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 Manger - 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

threatpost | CATEGORIES | FEATURED | PODCASTS | VIDEOS

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

InfoWorld FROM IDG

Home > Information Security

Attackers start wiping data from CouchDB an Hadoop databases

After MongoDB and Elasticsearch, attackers are looking for new database sto 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

eone Hijacking Unsecured MongoDB Databases for Ransom

ay, January 03, 2017 Swati K

Security

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

Passwords, server schematics and encryption keys

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

Security

Crypto-coin miners caugl away in hacked cloud bo

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.

by Michael Mimoso

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 folders and, in some cases, install malicious code.

toria, B.C

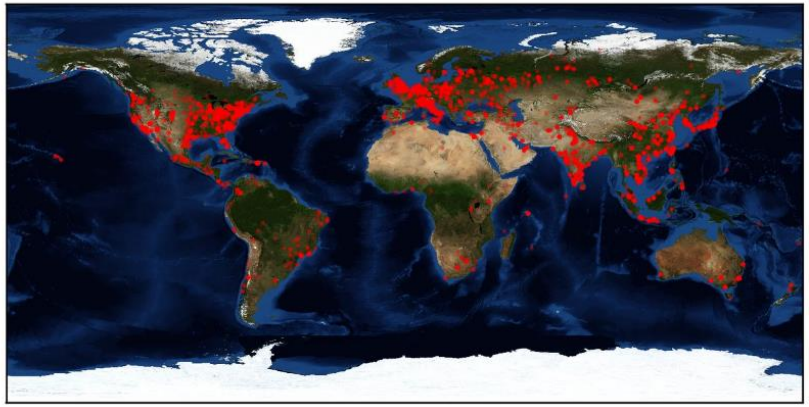
Unsecured ElasticSearch Server Exposed Data on 1,133 NFL Players

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.

