetcalf/buildcuckoo-trusty/blob/master/createVBox*.py)
  • [https://github.com/wmetcalf/buildcuckoo-trusty/tree/master/guest](https://github.com/wmetcalf/buildcuckoo-trusty/tree/master/guest) (in guest scripts)

• Doomed Raven for KVM

• Thin Provision a large HD, add more than one CPU to the VM.

• Fake Video Drivers, Install VLC, Bittorrent client etc. Make your machine look “real.”

• Pafish to test your progress. [https://github.com/aOrtega/pafish](https://github.com/aOrtega/pafish)
<table>
<thead>
<tr>
<th>Address</th>
<th>Function</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x6ce7aa5b 0x6ce7a982</td>
<td>InternetCrackUrlW</td>
<td>mhtml:file://progra-1/malwar-1</td>
</tr>
<tr>
<td>0x6ce7aa5b 0x6ce7a982</td>
<td>InternetCrackUrlW</td>
<td>mhtml:file://progra-1/malwar-1</td>
</tr>
<tr>
<td>0x6ce7aa5b 0x6ce06d34</td>
<td>InternetCrackUrlW</td>
<td>mhtml:file://progra-1/malwar-1</td>
</tr>
<tr>
<td>0x6ce7aa5b 0x6ce7a982</td>
<td>InternetCrackUrlW</td>
<td><a href="http://adsfranchise.com/">http://adsfranchise.com/</a></td>
</tr>
<tr>
<td>0x6ce7aa5b 0x6ce7a982</td>
<td>InternetCrackUrlW</td>
<td>mhtml:file://progra-1/kasper-1</td>
</tr>
<tr>
<td>0x6ce7aa5b 0x6ce7a982</td>
<td>InternetCrackUrlW</td>
<td>mhtml:file://progra-1/kasper-1</td>
</tr>
<tr>
<td>0x6ce7aa5b 0x6ce06d34</td>
<td>InternetCrackUrlW</td>
<td>mhtml:file://progra-1/kasper-1</td>
</tr>
<tr>
<td>0x6ce7aa5b 0x6ce7a982</td>
<td>InternetCrackUrlW</td>
<td><a href="http://adsfranchise.com/">http://adsfranchise.com/</a></td>
</tr>
<tr>
<td>0x6ce7aa5b 0x6ce7a982</td>
<td>InternetCrackUrlW</td>
<td>mhtml:file://progra-1/proxif-1</td>
</tr>
<tr>
<td>0x6ce7aa5b 0x6ce7a982</td>
<td>InternetCrackUrlW</td>
<td>mhtml:file://progra-1/proxif-1</td>
</tr>
<tr>
<td>0x6ce7aa5b 0x6ce06d34</td>
<td>InternetCrackUrlW</td>
<td>mhtml:file://progra-1/proxif-1</td>
</tr>
<tr>
<td>0x6ce7aa5b 0x6ce7a982</td>
<td>InternetCrackUrlW</td>
<td><a href="http://adsfranchise.com/">http://adsfranchise.com/</a></td>
</tr>
<tr>
<td>0x6ce7aa5b 0x6ce7a982</td>
<td>InternetCrackUrlW</td>
<td>mhtml:file://progra-1/suricata</td>
</tr>
<tr>
<td>0x6ce7aa5b 0x6ce7a982</td>
<td>InternetCrackUrlW</td>
<td>mhtml:file://progra-1/suricata</td>
</tr>
<tr>
<td>0x6ce7aa5b 0x6ce7a982</td>
<td>InternetCrackUrlW</td>
<td>mhtml:file://progra-1/suricata</td>
</tr>
<tr>
<td>0x6ce7aa5b 0x6ce06d34</td>
<td>InternetCrackUrlW</td>
<td><a href="http://adsfranchise.com/">http://adsfranchise.com/</a></td>
</tr>
<tr>
<td>0x6ce7aa5b 0x6ce7a982</td>
<td>InternetCrackUrlW</td>
<td>mhtml:file://progra-1/winpcap</td>
</tr>
</tbody>
</table>
## Anti-* Checks Neutrino-v

