

Tracking Exploit Kits

John Bambenek, Manager of Threat Systems
Fidelis Cybersecurity

Botconf – Dec 2, 2016

John.Bambenek@fidelissecurity.com
@bambenek



Sharing Restrictions

- You can consider the slides TLP:WHITE, this presentation is being live streamed. Tweet away.
- There is some more confidential info that I can show you, find me after. For obvious reasons, these probably shouldn't be livestreamed on the Internet.
😊



Introduction

- Manager of Threat Systems with Fidelis Cybersecurity
- Part-Time Faculty at University of Illinois in CS
- Handler at the SANS Internet Storm Center
- Provider of open-source intelligence feeds... DGAs! 😊
- Run several takedown oriented groups and surveil threats



Why track exploit kits?

- After investigating and occasionally getting malware operators prosecuted, new malware always shows up to take its place.
- Operation Tovar ended Gameover Zeus and Cryptolocker, now have Vawtrak and Locky.



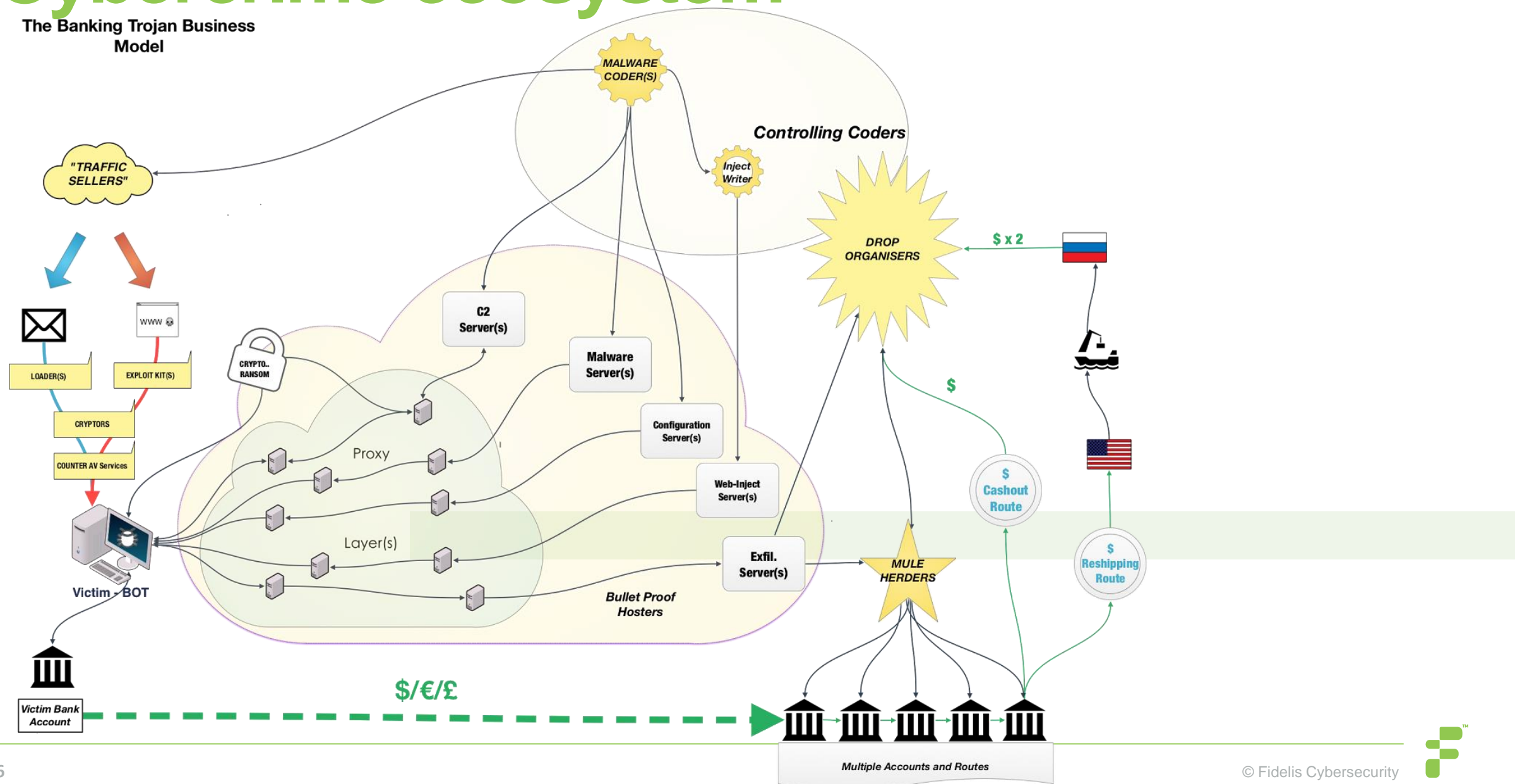
Why track exploit kits?