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

By Catalin Cimpanu April 21, 2017 05:10 PM



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: 2500+ VM's compromised

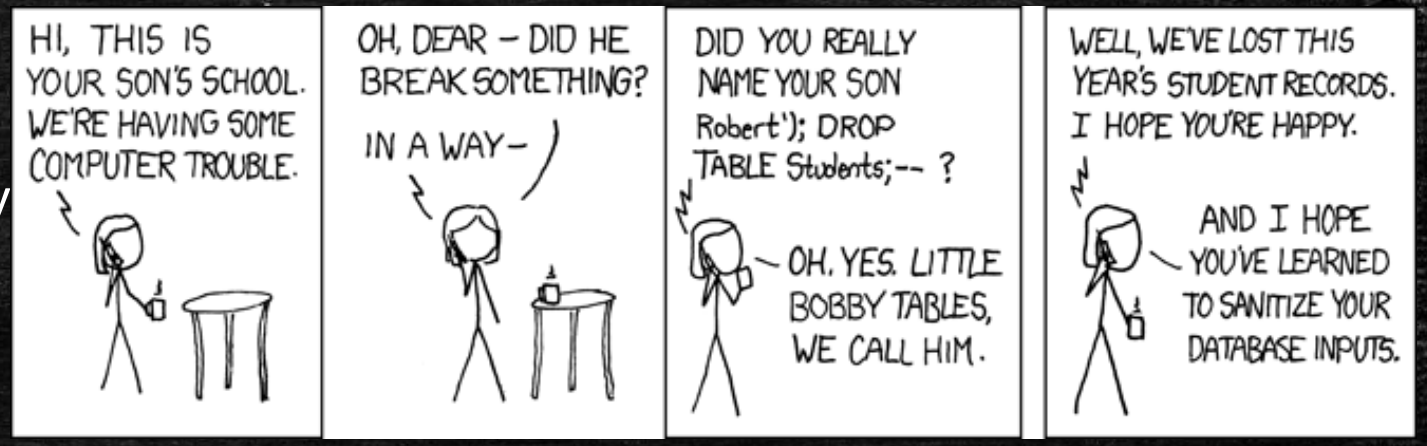


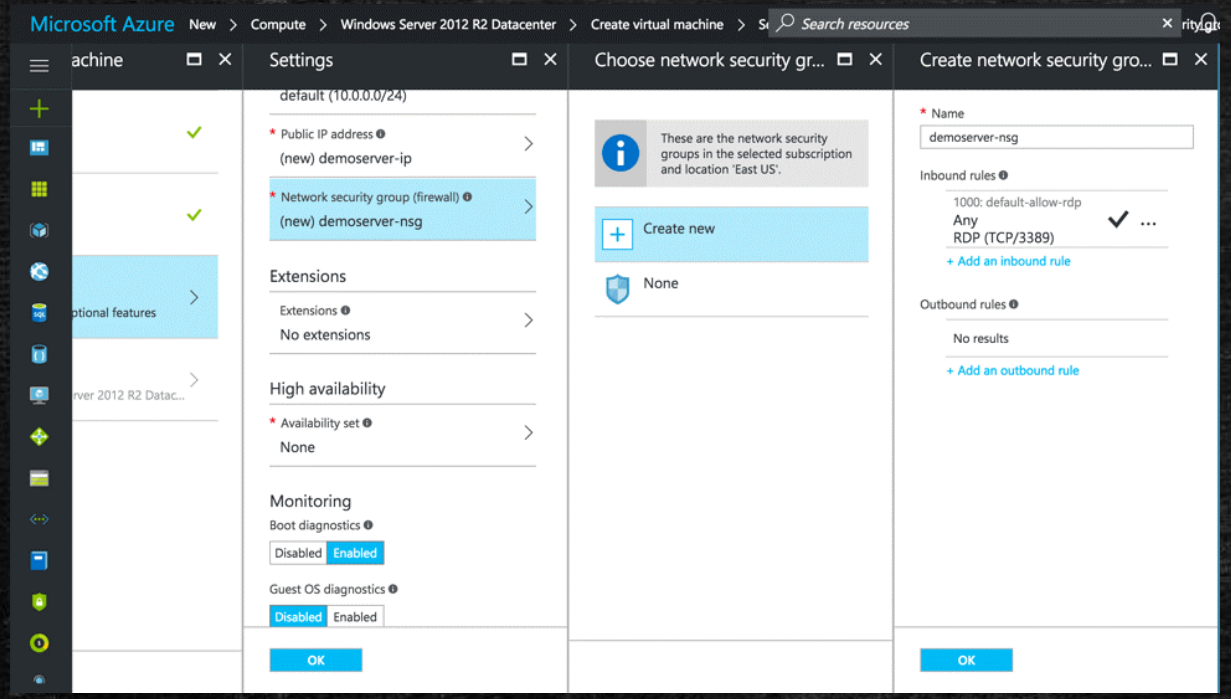
Image Source: https://imgs.xkcd.com/comics/exploits_of_a_mom.png

