# All Your Cloud Are Belong to Us

Hunting Compromise in Azure

Nate Warfield – Microsoft Security Response Center

# Whoami: Nate Warfield

- Senior Security Program Manger - 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 Insecurable 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
- Internet-facing servers in DMZ
- All changes to Firewall/ACL 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 deploy systems
- 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

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

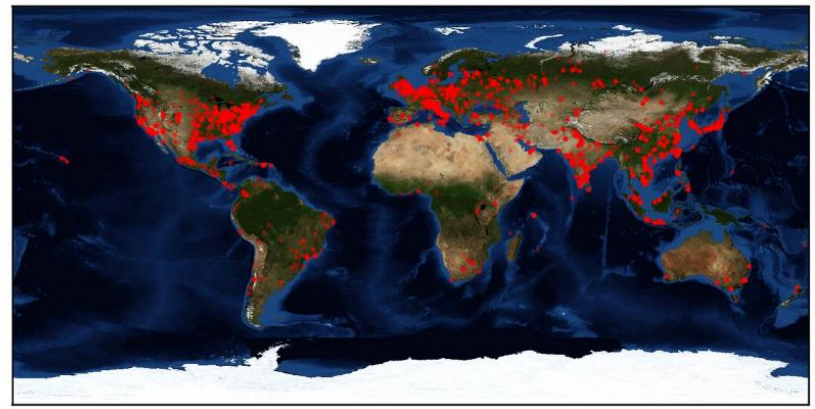
Security

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

Passwords, server schematics and encryption keys

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

By Catalin Cimpanu April 21, 2017 05:10 PM



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 September 1, 201

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 w folders and, in some cases, install malicious code.

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.

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.

# 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

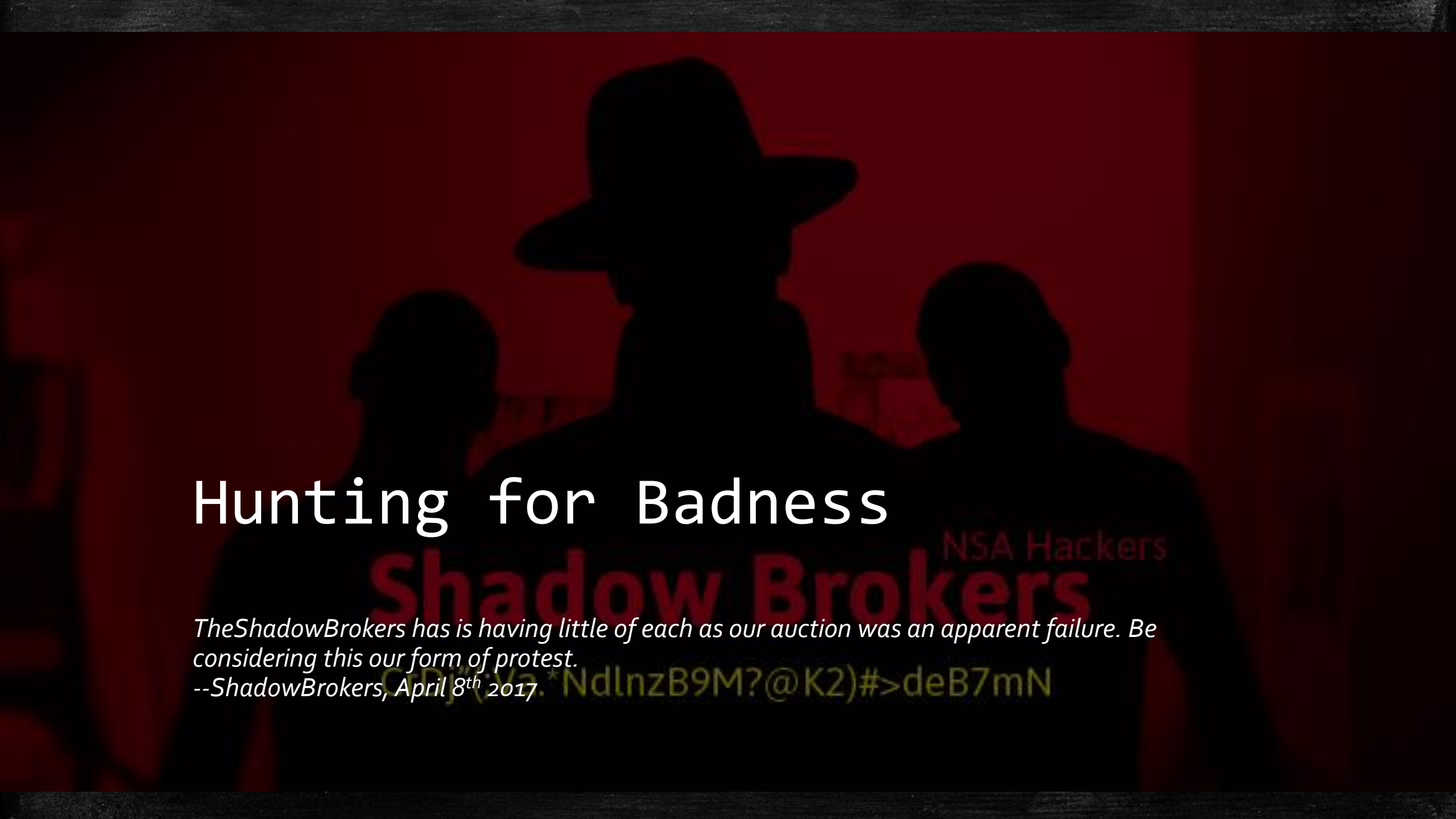
- NoSQL solutions were not designed to be Internet-facing
  - "..it is not a good idea to expose the Redis instance directly to the internet"
  - "Allow only trusted clients to access the network interfaces and ports on which MongoDB instances are available."
  - "Elasticsearch installations are not 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 pwned

# Finding NoSQL Compromise in Azure

- Large attack surface – 1.6million IP addresses
- Each NoSQL solution runs on a different port
- Open port != compromise
- 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




# Hunting for Badness

*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..


# 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 it’s existence
- Manually scanned all IP’s exposing TCP/445
- Low number of implants (<50)

- That means everyone patched!!!


MISSION ACCOMPLISHED

# 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

*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
- Infection rate of ~500 systems/minute
- 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

# Exposure & Collateral Damage

# 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 checking indicates Amazon Marketplace has same issues
- 21k AMI’s in AWS – 10x as many as Azure
- Anyone from AWS API team in the audience?

# 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?

```
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
```

# 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?