



# 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 scars: 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
  - BSidesLV 2018
- **Twitter: @dk\_effect**
- **GitHub: n0x08**



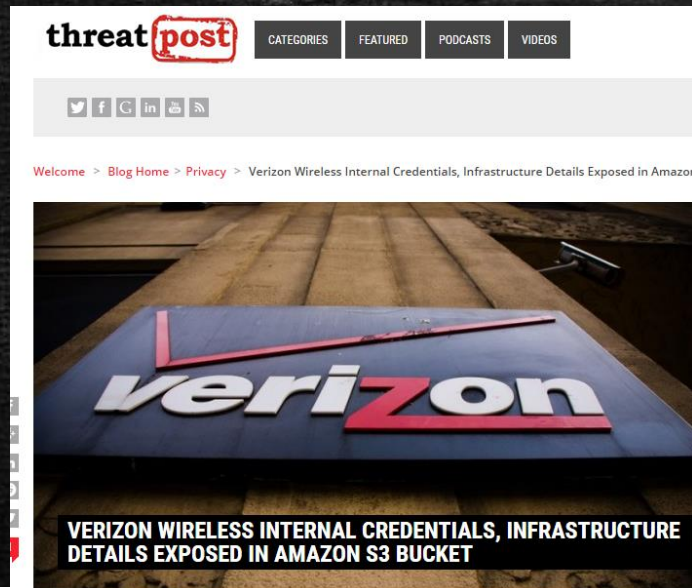
# Captain: What happen?

---

- **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

January 03, 2017 Swati K

Security

tweet G+ Share

## 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



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.

CNN tech

BUSINESS

CULTURE

GADGETS

FUTURE

STARTUPS



Cyber-Safe

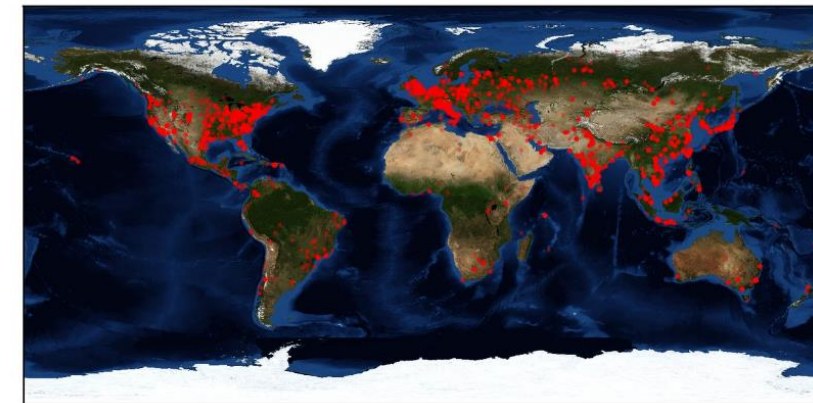
## Data of almost 200 million voters leaked online by GOP analytics firm

by Selena Larson @selenalarson

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

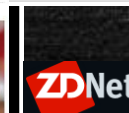
By Catalin Cimpanu

April 21, 2017 05:10 PM



## 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.



MUST READ

Security

## Crypto-coin miners caught away in hacked cloud boxes

Manic miners don't even pwn your 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.



by Michael Mimoso @mimoso

September 1, 2017

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 web folders and, in some cases, install malicious code.