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
```

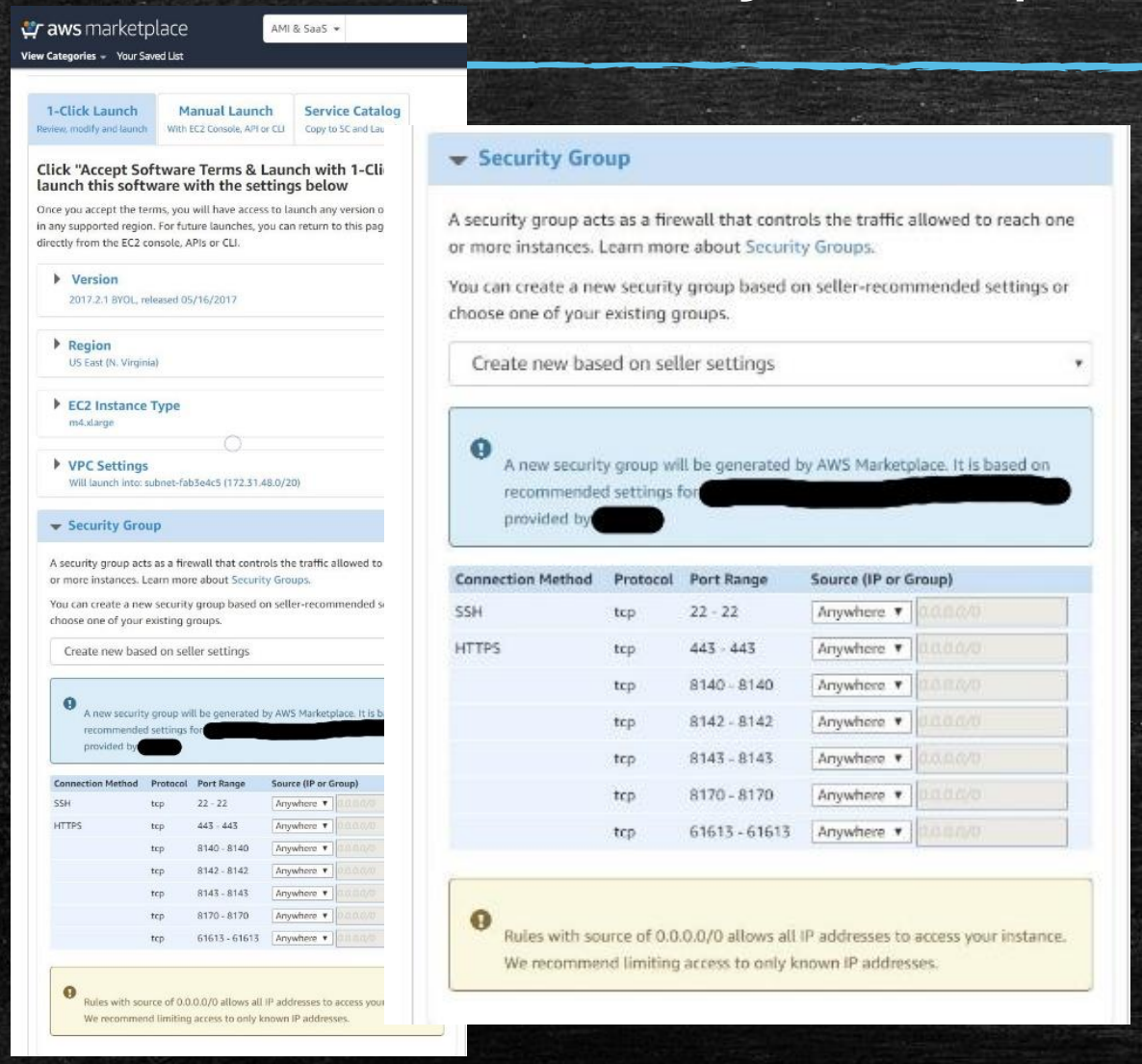
- 2.1 million Internet exposed IPs in Azure
- Port scans are slow; open port != pwned
- Each NoSQL solution runs on different port
- DB names only indication of compromise
- TL;DR – I use Shodan (what, you don't?)
  - Accurate to with 0.14% of in-house solution
  - Rich metadata for each IP
  - DB names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



- 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

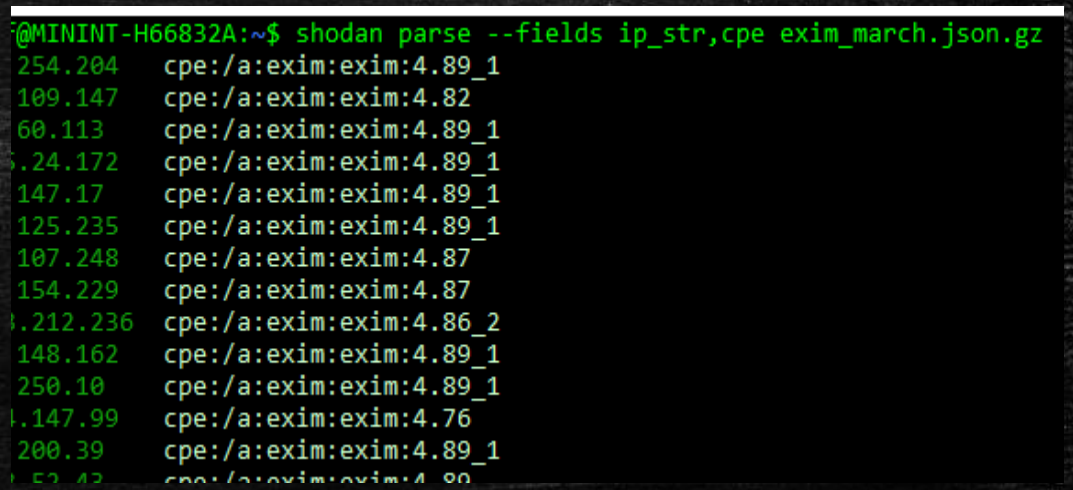
