All Your Cloud Are Belong to Us

Hunting Compromise in Azure
Nate Warfield – Microsoft Security Response Center
The opinions expressed are my own and do not necessarily reflect those of Microsoft Corporation.

Whoami: Nate Warfield (@dk_effect)

- Hacker – Microsoft Security Response Team
  - Vulnerability Management for Azure, Windows, Hyper-V
  - Battle tested: MS17-010, WannaCry, NotPetya, Spectre/Meltdown
- cat ~/.bash_history
  - 18 years in Network Engineering; 20 year Grey Hat
  - First hack: BBS over 2400 baud
  - Kaspersky SAS 2018
  - Troopers 18

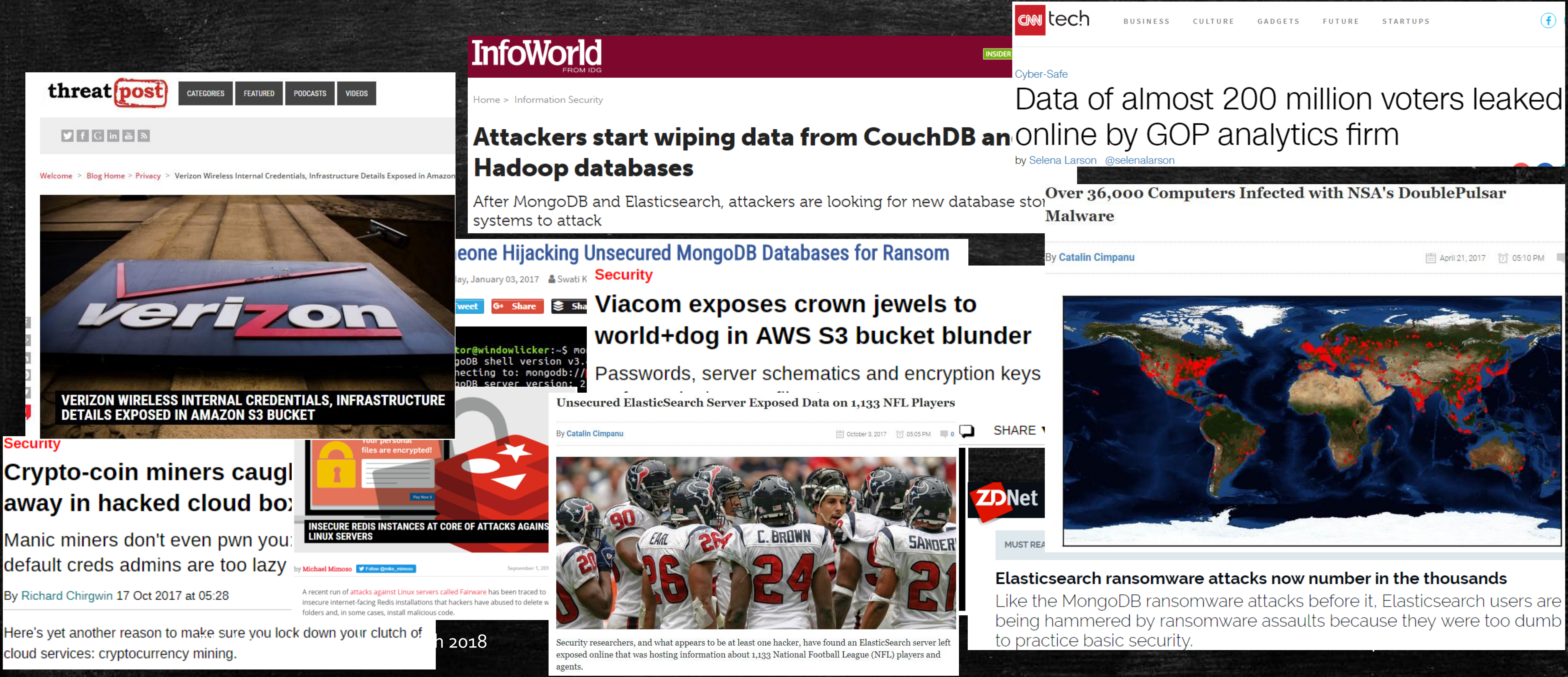
  - **Twitter: @dk_effect**
  - **GitHub: n0x08**

Captain: What happen?

- **Traditional Networking (then)**
- Server exposure was restricted
- Many layers of ACLs + segmentation
- Dedicated deployment teams
- Well-defined patching cadence
- Servers deployed from the ground up
- Only expose required services

- **Cloud Networking (now)**
- Every VM exposed to the Internet
- VM’s deploy with predefined firewall
- Anyone with access can expose BadThings
- Patch management decentralized
- VM’s inherit the sins of their creators
- NoSQL open to the Internet? #yolo

2017: Somebody set us up the bomb



threatpost CATEGORIES FEATURED PODCASTS VIDEOS

Welcome > Blog Home > Privacy > Verizon Wireless Internal Credentials, Infrastructure Details Exposed in Amazon

VERIZON WIRELESS INTERNAL CREDENTIALS, INFRASTRUCTURE DETAILS EXPOSED IN AMAZON S3 BUCKET

InfoWorld FROM IDG INSIDER

Home > Information Security

Attackers start wiping data from CouchDB an Hadoop databases

After MongoDB and Elasticsearch, attackers are looking for new database stor systems to attack

CNN tech BUSINESS CULTURE GADGETS FUTURE STARTUPS

Cyber-Safe

Data of almost 200 million voters leaked online by GOP analytics firm

by Selena Larson @selenalarson

Over 36,000 Computers Infected with NSA's DoublePulsar Malware

By Catalin Cimpanu April 21, 2017 05:10 PM

eone Hijacking Unsecured MongoDB Databases for Ransom

lay, January 03, 2017 Swati K

weet G+ Share Sha

```
tor@windowlicker:~$ mo
goDB shell version v3.
necting to: mongodb://
goDB server version: 2
```

Security

Viacom exposes crown jewels to world+dog in AWS S3 bucket blunder

Passwords, server schematics and encryption keys

Unsecured ElasticSearch Server Exposed Data on 1,133 NFL Players

By Catalin Cimpanu October 3, 2017 05:05 PM 0 SHARE

Security researchers, and what appears to be at least one hacker, have found an ElasticSearch server left exposed online that was hosting information about 1,133 National Football League (NFL) players and agents.

Security

Crypto-coin miners caugl away in hacked cloud box

Manic miners don't even pwn you: default creds admins are too lazy

By Richard Chirgwin 17 Oct 2017 at 05:28

Here's yet another reason to make sure you lock down your clutch of cloud services: cryptocurrency mining.

files are encrypted!

INSECURE REDIS INSTANCES AT CORE OF ATTACKS AGAINS LINUX SERVERS

by Michael Mimoso Follow @mike_mimoso September 1, 201

A recent run of attacks against Linux servers called Fairware has been traced to insecure internet-facing Redis installations that hackers have abused to delete w folders and, in some cases, install malicious code.

n 2018

ZDNet

MUST REA

Elasticsearch ransomware attacks now number in the thousands

Like the MongoDB ransomware attacks before it, Elasticsearch users are being hammered by ransomware assaults because they were too dumb to practice basic security.

Operator: We get signal

- NoSQL solutions were never intended for Internet exposure
  - “..it is not a good idea to expose the Redis instance directly to the internet”
  - “Allow only trusted clients to access the network interfaces and ports on which MongoDB instances are available.”
  - “Elasticsearch installations are not designed to be publicly accessible over the Internet.”
- Naturally, people exposed them to the Internet
- To date: MongoDB, CouchDB, Hadoop, Elastic, Redis, CassandraDB
- DB dropped; ransom note added
- 100k+ systems compromised globally
- Azure: 3800+ VM’s compromised

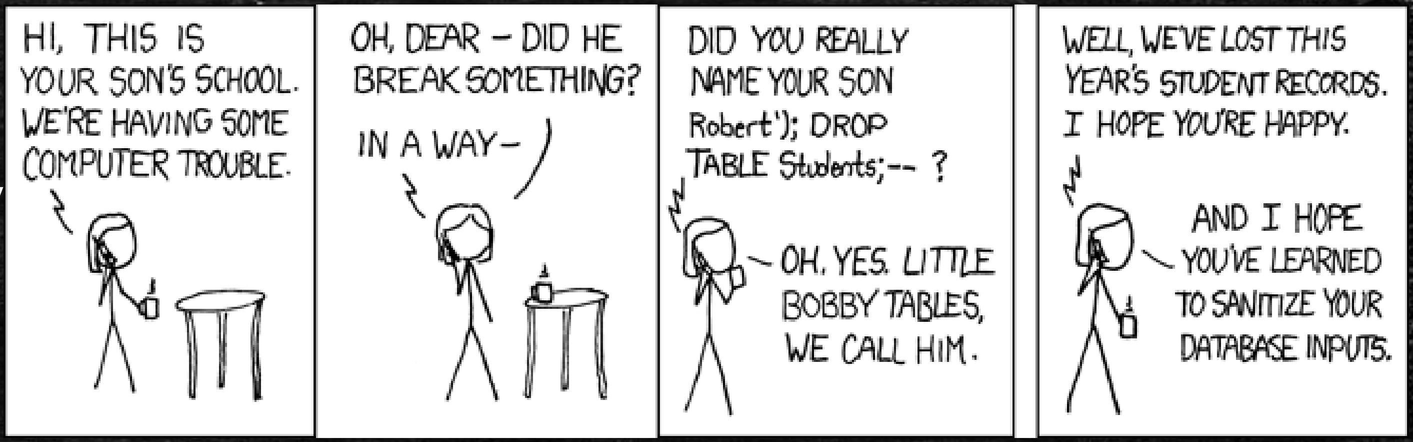
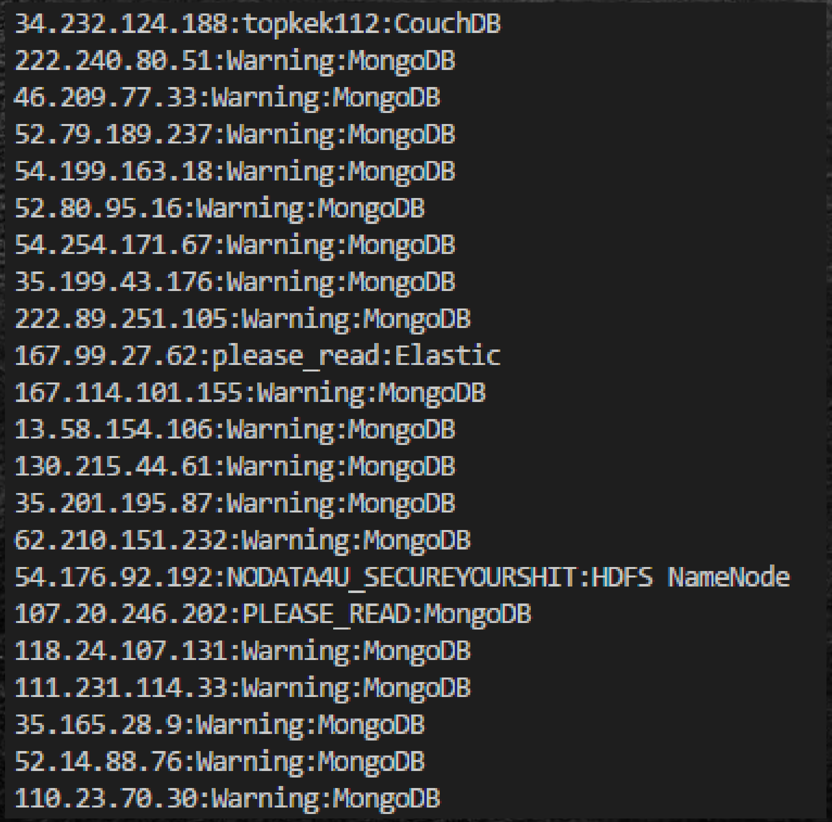

HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Image Source: https://imgs.xkcd.com/comics/exploits_of_a_mom.png

Hunting NOSQL Compromise in Azure

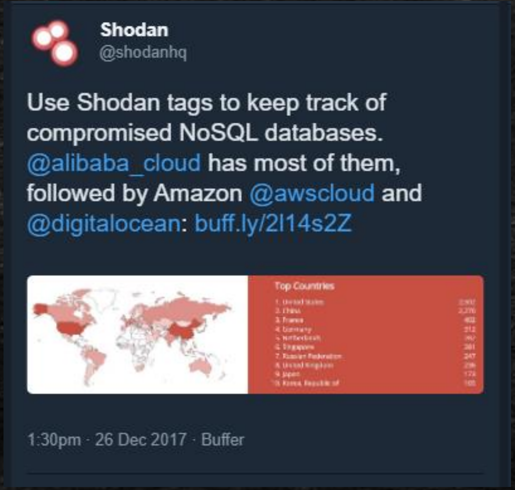


```
34.232.124.188:topkek112:CouchDB
222.240.80.51:Warning:MongoDB
46.209.77.33:Warning:MongoDB
52.79.189.237:Warning:MongoDB
54.199.163.18:Warning:MongoDB
52.80.95.16:Warning:MongoDB
54.254.171.67:Warning:MongoDB
35.199.43.176:Warning:MongoDB
222.89.251.105:Warning:MongoDB
167.99.27.62:please_read:Elastic
167.114.101.155:Warning:MongoDB
13.58.154.106:Warning:MongoDB
130.215.44.61:Warning:MongoDB
35.201.195.87:Warning:MongoDB
62.210.151.232:Warning:MongoDB
54.176.92.192:NODATA4U_SECUREYOURSHIT:HDFS NameNode
107.20.246.202:PLEASE_READ:MongoDB
118.24.107.131:Warning:MongoDB
111.231.114.33:Warning:MongoDB
35.165.28.9:Warning:MongoDB
52.14.88.76:Warning:MongoDB
110.23.70.30:Warning:MongoDB
```

- 2.1 million Internet exposed IPs in Azure
- Port scans are slow; open port != pwned
- Each NoSQL solution runs on different port
- DB names only indication of compromise
- TL;DR – I use Shodan (what, you don't?)
  - Accurate to with 0.14% of in-house solution
  - Rich metadata for each IP
  - DB names are indexed & searchable
  - JSON export allows for automated hunting

Operator: Main screen turn on

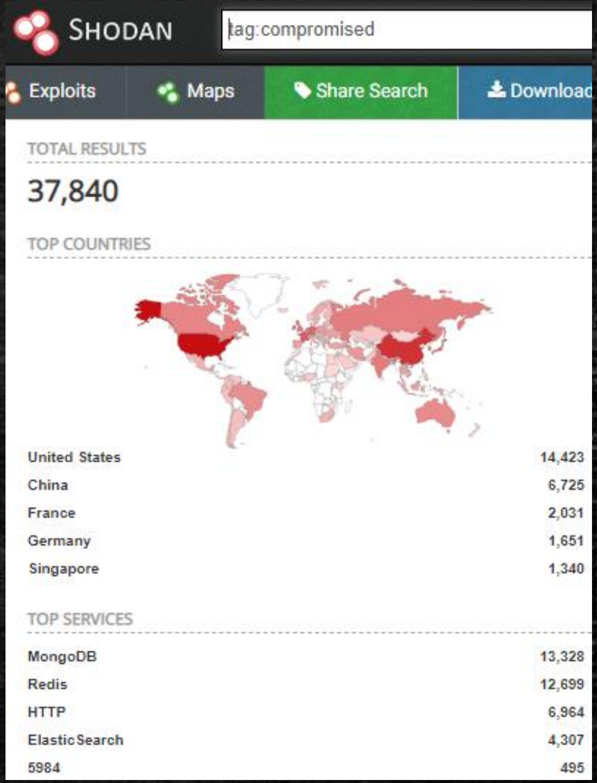
- Use master list of all pwned DB names seen globally
- My code was added to Shodan in December 2017
- tag:compromised – automatically tags pwned NoSQL DBs
- 37k pwned VMs as of 8/3/2018
- Requires Shodan Enterprise API
- ..or..
- https://gist.github.com/n0x08



Shodan
@shodanhq

Use Shodan tags to keep track of compromised NoSQL databases. @alibaba_cloud has most of them, followed by Amazon @awscloud and @digitalocean: buff.ly/2l14s2Z

1:30pm · 26 Dec 2017 · Buffer



TOTAL RESULTS

37,840

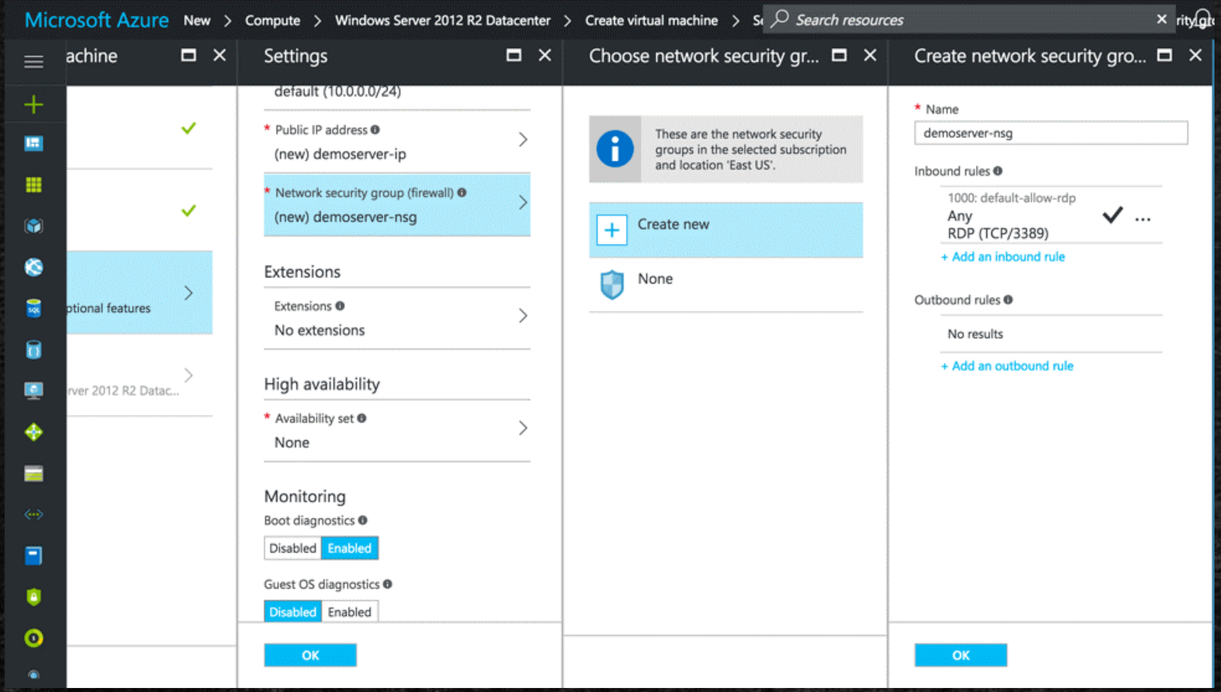
TOP COUNTRIES

United States	14,423
China	6,725
France	2,031
Germany	1,651
Singapore	1,340

TOP SERVICES

MongoDB	13,328
Redis	12,699
HTTP	6,964
ElasticSearch	4,307
5984	495

Network Security Group (Azure)


Microsoft Azure
New > Compute > Windows Server 2012 R2 Datacenter > Create virtual machine > Se
Search resources

achine

ptional features

rver 2012 R2 Datac...

Settings

default (10.0.0.0/24)

* Public IP address
(new) demoserver-ip

* Network security group (firewall)
(new) demoserver-nsg

Extensions

Extensions
No extensions

High availability

* Availability set
None

Monitoring

Boot diagnostics
Disabled [✓ Enabled]

Guest OS diagnostics
[✓ Disabled] Enabled

OK

Choose network security gr...