2018



# 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

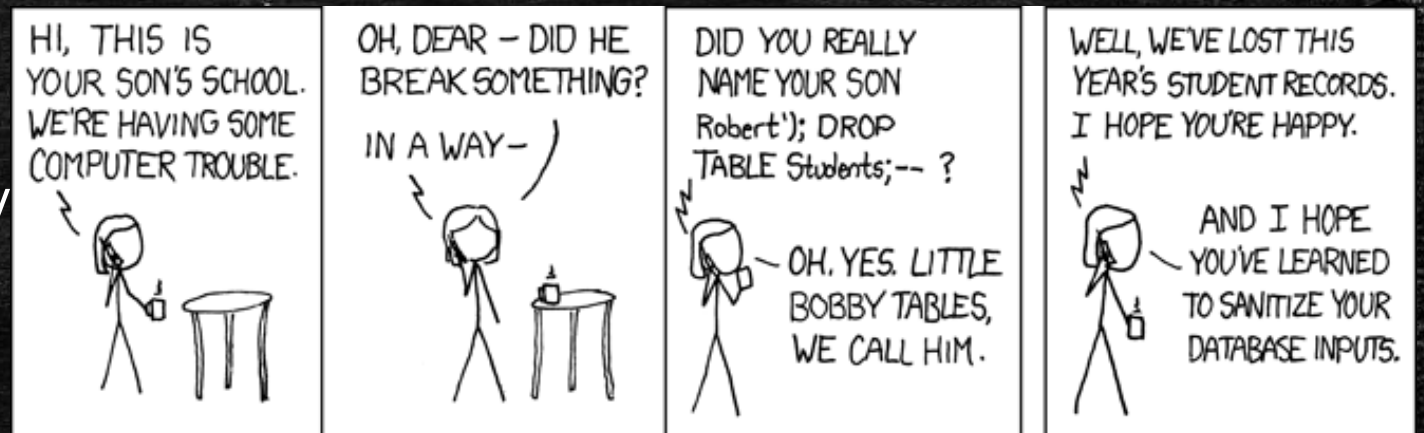


Image Source: [https://imgs.xkcd.com/comics/exploits\\_of\\_a\\_mom.png](https://imgs.xkcd.com/comics/exploits_of_a_mom.png)



# 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



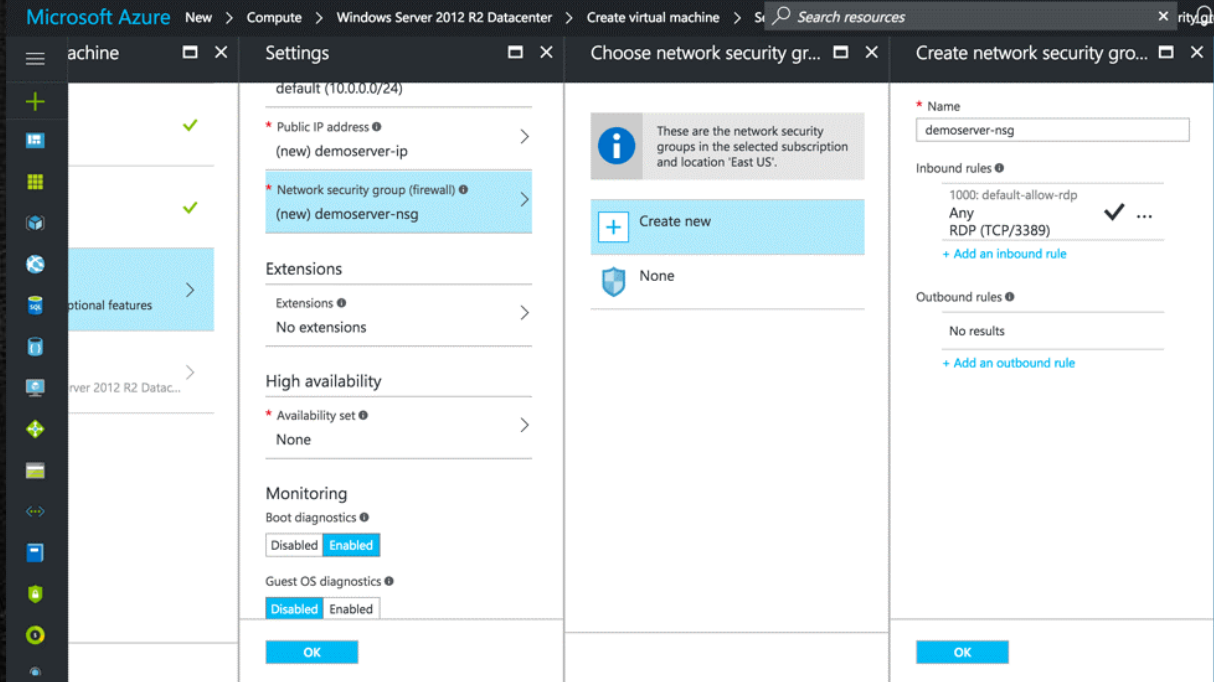
# Operator: Main screen turn on

- 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
- Requires Shodan Enterprise API
- ..or..
- <https://gist.github.com/n0x08>





