



WILD WEST HACKIN' FEST

All Your Clouds Are Belonging 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.

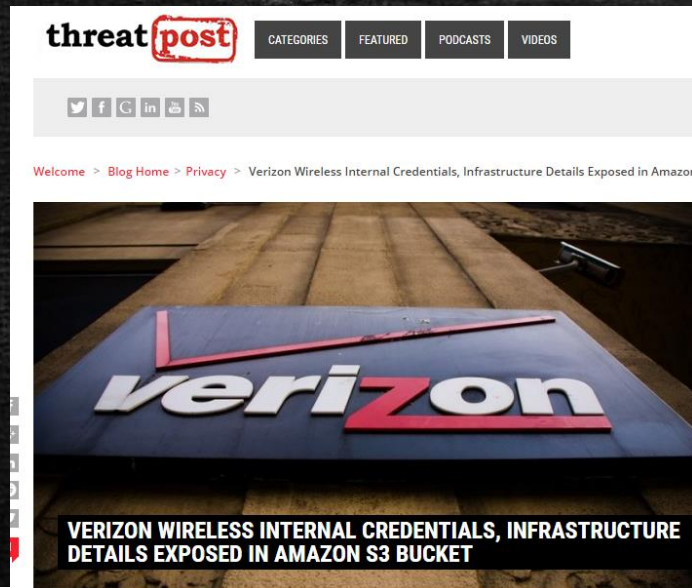
Whoami: Nate Warfield (@dk_effect)

- Hacker – Microsoft Security Response Team
 - Vulnerability Management for Azure, Windows, Hyper-V
 - Battle scars: MS17-010, WannaCry, NotPetya, Spectre/Meltdown
- `cat ~/.bash_history`
 - 18 years in Network Engineering; 20-year Grey Hat
 - Kaspersky SAS 2018
 - Troopers 18
 - BSidesLV 2018
 - BruCON 0x0A
- 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



InfoWorld
FROM IDG

Home > Information Security

Attackers start wiping data from CouchDB and Hadoop databases

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

Someone Hijacking Unsecured MongoDB Databases for Ransom

Swati K

Security

January 03, 2017

```
cor@windowlicker:~$ mongo
MongoDB shell version v3.6.0
connecting to: mongodb://10.10.10.10:27021/
MongoDB server version: 3.6.0
```

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

SHARE



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.

CNN tech

BUSINESS

CULTURE

GADGETS

FUTURE

STARTUPS



Cyber-Safe

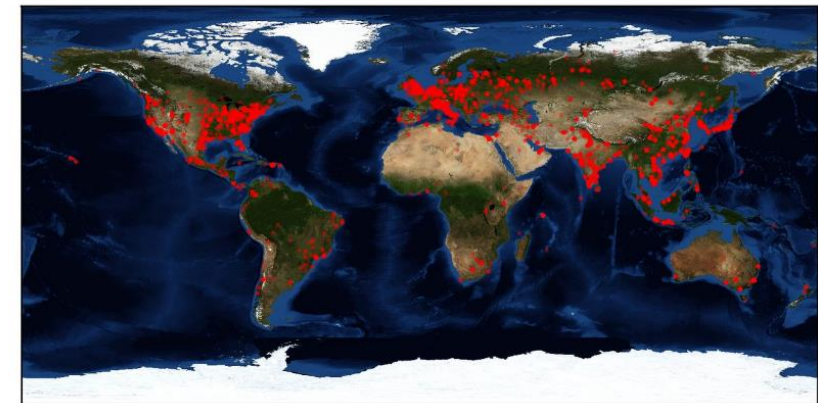
Data of almost 200 million voters leaked online by GOP analytics firm