These are the network security groups in the selected subscription and location 'East US'.

Create new

None

Create network security gro...

* Name
demoserver-nsg

Inbound rules

1000: default-allow-rdp
Any
RDP (TCP/3389) ✓ ...

+ Add an inbound rule

Outbound rules

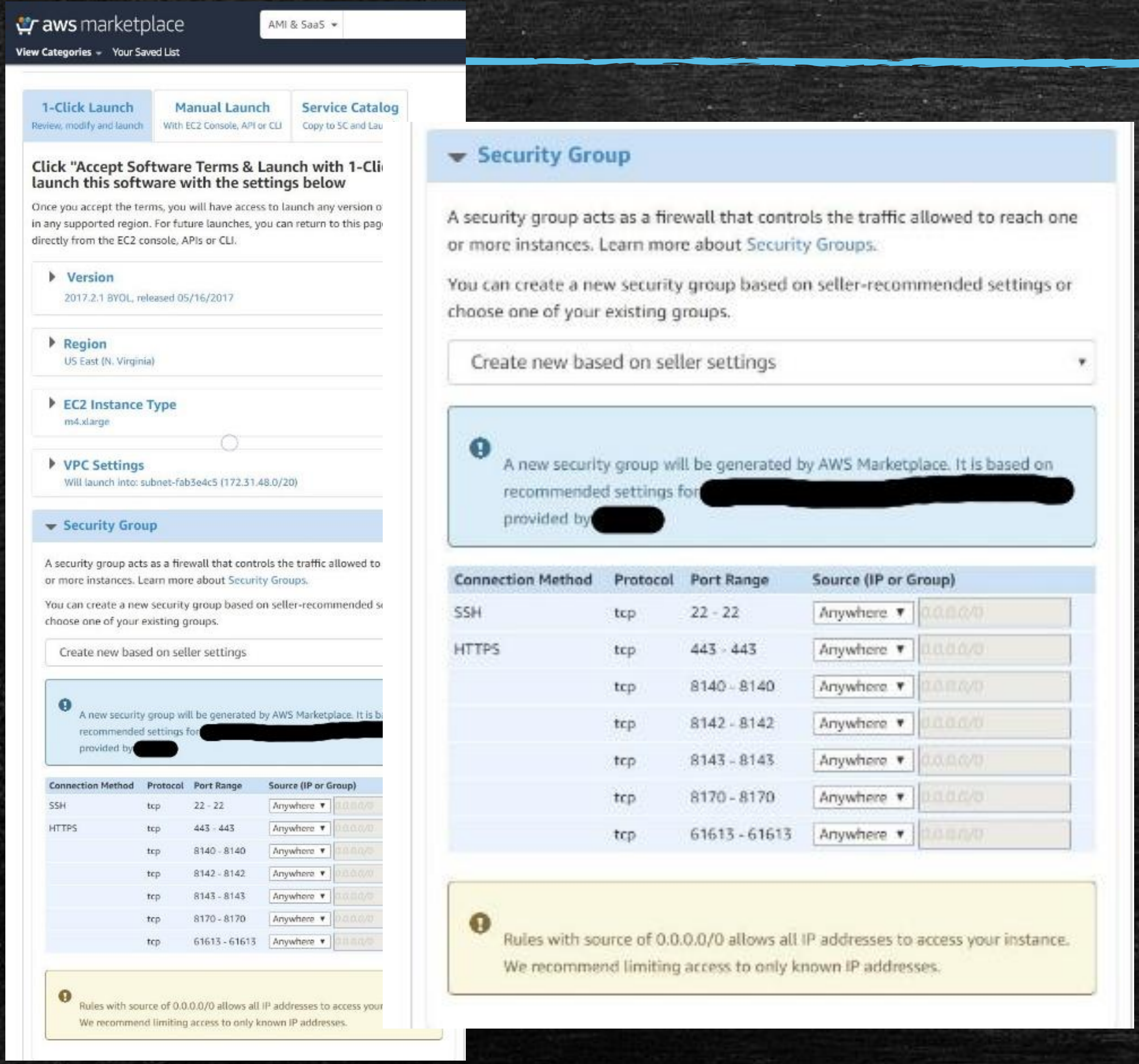
No results

+ Add an outbound rule

OK

- Network Security Group is the VM firewall
- Firewall config hard-coded by VM vendor
- Configurable during deployment (optional)
- 46% of images expose ports by default
- 96% expose more than management
- 562 unique ports exposed in Azure Gallery

AMI Security Groups (AWS)



aws marketplace | AMI & SaaS ▾

View Categories ▾ | Your Saved List

- **1-Click Launch** – Review, modify and launch
- **Manual Launch** – With EC2 Console, API or CLI
- **Service Catalog** – Copy to SC and Lau

Click "Accept Software Terms & Launch with 1-Cli launch this software with the settings below

Once you accept the terms, you will have access to launch any version o in any supported region. For future launches, you can return to this pag directly from the EC2 console, APIs or CLI.

- **Version**: 2017.2.1 BYOL, released 05/16/2017
- **Region**: US East (N. Virginia)
- **EC2 Instance Type**: m4.xlarge
- **VPC Settings**: Will launch into: subnet-fab3e4c5 (172.31.48.0/20)

Security Group

A security group acts as a firewall that controls the traffic allowed to reach one or more instances. Learn more about Security Groups.

You can create a new security group based on seller-recommended settings or choose one of your existing groups.

Create new based on seller settings ▾

A new security group will be generated by AWS Marketplace. It is based on recommended settings for [redacted] provided by [redacted]

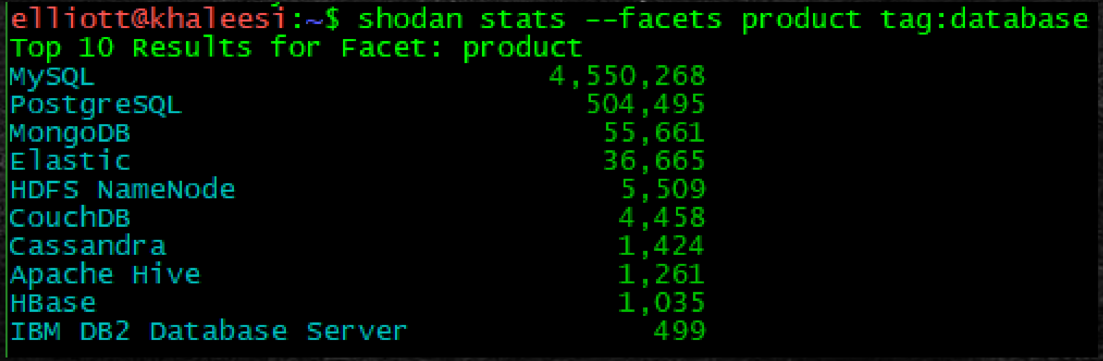
Connection Method	Protocol	Port Range	Source (IP or Group)
SSH	tcp	22 - 22	Anywhere ▾ 0.0.0.0/0
HTTPS	tcp	443 - 443	Anywhere ▾ 0.0.0.0/0
	tcp	8140 - 8140	Anywhere ▾ 0.0.0.0/0
	tcp	8142 - 8142	Anywhere ▾ 0.0.0.0/0
	tcp	8143 - 8143	Anywhere ▾ 0.0.0.0/0
	tcp	8170 - 8170	Anywhere ▾ 0.0.0.0/0
	tcp	61613 - 61613	Anywhere ▾ 0.0.0.0/0

Rules with source of 0.0.0.0/0 allows all IP addresses to access your instance. We recommend limiting access to only known IP addresses.

- Amazon Marketplace Image is 3rd party IaaS
- AWS doesn't expose AMI SG config via API*
  - *Until you deploy it =)
- Feature request filed with AWS
- 11k AMI's in AWS – 5x as many as Azure
- Data indicates many clouds have this problem

Default Passwords

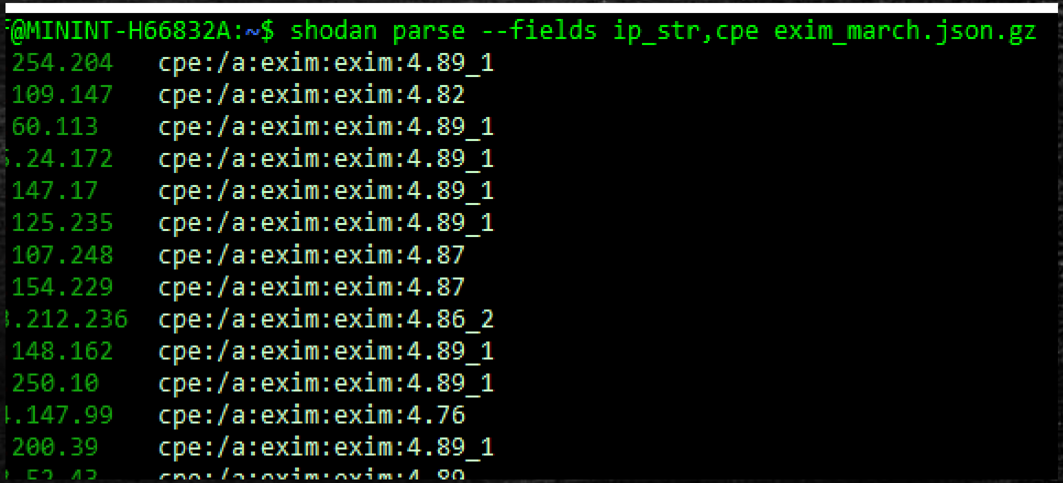
- 3rd party IaaS images occasionally contain a default password
- At least it's a strong* PW!: P@sswOrd123
  - *actual PW changed to protect the innocent
- Users always change passwords after installation ;)
- Mostly for services like MySQL, SQL, etc…



```
elliott@khaleesi:~$ shodan stats --facets product tag:database
Top 10 Results for Facet: product
MySQL                          4,550,268
PostgreSQL                       504,495
MongoDB                           55,661
Elastic                           36,665
HDFS NameNode                      5,509
CouchDB                            4,458
Cassandra                          1,424
Apache Hive                        1,261
HBase                              1,035
IBM DB2 Database Server              499
```