# Network Security Group (Azure)



- 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 Launch

Click "Accept Software Terms & Launch with 1-Click" 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 3<sup>rd</sup> 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



# 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 **+1485%** 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)
```

```
mysql> select * from stats where facet_date like '2018-09-25' and port = 1883;
+-----+-----+-----+
| facet_date | port | count |
+-----+-----+-----+
| 2017-09-25 | 1883 | 34058 |
| 2018-09-25 | 1883 | 505960 |
+-----+-----+-----+
```





# ...I'll be tracking you

**SHODAN** port:1883 owntracks

**Exploits** **Maps** **Share Search** **Download Results** **Create Report**

**TOTAL RESULTS**  
871

**TOP COUNTRIES**

- United States
- Germany
- United Kingdom
- Netherlands
- Sweden

**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/m...  
owntracks/homeassistant/m...

**MQTT Connection Code:** 0

**Topics:**  
owntracks/...  
owntracks/...  
owntracks/...  
owntracks/...  
owntracks/...

**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 threatpost.com

**OwnTracks**  
@OwnTracks  
Follow

Replying to @dk\_effect

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/...](https://owntracks.org/booklet/guide/)

12:56 AM - 23 Aug 2018

48.719767,21.2282578

311.2°N 21°13'41.7"E

**Directions**

**Pinet Club**

**Home Goods Store**  
Vodár Pumpy, s.r.o.

**Katkin Park**

**Súkromné Gymnázium**  
Katkin Park

**Popradská**

**Hronská**

**Výšavky**

**Shoping oc**

