

# All Your Cloud Are Belong to Us – Hunting Compromise in Azure

**Nate Warfield**

Senior Security Program Manager

Microsoft

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



ANAHEIM, CA | MAY 21-24, 2018

# 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

threatpost

CATEGORIES FEATURED PODCASTS VIDEOS

Twitter Facebook LinkedIn

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



Security

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

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

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.

InfoWorld FROM IDS

Home > Information Security

## Attackers start wiping data from CouchDB and Hadoop databases

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

### Someone Hijacking Unsecured MongoDB Databases for Ransom

Tuesday, January 03, 2017 Swati Khandelwal

Twitter Share 20 LinkedIn

Security

## Viacom exposes crown jewel world+dog in AWS S3 bucket

Passwords, server schematics and more

### Unsecured Elasticsearch Server Exposed Data on 1,133 NFL Players

By Catalin Cimpanu

October 3, 2017 05:05 PM



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

f

Cyber-Safe

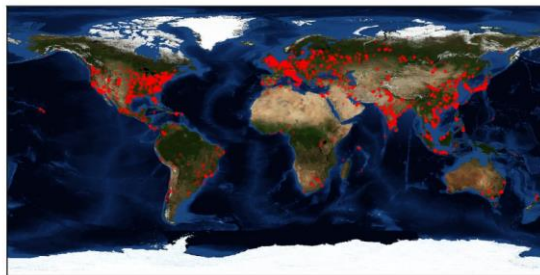
## Data of almost 200 million voters leaked online by GOP analytics firm

by Selena Larson @selenalarson

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

By Catalin Cimpanu

April 21, 2017 05:10 PM



MUST READ WANNACRY RANSOMWARE WAS THE BIGGEST CHALLENGE OF THE YEAR, SAYS CYBERSECURITY CENTRE

## 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.

ignite18  
U. S. A.

Palo Alto Networks Proprietary and Confidential

paloalto  
networks

4

4



# 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



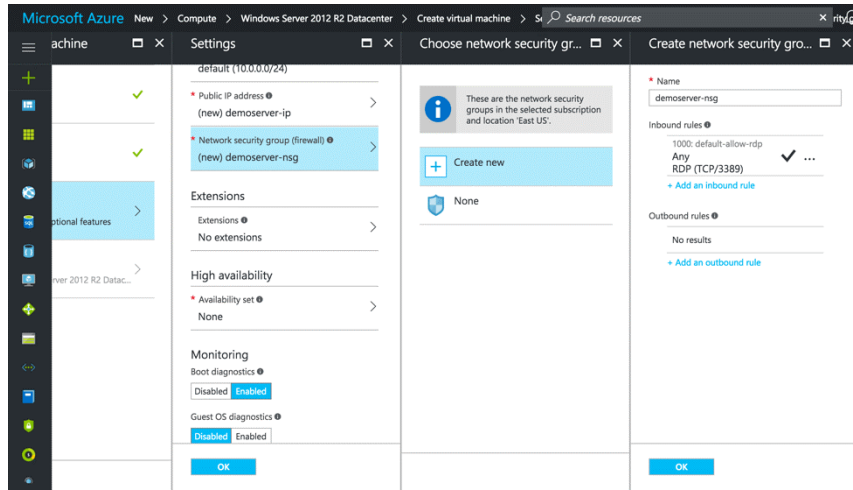
Image Source: [https://imgs.xkcd.com/comics/exploits\\_of\\_a\\_mom.png](https://imgs.xkcd.com/comics/exploits_of_a_mom.png)

# 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)

**1-Click Launch**  
Review, modify and launch

**Manual Launch**  
With EC2 Console, API or CLI

**Service Catalog**  
Copy to SC and LA

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 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 BVDL, released 05/16/2017

**Region**  
US East (N. Virginia)

**EC2 Instance Type**  
m4.xlarge

**VPC Settings**  
Will launch into subnet-fabbed6d (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
	tcp	443 - 443	Anywhere ▾ 0.0.0.0/0
HTTPS	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
	tcp	61613 - 61613	Anywhere ▾ 0.0.0.0/0

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

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



# 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

- 3<sup>rd</sup> 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@khaleesi1:~$ 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

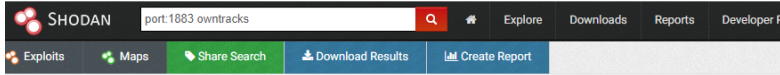
```
@MININT-H66832A:~$ shodan parse --fields ip_str,cpe exim_march.json.gz
254.204 cpe:/a:exim:exim:4.89_1
109.147 cpe:/a:exim:exim:4.82
60.113 cpe:/a:exim:exim:4.89_1
.24.172 cpe:/a:exim:exim:4.89_1
147.17 cpe:/a:exim:exim:4.89_1
125.235 cpe:/a:exim:exim:4.89_1
107.248 cpe:/a:exim:exim:4.87
154.229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

# 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



TOTAL RESULTS

871

TOP COUNTRIES



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

TOP ORGANIZATIONS

Virgin Media	31
Ziggo	29
Comcast Cable	29
Deutsche Telekom AG	18
BT	9

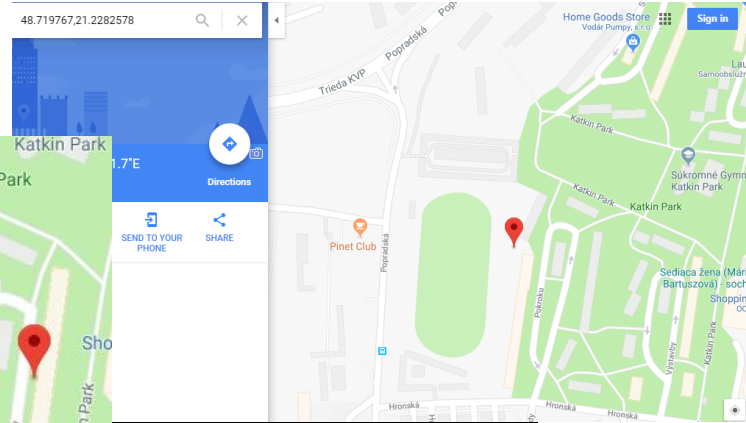
83.83.30.175

53531EAF.am-8-4a.dynamic.ziggo.nl  
Ziggo  
Added on 2018-03-12 21:05:00 GMT  
Netherlands  
Details



Details

MQTT Connection Code: 0



