All Your Cloud Are Belong to Us

Hunting Compromise in Azure
Nate Warfield – Microsoft Security Response Center
DISCLAIMER

The views, images and tools expressed and referenced in this presentation are my own and do not necessarily reflect those of Microsoft Corporation.
Whoami: Nate Warfield

• Senior Security Program Manager - MSRC
  • Vulnerability Management for Azure, Windows, Hyper-V
  • Battle tested: MS17-010, WannaCry, NotPetya, Spectre/Meltdown

• Background
  • 18 years of Network Engineering
  • Grey hat
  • Internet of Insecureable Things
  • Radio hacking (SDR, BT/BLE, LoRaWAN, RFID/NFC)

• Twitter: @dk_effect
• GitHub: n0x08
Framing the Problem

You exposed WHAT to the Internet?!?!
Network Security 101

- Limit inbound access from the Internet
  - Default deny
- ACLs on all network devices
- Authentication. Everywhere.
- Install security updates. Seriously. Install them.
- Internet-facing servers in DMZ
- All changes to firewalls/ACLs done by security team
How Cloud Changes This Model

• Every Virtual Machine is exposed to the Internet
  • SSH or RDP, required for administration
• Anyone with access can expose BadThings™
• Patch management decentralized
• VM’s deploy with predefined firewall configuration
• One insecure image == thousands of insecure deployments
• This is not unique to Azure; AWS & others see similar problems
2017: All Your Cloud Are Belong to Us

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 bo:

Elasticsearch ransomware attacks now number in the thousands

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

When the past is always with you, it may as well be present; and if it is present, it will be future as well.
— William Gibson, Neuromancer
NoSQL - Exposure & Impact

• NoSQL solutions were not designed to be Internet-facing
  • “...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
• DB dropped; ransom note added
• 100k+ systems compromised globally
• Azure: 2500+ VM’s compromised
Finding NoSQL Compromise in Azure

- Large attack surface – 1.6 million IP addresses
- Each NoSQL solution runs on a different port
- Port scans are slow; open port != pwned
- DB names are only indication of compromise
- TL;DR – I use Shodan.io
  - Can search by organization
  - DB names are indexed & searchable
  - Results downloadable in JSON format for post-processing
Extending Shodan

• Tag: compromised – automatic tagging of pwned NoSQL DB’s
• Added to Shodan in December 2017
• 15k hosts found as of 1/25/2018
• Requires Shodan Enterprise API
• https://gist.github.com/n0x08
Don’t Forget Your Base

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
Exposure & Impact

- [REDACTED] weaponized an SMBv1 exploit (EternalBlue)
- [REDACTED] added it to their Metasploit clone
- [REDACTED] lost control of this tool
- Microsoft patched in March 2017 (MS17-010)
- Nobody in their right mind would expose SMB to the Internet..

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

• “Only” 14k hosts exposing TCP/445
• DoublePulsar implant does not visibly alter the system
• It did allow operators to test for its existence
• Manually scanned all IP’s exposing TCP/445
• Low number of implants (<50)

• That means everyone patched!!!
WannaCry: Exposure & Impact

- Attack started May 12, 2017
- Targeted systems missing MS17-010 patches
- 230k+ systems in 150 countries affected
- Initial infection via Internet-exposed SMB port*
- Lateral movement via EternalBlue
- Comparatively low-tech
- Azure exposed SMB: 14,480 hosts

*https://nakedsecurity.sophos.com/2017/05/17/wannacry-the-ransomware-worm-that-didnt-arrive-on-a-phishing-hook/
NotPetya: Exposure & Impact

- Attack started June 27, 2017
- Specifically targeted Ukraine
- Initial infection via backdoored MEDocs software
- Lateral movement via psexec, WMIC, mimikatz and MS17-010
- Blast radius increased by VPN links to Ukraine
- Comparatively high-tech
- Azure exposed SMB: 16,750 hosts (+13.55%)
Lateral Movement via ExpressRoute

• What’s ExpressRoute?
  • “Microsoft Azure ExpressRoute lets you extend your on-premises networks into the Microsoft cloud....”
• That sounds like a VPN!
• (spoiler alert: it is)
• Amazon: Direct Connect – AWS version of ExpressRoute
• Is the cloud actually isolated from your corporate network?
• Unexplored but interesting attack scenarios
Network Security Group (Azure)

- Network Security Group is the image firewall
- Firewall config hard-coded by image vendor
- Configurable during deployment (but not required)
- 46% of Azure Gallery Images expose ports by default
- 96% of those expose more than management
- 500 different ports exposed across Azure Gallery
AMI Security Groups (AWS)

- AMI == Amazon Marketplace Image == Azure Gallery Image
- AWS doesn’t expose default Security Group config via API*  
  - *Unless you deploy it
- Feature request filed since November 2017
- Spot checks indicate Amazon Marketplace has same issues
- 21k AMI’s in AWS – 10x as many as Azure
Default Passwords

- VM Descriptions occasionally contain a default password
- At least it’s a strong* PW!: P@sswOrd123
  - *actual PW changed to protect the innocent
- Users are advised to change PW after installation
- Fortunately “only” for services like MySQL, SQL, etc.
- Do databases *really* need to be Internet facing?
2018 – Year of the CryptoMiner?

- Ransomware is low yield; kills the host
- Surreptitiously mining $COINZ is profitable
- Remotely stealing resources at scale is hard….
- …..until now.
Questions?