- Law enforcement operations for cybercrime take months or years and only pursue a limited amount of threats.
- However, almost all criminal malware comes via two methods, spam botnets or exploit kits.
- What if you could smash the entire malware delivery ecosystem instead?



Cybercrime ecosystem

The Banking Trojan Business Model



EK Ecosystem

- Malware writers/operators
- EK operators
- Exploit writers
- Traffic generators
- Selling of compromised websites
- “Marketplace” operators
- The ecosystem behind malware (i.e. mules, carders, etc)
- Bitcoin washing services 😊 😊



Why track exploit kits?

- Earlier this year, Russian authorities arrested the Lurk group who had direct connections to Angler Exploit Kit (EK) operations.
- Recall Vladimir Kropotov's presentation yesterday.
- Angler EK went away overnight.



Intelligence Priorities

- Priority 1: Ensure current products detect new malware and changes in EKs to protect customers.
- Priority 2: Develop intelligence to track EK operators and customers ultimately to disrupt an entire ecosystem instead of one small crime group.
- Non-Priority: Direct operationalization of data.



Why not operationalize?



What is an Exploit Kit?

- Set of tools (prominently web-based) that exploit vulnerabilities in software (browser, Adobe, Java, etc) to spread malware.
- Relatively static list of exploits each kit uses and they vary.
- Rarely (but sometimes) use 0-days.
- They operate as a criminal service and “sell infections” of whatever provided malware.
- Primary defense: patch your OS and applications.



Exploit Kits (see MalwareBytes Fall EK Roundup)

- RIG (RIG-V, Empire Pack)
- Sundown (and Bizarro)
- Neutrino-v
- Magnitude
- Astrum
- ~~Angler~~
- Many more...
- Many are "Dead"
- <http://www.kahusecurity.com/2016/wild-wild-west-112016/>



Campaign / Affiliate IDs

- Many, but not all, malware operators use multiple means of delivery and they compartmentalize using Campaign IDs.
 - Sometimes the campaign ID refers to an affiliate.
 - Sometimes it's just for a specific run of their malware.
- Correlating affiliates across malware delivery mechanisms can provide interesting insights into the marketplace behind the malware delivery.



Locky Example

```
{ [-]
  Affid: 3
  Date: 2016-07-25 15:16:28
  Delay: 52
  Domain: 185.117.153.176
  Origin: vt
  Persistence: 0
  Russian_language: 1
  Seed: 6721
  Svchost_inject: 0
  URL: /upload/_dispatch.php
  compile_date: 2010-09-07 20:11:05
  imphash: 66ebbcfb37c7095ce144ec66699570b9
  magic: PE32 executable for MS Windows (GUI) Intel 80386 32-bit
  md5: 6a30c749814d91c67cfc4c892d8a9963
  rat_name: Locky
  run_date: 2016-07-26
  section_.CDATA: 5d6cdf84fd4053271bb8dc45b01991de
  section_.DATA: 96c6082ee104ac9f6ff4935a04673099
  section_.RDATA: d01ac51ed5fe18de11f75e15831798c1
  section_.RELOC: 568d6bcade9c5e8d1d30773530acce8c
  section_.TEXT: f14dbfe601eaea76c74436ab4e84d2eb
  sha1: c989ec87782326172e86e1e157ebc56434f3bd9a
  sha256: 39a020f98263758b7ffea00c8343ebf5d0e7aebcd5be62ee1fbc351cec71b6c1
  times_submitted: 1
  unique_sources: 1
}
```