```
~$ mosquitto_sub -h 83.83.30.175 -t #/owntracks/+/+/  
ericsson {"_type":"location","tid":"er","acc":23,"batt":48,"conn":"m","doze":false,"lat":48.7199544,"lon":14.55842577,"acc":20,"batt":57,"tid":"1"}  
ko/lenovo {"_type":"location","tid":"1","acc":20,"lat":48.719861,"lon":21.2292008,"tst":1468909185,"batt":46}  
ko/vibeshot {"_type":"location","tid":"er","acc":23,"batt":48,"conn":"m","doze":false,"lat":48.7199544,"lon":14.55842577,"acc":20,"batt":57,"tid":"1"}  
o/s3mini {"_type":"location","tid":"ni","conn":"w","lat":48.7197932,"lon":21.2294988,"tst":1516035896,"acc":20}  
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":1468909185,"batt":46}  
/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":21.2290371,"batt":8}
```



# 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*

# 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.....



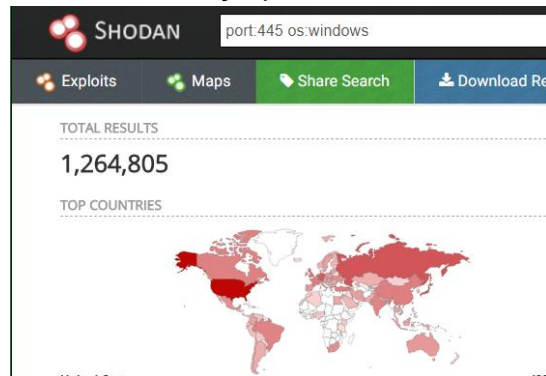
Technology

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



## The NSA: Still F\*cking Up

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



# 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 66 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
[*] ETHERNALBLUE overwrite completed successfully (0xC0000000)!
[*] 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



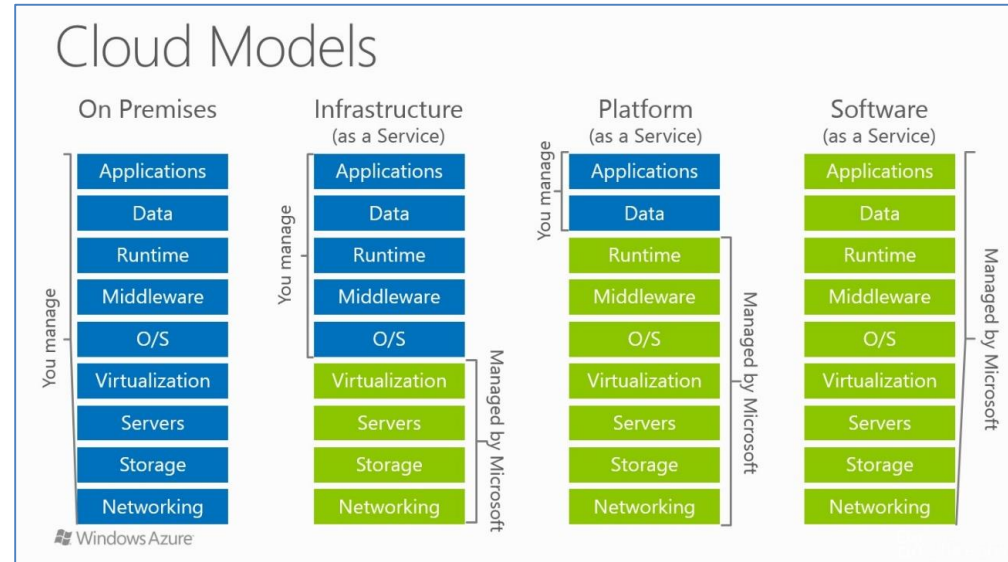
# Your IaaS security *is your responsibility*

- 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 3<sup>rd</sup> party IaaS VM images
- 3<sup>rd</sup> party IaaS images are **OLD**
  - Average Azure Age: **123 days**
  - Average AWS Age: **717 days**
- Updating IaaS VM images is not retroactive



**welivesecurity**  
News, views, and insight from the ESET security community

All Posts Latest Research How To Multimedia Papers Our Experts

## Multi-stage malware sneaks into Google Play

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

BY LUKAS STEFANKO

**ars TECHNICA**

BIZ & IT TECH SCIENCE POLICY CARS GAMING & C

UNFOLDING MYSTERY —

## CCleaner malware outbreak is much worse than it first appeared

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

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

# 2018: Year of the CryptoMiner

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

**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

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



Sujiha Sundararajan  
Nov 14, 2017 at 12:00 UTC

NEWS

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



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

ix report, the CoinHive variant became a script program that lurks unseen on s' computers to mine monero.

[Home](#) [Categories](#)

[Home](#) » [Vulnerabilities](#) » Vulnerabilities in Apache CouchDB Open the Door to Monero Miners

### Vulnerabilities in Apache CouchDB Open the Door to Monero Miners

Monero Charts

Posted on: February 1



# 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.*