Threat hunting (old way): CVE-2018-6789

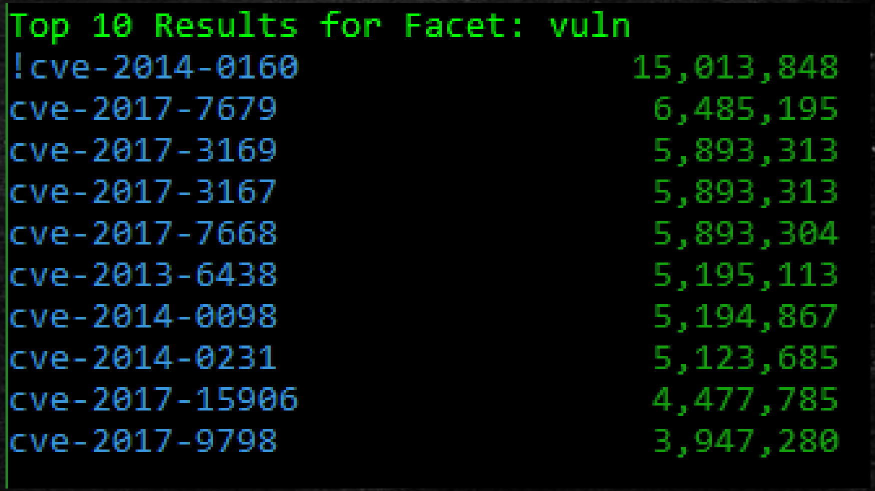
- Azure exposure: 17k IPs running an email server
- ‘shodan download product:exim org:microsoft’
- Common Platform Enumeration field FTW
- ‘shodan parse --fields ip_str,cpe’
- VMs found: 1221
- Total time: ~5 minutes
- Can we do better?



```
f@MININT-H66832A:~$ shodan parse --fields ip_str,cpe exim_march.json.gz
254.204   cpe:/a:exim:exim:4.89_1
109.147   cpe:/a:exim:exim:4.82
60.113    cpe:/a:exim:exim:4.89_1
.24.172   cpe:/a:exim:exim:4.89_1
147.17    cpe:/a:exim:exim:4.89_1
125.235   cpe:/a:exim:exim:4.89_1
107.248   cpe:/a:exim:exim:4.87
154.229   cpe:/a:exim:exim:4.87
.212.236  cpe:/a:exim:exim:4.86_2
148.162   cpe:/a:exim:exim:4.89_1
250.10    cpe:/a:exim:exim:4.89_1
.147.99   cpe:/a:exim:exim:4.76
200.39    cpe:/a:exim:exim:4.89_1
.52.43    cpe:/a:exim:exim:4.89
```

Threat hunting (new way): The vuln: tag

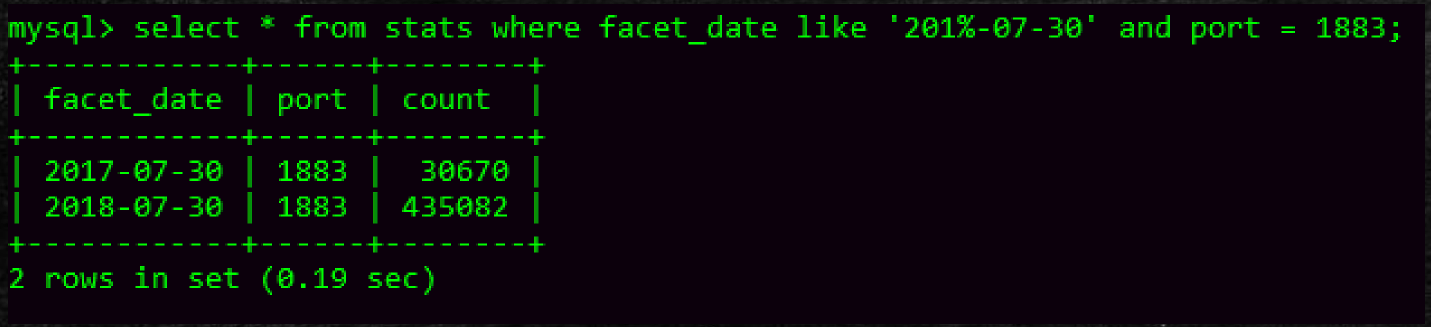
- Worked with Shodan incorporate CPE ←→ CVE detections
- Accessible via ‘vuln:’ tag (Enterprise API only)
- ‘shodan count vuln:cve-2018-6789 org:microsoft’ = 152
- Verified: False == *implied* vulnerable
  - Based off version data
- Verified: True == confirmed vulnerable
  - Ex: MS17-010



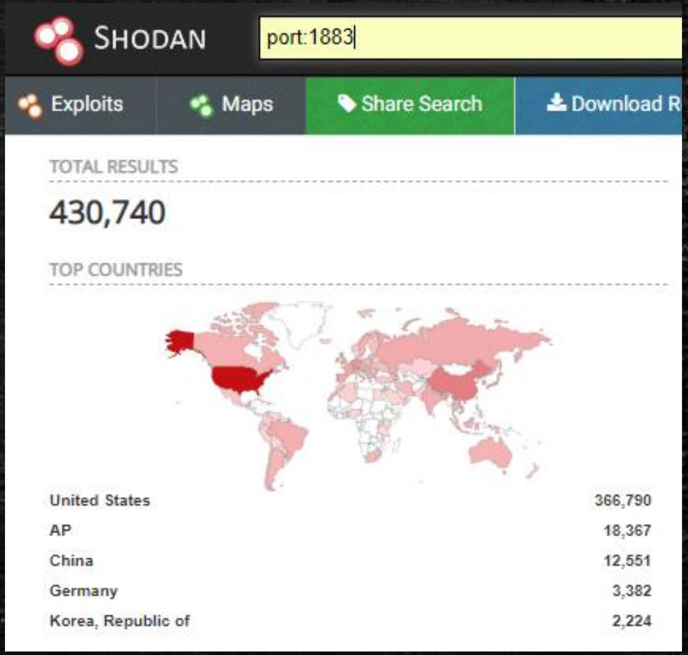
```
Top 10 Results for Facet: vuln
!cve-2014-0160                    15,013,848
cve-2017-7679                      6,485,195
cve-2017-3169                      5,893,313
cve-2017-3167                      5,893,313
cve-2017-7668                      5,893,304
cve-2013-6438                      5,195,113
cve-2014-0098                      5,194,867
cve-2014-0231                      5,123,685
cve-2017-15906                     4,477,785
cve-2017-9798                      3,947,280
```

Every (MQTT) step you take…

- MQTT – publish/subscribe message protocol
- Used by IoT, Facebook Messanger, many more
- Azure & AWS offer MQTT-based solutions
- Internet exposure **+1450%** in last year



```
mysql> select * from stats where facet_date like '201%-07-30' and port = 1883;
+------------+------+--------+
| facet_date | port | count  |
+------------+------+--------+
| 2017-07-30 | 1883 |  30670 |
| 2018-07-30 | 1883 | 435082 |
+------------+------+--------+
2 rows in set (0.19 sec)
```



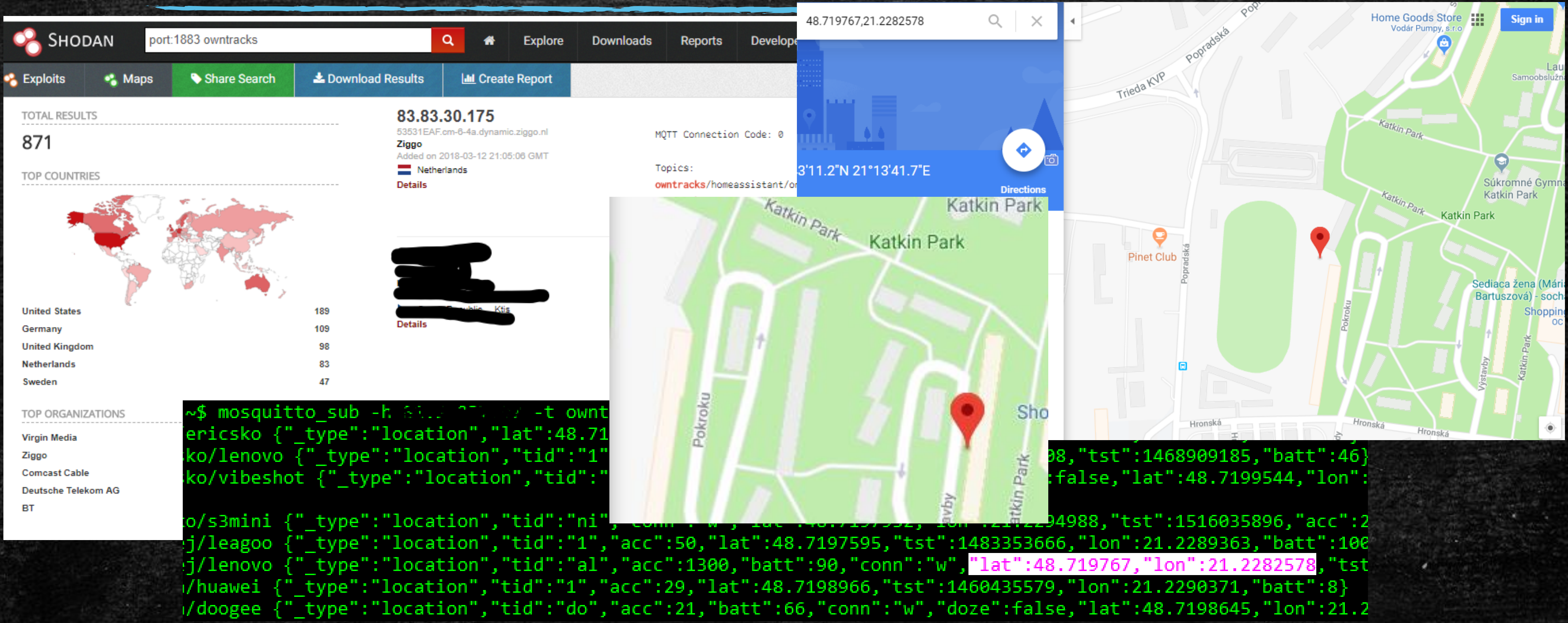
TOTAL RESULTS

430,740

TOP COUNTRIES

United States	366,790
AP	18,367
China	12,551
Germany	3,382
Korea, Republic of	2,224