### Full Dump Information

<table>
<thead>
<tr>
<th>Process Name</th>
<th>iexplore.exe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executable Path</td>
<td>C:\Program Files\Internet Explorer\iexplore.exe</td>
</tr>
<tr>
<td>Yara</td>
<td>Match: CVE_2016_3298_Mem -</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 17.0.0\kas_engine.dll/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\Wireshark\wireshark.exe/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\Kaspersky Lab\Kaspersky Total Security 17.0.0\kas_engine.dll/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\arch%\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\ushata.dll/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\VMware\VMware Tools\deploy\pkg.dll/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\Kaspersky Lab\Kaspersky Small Office Security 17.0.0\kas_engine.dll/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\arch%\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows SP2\ushata.dll/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\arch%\FFDec\Uninstall.exe/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\arch%\Kaspersky Lab\Kaspersky Small Office Security 15.0.2\kas_engine.dll/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\arch%\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows SP1\ushata.dll/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\arch%\Wireshark\wireshark.exe/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\arch%\Fiddler2\uninst.exe/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\Kaspersky Lab\Kaspersky Small Office Security 15.0.2\kas_engine.dll/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\arch%\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows SP1\ushata.dll/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows SP2\ushata.dll/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\Kaspersky Lab\Kaspersky Internet Security 17.0.0\kas_engine.dll/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\Kaspersky Lab\Kaspersky Small Office Security 17.0.0\kas_engine.dll/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\ESET\ESET NOD32 Antivirus\gui.exe/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\Oracle\VirtualBox Guest Additions\VBoxDisp.dll/#1</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\ushata.dll/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\Bitdefender\Agent\Product\AgentService.exe/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows SP3\ushata.dll/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\arch%\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows SP3\ushata.dll/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\arch%\Kaspersky Lab\Kaspersky Internet Security 17.0.0\kas_engine.dll/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\arch%\Kaspersky Lab\Kaspersky Anti-Virus 17.0.0\kas_engine.dll/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\Quick Heal\Quick Heal Internet Security\NTSYS.dll/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\FFDec\Uninstall.exe/#2</td>
</tr>
<tr>
<td></td>
<td>res://C:\Program Files\arch%\Kaspersky Lab\Kaspersky Total Security 17.0.0\kas_engine.dll/#2</td>
</tr>
</tbody>
</table>

### Full Dump

- Download

### Process Strings

- Download
Exploit kit IP based anti-analysis

- Some exploit kits have connection limits such as a single IP visiting in a 24-hour period.
- Some have blacklists and modes for discovering analysts after campaigns end.
- Restrict access from networks such as Tor.
- Some require Referer. Upper must be search engine or in some cases specific site.
- GeoIP targeting.
- Extreme filtering: Only serve up landings and exploits to U.S.-based residential IP blocks. Or filtering of IPs belonging to hosting providers and cloud services.
Tor

- The Good:
  - IP addresses change on their own, frequently and from diverse geographical locations.
  - Can specify geo location of exit to take via “StrictExitNodes 1 ExitNodes {us}”
  - Cost: free

- The Bad:
  - No UDP over Tor (with the exception of DNS). Make sure you drop/otherwise handle in routing.
  - Many EKs and redirectors filter all exit nodes.
  - Frequently used by researchers, so somebody might have burned the exit node IP already in the timeout window.
  - Nice for analyzing payloads. Not so great for analyzing EKs.

https://www.torproject.org/
Commercial VPN Services

The Good:
- Full IP VPN. You can tunnel everything. Get one or many that support OpenVPN.
- Cheap. Generally no bandwidth caps/limitations.
- Fast IP swap. Simply connect vpn to different server.
- Most allow you to choose the GeoIP region to exit from.
- Have a lot of IP space to go around. HMA advertises 120,000+ IP addresses in 190+ countries
- Examples: HideMyAss, Private Internet Access, IPVanish, PureVPN, many more

The Bad:
- Cost?
- Accounting can be a problem for these services if using for frequent IP rolls. HMA advertises two simultaneous connections, but connect/disconnect have to be ~5 minutes apart.
- Make sure you tell them you are a researcher and your use aligns with their TOS.
- In the past we had great luck with these. Harder to use now. Many redirectors/EKs seem to be filtering on “DataCenter” connections as well.
Cloud Servers

 ➔ The Good:
 ➔ Examples: EC2, Vulture, Azure.
 ➔ With flux in EC2, you probably will get a fresh IP address by restarting an instance.
 ➔ EC2 is easily scriptable with boto and an instance running Openvpn.
 ➔ Vultr has diverse geographic locations, also cheap.

