



Kaspersky®

SECURITY ANALYST SUMMIT

#TheSAS2018

ALL YOUR CLOUD ARE BELONG TO US

Nate Warfield (@dk_effect)

Microsoft Security Response Center

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

CAPTAIN: WHAT HAPPEN?

- **Traditional Networking (then)**

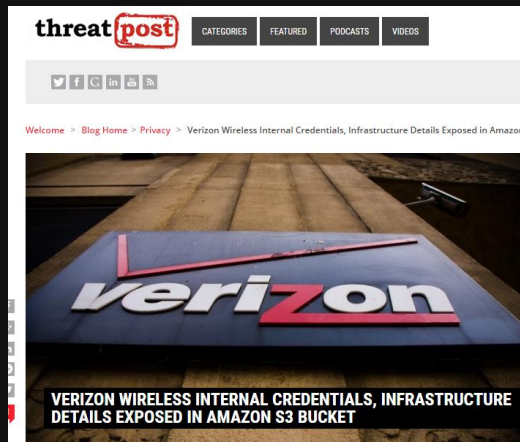
- Internet exposure was limited
- Many layers of ACLs + segmentation
- Dedicated deployment teams
- Well-defined patching cadence
- Servers deployed from the ground up
- Only expose required services

- **Cloud Networking (now)**

- Every Virtual Machine 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 UP US THE BOMB



InfoWorld
FROM IDG

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

by Swati K

January 03, 2017

Security

```
cor@windwlicker:~$ mongo
MongoDB shell version v2.6.12
connecting to: mongodb://127.0.0.1:27021/
MongoDB server version: 2.6.12
```

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

Passwords, server schematics and encryption keys

Unsecured Elasticsearch Server Exposed Data on 1,133 NFL Players

By Catalin Cimpanu

October 9, 2017

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.

CNN tech

BUSINESS

CULTURE

GADGETS

FUTURE

STARTUPS



Cyber-Safe

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

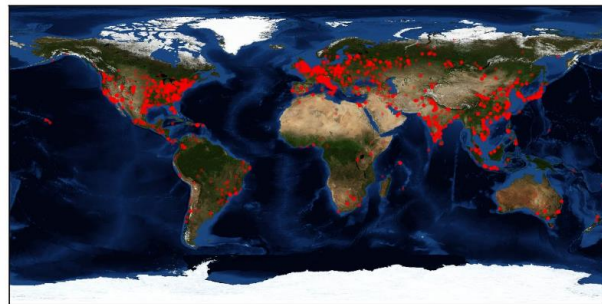
by Selena Larson @selenalarson

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

By Catalin Cimpanu

April 21, 2017

05:10 PM



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.

Security

Crypto-coin miners caught away in hacked cloud box

Manic miners don't even pwn your 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 Mitson

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 files and, in some cases, install malicious code.



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

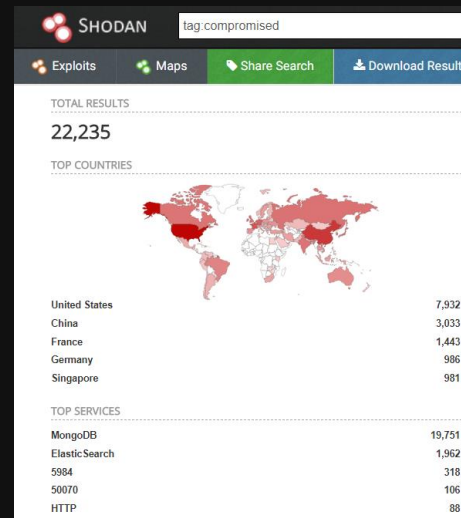
HUNTING NOSQL COMPROMISE IN AZURE



- Large attack surface – 1.6million IP addresses
- Port scans are slow; open port != pwned
- Each NoSQL solution runs on a different port
- DB names are 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

OPERATOR: MAIN SCREEN TURN ON 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>