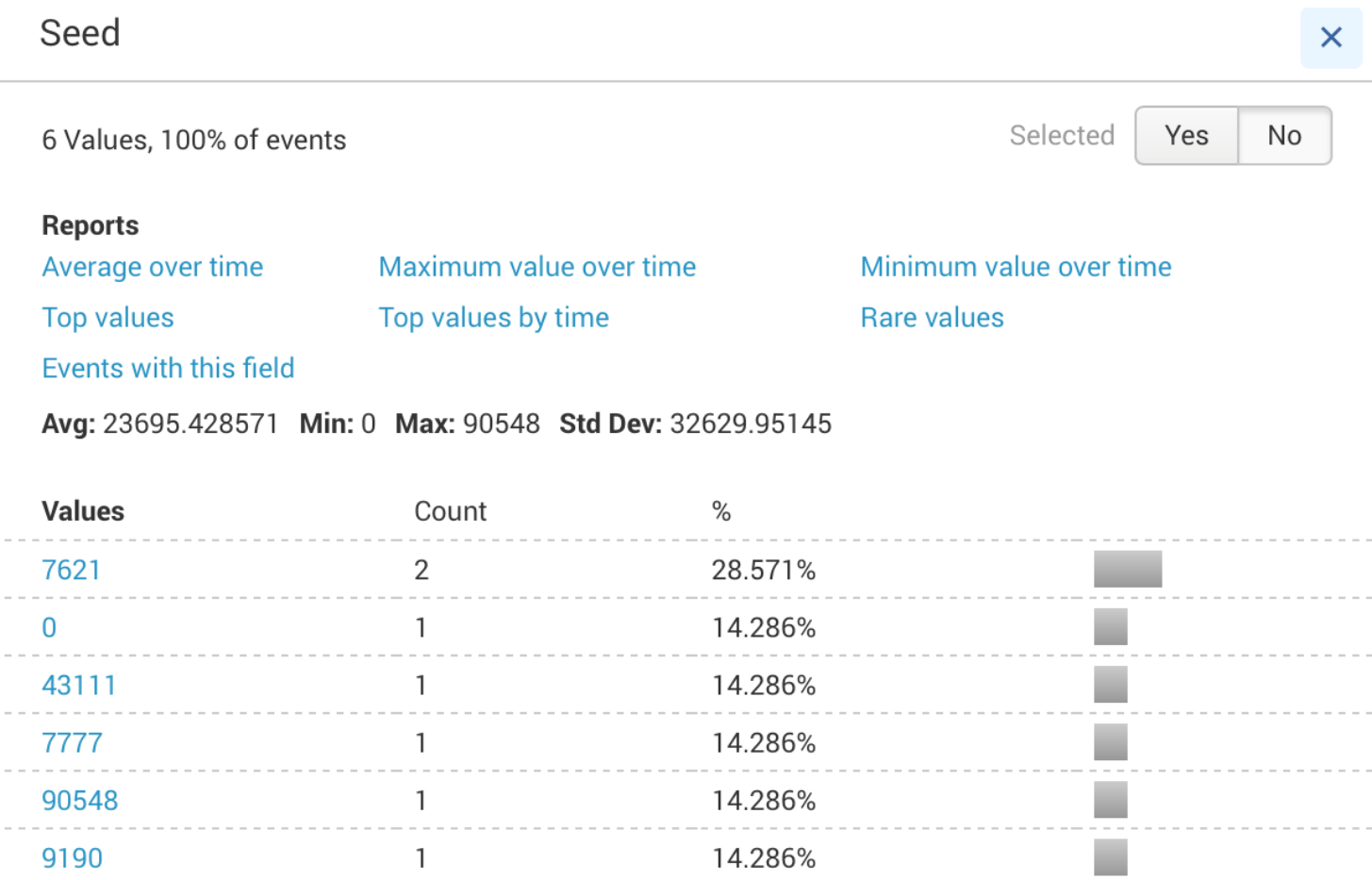


Data-mining malware

- Taking data downloaded from malware, you can rip configs and get information.
- Cross-correlate based on delivery method and now you have insight in who is buying service from whom.
- Now you have raw building blocks for an operation similar to what Russia did to the Lurk group that ended Angler.