 ➔ The Bad:
 ➔ Cost. Expensive compared to commercial VPN providers. Heavy usage can cost you (bandwidth).
 ➔ Slow. Restarting EC2 instances can take quite a bit of time. Plan for downtime between instance restarts. Multiple instances always an option. Vultr is worse; once you provision a server you are stuck with an IP. Have to provision from snapshots and destroy old.
 ➔ Filtering of these services.

http://aws.amazon.com/ec2/
https://www.vultr.com/
Cheap VPS's (a lot of them)

➤ The Good:
➤ Cheaper than EC2/Vultr. More control than with commercial VPN.
➤ Did I mention cheap? Chicago VPS: Buy a server for $1 a month.
➤ Not limited to a handful of providers or geos. Pick and choose.

➤ The Bad:
➤ Quality varies greatly. Reviews at lowendbox.com
➤ Some don't enable TUN/TAP support in OpenVZ (required for OpenVPN), etc. Make sure this functionality is an option before purchase.
➤ You are stuck with a static IP once it's provisioned. (If your IP is burned you can turn it into a honeypot.)
Whatever you do, redirect or block SMTP

- VPN Providers and EC2 don't like when their IP addresses get blacklisted. Not a lot of evil is performed in the automated analysis time-frame with the exception of spam.
- Transparently redirect SMTP traffic to an INetSim instance running on your router or VM network. Study spam campaigns without sending out spam.
- Having INetSim VM running and configured to accept all traffic to InetSim is a good idea. Analyze malware samples where the C2 may be down and/or no longer exists. Malware may at least give up client side C2 coms in these cases.

Dear EC2 Customer,

You recently reached a limit on the volume of email you were able to send out of SMTP port 25 on your instance:

http://www.inetsim.org/index.html
Yes, but how do I get samples to replay
Without a Zorg Zf-1?

One shot...and replay sends every
following shot to the same location.
Yes, but how do I get samples to replay?

- IDS, AV, spam traps, and HTTP and logs from your own network.
- No enterprise-sized network to extract data from? No problem. Plenty of free and open sources
  - @malware_traffic http://www.malware-traffic-analysis.net/
  - @threatglass http://www.threatglass.com/
  - @broadanalysis http://www.broadanalysis.com/
  - @kafeine
  - @Oddly_Normal http://malwarebreakdown.com/
- Your vertical has a trust group. Join it :). Or the myriad general vetted trust groups.
- PAN published a list of PDarkleech compromised sites. Many of them are still pwn'd. https://raw.githubusercontent.com/pan-unit42/iocs/master/angler/compromised_domains
- Ask me.
More on NIDS and Cuckoo

- I created a tool called “Shrike.” A shrike is a bird that impales its prey on barbed wire or tree branches to pick apart later.
- Similar goal for replaying and analyzing EKs in near real time.
- Using Suricata's json output to log http and alert data into a unified file.
- Correlates alerts we are interested in. Matches http logs by hashing either based on ip pair, or 5 tuple. Shrike submits a url task to cuckoo in near real time using the referer, matching url, or landing page. Needs optimization to use redis for lookups, flowid's etc. also download and detonation of exe content etc.
- The submitted url along with the upper referer, signature id and signature msg are then stored in the Cuckoo db and are search-able within the ui.

https://github.com/EmergingThreats/shrike
The Shrike.
Everybody Steals RC4 Encryption key shared by RIG/SunDown/KaiXin
From ClamAV to suri sigs WordJS->GreenFlash SunDown

Signatures

Clamav Hits in Target/Dropped/SuriExtracted

suri_extracted: clamav:MiscreantPunch.SWF.WordJS.FlashRedir.UNOFFICIAL, sha256:5f958701ecda3ad94f21371007045168b5b33ba3a5346a2462a636010a253ec0, (compressed), version 32

suri_extracted: clamav:MiscreantPunch.SWF.Huer.LBCAPNOFXLV.UNOFFICIAL, sha256:a29a646062a9oc2e6977d4174fbc5035c2a0d1fe8d99ca9b7712331956bcoafa92, type:Macromedia Flash data (compressed), version 32

Created network traffic indicative of malicious activity

signature: ETPRO CURRENT_EVENTS Possible Bizarro SunDown Payload
signature: ET EXPERIMENTAL (data) download with high entropy after plugin file download
signature: ET EXPERIMENTAL PE EXE or DLL binary after plugin file download
signature: ETPRO CURRENT_EVENTS Bizzaro SunDown EK Payload Oct 28 2016 M1

dp:38577, ua:Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko, uri:/es2013/www/images/1x1.swf, referer:http://?

dp:45650, ua:Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko, uri:/index.php?advbannerid=21, referer:http://?