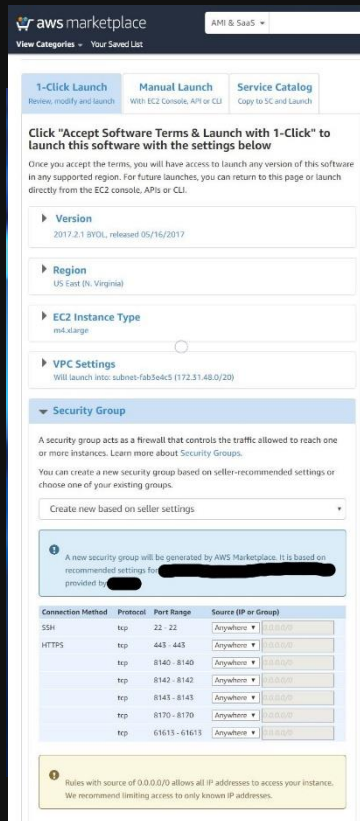


NETWORK SECURITY GROUP (AZURE)



- Network Security Group is the VM firewall
- Firewall config hard-coded by VM vendor
- Configurable during deployment (optional)
- 46% of Azure Images expose ports by default
- 96% of those expose more than management
- 562 different ports exposed across Azure Gallery

AMI SECURITY GROUPS (AWS)



aws marketplace

AMI & SaaS

View Categories - Your Saved List

1-Click Launch Manual Launch Service Catalog

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 of this software in any supported region. For future launches, you can return to this page or launch directly from the EC2 console, APIs or CLI.

Version
2017.2.1 BYOL, released 05/16/2017

Region
US East (N. Virginia)

EC2 Instance Type
m4.xlarge

VPC Settings
Will launch into: subnet-fab5e6c5 (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
HTTPS	tcp	443 - 443	Anywhere
	tcp	8140 - 8140	Anywhere
	tcp	8142 - 8142	Anywhere
	tcp	8143 - 8143	Anywhere
	tcp	8170 - 8170	Anywhere
	tcp	61613 - 61613	Anywhere

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.



- AMI is synonymous with Azure Gallery Image
- AWS doesn't expose vendor 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
- Industry-wide collaboration is key

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 0day 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 specific unused SMB error code
- Manually scanned all IP's exposing TCP/445
- Low number of implants (<50)
- That means everyone patched!!!