Example (DGA Seeds used in Locky by Affid=3)



Basic EK Process

- Victim clicks on (usually compromised) webpage.
- There is validation of suitability.
 - Geo-blacklisting
 - Likely vulnerable browser
 - Blacklisting of suspected sandboxes, security researchers
- Victim is directed to actual exploit.
- Victim downloads and installs malware.



Magnitude to Cerber example

Filter: http.request						Expression...	Clear	Apply	Save	Filter	Filter	Filter
Date/Time	Dst	port	Host	Info								
2016-08-05 16:18:53	185.143.241.126	80	logotypemakers.org	GET / HTTP/1.1								
2016-08-05 16:18:54	185.143.240.105	80	didpart.vip	GET /?f1bkek5z9b2qd6=24&9ld1ycz35blfq=1024&c49970x1y525g=76								
2016-08-05 16:18:55	185.30.232.65	80	3ase6dze33uasab96oep.toremain.gdn	GET / HTTP/1.1								
2016-08-05 16:18:55	185.30.232.65	80	3ase6dze33uasab96oep.toremain.gdn	GET /a65036f2s HTTP/1.1								
2016-08-05 16:18:55	185.30.232.65	80	3ase6dze33uasab96oep.toremain.gdn	GET /cfwd5fc7964 HTTP/1.1								
2016-08-05 16:18:55	185.30.232.65	80	3ase6dze33uasab96oep.toremain.gdn	GET /5dy6f2x60lp?win%2021,0,0,213 HTTP/1.1								
2016-08-05 16:18:56	185.30.232.65	80	3ase6dze33uasab96oep.toremain.gdn	GET /favicon.ico HTTP/1.1								
2016-08-05 16:18:56	185.30.232.65	80	185.30.232.65	GET /1f4be45ac942b1c7cbf81a11a6e8d4f2 HTTP/1.1								
2016-08-05 16:19:00	185.30.232.65	80	185.30.232.65	GET /782fcb43691a830ac6cd9070e0c8785b HTTP/1.1								
2016-08-05 16:19:01	185.30.232.65	80	185.30.232.65	GET /782fcb43691a830ac6cd9070e0c8785b HTTP/1.1								
2016-08-05 16:19:10	185.30.232.65	80	185.30.232.65	GET /782fcb43691a830ac6cd9070e0c8785b HTTP/1.1								
2016-08-05 16:19:25	69.195.146.130	80	ip-api.com	GET /json HTTP/1.1								
2016-08-05 16:20:13	148.251.6.214	80	btc.blockr.io	GET /api/v1/address/txs/[REDACTED]								
2016-08-05 16:20:13	148.251.6.214	80	btc.blockr.io	GET /api/v1/tx/info/[REDACTED]								
2016-08-05 16:20:13	5.255.78.147	80	unocl45trpuoefft.myaddress.link	GET /[REDACTED]-[REDACTED]-[REDACTED]-[REDACTED]-[REDACTED]?auto HTTP/1.1								
2016-08-05 16:20:14	5.255.78.147	80	unocl45trpuoefft.myaddress.link	GET /[REDACTED]-[REDACTED]-[REDACTED]-[REDACTED]-[REDACTED]/intro?nst HTTP/1.1								
2016-08-05 16:20:15	5.255.78.147	80	unocl45trpuoefft.myaddress.link	GET /[REDACTED]-[REDACTED]-[REDACTED]-[REDACTED]-[REDACTED]/language?t=8320829 HTTP/1.1								
2016-08-05 16:20:16	5.255.78.147	80	unocl45trpuoefft.myaddress.link	GET /media/bs3/css/bootstrap.min.css HTTP/1.1								
2016-08-05 16:20:16	5.255.78.147	80	unocl45trpuoefft.myaddress.link	GET /media/style.css HTTP/1.1								
2016-08-05 16:20:16	5.255.78.147	80	unocl45trpuoefft.myaddress.link	GET /media/images/logo.png HTTP/1.1								
2016-08-05 16:20:16	5.255.78.147	80	unocl45trpuoefft.myaddress.link	GET /media/ignov.min.js HTTP/1.1								