Default Passwords

- 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



Take off every ‘ZIG’!!

- Worked with Shodan to correlate CPE ←→ 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

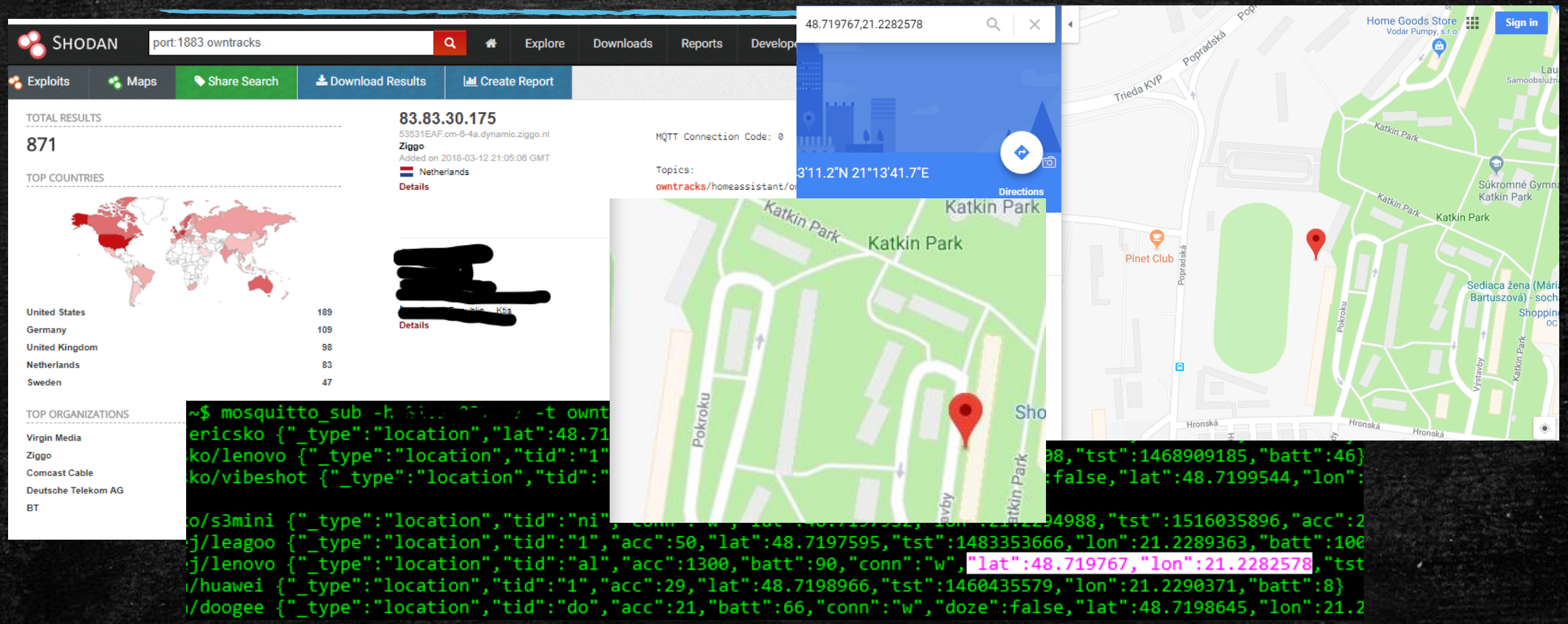
- TCP/2375 – HTTP Admin port for Docker Servers
  - Guess whether authentication is enabled ;)
- curl http://[ip address]:2375/containers/json | jq'.'
- Run via xmrigDaemon Command
- Proxying miner traffic thru hacked Azure VMs
- Impossible(?) to determine profitability
- Found via anonymous tip