```
{
  "type": "w",
  "lat": 48.719732,
  "lon": 21.2294988,
  "tst": 1516035896,
  "acc": 2
}, {
  "type": "w",
  "lat": 48.7197595,
  "tst": 1483353666,
  "lon": 21.2289363,
  "batt": 100,
  "acc": 1300,
  "batt": 90,
  "conn": "w",
  "lat": 48.719767,
  "lon": 21.2282578,
  "tst": 1460435579,
  "lon": 21.2290371,
  "batt": 8
}, {
  "type": "w",
  "lat": 48.7198966,
  "tst": 1460435579,
  "lon": 21.2290371,
  "batt": 8
}, {
  "type": "w",
  "lat": 48.7198645,
  "lon": 21.2294988,
  "tst": 1516035896,
  "acc": 2
}
```



# 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 incorporate CPE  $\leftrightarrow$  CVE detections
- Accessible via 'vuln:' tag (Enterprise API only)
- Verified: False == *implied* vulnerable
  - Based off version data
- Verified: True == confirmed vulnerable
  - Ex: MS17-010

City	London
Country	United Kingdom
Organization	Digital Ocean
ISP	Digital Ocean
Last Update	2018-10-03T13:23:18.239638
ASN	AS14061
<b>Web Technologies</b>	
Bootstrap	
Font Awesome	
Google Font API	
jQuery	
<b>Vulnerabilities</b>	
<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.