From malware-traffic-analysis.net – has great blogs on EK traffic



Exploit Kit URLs often have patterns

- Some older Nuclear EK URL patterns in PCRE:
- `\.(su|ru)\Vmod_articles-auth.*\dV(axa|jqy)\VbVshoeV[0-9]{4,10}`
- `^[^\\n]{1,99}?Vurl\?([\w]+=([\w\.]++)?&){5,10}url=https:\V[\w]+\.[a-z]{2,3}&([\w]+=([\w\.]++)?&){2,6}[\w]+=([\w\.]++)+$`
- `^[^\\n]{1,99}?Vsearch\?(?=[a-z]+=utf-8&)(?=[ei]=.*(\p{Li}\p{Lu}|\p{Lu}\p{Li}))(?=[ei]=.{20,})(?!=V)([a-z_]{1,8}=[\w\+-.\\x20]+\&?){2,5}$`
- `^[^\\n]{1,99}?V(?-i)([a-z0-9]+\V){0,3}\d{2,3}(_|-)[a-z]+(_|-)\d+\.[a-z]{3,6}$`
- `^[^\\n]{1,99}?V(?-i)([a-z0-9]+\V){0,3}[a-z-]+\?(([a-z_]|[0-9]){3,}=[a-z_]|[0-9]){3,}&){1,5}[a-z0-9_-]{2,}=[a-z0-9]{8,}$`




Non-Attributable Networks

- EKs do have a tendency to block obvious security researchers and security company netblocks.
- They don't do a good job blocking commodity VPN services.
 - You can pick what country you want to appear from. 😊
- Still limits to what you can retrieve using a VPN.
 - VPN inside or outside cuckoo VM?



Non-Attributable Networks



FilesURLs

Older →

Recent URLs				
ID	Timestamp	URL	MalScore	Status
109992	2016-08-06 13:48:11	http://www.instalki.pl/aktualnosci/hardware/16993-datatraveler-locker-g3.html	3.0	reported
109993	2016-08-06 13:49:45	http://www.keiyama.eu/	0.0	reported
109994	2016-08-06 13:47:52	http://www.mediapromo.site/	2.0	reported
109995	2016-08-06 13:50:37	http://www.nowpdp.org/	2.0	reported
109996	2016-08-06 13:51:31	http://123.yasykallyamhochy.info/megaadvertize/?czMsmHVR=mDFvOSIw&hSxavDzNqL=enymLaoEHQg&LBUpUUnmQB=myIkytODxWGJ&lBSkbSPXbfI=qjxRGMGrMIVUpq&QhXyOobHTTOMjkwUj=vOHUTwcLTWgrCSlwp&keyword=def7f48c011b4cddf88b6c914fdfc4c5&NiczOwVJuf=MgikydcjfdZ&qTXePro tEU=KURgyqmBdE&oJNRekJKcskFiJViz=UQAvFQjiS	3.0	reported
109997	2016-08-06 13:49:47	http://chiplawcoaching.com/	2.0	reported
109998	2016-08-06 13:51:48	http://funny-saying-tshirts.com/	3.0	reported
109999	2016-08-06 13:53:27	http://www.atwellandgent.com/	1.0	reported
110000	2016-08-06 13:51:47	http://www.camlock-fittings.com/	2.0	reported



Non-Attributable Network

- At present, there is no easy central way to manage multiple cuckoo instances that reach out to multiple geographies from the same instance.
- Solution is to run multiple physical cuckoo instances with VPN outside the VM and rotate IPs inside a geo each batch run.