by Selena Larson @selenalarson

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

By Catalin Cimpanu

April 21, 2017 05:10 PM



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

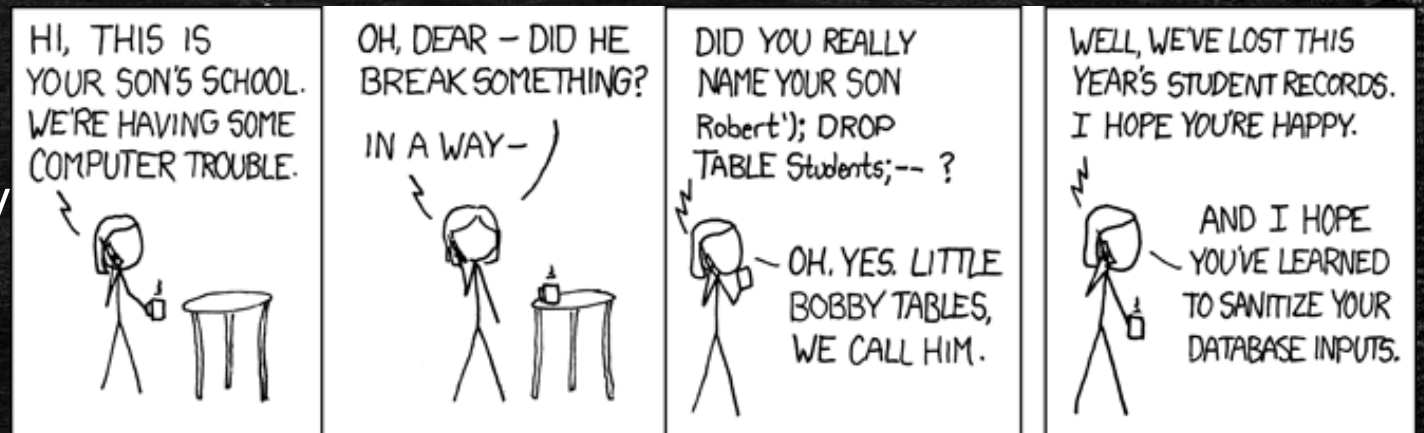


Image Source: https://imgs.xkcd.com/comics/exploits_of_a_mom.png

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 within 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
- 33k pwned DBs as of 9/28/2018
- 22k pwned DBs today: **33% decrease!**
- Requires Shodan Enterprise API

 **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



Country	Count
1. United States	7,747
2. China	4,291
3. France	1,227
4. Germany	947
5. India	1,137
6. Japan	1,005
7. Russia	1,005
8. South Korea	1,005
9. Taiwan	1,005
10. Thailand	1,005

1:30pm · 26 Dec 2017 · Buffer

 **SHODAN**

 Exploits  Maps  Share Search

TOTAL RESULTS
22,212

TOP COUNTRIES

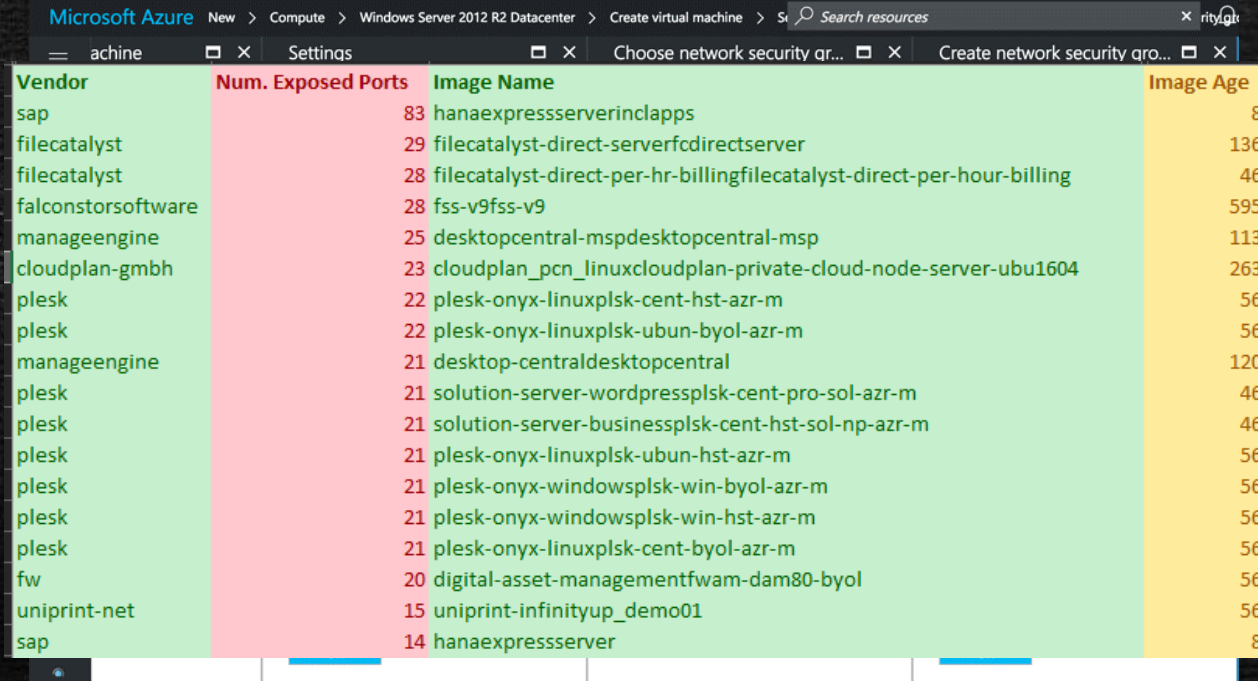


Country	Count
United States	7,747
China	4,291
France	1,227
India	1,137
Germany	947