```
{
  "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 Messanger, many more
- Azure & AWS offer MQTT-based solutions
- Internet exposure +25% in last year

…I'll be tracking you



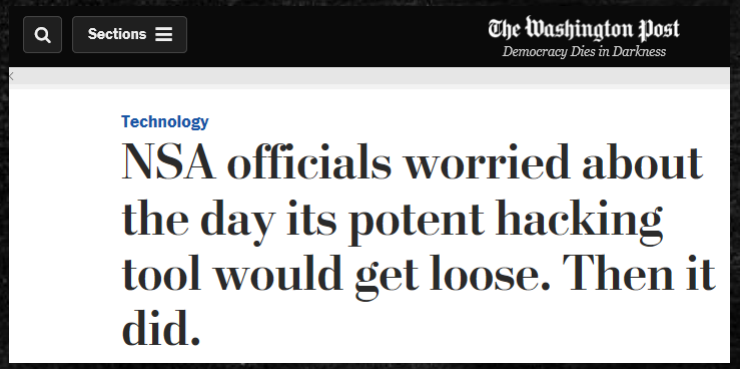
Cats: How are you gentlemen!!

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.

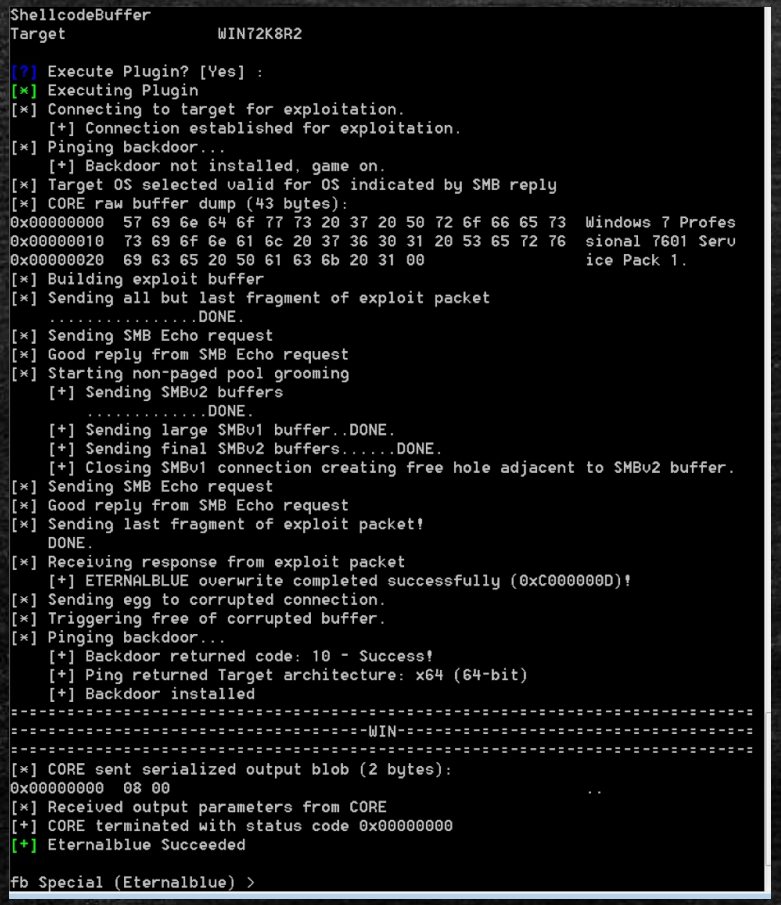
--ShadowBrokers, April 8th 2017

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…..