Exploit hunting

- Each exploit kit has a partially overlapping but unique set of exploits they use.
- To get cuckoo to execute the exploit, some care needs to be spent in choosing the images and vulnerable software based on exploit kit.
- An older tracking spreadsheet is available at: <https://docs.google.com/spreadsheet/ccc?key=0AjvsQV3iSLa1dE9EVGhjeUhvQTNReko3c2xhTmphLUE#gid=10> but a new version should be at ContagioDump.blogspot.com soon.



Exploit Hunting

R	S	T	U	V	W	X
Magnitude	Neutrino	Niteris	Nuclear	Nuclear 3.x	NullHole	Rig
			2010_0188	2010-0188		
2011_3402						
2012_0507			2012_0507			2012_0507
			2012_1723	2012-1723		
						2013_0025
	2013_0074		2013_0074			2013_0074
		2012_3993				
		2013_0422		2013_0422		
2013_0634		2013_0634				2013_0634
		2013_1710				
				2013_2423		
		2013_2460		2013_2460		
2013_2463						
		2013_2465	2013_2465			2013_2465
2013_2471			2013_2471			
2013_2551		2013_2551	2013_2551	replaced by CVE-2013-3918	2013_2551	2013_2551



Exploit Hunting

- Easiest way is to have a set of VM images for specific exploit kits.
- Still need to monitor for addition of new exploits.
- 0-days happen maybe once a year.



Decoding EK landing pages

- Open source tools available here:
<https://github.com/mak/ekdeco> for RIG, Sundown, Neutrino, Nuclear and Angler.
- Can export config and encryption keys, intermediate flash files, and the exploit outputs that are used and save those to files.
- Requires landing pages or first SWF file (available in PCAP or via Cuckoo).



Example

```
$ python neutrino.py -d out -e -i strong-special-green-tread-motive-happiness-warm-stre-slap-happy.swf
```

```
[+] embeded swf (SHA256: d977a418fa1cf5a0a78c768fade3223ead531ee25d766fa64a2e27ade0616a82) extracted, and saved to  
out/d977a418fa1cf5a0a78c768fade3223ead531ee25d766fa64a2e27ade0616a82.swf
```

```
[+] cfg key: uturwhahhdm820991, exploit key: czynukecllu385015
```

```
{u'debug': {u'flash': False},
```

```
  u'exploit': {u'nw22': {u'enabled': True},
```

```
    u'nw23': {u'enabled': True},
```

```
    u'nw24': {u'enabled': True},
```

```
    u'nw25': {u'enabled': True},
```

```
    u'nw8': {u'enabled': True}},
```

```
  u'key': {u'payload': u'yykrnnfwet'},
```

```
  u'link': {u'backUrl': u'',
```

```
    u'bot': u'http://muusikkopruflin.earclearclinic.co.uk/1994/05/16/jump/loom/have-september-meal-borrow-normal.html',
```

```
    u'flPing': u'http://muusikkopruflin.earclearclinic.co.uk/wobbler/1440055/carrot-every-hasten',
```

```
    u'jsPing': u'http://muusikkopruflin.earclearclinic.co.uk/1978/12/12/alley/knock-trial-guilty-knee-younger-sigh-suffer-fault-lamp.html',
```

```
    u'pnw22': u'http://muusikkopruflin.earclearclinic.co.uk/dull/aXF4Y21nYw',
```

```
    u'pnw23': u'http://muusikkopruflin.earclearclinic.co.uk/consciousness/clever-13253660',
```

```
    u'pnw24': u'http://muusikkopruflin.earclearclinic.co.uk/hospital/d2dxY3dkZw',
```

```
    u'pnw25': u'http://muusikkopruflin.earclearclinic.co.uk/disappointment/battle-31593215',
```

```
    u'pnw8': u'http://muusikkopruflin.earclearclinic.co.uk/another/hideous-33550406',
```

```
    u'soft': u'http://muusikkopruflin.earclearclinic.co.uk/belong/animal-none-western-14473008'},
```

```
  u'marker': u'rtConfig'}
```

```
[+] Exploit saved to ....
```