TOP SERVICES

Service	Count
MongoDB	11,005
Elastic Search	4,974
HTTP	3,083
Redis	2,781
5984	338

Network Security Group (Azure)



The screenshot shows the Microsoft Azure portal interface. The breadcrumb navigation at the top reads: Microsoft Azure > New > Compute > Windows Server 2012 R2 Datacenter > Create virtual machine > Search resources. Below the navigation, there are several tabs: 'achine', 'Settings', 'Choose network security gr...', and 'Create network security gro...'. The main content area displays a table with four columns: Vendor, Num. Exposed Ports, Image Name, and Image Age. The table lists various VM images from different vendors, including sap, filecatalyst, falconstorsoftware, manageengine, cloudplan-gmbh, plesk, fw, uniprint-net, and hanaexpressserver. The 'Num. Exposed Ports' column is highlighted in pink, and the 'Image Age' column is highlighted in yellow.

Vendor	Num. Exposed Ports	Image Name	Image Age
sap	83	hanaexpressserverinclapps	8
filecatalyst	29	filecatalyst-direct-serverfcdirectserver	136
filecatalyst	28	filecatalyst-direct-per-hr-billingfilecatalyst-direct-per-hour-billing	46
falconstorsoftware	28	fss-v9fss-v9	595
manageengine	25	desktopcentral-mspdesktopcentral-msp	113
cloudplan-gmbh	23	cloudplan_pcn_linuxcloudplan-private-cloud-node-server-ubu1604	263
plesk	22	plesk-onyx-linuxpls-cent-hst-azr-m	56
plesk	22	plesk-onyx-linuxpls-ubun-byol-azr-m	56
manageengine	21	desktop-centraldesktopcentral	120
plesk	21	solution-server-wordpresspls-cent-pro-sol-azr-m	46
plesk	21	solution-server-businesspls-cent-hst-sol-np-azr-m	46
plesk	21	plesk-onyx-linuxpls-ubun-hst-azr-m	56
plesk	21	plesk-onyx-windowspls-win-byol-azr-m	56
plesk	21	plesk-onyx-windowspls-win-hst-azr-m	56
plesk	21	plesk-onyx-linuxpls-cent-byol-azr-m	56
fw	20	digital-asset-managementfwam-dam80-byol	56
uniprint-net	15	uniprint-infinityup_demo01	56
sap	14	hanaexpressserver	8

- 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

API ALL THE THINGS!

- We ♥ APIs
- Most things in Azure have an API
- Azure Marketplace Gallery is no exception
- VM artifacts == additional files used for deployment
- Everything accessible via unauthenticated API
- Lots of...stuff...gets uploaded as an artifact
- Official GitHub: <https://github.com/Azure/portaldocs>

```
__MACOSX_.json 5
website_NewHostingPlan_MySQL... 10
Thumbnails_5b89f42b-7dfa-48... 10
iot-edge-metadata.json 15
__MACOSX_.storageAccount-e... 15
Thumbnails_8e7d1b81-fff4-47... 15
__MACOSX_.storageAccount-n... 15
Thumbnails_33778f36-d78f-4e... 15
__MACOSX_.vnet-existing.json 15
__MACOSX_.vnet-new.json 15
Thumbnails_bced8d55-2dfc-42... 15
readme.txt 16
__MACOSX_.publicip-existin... 17
__MACOSX_.publicip-new.json 17
website_NewHostingPlan_SQL... 17
provisioner-first-boot.sh 18
README.md 24
website_NewHostingPlan-Default 26
__MACOSX_.createUiDefiniti... 30
__MACOSX_.mainTemplate.json 31
storageAccount-new.json 37
storageAccount-existing.json 37
Details 41
vnet-existing.json 44
vnet-new.json 46
CreateResources 47
publicIP-existing.json 48
publicIP-new.json 48
CreateResource 54
MainTemplate 62
metadata.json 108
createuidefinition 2724
DefaultTemplate 2803
```


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 Launch

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

Once you accept the terms, you will have access to launch any version of in any supported region. For future launches, you can return to this page 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.large

