

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.

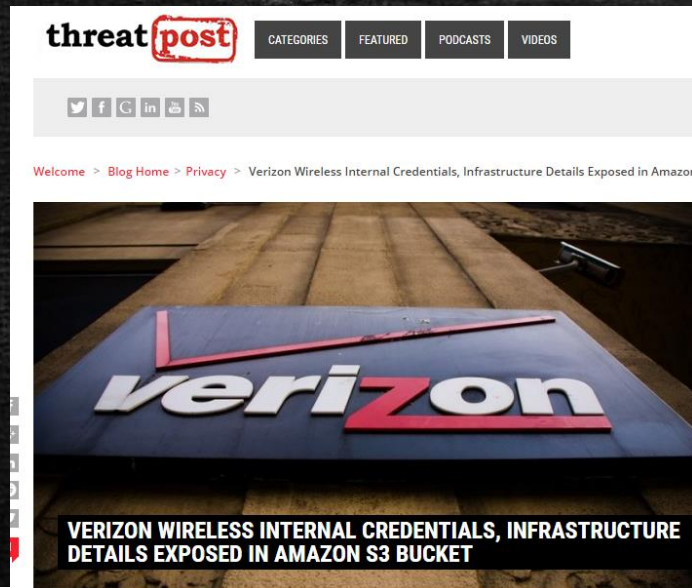
Whoami: Nate Warfield (@dk_effect)

- Senior Security Program Manager - MSRC
 - 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



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

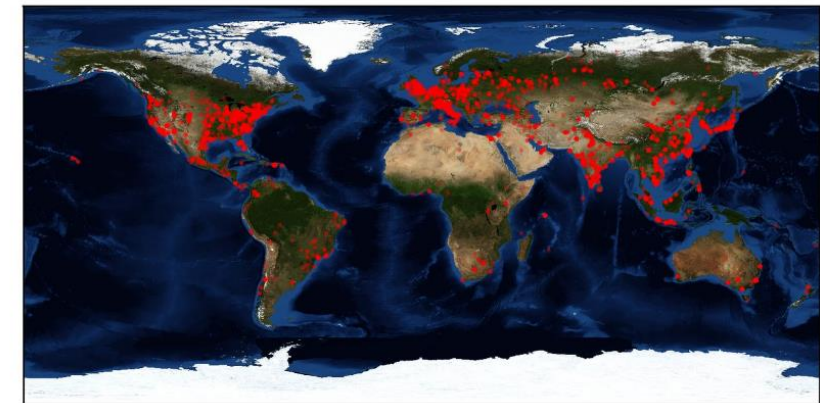
Data of almost 200 million voters leaked online by GOP analytics firm

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

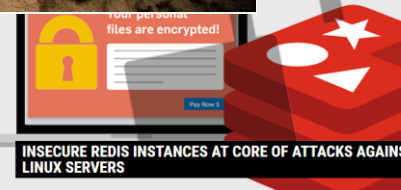
Security

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.