Example

```
$ xxd 7ccc54cd4e819ee0a8b291917cf321acc058ccc6e4d35ad6f21db09491e05332.ek.bin
```

```
0000000: 5a57 5312 c741 0000 6820 0000 5d00 0020  ZWS..A..h ..].  
0000010: 0000 3bff fc8e 19fa dfe7 6608 a03d 3e85  ..;.....f..=>.  
0000020: f575 6fd0 7e61 351b 1a8b 164d df05 32fe  .uo.~a5....M..2.  
0000030: a44c 4649 b77b 6b75 f92b 5c37 290b 9137  .LFI.{ku.+\\7)..7  
0000040: 0137 0ee9 f2e1 fc9e 64da 6c11 2133 eda0  .7.....d.l.!3..  
0000050: 0e76 70a0 cd98 2e76 80f0 e059 5606 08e9  .vp....v...YV...  
0000060: caeb a2c6 db5a 867b 47de 995d 6876 3816  ....Z.{G..]hv8.  
0000070: bd93 3cd3 d09e d355 635a dab0 db27 e67c  ..<....UcZ...'|. |  
0000080: 213d accc 90a1 7658 7308 c858 95d6 680b  !=....vXs..X..h.  
0000090: f2b8 c7c7 1255 4087 e759 c04e df21 aee8  ....U@..Y.N.!..  
00000a0: a06a 8ec4 ecd8 3838 a5f4 55b9 284e 31d5  .j....88..U.(N1.  
00000b0: 1256 5f00 c2ea 9c36 e8be b710 5aa6 2909  .V_....6....Z.).  
00000c0: 3d49 3471 1ec5 14ee 224f 7b31 40e3 fb00  =l4q...."O{1@...  
00000d0: d5f1 bfe2 2fbe 4458 10a8 01f4 3108 fa24  ..../.DX....1..$.  
00000e0: 0d9a aefd c5cf cfa2 350b aeed dc41 39c8  ....5....A9.  
00000f0: 4f5f 1f63 6f38 20e8 69e4 4785 e82e ba36  O_.co8 .i.G....6
```



Other Cuckoo considerations

- Cuckoo stores tons of information, but for EKs we are only interested in getting the dropped binary.
- Turn off all the logging except that directly related to dropped files.
- Running Yara and using volatility can help quickly identify dropped files.
- Remember, use a non-attributable network. :)



Finding EK landing pages

- All this automation still has to be fed with targets to sandbox.
- Work backwards from an infection event.
- Use web proxy logs / telemetry and PCREs.
- Use a crawler.
- Trick EK to give you the initial gates.



Working backwards from an infection

- Least efficient way of doing it but in some cases (new EK, significant changes to an existing EK) it's all we can do.
- Initial gates are transient resources, so manually identifying them has limited utility.
- Also limited only by what is attacking you or your customer.



Using PCREs to hunt

- Still requires users to visit but can be programmatically pipelined into a sandbox system for relatively real time analysis.
- Everyone has a user-base and telemetry that has geographic or demographic biases that create holes in visibility.



Using a crawler

- Inefficient because it will request more than what you are looking for.
- Crawlers are also resource intensive the broader you are looking for behavior.
- It can, however, have a global footprint and be thorough.



Using a crawler

- Luckily, we don't have to make our own crawler when Microsoft will give Bing crawler malicious URLs to MAPP/VIA members.
- On 4 August 2016, over 26M malicious webpages were seen which Microsoft gives a 99% confidence interval too.
- Much more than EKs.