VPC Settings
Will launch into: subnet-fab5edc5 (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 (Nov 2017)
- 11k AMI's in AWS – 5x as many as Azure
- Data indicates many clouds have this problem

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?

```
@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
5.24.172 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
1.212.236 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
1.147.99 cpe:/a:exim:exim:4.76
200.39 cpe:/a:exim:exim:4.89_1
1.52.42 cpe:/a:exim:exim:4.80
```


Threat hunting (new way): The vuln: tag

- Worked with Shodan to incorporate CPE ↔ CVE detections
- Search via 'vuln:' tag (Enterprise API only)
- Verified: False == *implied* vulnerable
 - Based off version data
- Verified: True == confirmed vulnerable
 - Ex: MS17-010

```
elliott@doknowevil:~$ shodan count vuln:CVE-2018-6789
267082
elliott@doknowevil:~$ shodan count vuln:CVE-2018-6789 org:microsoft
161
```

City	London
Country	United Kingdom
Organization	Digital Ocean
ISP	Digital Ocean
Last Update	2018-10-03T13:23:18.239638
ASN	AS14061
Web Technologies	
Bootstrap	
Font Awesome	
Google Font API	
jQuery	
Vulnerabilities	
<small>Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.</small>	
CVE-2014-8109	mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives, as demonstrated by a configuration that specifies authorization for one group to access a certain directory, and authorization for a second group to access a second directory.
CVE-2015-3185	The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.
CVE-2014-0226	Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/ua/lua_request.c.

Every (MQTT) step you take...

- MQTT – publish/subscribe message protocol
- Used by IoT, Facebook Messenger, many more
- Azure & AWS offer MQTT-based solutions
- Internet exposure **+1559%** 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)
```

```
+-----+-----+-----+
| facet_date | port | count |
+-----+-----+-----+
| 2017-10-26 | 1883 | 38285 |
| 2018-10-26 | 1883 | 597172 |
+-----+-----+-----+
```



...I'll be tracking you

SHODAN port:1883 owntracks

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

871

TOP COUNTRIES

- United States
- Germany
- United Kingdom
- Netherlands

Nate Warfield at BruCON0x0A @dk_effect · Aug 16
threatpost.com/open-mqtt-serv... - Gee, I remember someone else talking about MQTT & Owntracks this year. I guess I should be flattered others are following my research?

Open MQTT Servers Raise Physical Threats in Sm...
Tens of thousands of consumer-grade Internet of Things (IoT) servers have been found wide-open on the internet, allowing cybercriminals to potentially compromise

48.719767,21.2282578
311.2°N 21°13'41.7"E
Directions

Pinet Club

zanzito/Dennis2/device_info {"time":1521550330,"device_info":"ZTE Z958 (6.0.1)","charge_type":"None","battery_charging":false,"battery_level":92,"current_foreground_app":"Zanzito","screen_locked":false,"screen_on":true,"screen_orientation":"Portrait","current_wifi":"\\\"NETGEAR_EXT\\\"","current_operator":"AT&T"

lat":48.719767,"lon":21.2282578

It's unfortunate that users pay so little attention to security, in spite of us clearly documenting that in our booklet.
[owntracks.org/booklet/guide/...](http://owntracks.org/booklet/guide/)

12:56 AM - 23 Aug 2018

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

NSA Hackers
Shadow Brokers

CrDj"(;Va.*NdlnzB9M?@K2)#>deB7mN

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.....



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 SMBu2 buffers
    .....DONE.
    [+] Sending large SMBu1 buffer..DONE.
    [+] Sending final SMBu2 buffers.....DONE.
    [+] Closing SMBu1 connection creating free hole adjacent to SMBu2 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
=====
[+] CORE sent serialized output blob (2 bytes):
0x00000000  08 00
[*] Received output parameters from CORE
[+] CORE terminated with status code 0x00000000
[+] Eternalblue Succeeded

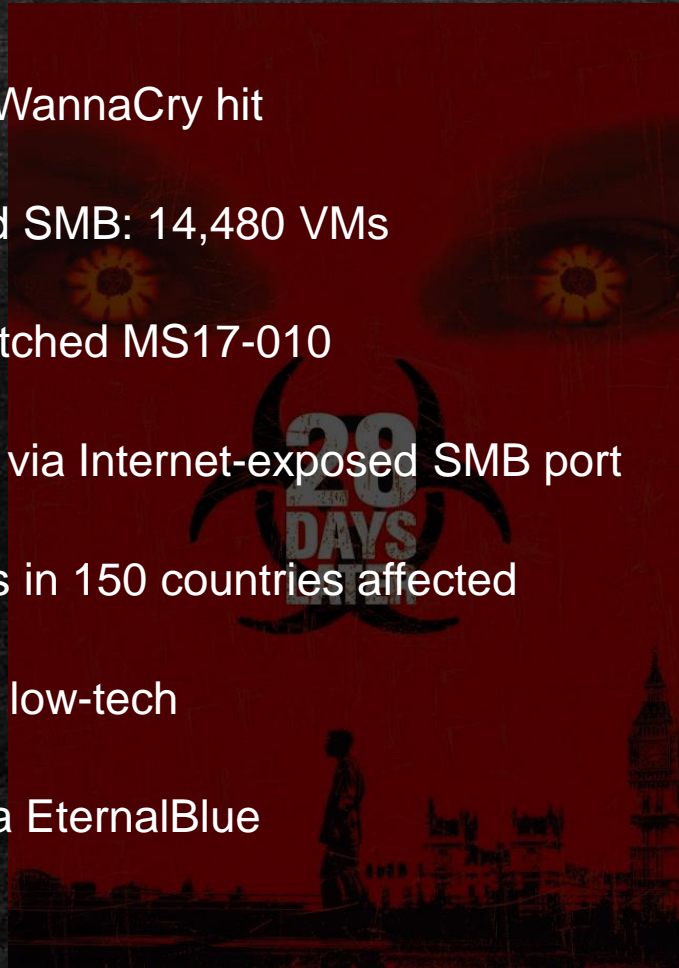
fb Special (Eternalblue) >
```