Victoria, B.C

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: 2500+ VM's compromised

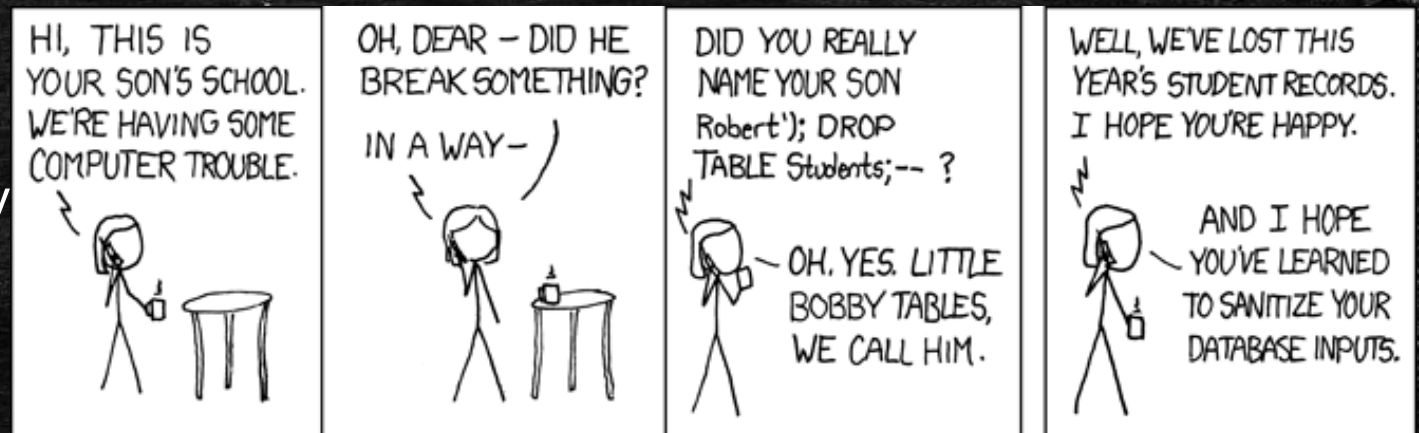


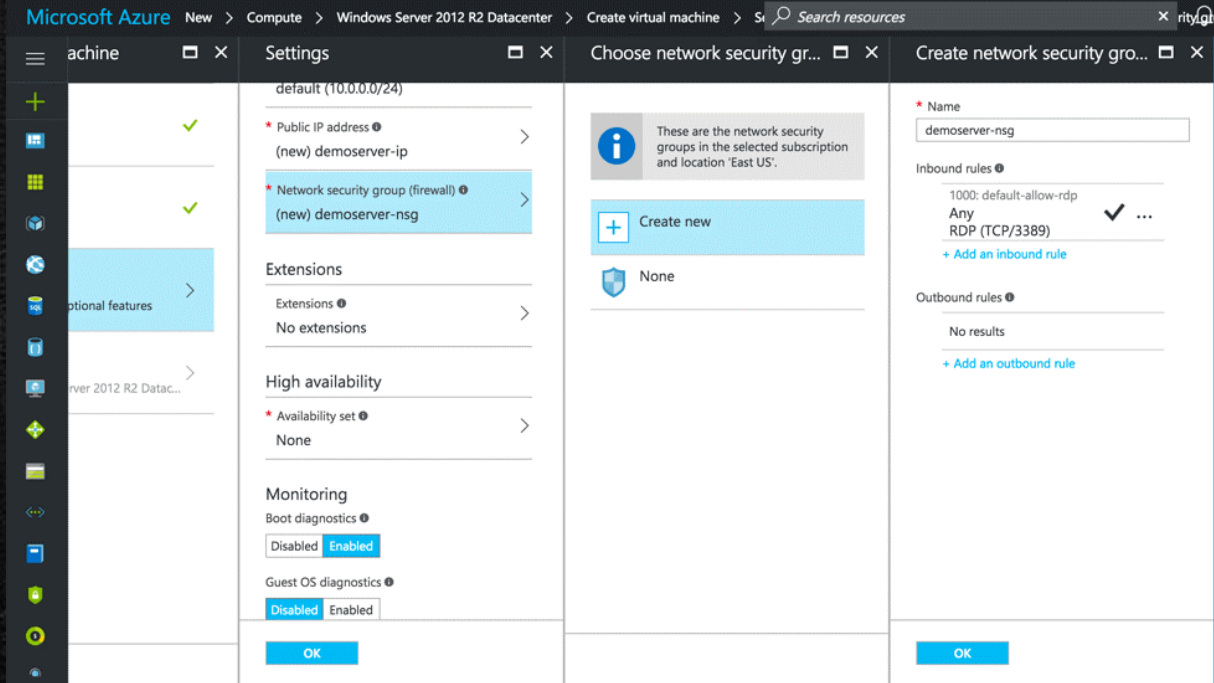
Image Source: https://imgs.xkcd.com/comics/exploits_of_a_mom.png

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

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
		443 - 443	Anywhere ▾ 0.0.0.0/0
HTTPS	tcp	8140 - 8140	Anywhere ▾ 0.0.0.0/0
		8142 - 8142	Anywhere ▾ 0.0.0.0/0
		8143 - 8143	Anywhere ▾ 0.0.0.0/0
		8170 - 8170	Anywhere ▾ 0.0.0.0/0
		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

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
- 22k VM's found as of 3/6/2018
- Requires Shodan Enterprise API
- ..or..
- <https://gist.github.com/n0x08>



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 like a BOSS: CVE-2018-6789

- Exim mail server RCE; Azure had 1237 VMs exposed
- 'shodan download product:exim org:microsoft'
- Common Platform Enumeration field FTW
- 'shodan parse --fields ip_str,cpe'
- VMs found: 1221
- Total time: 5 minutes

```
@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:4.89_1
```


Take off every 'ZIG'!!

- Worked with Shodan to correlate CPE \leftrightarrow CVE
- Based off <https://github.com/cve-search/cve-search>
- Accessible via 'vuln:' tag (Enterprise API only)
- Verified: False is implied vulnerability
- Verified: True confirmed vulnerable

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

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
- Found via anonymous tip

```
{
  "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
      }
    }
  }
}
```


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 +25% in last year



...I'll be tracking you

The screenshot shows a Shodan search for 'port:1883 owntracks'. The results page displays 871 total results, with the top countries being the United States, Germany, United Kingdom, Netherlands, and Sweden. A world map highlights these countries. The top organizations listed are Virgin Media, Ziggo, Comcast Cable, Deutsche Telekom AG, and BT. A detailed view of a specific result shows the IP address 83.83.30.175, identified as belonging to Ziggo, with an MQTT connection code of 0. A map of Katkin Park shows a red pin at the location 48.719767, 21.2282578. A terminal window at the bottom shows a list of location data for various devices, including a Lenovo and a Huawei, with the specific coordinates 48.719767, 21.2282578 highlighted in pink.