Using Bing Malicious URLs

8/4/2016 4:58:27 PM <http://0000-programasnet.blogspot.com.ar/2011/03/my-defragmenter-my-defragmenter-es-un.html?action=backlinks&widgetId=Blog1&widgetType=Blog&responseType=js&postID=6994789541307753585> 216.58.216.193 us 15169 MalwareNetwork

8/4/2016 4:51:46 PM <http://0000-programasnet.blogspot.com.ar/2011/03/pocopique-tv-programa-para-ver-tv.html?action=backlinks&widgetId=Blog1&widgetType=Blog&responseType=js&postID=7841830628282890204> 216.58.192.129 us 15169 ES

8/4/2016 6:06:13 PM <http://0000-programasnet.blogspot.com.ar/2011/07/reparacion-de-impresoras.html> 216.58.192.129 us 15169 ES

8/4/2016 6:26:04 PM http://0000-programasnet.blogspot.com.ar/2011_02_24_archive.html 216.58.192.129 us 15169 MalwareNetwork

8/4/2016 4:34:23 PM <http://0000-programasnet.blogspot.com.es/2011/02/descarga-chat-para-facebook.html?action=backlinks&widgetId=Blog1&widgetType=Blog&responseType=js&postID=2134381520774268527> 216.58.192.225 us 15169 MalwareNetwork



Bing Malicious URLs

- On 4 August, 524,713 of those URLs pointed to IPs inside China.
- Number is misleading because it includes multiple URLs under same domain.
- Also flags “interesting” advertiser behavior.
- Need to filter based on the PCREs we have seen before or other alerting technology.
- We are running all these URLs through cURL with a spoofed user agent just to see request and first response.



Bing Malicious URLs

- Dealing with compromised websites and bulk malicious behavior is hard to do.
- With proper filtering of the above, it also becomes possible to programmatically start notifying hosting providers of such content so they can start cleaning these websites.
- Subscribe to Shadowserver's Netblock Reporting Service to get alerts on malicious activity seen on your network.
- <https://www.shadowserver.org/wiki/pmwiki.php/Involve/GetReportsOnYourNetwork>



Bing Malicious URLs

```
# grep -P '$pcre' Bing_mUrls_2016_08_04_8.tsv
```

```
http://melnoosh.narod.ru/p3aa1.html
```

```
http://mr-hijacker.blogspot.com/indexEN.html
```

```
http://peterbronkhorst.rusa.nl/pag013l.htm
```

```
http://peterscott.0catch.com/vk3en62w.htm
```

```
http://portvein777.narod.ru/MirChiselChast10.htm
```

```
http://portvein777.narod.ru/MirChiselChast26.htm
```

```
http://redirectionn.weebly.com/fadi7a.html
```

```
http://remeslo.okis.ru/15moda2.html
```

```
http://remeslo.okis.ru/15moda3.html
```

```
http://ruza-gimnazia.narod.ru/p13aa1.html
```

```
http://ruza-gimnazia.narod.ru/p15aa1.html
```



Trick EKs to give you landing pages

- EKs have a hierarchical structure but the deeper levels also need to be aware of the landing pages to prevent people artificially getting malware directly from the source.

[[Censored]] 😊

....



Putting it together

- Now we have all the pieces. Use telemetry/web logs, Bing Malicious URLs and EK bugs to put URLs into your sandbox.
- Use non-attributed network from multiple geographies to maximize visibility.
- Retrieve first landing page / exploit file and dropped malware.



Putting it together

- Tie dropped malware to country and exploit kit (note, repeat visits from same IP will not give you malware).
- EKs sell “by infection” so often the same landing page will drop other malware as the infection orders are fulfilled.
- Further mine dropped malware for intelligence and correlate to other malware delivery networks.



Resources

- If you are interested in Exploit Kit tracking and disruption, please get in touch.
- Send me an email for access to Barncat Malware Config MISP or our EK Tracking MISP.
- My DGA feeds are at <http://osint.bambenekconsulting.com/feeds>



Shameless Plug

- I run a charity raising funds to build schools in rural Tanzania and to send medical supplies to rural Côte d'Ivoire, please donate 😊
- <http://thetumainifoundation.org/>



Questions & Thank You!

John Bambenek / john.bambenek@fidelissecurity.com



FidelisTM
Cybersecurity