…I’ll be tracking you



TOTAL RESULTS

871

TOP COUNTRIES

United States	189
Germany	109
United Kingdom	98
Netherlands	83
Sweden	47

TOP ORGANIZATIONS

Virgin Media
Ziggo
Comcast Cable
Deutsche Telekom AG
BT

83.83.30.175
53531EAF.cm-6-4a.dynamic.ziggo.nl
Ziggo
Added on 2018-03-12 21:05:06 GMT
Netherlands
Details

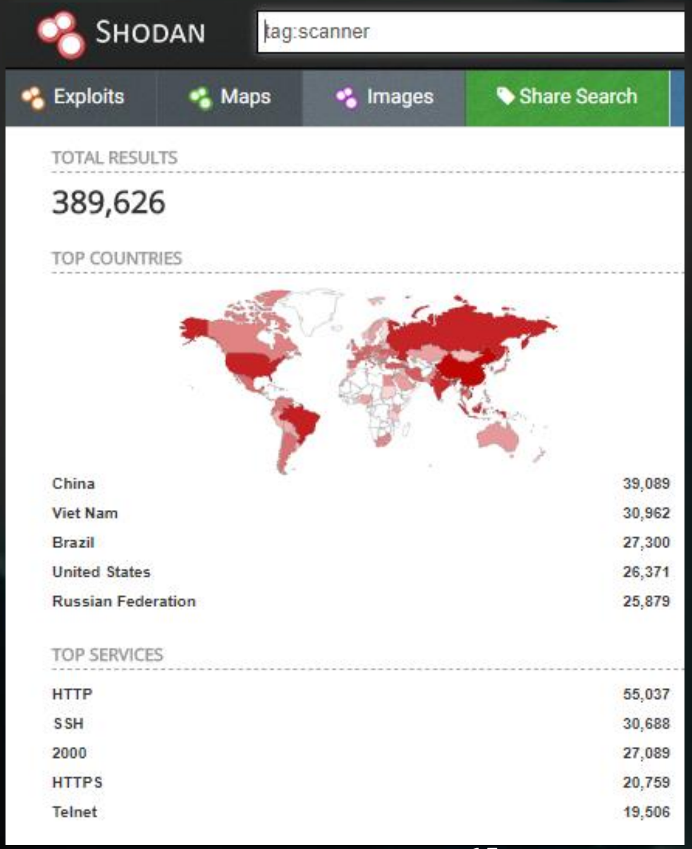
```
MQTT Connection Code: 0

Topics:
owntracks/homeassistant/or
```

[redacted]
Details

```
~$ mosquitto_sub -h [redacted] -t ownt
ericsko {"_type":"location","lat":48.71
ko/lenovo {"_type":"location","tid":"1"                              98,"tst":1468909185,"batt":46}
ko/vibeshot {"_type":"location","tid":"                              :false,"lat":48.7199544,"lon":

o/s3mini {"_type":"location","tid":"ni",                             94988,"tst":1516035896,"acc":2
j/leagoo {"_type":"location","tid":"1","acc":50,"lat":48.7197595,"tst":1483353666,"lon":21.2289363,"batt":100
j/lenovo {"_type":"location","tid":"al","acc":1300,"batt":90,"conn":"w","lat":48.719767,"lon":21.2282578,"tst
/huawei {"_type":"location","tid":"1","acc":29,"lat":48.7198966,"tst":1460435579,"lon":21.2290371,"batt":8}
/doogee {"_type":"location","tid":"do","acc":21,"batt":66,"conn":"w","doze":false,"lat":48.7198645,"lon":21.2
```

If only you could see what I’ve seen...

- Shodan is amazing, but botnets, RDP/SMB bruters/etc. are invisible!
- ….no they’re not
- Enter Greynoise.io & its network of sensors
- Shodan consumes this data too
  - Searchable via tag:scanner
- Andrew Morris speaking at DC26
  - AI Village, Friday @ 1320hrs



TOTAL RESULTS

389,626

TOP COUNTRIES

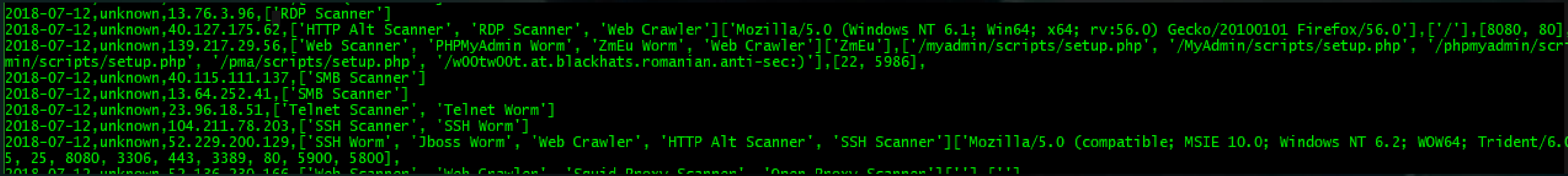
China	39,089
Viet Nam	30,962
Brazil	27,300
United States	26,371
Russian Federation	25,879

TOP SERVICES

HTTP	55,037
SSH	30,688
2000	27,089
HTTPS	20,759
Telnet	19,506

…with your eyes

- Correlate probe activity ←→ port exposure
- Port probes against same port exposed? Probably a bot!
  - RDP, SMB, SSH, Telnet
  - JBoss, Drupal worms
  - Muhstik, ZmEu advertise via User-Agent 🤦



```
2018-07-12,unknown,13.76.3.96,['RDP Scanner']
2018-07-12,unknown,40.127.175.62,['HTTP Alt Scanner', 'RDP Scanner', 'Web Crawler']['Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0'],['/'],[8080, 80],
2018-07-12,unknown,139.217.29.56,['Web Scanner', 'PHPMyAdmin Worm', 'ZmEu Worm', 'Web Crawler']['ZmEu'],['/myadmin/scripts/setup.php', '/MyAdmin/scripts/setup.php', '/phpmyadmin/scri
min/scripts/setup.php', '/pma/scripts/setup.php', '/w00tw00t.at.blackhats.romanian.anti-sec:)'],[22, 5986],
2018-07-12,unknown,40.115.111.137,['SMB Scanner']
2018-07-12,unknown,13.64.252.41,['SMB Scanner']
2018-07-12,unknown,23.96.18.51,['Telnet Scanner', 'Telnet Worm']
2018-07-12,unknown,104.211.78.203,['SSH Scanner', 'SSH Worm']
2018-07-12,unknown,52.229.200.129,['SSH Worm', 'Jboss Worm', 'Web Crawler', 'HTTP Alt Scanner', 'SSH Scanner']['Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)
5, 25, 8080, 3306, 443, 3389, 80, 5900, 5800],
2018-07-12,unknown,52.136.230.166,['Web Scanner', 'Web Crawler', 'Squid Proxy Scanner', 'Open Proxy Scanner'][''],['']
```

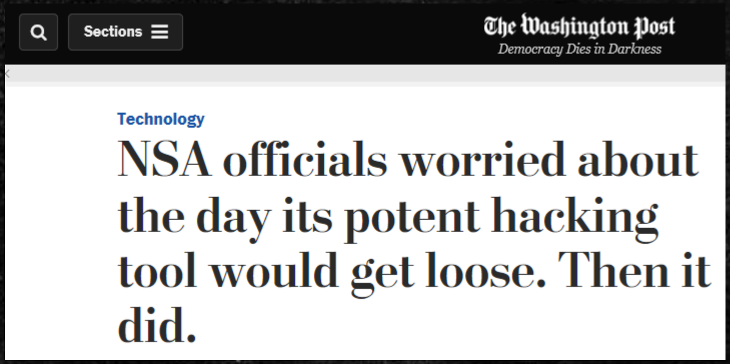
Cats: How are you gentlemen!!

We view this as keeping our oath to protect and defend against enemies foreign and domestic. TheShadowBrokers has is having little of each as our auction was an apparent failure. Be considering this our form of protest.

--ShadowBrokers, April 8th 2017

Cats: You are on the way to destruction

- [REDACTED] weaponized an SMBv1 exploit (EternalBlue)
- [REDACTED] added it to their Metasploit clone
- [REDACTED] lost control of this tool
- Microsoft patched in March 2017 via MS17-010
- ShadowBrokers dropped 0-day on April 14th, 2017 (MS17-010 +31 days)
- No sane person would expose SMB to the Internet…..



Technology

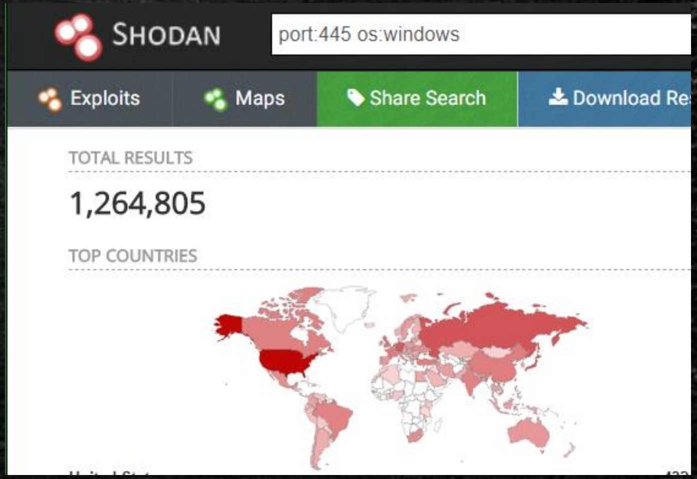
NSA officials worried about the day its potent hacking tool would get loose. Then it did.

