RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: HTA-R14

COMMON INFRASTRUCTURE EXPLOITS IN AWS/GCP/AZURE SERVERS & CONTAINERS

Alexi Papaleonardos

Principal Consultant
CrowdStrike Services
@ixe_la

Overview

- Exploiting DNS tunneling in IaaS
- Exploiting VPC / VNet service endpoints
- Practical defenses
- Amazon Web Services, Microsoft Azure, and Google Cloud Platform

Motivation

- DNS Tunneling
  - “Hackers have recently used this technique in cases involving the theft of millions of accounts” – Ed Skoudis, RSAC 2012
  - Hasn’t gone away
- VPC/Vnet Service endpoints
  - New “side channels” that didn’t exist in legacy data centers
- By understanding the risk you can drive change for your organization

Important notes

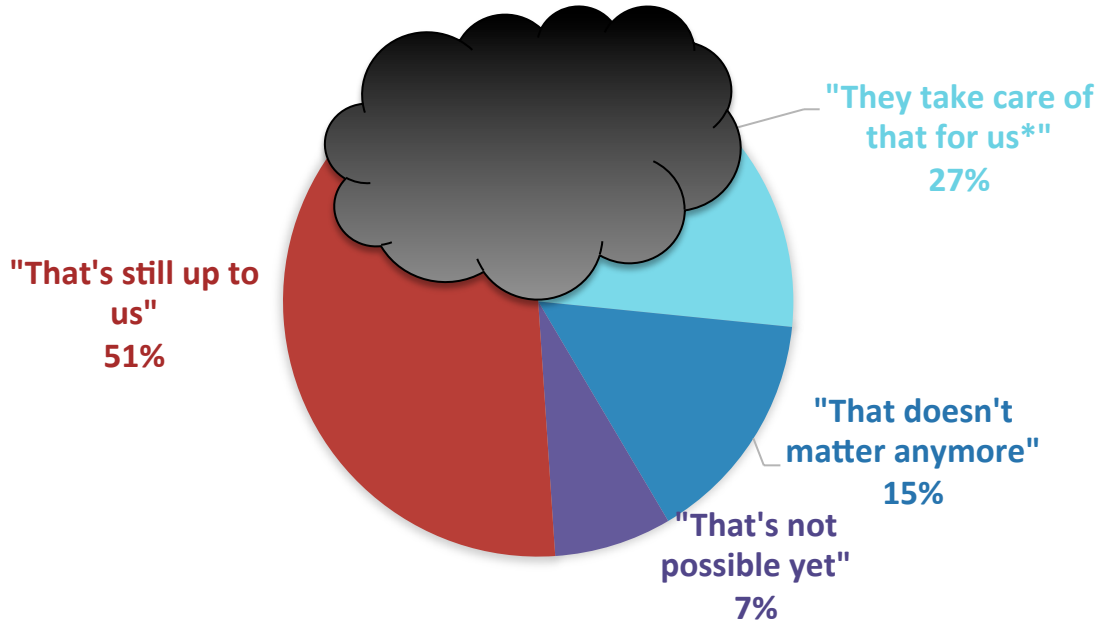
- These techniques might not be attackers' first choice if your cloud hosts have unrestricted access to the Internet
  - Prioritize accordingly
  - Specific defensive investments would best be reserved for environments with high security needs
  - Otherwise, address these techniques with more general security controls
- These are not bugs in cloud providers' services
  - They are published specifications
  - They can be misused

This talk in one slide

- You already know unrestricted outbound Internet access is high risk
  - DNS tunneling and service endpoints are part of of that risk family
- DNS tunneling still works in cloud environments
  - Less obvious that it is possible in your designs (vs legacy data centers)
  - Less obvious that it is happening from operational analysis
- Growing trend of “Cloud services as cover” for malicious activity
  - Service endpoints are a safer way to access them
  - Service endpoints can still be abused
- These are not bugs in cloud providers’ services
  - They are published specifications
  - They can be misused

Avoiding unexpected outcomes

TECHNOLOGY RESPONSIBILITIES IN THE CLOUD



DNS TUNNELING – RAPID REVIEW

DNS Tunneling – Rapid Review

- Using DNS to evade firewalls and detection
- Encodes data in DNS packets
- Usually quite low performance vs network
- MITRE ATT&CK mapping
  - T1043 “Commonly Used Port” – traffic blends in
  - T1071 “Standard Application Layer Protocol” – Command & Control (C2)
  - T1048 “Exfiltration Over Alternative Protocol”
  - PRE-T1097 “Data hiding” – exfiltration and C2