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 8<sup>th</sup> 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 14<sup>th</sup>, 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!!!

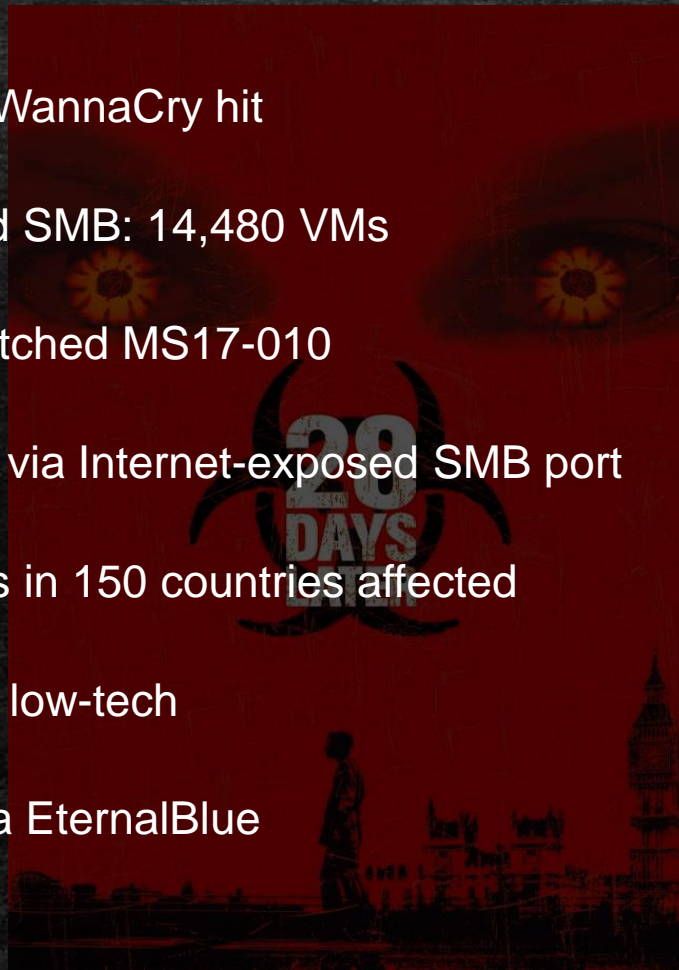




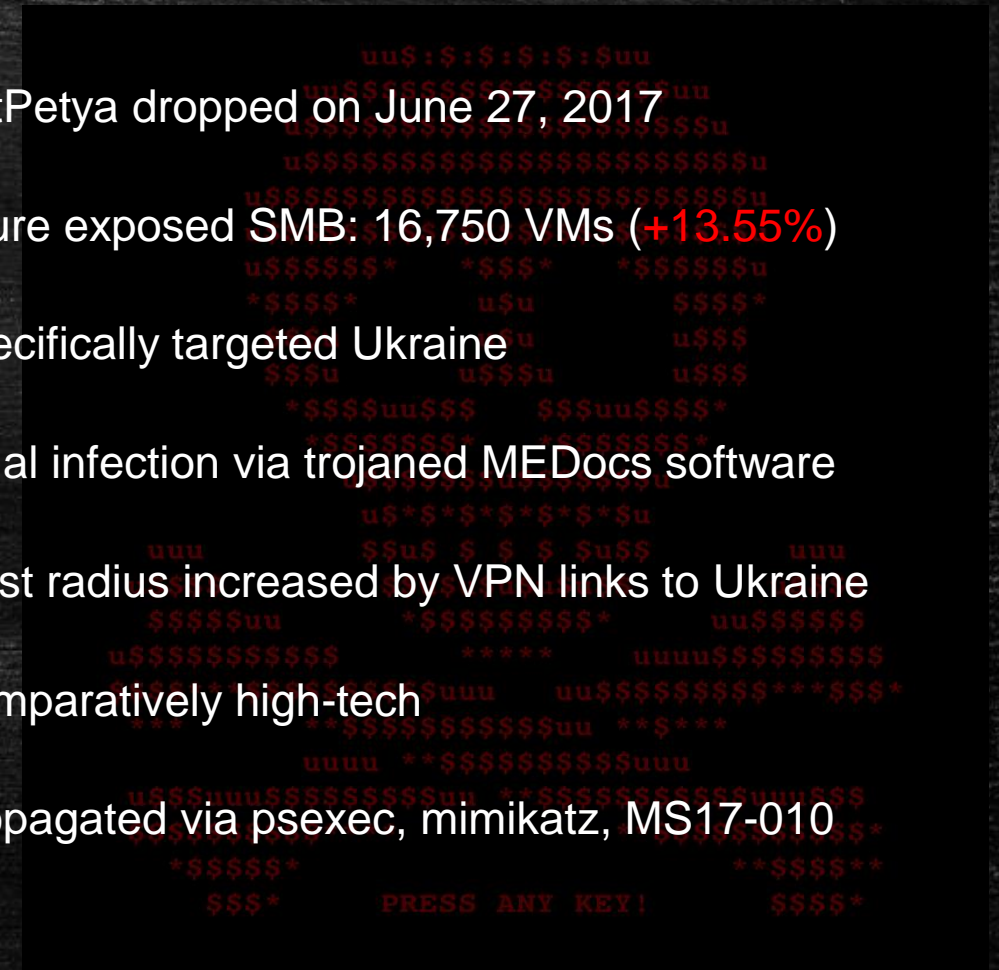


# Cats: You have no chance to survive make your time

- 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?



**Jeffrey Snover**   
@jsnover

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

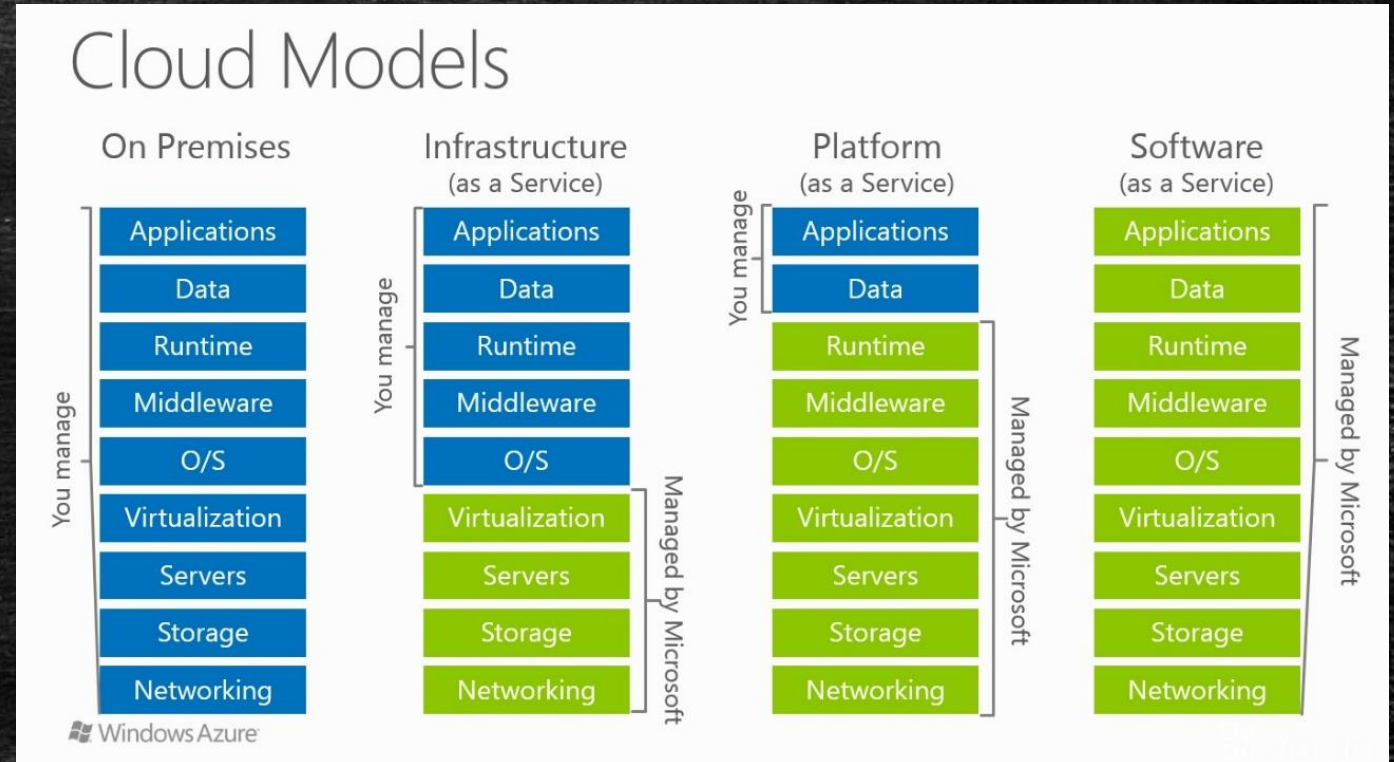
**But.. users are responsible for the security of their VMs and Apps.**

9:11am · 15 Feb 2018 · Twitter Lite



# PaaS & SaaS are shared responsibility

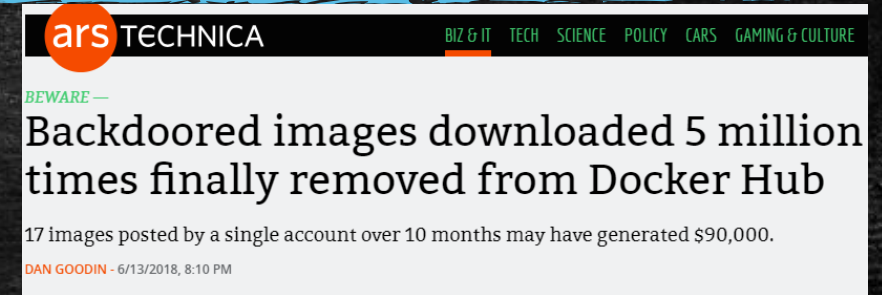
- “Patching causes downtime”
- “My cloud provider handles patching”
- Not necessarily & never with IaaS
- P/SaaS are shared responsibility
- Patching handled by Microsoft
  - SaaS = 100% transparent to you
  - PaaS requires configuration





# Cloud marketplaces are supply chains

- Supply chain attacks are increasingly common
- Cloud marketplaces are next
- Lots of resources; high value targets
- Minimal validation of 3<sup>rd</sup> party images