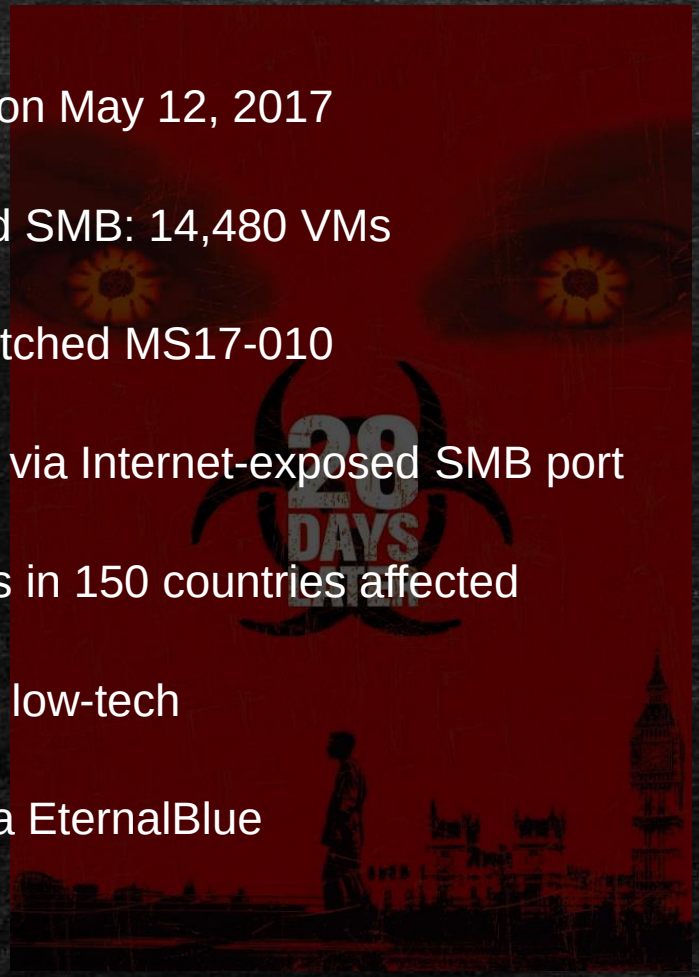
Finding DoublePulsar in Azure



- 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

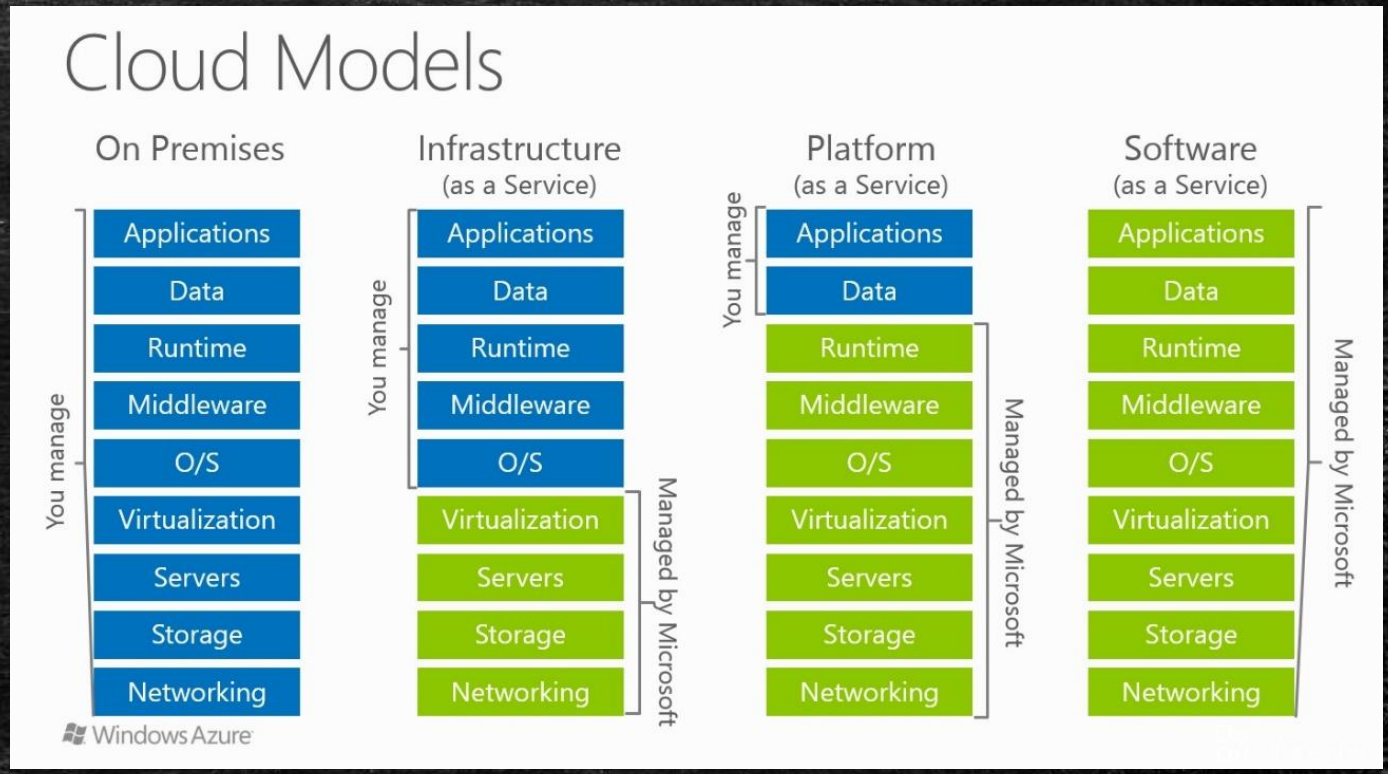
- NotPetya hit on June 27, 2017
- Azure exposed SMB: 16,750 VMs (+13.55%)
- Specifically targeted Ukraine
- Initial infection via trojaned MEDocs software
- Blast radius increased by VPN links to Ukraine
- Comparatively high-tech
- Propagated via psexec, mimikatz, MS17-010

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?

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)

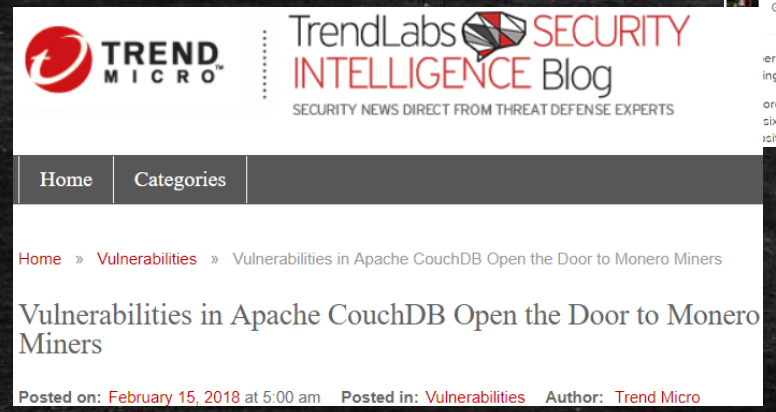


Cloud marketplaces are supply chains

- 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



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.