- 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!!!



Cats: You have no chance to survive make your time

- 28 days later, WannaCry hit
- 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 dropped 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



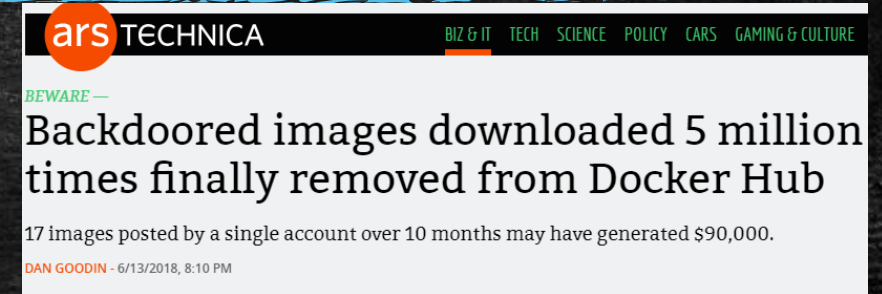
Your IaaS security *is your responsibility*

- 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! (Narrator: it's totally a VPN)
- 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?



Cloud marketplaces are supply chains

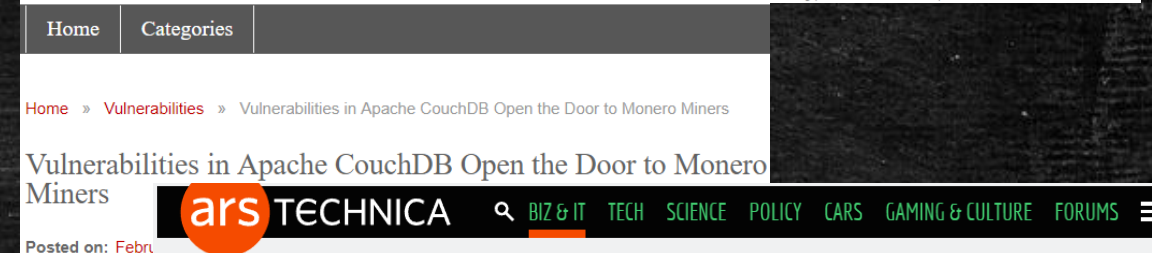
- Supply chain attacks are increasingly common
- Cloud marketplaces are next
- Lots of resources; high value targets
- Minimal validation of 3rd party images
- 3rd party IaaS images are *OLD*
 - Average Azure Age: 140+ days
 - Average AWS Age: 717 days
- Updating IaaS VM images is not retroactive



2018: Year of the CryptoMiner

- Cryptomining is the new Ransomware
- NoSQL attack campaign shifted
- Payout is low, cost to business is high
- Any vulnerable system is a target

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



ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

THANKS FOR THE HASHES —

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

Exploit published in December makes cracking unpatched Oracle servers easy.