SHODAN port:1883 owntracks

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

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
53531 EAF: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/owntracks

48.719767,21.2282578
53°11.2'N 21°13'41.7"E
Directions

Katkin Park
Pokroku
Vystavby
Hronská
Popradská
Pinet Club
Súkromné Gymnázium Katkin Park
Sediaca žena (Mária Bartuszová) - socha
Shopping center

```
$ mosquitto_sub -h 83.83.30.175 -t owntracks/homeassistant/owntracks -u ericsko {"_type":"location","lat":48.7197595,"lon":21.2289363,"batt":100}
ko/lenovo {"_type":"location","tid":"1","acc":1300,"batt":90,"conn":"w","lat":48.719767,"lon":21.2282578,"tst":1483353666}
ko/vibeshot {"_type":"location","tid":"1","acc":29,"lat":48.7198966,"tst":1460435579,"lon":21.2290371,"batt":8}
ko/s3mini {"_type":"location","tid":"ni","acc":21,"batt":66,"conn":"w","doze":false,"lat":48.7198645,"lon":21.22904988,"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":1483353666}
/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":21.22904988,"tst":1516035896,"acc":2}
```




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.....



Finding DoublePulsar in Azure

```
ShellcodeBuffer
Target WINTZK8R2

[?] 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
=====
=====WIN=====
=====
[*] CORE sent serialized output blob (2 bytes):
0x00000000 08 00
[*] Received output parameters from CORE
    [+] CORE terminated with status code 0x00000000
    [+] Eternalblue Succeeded

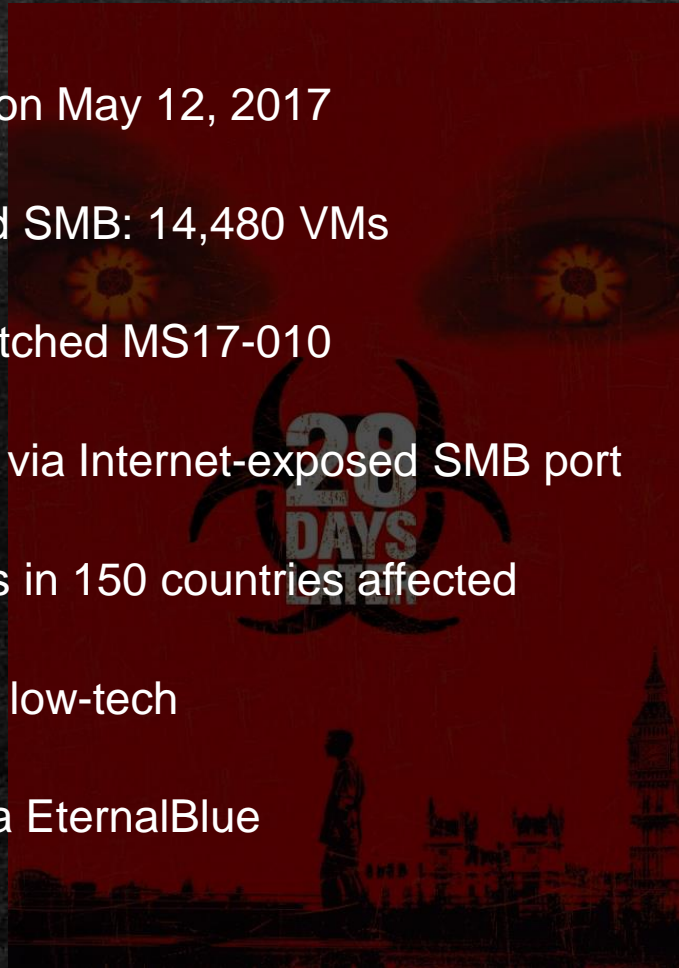
fb Special (Eternalblue) >
```

- 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!!!