- 3<sup>rd</sup> 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
- Open S3 buckets being attacked
- Any vulnerable system is a target



**TREND MICRO** TrendLabs **SECURITY INTELLIGENCE** Blog  
SECURITY NEWS DIRECT FROM THREAT DEFENSE EXPERTS

Home Categories

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

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

Sulha Sunderarajan  
Nov 14, 2017 at 12:00 UTC

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

According 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 websites – works by tapping the processing power of visitors' computers to mine monero.

**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.

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



# Docker Monero Mining Campaign

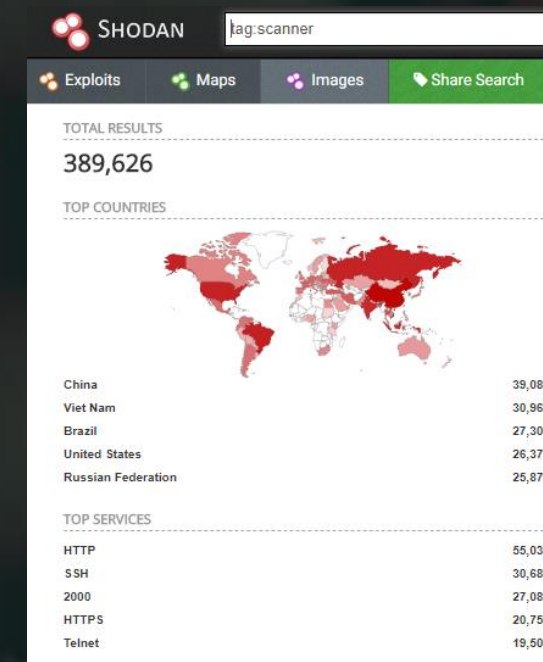
- TCP/2375 – HTTP Admin port for Docker Servers
  - No auth because of course not 🤖
- `curl http://[ip address]:2375/containers/json | jq.'`
- Run via xmrigDaemon Command
- Proxying miner traffic thru hacked Azure VMs
- Impossible to determine profitability?
- Make The World a Safer Place #TR18