The NSA: Still F*cking Up

The deepest of the deep state managed to get itself hacked.

BY CHARLES P. PIERCE NOV 13, 2017

267



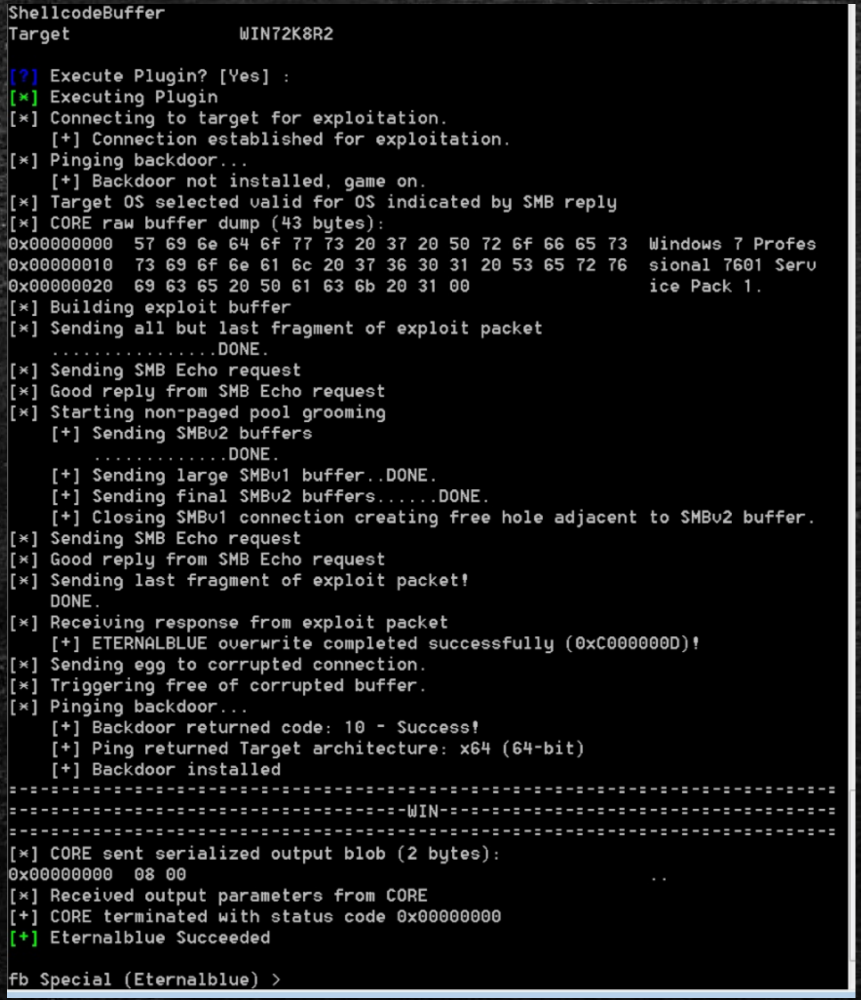
port:445 os:windows

TOTAL RESULTS

1,264,805

TOP COUNTRIES

Finding DoublePulsar in Azure

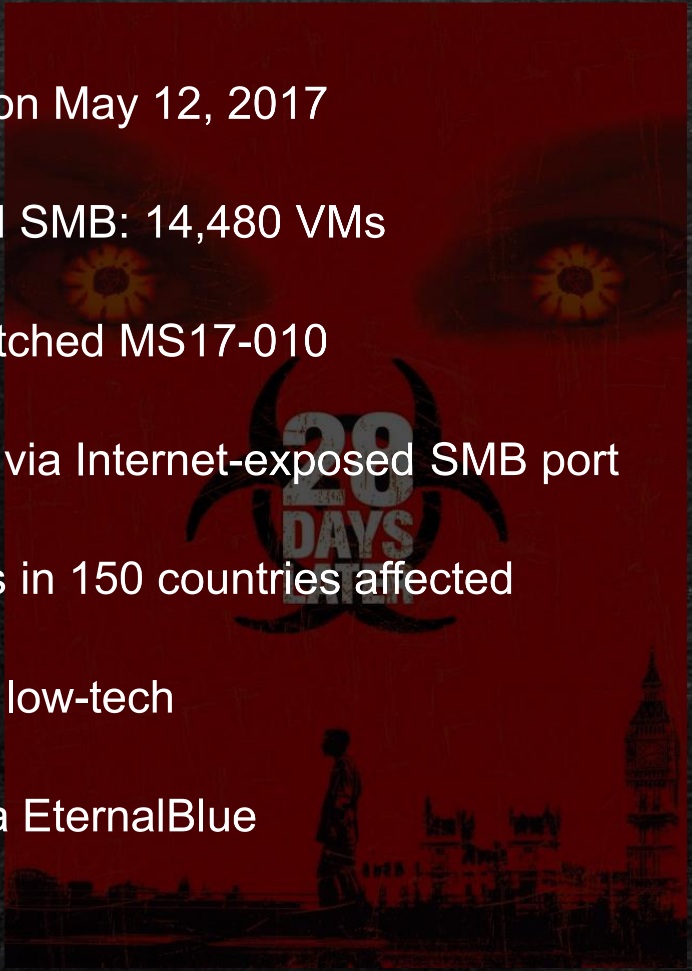


```
ShellcodeBuffer
Target                WIN72K8R2

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[*] Connecting to target for exploitation.
    [+] Connection established for exploitation.
[*] Pinging backdoor...
    [+] Backdoor not installed, game on.
[*] Target OS selected valid for OS indicated by SMB reply
[*] CORE raw buffer dump (43 bytes):
0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
0x00000020  69 63 65 20 50 61 63 6b 20 31 00                 ice Pack 1.
[*] Building exploit buffer
[*] Sending all but last fragment of exploit packet
    ................DONE.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Starting non-paged pool grooming
    [+] Sending SMBv2 buffers
        .............DONE.
    [+] Sending large SMBv1 buffer..DONE.
    [+] Sending final SMBv2 buffers......DONE.
    [+] Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Sending last fragment of exploit packet!
    DONE.
[*] Receiving response from exploit packet
    [+] ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] Sending egg to corrupted connection.
[*] Triggering free of corrupted buffer.
[*] Pinging backdoor...
    [+] Backdoor returned code: 10 - Success!
    [+] Ping returned Target architecture: x64 (64-bit)
    [+] Backdoor installed
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] CORE sent serialized output blob (2 bytes):
0x00000000  08 00                                            ..
[*] Received output parameters from CORE
[+] CORE terminated with status code 0x00000000
[+] Eternalblue Succeeded

fb Special (Eternalblue) >
```

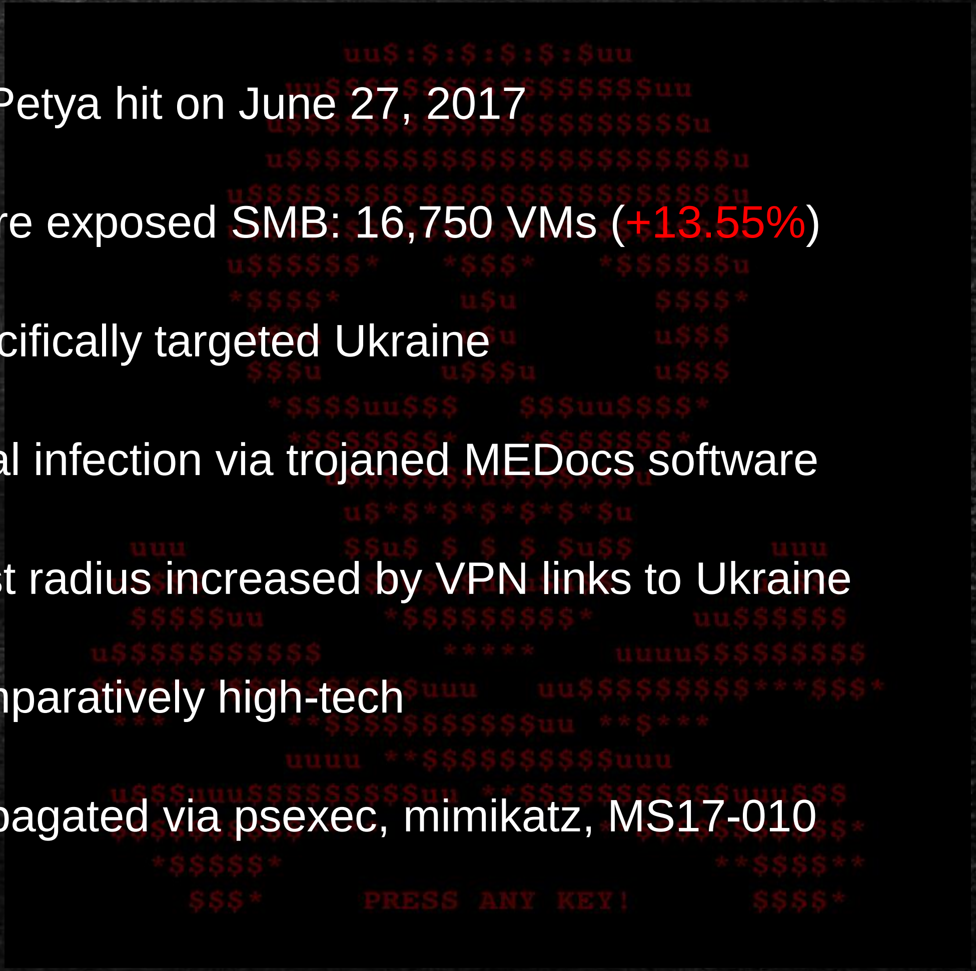
- Only 14k VM's exposing TCP/445
- Initially undetectable by Shodan
- Detection via unused SMB error code (0x51)
- Manually scanned all IP's exposing TCP/445
- Low number of implants (<50)
- That means everyone patched!!!