Monero Charts

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



SOFTPEDIA® NEWS REVIEWS APPLE MICROSOFT MOBILE LINUX & OSS SECURITY

Softpedia > News > Security

Cryptojacking Is the Top Cybersecurity Threat For the First Half of 2018

Dethrones ransomware from top dog position

Oct 11, 2018 17:18 GMT · By Sergiu Gatlan · Comment · Share: [Twitter](#) [Reddit](#) [Facebook](#) [Google+](#) [Print](#)

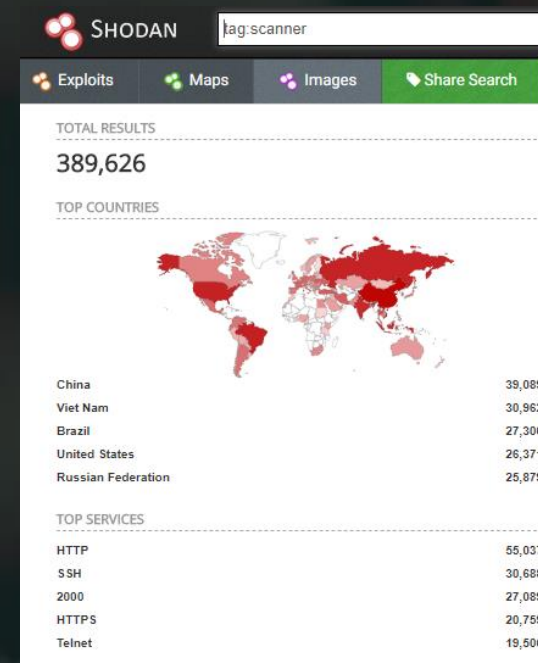
Docker Monero Mining Campaign

- TCP/2375 – HTTP Admin port for Docker Servers
 - No auth because of course not 🤖
- `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
      }
    }
  }
}
```


I've seen things...

- 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
- Greynoise is metadata heavy (w00t!)
 - Ports, paths, user-agent, ASN



..you people wouldn't believe.

- Correlate probe activity \leftrightarrow port exposure
- Port probes against same port exposed? Probably a bot!
 - RDP, SMB, SSH, Telnet, IIS
 - JBoss, Drupal worms, Mirai, etc.
 - Muhstik, ZmEu advertise via User-Agent 
 - Trends over time FTW

asn	date	port	count
AS21928	2018-09-20	5555	500
AS21928	2018-09-22	5555	491
AS21928	2018-09-23	5555	568
AS21928	2018-09-24	5555	575
AS21928	2018-09-25	5555	615
AS21928	2018-09-26	5555	652
AS21928	2018-09-27	5555	662
AS21928	2018-09-28	5555	790
AS21928	2018-09-29	5555	675
AS21928	2018-09-30	5555	752
AS21928	2018-10-01	5555	919
AS21928	2018-10-02	5555	929

```
mysql> select * from tags where tag like '%DAV%' and count >10;
```

asn	date	tag	count
AS45090	2018-09-28	IIS WebDAV Remote Code Execution CVE-2017-7269	26
AS45090	2018-09-29	IIS WebDAV Remote Code Execution CVE-2017-7269	15
AS45090	2018-09-30	IIS WebDAV Remote Code Execution CVE-2017-7269	24
AS45090	2018-10-01	IIS WebDAV Remote Code Execution CVE-2017-7269	30
AS45090	2018-10-02	IIS WebDAV Remote Code Execution CVE-2017-7269	34

Attacks coming from South Dakota..

- 2 big ISPs are Midco & CenturyLink
 - Midco: AS11232
 - CenturyLink: AS209
- South Dakota bad traffic is mostly Mirai
- Script is on my GitHub

```
elliott@doknowevil:~$ python3 gnMonthlyInfected.py AS209
Looking up AS209
Finding infection stats for Qwest Communications Company, LLC
[('Mirai', 171),
 ('Telnet Worm', 137),
 ('SSH Worm', 18),
 ('Unknown Linux Worm', 5),
 ('Windows RDP Cookie Hijacker CVE-2014-6318', 1),
 ('Wordpress Worm', 1)]
Total infected hosts in AS209: 333
```

```
elliott@doknowevil:~$ python3 gnMonthlyInfected.py AS11232
Looking up AS11232
Finding infection stats for Midcontinent Communications
[('Mirai', 29), ('Telnet Worm', 13), ('SSH Worm', 1)]
Total infected hosts in AS11232: 43
```