```
{
  "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



# Attack patterns coming from Belgium..

- 2 big ISPs are Skynet Belgium & Telenet BVBA
  - Skynet: AS6848
  - Telenet: AS5432
  - Novotel hotel network: AS9031
- Belgian networks are quite clean!



```
"2018-10-03 06:23:40,AS5432,Telnet Worm,Proximus NV"  
"2018-10-03 06:17:45,AS5432,Mirai,Proximus NV"  
"2018-10-03 06:05:54,AS5432,SSH Worm,Proximus NV"  
"2018-10-03 04:14:19,AS5432,SSH Worm,Proximus NV"  
"2018-10-02 19:13:19,AS5432,SSH Worm,Proximus NV"  
"2018-10-02 09:01:28,AS5432,SSH Worm,Proximus NV"  
"2018-10-02 05:19:12,AS5432,Mirai,Proximus NV"  
"2018-10-02 03:20:45,AS5432,Telnet Worm,Proximus NV"  
"2018-10-02 00:58:15,AS5432,PHPMyAdmin Worm,Proximus NV"  
"2018-10-02 00:56:23,AS5432,IIS WebDAV Remote Code Execution CVE-2017-7269,Proximus NV"
```

```
"2018-10-03 04:09:21,AS6848,Telnet Worm,Telenet N.V. Residentials"  
"2018-10-03 03:08:56,AS6848,Mirai,Telenet Operaties N.V."  
"2018-10-03 01:48:26,AS6848,Mirai,Telenet N.V. Residentials"  
"2018-10-02 21:06:54,AS6848,Telnet Worm,Telenet BVBA"  
"2018-10-02 21:06:03,AS6848,Mirai,Telenet BVBA"  
"2018-10-02 17:53:45,AS6848,Mirai,Telenet N.V. Residentials"  
"2018-10-02 15:19:00,AS6848,Mirai,Telenet N.V. Residentials"  
"2018-10-02 11:04:19,AS6848,Telnet Worm,Telenet Operaties N.V."  
"2018-10-02 11:03:49,AS6848,Mirai,Telenet Operaties N.V."  
"2018-10-02 04:54:48,AS6848,Telnet Worm,Telenet operaties N.V."  
"2018-10-02 04:54:18,AS6848,Mirai,Telenet operaties N.V."  
"2018-10-02 03:40:58,AS6848,Mirai,Telenet Operaties N.V."  
"2018-10-02 00:38:26,AS6848,Mirai,Telenet Operaties N.V."
```

```
"2018-09-26 23:05:34,AS9031,Mirai,EDPNET"  
"2018-09-26 12:34:29,AS9031,Telnet Worm,EDPNET"  
"2018-09-14 20:25:54,AS9031,Unknown Linux Worm,EDPnet_AD_SL_Dynamic"  
"2018-09-11 00:03:35,AS9031,SSH Worm,EDPNET"  
"2018-09-05 04:47:01,AS9031,SSH Worm,EDPnet_AD_SL_Dynamic"
```



# Cloud networks scanning the world..

- Malicious cloud tenants
- My cell carrier is full of Mirai? WTF T-Mobile!

```
110 "AS21928,ADB Worm"  
6465 "AS21928,Mirai"
```