MISSION ACCOMPLISHED

Cats: You have no chance to survive make your time



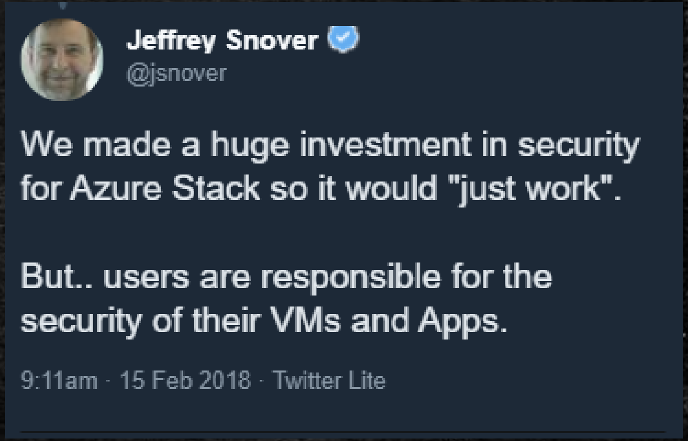
- WannaCry hit on May 12, 2017
- Azure exposed SMB: 14,480 VMs
- Targeted unpatched MS17-010
- Initial infection via Internet-exposed SMB port
- 230k+ systems in 150 countries affected
- Comparatively low-tech
- Propagated via EternalBlue



- NotPetya hit on June 27, 2017
- Azure exposed SMB: 16,750 VMs (+13.55%)
- Specifically targeted Ukraine
- Initial infection via trojaned MEDocs software
- Blast radius increased by VPN links to Ukraine
- Comparatively high-tech
- Propagated via psexec, mimikatz, MS17-010

Your IaaS security *is your responsibility*

- Ever hear about Express Route and Direct Connect?
  - "Microsoft Azure ExpressRoute lets you extend your on-premises networks into the Microsoft cloud…."
  - "Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS."
- That sounds like a VPN! (spoiler alert: it is)
- How are you managing ACL's on P2P cloud connections?
- Is your cloud *actually* isolated from on-premises network?
- Do your IT policies extend to your cloud subscriptions?
  - Who is patching your IaaS servers?



Jeffrey Snover
@jsnover

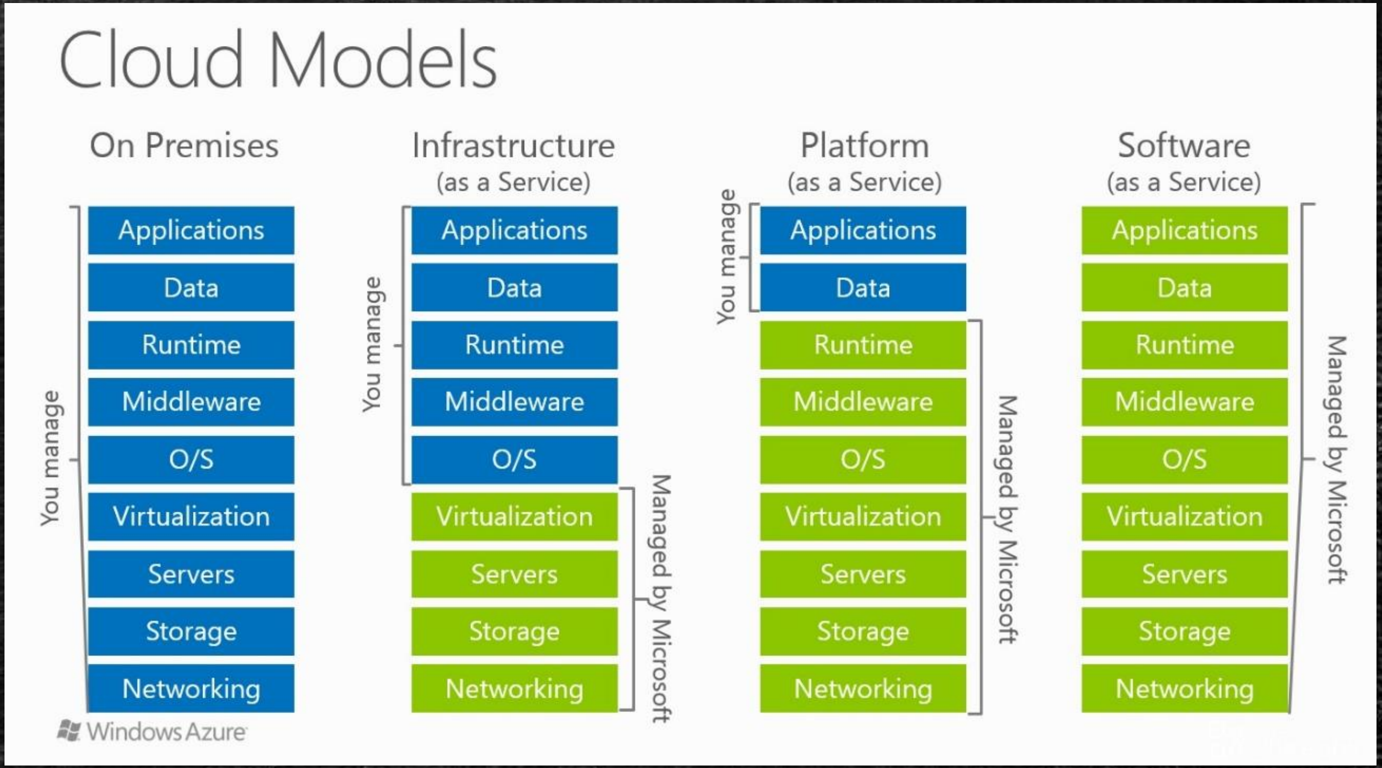
We made a huge investment in security for Azure Stack so it would "just work".

But.. users are responsible for the security of their VMs and Apps.

9:11am · 15 Feb 2018 · Twitter Lite

PaaS & SaaS are shared responsibility

- “Patching causes downtime”
- “My cloud provider handles patching”
- PaaS & SaaS can help!
- Understand shared responsibility
- Patching handled by Microsoft
  - SaaS
  - PaaS (if you let us)

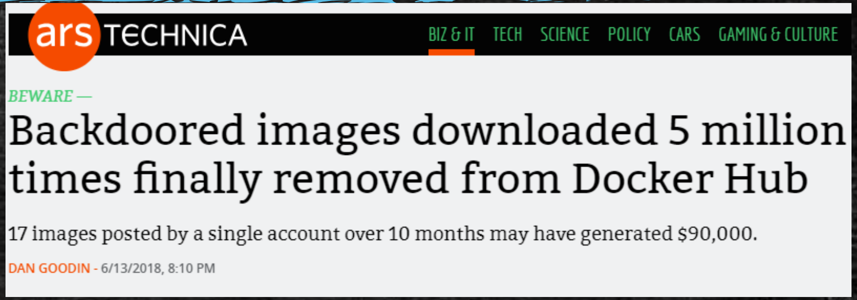


Cloud Models

On Premises	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

Cloud marketplaces are supply chains

- Supply chain attacks are increasingly common
- Cloud marketplaces are next
- Lots of resources; high value targets
- Minimal validation of 3rd party IaaS VM images
- 3rd party IaaS images are ***OLD***
  - Average Azure Age: **172 days**
  - Average AWS Age: **717 days**
- Updating IaaS VM images is not retroactive

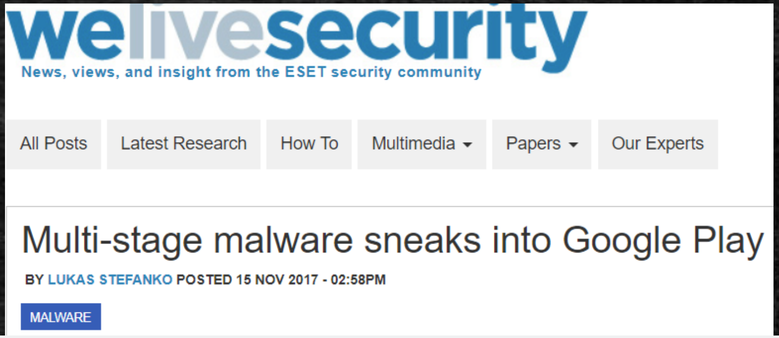


BEWARE —

Backdoored images downloaded 5 million times finally removed from Docker Hub

17 images posted by a single account over 10 months may have generated $90,000.

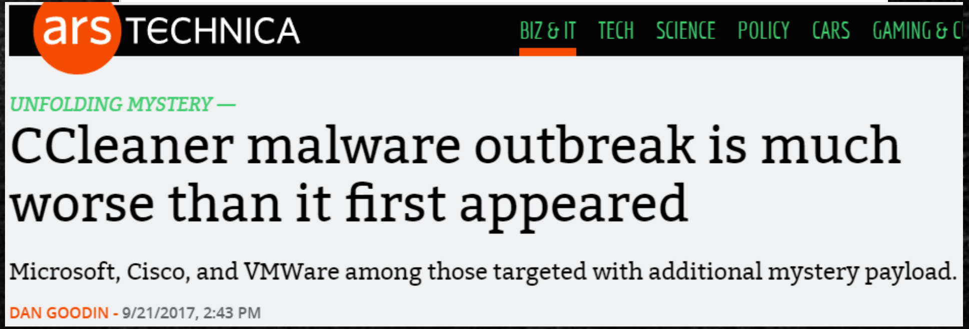
DAN GOODIN - 6/13/2018, 8:10 PM



Multi-stage malware sneaks into Google Play

BY LUKAS STEFANKO POSTED 15 NOV 2017 - 02:58PM

MALWARE



UNFOLDING MYSTERY —

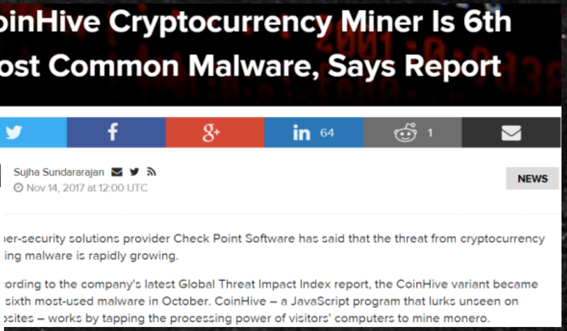
CCleaner malware outbreak is much worse than it first appeared

Microsoft, Cisco, and VMWare among those targeted with additional mystery payload.