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ETPRO CURRENT_EVENTS GreenFlash SunDown EK Flash Exploit"; flow:established,to_server; content:"?advbannerid="; http_uri; nocase; fast_pattern; content:"/adv.swf"; nocase; http_header; pcre:"/^Referer\x3a[^r\n]*/adv\x2e.swf(?:(?x3a)d\{1,5})?r$/Hi"; pcre:"/^([^\&=?]+)?advbannerid=d{2}$/Ui"; classtype:trojan-activity; sid:2823077; rev:2;)

coz@3d8:/storage/Downloads/clam-punch5 /clamdigger.py --target 11 -wall-s "MiscreantPunch.SWF.WordJS.FlashRedir" -t "C:\\Users\\user\\Documents\\redirect2\\src;" coz@3d8:/storage/Downloads/clam-punch5 clamscan -d @99.ldb /home/coz/Downloads/flashredir.swf /home/coz/Downloads/flashredir.swf; MiscreatPunch.SWF.WordJS.FlashRedir.UNOFFICIAL FOUND
Our ClamAV repo. YMMV

- We started making our own ClamAV sigs for fun. Warning: YMMV. Just me and @malwareforme. Send in sigs or FP reports. Main focus is maldocs and EKs. Used as secondary indicators for Cuckoo.
- Why ClamAV? ClamAV 0.99 supports Yara, logical signatures that give you conditionals, PCRE support, etc. Plus you get the power of nested file unrolling/inspection. It's pretty hot...

https://github.com/wmetcalf/clam-punch
MOLOCH

- We can tag each cuckoo run with metadata. Malscore, Cuckoo sigs, VT detections etc
- Ability to tag individual sessions with Suricata/Yara/ClamAV hits.
- Let’s you ask really interesting questions about your traffic from a nice web-ui. Things like how many url tasks had IE martian children in the last 24 hours and now suricata hits. Hella fast compared to corresponding Mongo queries (yes we indexed).
- Some pitfalls: All tags share a single index. No tag data removed on pcap/session removal. Session tagging broke for me post Moloch 0.12 due to slow indexing at PCAP import time.
For versions of IE prior to 11 we can observe some interesting EK related artifacts in the “browser” tab of behavior in cuckoo via hooked JSEval/ColeScript_ParseScriptText functions. But it’s not always enough.
Most EK’s today store actual flash exploits in encrypted blobs inside of BinaryData tags inside the flash file itself then they decode/decrypt and use LoadBytes or similar to load the actual exploit. In most cases this means that we get the full flash exploit unencrypted and uncompressed in process memory dumps.
Yara Memory Sigs Flash Exploits

- Can use JPEXS to carve flash from memdumps for further inspection.
- java -jar /usr/share/java/ffdec/ffdec.jar -onerror ignore -extract ~/Downloads/1244.dmp -o ~/rigflash/ all
- Leads to flash file containing more potential for yara sigs.
So now what?

cuckoo + SURICATA + EMERGING THREATS + moloch + yara

vs EKs

http://securityonion.blogspot.com/
http://code.google.com/p/security-onion/
http://www.emergingthreats.net/
https://github.com/aol/moloch
What Now?

- Use shrike to submit URL tasks requests toward free Dynamic DNS domains. See the Dynamic DNS rules here. Same for firesale gTLDs.
- [https://github.com/EmergingThreats/et-luajit-scripts](https://github.com/EmergingThreats/et-luajit-scripts)
- Search for ie_martians in cuckoo/moloch results.
- If it’s infected today it will probably be infected tomorrow. Start building a list of pwn’d websites for replay. Cron them up.
- Working on notify reporting module for cuckoo to e-mail when we miss portions of Eks or Redirectors.
- Use various OS’s and plugin versions (esp) flash
Contact me

Will Metcalf, Ornament

• wmetcalf@emergingthreats.net

• @node5 on Twitter