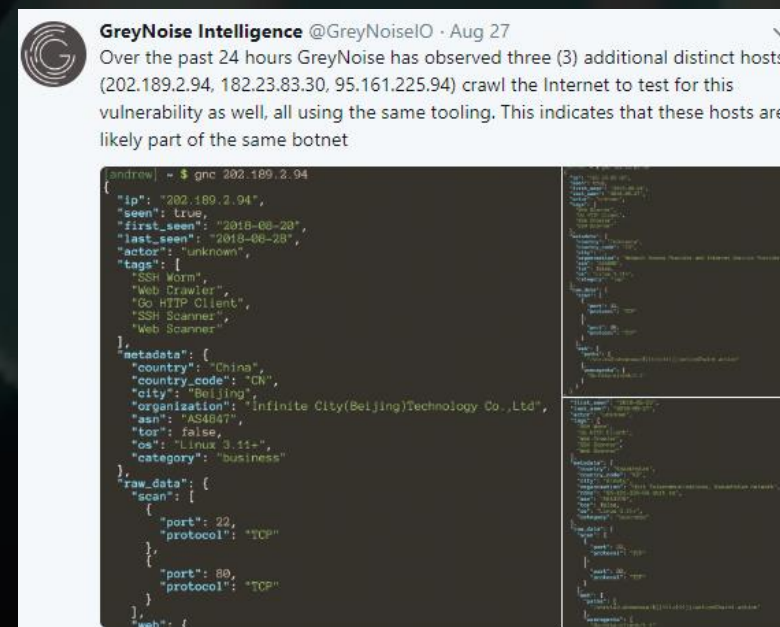
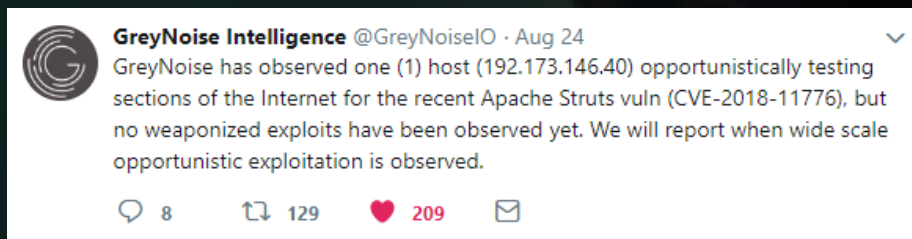
```
2 "AS45090,Huawei HG532 UPnP Worm CVE-2017-17215"  
225 "AS45090,IIS WebDAV Remote Code Execution CVE-2017-7269"  
2 "AS45090,Jboss Worm"  
107 "AS45090,Mirai"  
4 "AS45090,Oracle WebLogic CVE-2017-10271 Worm"  
506 "AS45090,PHPMyAdmin Worm"  
504 "AS45090,SSH Worm"  
120 "AS45090,Telnet Worm"  
1 "AS45090,Windows RDP Cookie Hijacker CVE-2014-6318"  
4 "AS45090,Wordpress Worm"  
3 "AS45090,ZmEu Worm"
```

```
2 "AS14061,Belkin N750 Worm CVE-2014-1635"  
1 "AS14061,Drupal CVE-2018-7600 Worm"  
2 "AS14061,Embedded Device Worm"  
2 "AS14061,GPON CVE-2018-10561 Router Worm"  
2 "AS14061,IIS WebDAV Remote Code Execution CVE-2017-7269"  
139 "AS14061,Mirai"  
38 "AS14061,PHPMyAdmin Worm"  
1 "AS14061,Realtek Miniigd UPnP Worm CVE-2014-8361"  
745 "AS14061,SSH Worm"  
224 "AS14061,Telnet Worm"  
7 "AS14061,Unknown Linux Worm"  
7 "AS14061,Windows RDP Cookie Hijacker CVE-2014-6318"  
1 "AS14061,Wordpress Worm"  
8 "AS14061,ZmEu Worm"  
2 "AS16509,ADB Worm"  
1 "AS16509,IIS WebDAV Remote Code Execution CVE-2017-7269"  
2 "AS16509,Jboss Worm"  
24 "AS16509,Mirai"  
24 "AS16509,PHPMyAdmin Worm"  
196 "AS16509,SSH Worm"  
17 "AS16509,Telnet Worm"  
1 "AS16509,Windows RDP Cookie Hijacker CVE-2014-6318"  
1 "AS16509,ZmEu Worm"  
4 "AS8075,Embedded Device Worm"  
3 "AS8075,IIS WebDAV Remote Code Execution CVE-2017-7269"  
4 "AS8075,Jboss Worm"  
5 "AS8075,Mirai"  
8 "AS8075,PHPMyAdmin Worm"  
119 "AS8075,SSH Worm"  
12 "AS8075,Telnet Worm"  
7 "AS8075,Unknown Linux Worm"  
6 "AS8075,Windows RDP Cookie Hijacker CVE-2014-6318"  
2 "AS8075,Wordpress Worm"  
1 "AS8075,Wordpress XML RPC Worm"
```



# None of this data will be lost in time..

- It may be possible to predict attacks based on trends
- Time-to-weaponize may become calculatable
- Iran is doing something....interesting
- More on that in 2019....





# 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







---

Nate Warfield – @dk\_effect

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