```
Looking up AS7922
Finding infection stats for Comcast Cable Communications, LLC
[('Mirai', 1196),
 ('Telnet Worm', 879),
 ('SSH Worm', 154),
 ('Unknown Linux Worm', 118),
 ('PHPMYAdmin Worm', 3),
 ('Wordpress Worm', 2),
 ('Windows RDP Cookie Hijacker CVE-2014-6318', 1),
 ('Huawei HG532 UPnP Worm CVE-2017-17215', 1),
 ('IIS WebDAV Remote Code Execution CVE-2017-7269', 1),
 ('Wordpress XML RPC Worm', 1)]
Total infected hosts in AS7922: 2356
elliott@doknowevil:~$ python3 gnMonthlyInfected.py AS5650
Looking up AS5650
Finding infection stats for Frontier Communications of America, Inc.
[('Mirai', 221),
 ('Telnet Worm', 180),
 ('SSH Worm', 15),
 ('Unknown Linux Worm', 10),
 ('PHPMYAdmin Worm', 3)]
Total infected hosts in AS5650: 429
```


..cloud networks scanning the world..

- Malicious cloud tenants
- 'member how your cloud security is still your job?
- My cell carrier is full of Mirai? WTF T-Mobile!

```
Looking up AS21928
Finding infection stats for T-Mobile USA, Inc.
[('Mirai', 6531), ('ADB Worm', 105)]
Total infected hosts in AS21928: 6636
```

```
Looking up AS45090
Finding infection stats for Shenzhen Tencent Computer Systems Company Limited
[('PHPMYAdmin Worm', 586),
 ('SSH Worm', 514),
 ('IIS WebDAV Remote Code Execution CVE-2017-7269', 368),
 ('Mirai', 119),
 ('Telnet Worm', 110),
 ('ZmEu Worm', 5),
 ('Wordpress Worm', 4),
 ('Huawei HG532 UPnP Worm CVE-2017-17215', 4),
 ('Oracle WebLogic CVE-2017-10271 Worm', 3),
 ('Jboss Worm', 1),
 ('Windows RDP Cookie Hijacker CVE-2014-6318', 1)]
Total infected hosts in AS45090: 1715
```