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



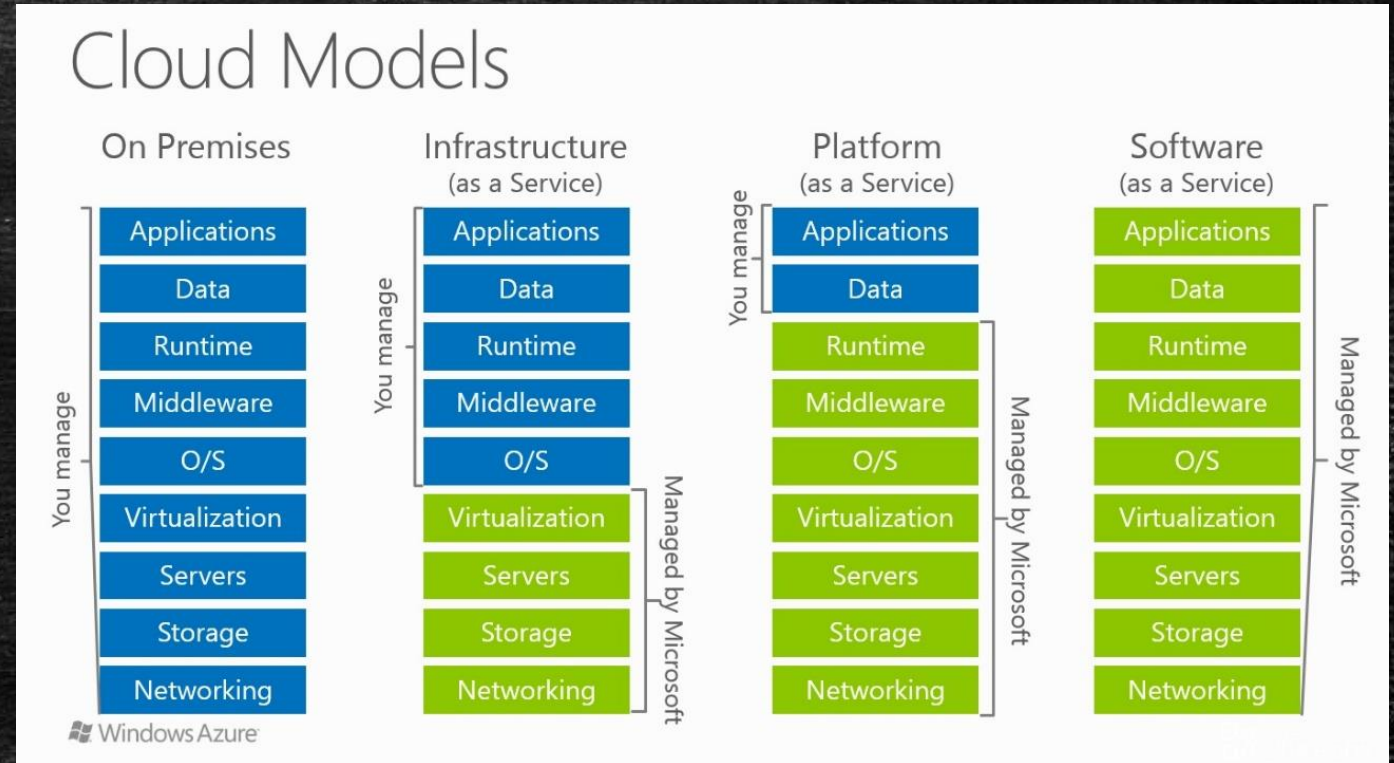
Your IaaS security *is your responsibility*

- 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?



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 marketplaces are supply chains

- Supply chain attacks are increasingly common
- Cloud marketplaces could be next
- Lots of resources; high value targets
- Minimal validation of 3rd party IaaS VM images
- 3rd party IaaS images are *OLD*
 - Average Azure Age: 123 days
 - Average AWS Age: 717 days
- Updating IaaS VM images is not retroactive

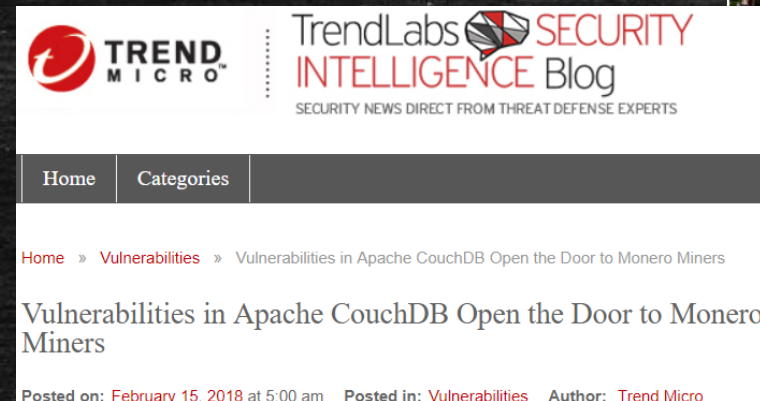
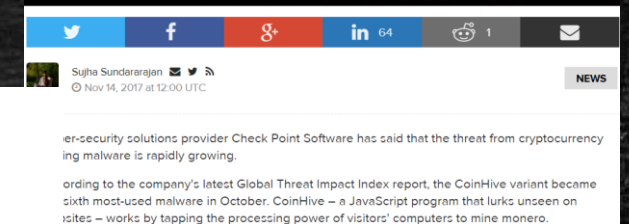


2018: Year of the CryptoMiner

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



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



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



Questions?

Nate Warfield – @dk_effect

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