Kaspersky®

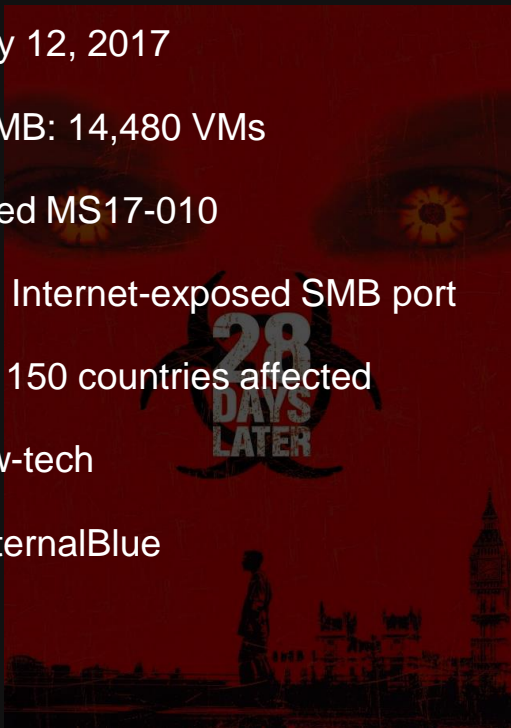
SECURITY ANALYST SUMMIT

#TheSAS2018

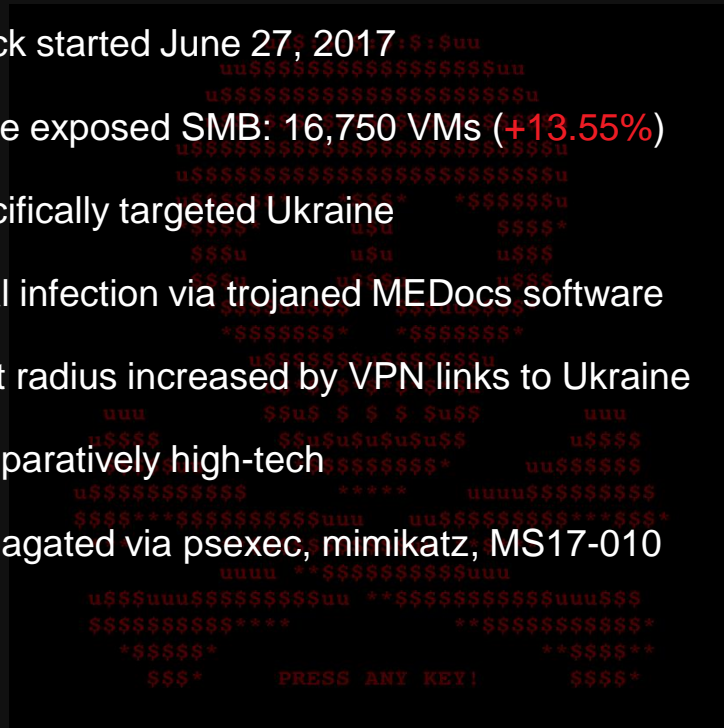
**YOU HAVE NO CHANCE TO
SURVIVE MAKE YOUR TIME**

WANNACRY VS. NOTPETYA

- Attack started 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



- Attack started 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



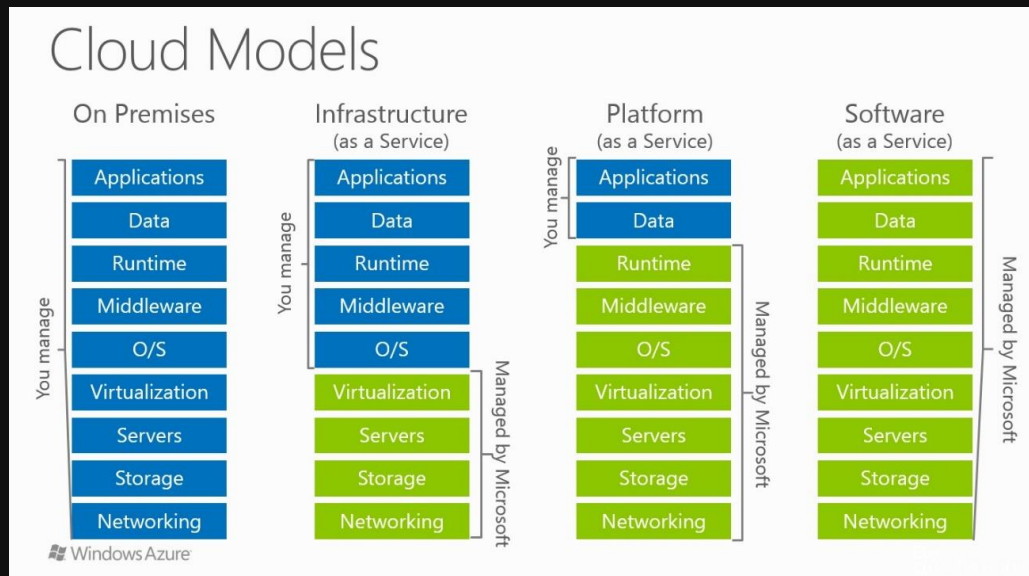
YOUR IAAS SECURITY *IS YOUR RESPONSIBILITY*

- 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 do you manage ACL’s on P2P cloud connections?
- Is the cloud *actually* isolated from your 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 are here to 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



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

Home Categories

Home » Vulnerabilities » Vulnerabilities in Apache CouchDB Open the Door to Monero Miners

Vulnerabilities in Apache CouchDB Open the Door to Monero Miners

Posted on: February 15, 2018 at 5:00 am Posted in: Vulnerabilities Author: Trend Micro

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

Sujha Sundarajan

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

ording to the company's latest Global Threat Impact Index report, the CoinHive variant became sixth most-used malware in October. CoinHive – a JavaScript program that lurks unseen on sites – works by tapping the processing power of visitors' computers to mine monero.

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



CAPTAIN: FOR GREAT JUSTICE

- Update your IaaS VMs immediately after deployment
- Review firewall settings before deployment
- 3rd party IaaS VMs may be outdated
- 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





Kaspersky®

SECURITY ANALYST SUMMIT

#TheSAS2018

THANK YOU SAS!

Nate Warfield (@dk_effect)

Microsoft Security Response Center