DAN GOODIN - 9/21/2017, 2:43 PM

2018: Year of the CryptoMiner

- Cryptomining is the new Ransomware
- NoSQL attack campaign shifted
- Open S3 buckets being attacked
- Any vulnerable system is a target



CoinHive Cryptocurrency Miner Is 6th Most Common Malware, Says Report

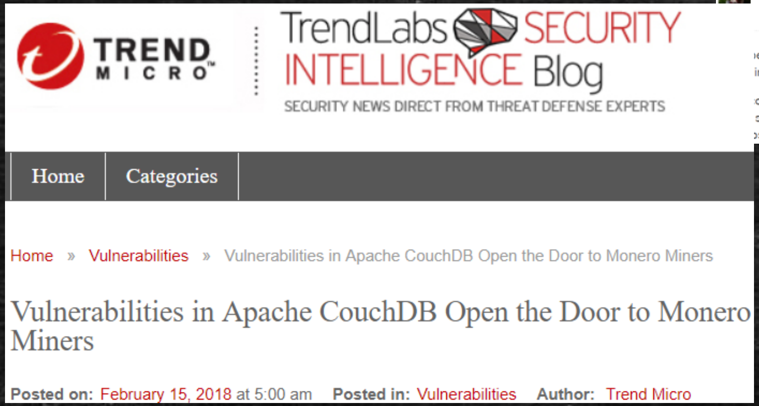
Sujha Sundararajan

Nov 14, 2017 at 12:00 UTC

NEWS

ɔer-security solutions provider Check Point Software has said that the threat from cryptocurrency ing malware is rapidly growing.

ːording to the company's latest Global Threat Impact Index report, the CoinHive variant became sixth most-used malware in October. CoinHive – a JavaScript program that lurks unseen on ɔsites – works by tapping the processing power of visitors' computers to mine monero.



TREND MICRO

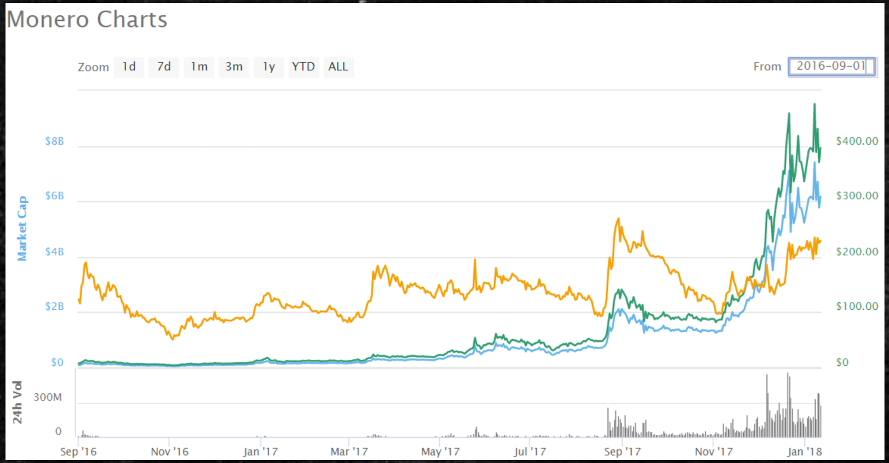
TrendLabs SECURITY INTELLIGENCE Blog

SECURITY NEWS DIRECT FROM THREAT DEFENSE EXPERTS

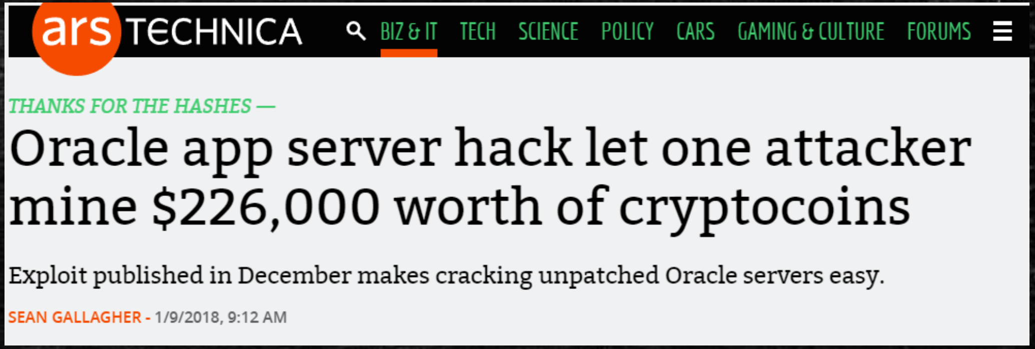
Home » Vulnerabilities » Vulnerabilities in Apache CouchDB Open the Door to Monero Miners

Vulnerabilities in Apache CouchDB Open the Door to Monero Miners

Posted on: February 15, 2018 at 5:00 am Posted in: Vulnerabilities Author: Trend Micro



Monero Charts



ars TECHNICA

THANKS FOR THE HASHES —

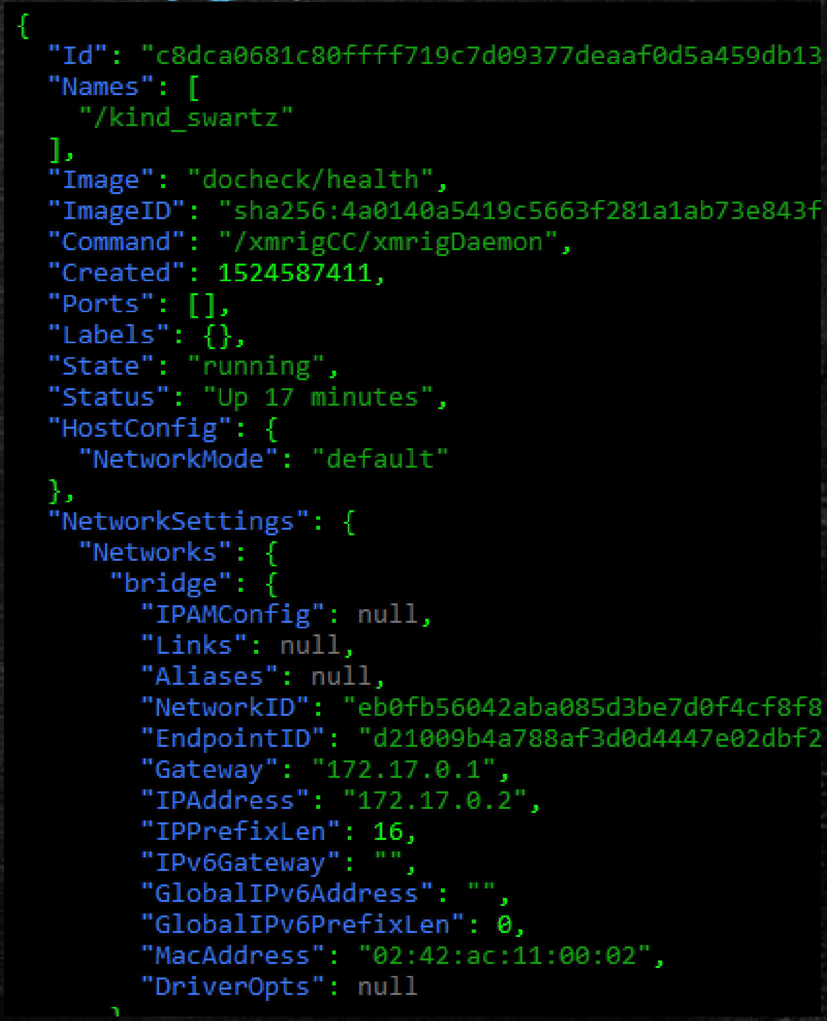
Oracle app server hack let one attacker mine $226,000 worth of cryptocoins

Exploit published in December makes cracking unpatched Oracle servers easy.

SEAN GALLAGHER - 1/9/2018, 9:12 AM

Docker Monero Mining Campaign

- TCP/2375 – HTTP Admin port for Docker Servers
  - Guess whether authentication is enabled ;)
- curl http://[ip address]:2375/containers/json | jq’.’
- Run via xmrigDaemon Command
- Proxying miner traffic thru hacked Azure VMs
- Impossible to determine profitability?
- Make The World a Safer Place #TR18



```
{
  "Id": "c8dca0681c80ffff719c7d09377deaaf0d5a459db13
  "Names": [
    "/kind_swartz"
  ],
  "Image": "docheck/health",
  "ImageID": "sha256:4a0140a5419c5663f281a1ab73e843f
  "Command": "/xmrigCC/xmrigDaemon",
  "Created": 1524587411,
  "Ports": [],
  "Labels": {},
  "State": "running",
  "Status": "Up 17 minutes",
  "HostConfig": {
    "NetworkMode": "default"
  },
  "NetworkSettings": {
    "Networks": {
      "bridge": {
        "IPAMConfig": null,
        "Links": null,
        "Aliases": null,
        "NetworkID": "eb0fb56042aba085d3be7d0f4cf8f8
        "EndpointID": "d21009b4a788af3d0d4447e02dbf2
        "Gateway": "172.17.0.1",
        "IPAddress": "172.17.0.2",
        "IPPrefixLen": 16,
        "IPv6Gateway": "",
        "GlobalIPv6Address": "",
        "GlobalIPv6PrefixLen": 0,
        "MacAddress": "02:42:ac:11:00:02",
        "DriverOpts": null
      }
```

Captain: For great justice

- Update your IaaS VMs immediately after deployment
- Review firewall settings before deployment
- For sensitive roles consider building your IaaS Image
- Better visibility into out-of-the-box IaaS VM security
  - Age of IaaS VM image
  - Default firewall policies
  - Version info of daemons/services
- Azure Security Center: Free tier provides recommendations

THANK YOU BSIDESLV!

Questions?

Nate Warfield – @dk_effect

The opinions expressed are my own and do not necessarily reflect those of Microsoft Corporation.