```
elliott@doknowevil:~$ python3 gnMonthlyInfected.py AS14061
Looking up AS14061
Finding infection stats for DigitalOcean, LLC
[('SSH Worm', 750),
 ('Telnet Worm', 266),
 ('Mirai', 239),
 ('PHPMYAdmin Worm', 36),
 ('ZmEu Worm', 7),
 ('Windows RDP Cookie Hijacker CVE-2014-6318', 5),
 ('GPON CVE-2018-10561 Router Worm', 5),
 ('Unknown Linux Worm', 4),
 ('Embedded Device Worm', 3),
 ('IIS WebDAV Remote Code Execution CVE-2017-7269', 2),
 ('Wordpress Worm', 1),
 ('Realtek Miniigd UPnP Worm CVE-2014-8361', 1),
 ('Drupal CVE-2018-7600 Worm', 1),
 ('Huawei HG532 UPnP Worm CVE-2017-17215', 1)]
Total infected hosts in AS14061: 1321
elliott@doknowevil:~$ python3 gnMonthlyInfected.py AS16509
Looking up AS16509
Finding infection stats for Amazon.com, Inc.
[('SSH Worm', 185),
 ('Mirai', 31),
 ('Telnet Worm', 23),
 ('PHPMYAdmin Worm', 22),
 ('Embedded Device Worm', 3),
 ('ADB Worm', 2),
 ('Jboss Worm', 2),
 ('IIS WebDAV Remote Code Execution CVE-2017-7269', 2),
 ('Windows RDP Cookie Hijacker CVE-2014-6318', 1),
 ('ZmEu Worm', 1)]
Total infected hosts in AS16509: 272
elliott@doknowevil:~$ python3 gnMonthlyInfected.py AS8075
Looking up AS8075
Finding infection stats for Microsoft Corporation
[('SSH Worm', 118),
 ('PHPMYAdmin Worm', 8),
 ('Mirai', 7),
 ('Windows RDP Cookie Hijacker CVE-2014-6318', 6),
 ('Jboss Worm', 6),
 ('Telnet Worm', 5),
 ('Unknown Linux Worm', 4),
 ('IIS WebDAV Remote Code Execution CVE-2017-7269', 3),
 ('Wordpress Worm', 3),
 ('Embedded Device Worm', 2),
 ('D-Link 2750B Worm', 1)]
Total infected hosts in AS8075: 163
```


ASN's on fire off the shoulder of Orion

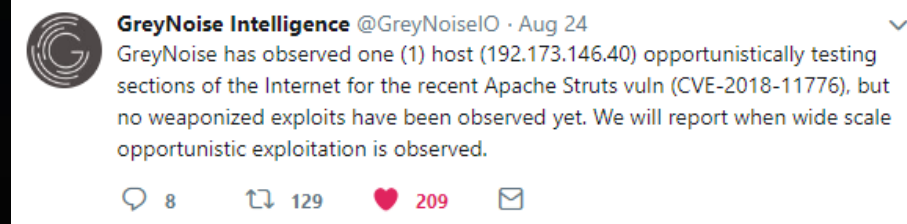
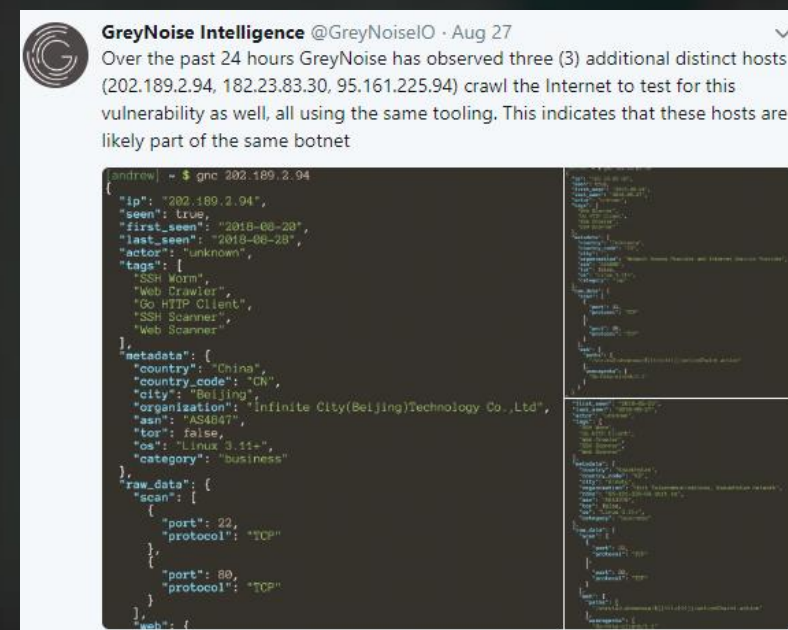
- Tracking activity by ASN is easy
- Daily collection of data → Database → Profit?
- 50 worst ASN's from Greynoise
- Azure, AWS, Comcast, Frontier, others

```
Looking up AS11232
Finding daily stats for Midcontinent Communications
AS11232 Daily Ports:
[(23, 4),
 (2323, 4),
 (88, 3),
 (85, 3),
 (84, 3),
 (83, 3),
 (82, 3),
 (8081, 3),
 (80, 3)]
AS11232 Daily Paths:
[(u'/', 2)]
AS11232 Daily Tags:
[(u'Mirai', 4),
 (u'Telnet Scanner', 4),
 (u'HTTP Alt Scanner', 3),
 (u'Web Scanner', 3),
 (u'Web Crawler', 2),
 (u'SMB Scanner', 2)]
AS11232 Daily UserAgents:
[(u'', 2)]

Looking up AS209
Finding daily stats for Qwest Communications
AS209 Daily Ports:
[(445, 12),
 (23, 8),
 (81, 4),
 (2323, 4),
 (80, 3),
 (8081, 3),
 (22, 2),
 (8080, 2),
 (8181, 1)]
AS209 Daily Paths:
[(u'/', 2), (u'/wp-login.php', 1)]
AS209 Daily Tags:
[(u'SMB Scanner', 12),
 (u'Mirai', 9),
 (u'Telnet Scanner', 8),
 (u'HTTP Alt Scanner', 4),
 (u'Telnet Worm', 4),
 (u'Web Crawler', 3),
 (u'Web Scanner', 3),
 (u'SSH Scanner', 2),
 (u'SSH Worm', 1)]
AS209 Daily UserAgents:
[(u'', 2),
 (u'Mozilla/5.0 (Windows NT 6.1; rv:52.0) Gecko/20100101 Firefox/52.0', 1)]
```


None of this data will be lost in time..

- It may be possible to predict attacks based on trends
- Time-to-weaponize becomes calculatable?
- Iran is doing something....interesting
- 24hr ASN activity code on my GitHub



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







WILD WEST HACKIN' FEST 2018

Nate Warfield – @dk_effect

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