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
  • First hack: BBS over 2400 baud
  • Internet of Insecureable Things
  • Radio hacking hobbyist

• Twitter: @dk_effect
• GitHub: n0x08

Make The World A Safer Place - #TR18
Captain: What happen?

- **Traditional Networking (then)**
  - Internet 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

Attacker start wiping data from CouchDB and Hadoop databases

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

Crypto-coin miners caug away in hacked cloud box

Elasticsearch ransomware attacks now number in the thousands
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

- 1.6 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](https://gist.github.com/n0x08)
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

Make The World A Safer Place - #TR18
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
```
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
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!!!
Make The World A Safer Place - #TR18
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.