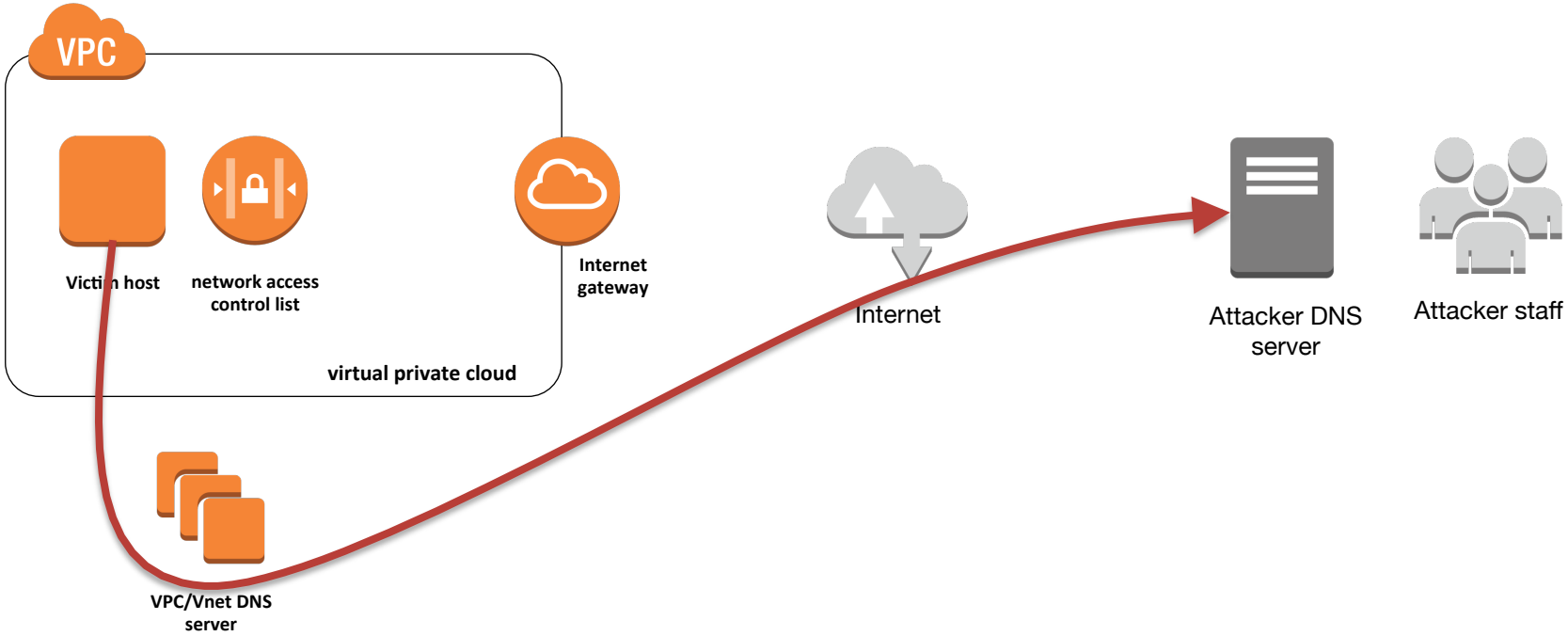
ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge

DNS Tunneling – Rapid Review

- For data transmission: queries w/ max record size 250 characters
- = 6 Primary Account Numbers + CVV2 & Expiration dates (base64*)
  - Mzc4MjgyMjQ2MzEwMDA1LjAxMTkuMTIzNAo-.NjAxMTAwMDk5MDEzOTQyNC4wMjIwLjEyMwo-.MzU2NjAwMjAyMDM2MDUwNS4wMzIxLjQ1Ngo-.NDAxMjg4ODg4ODg4MTg4MS4wNDIyLjc4OQo-.NTEwNTEwNTEwNTEwNTEwNTEwMC4wNTIzLjAxMjMK .MzA1NjkzMDkwMjU5MDQuMDExOS40NTYK.xfil.ml

    1 record
  - DNS should be case insensitive but case is often preserved
- For data reception: TXT records typically – much larger data payload

DNS Tunneling in public clouds



DNS resolution by provider

AWS	Azure	GCP
DNS Resolver IP: 169.254.169.253, “VPC+2”	168.63.129.16 (internal API server IP)	169.254.169.254 (the metadata server IP)
Can disable on per VPC basis; req’d for certain features, *eg* PrivateLink	Cannot disable	Cannot disable
Cannot block with VPC Security Groups	Cannot block with Network Security Groups	Cannot block with GCP Firewall Rules
Invisible in VPC Flow logs	-	-
Max 1024 q/sec per host	No published rate limit	No published rate limit

Most critical difference vs legacy data centers

- No user-accessible DNS query logs

DEMO SETUP #1
DNS TUNNELING IN CLOUD IAAS

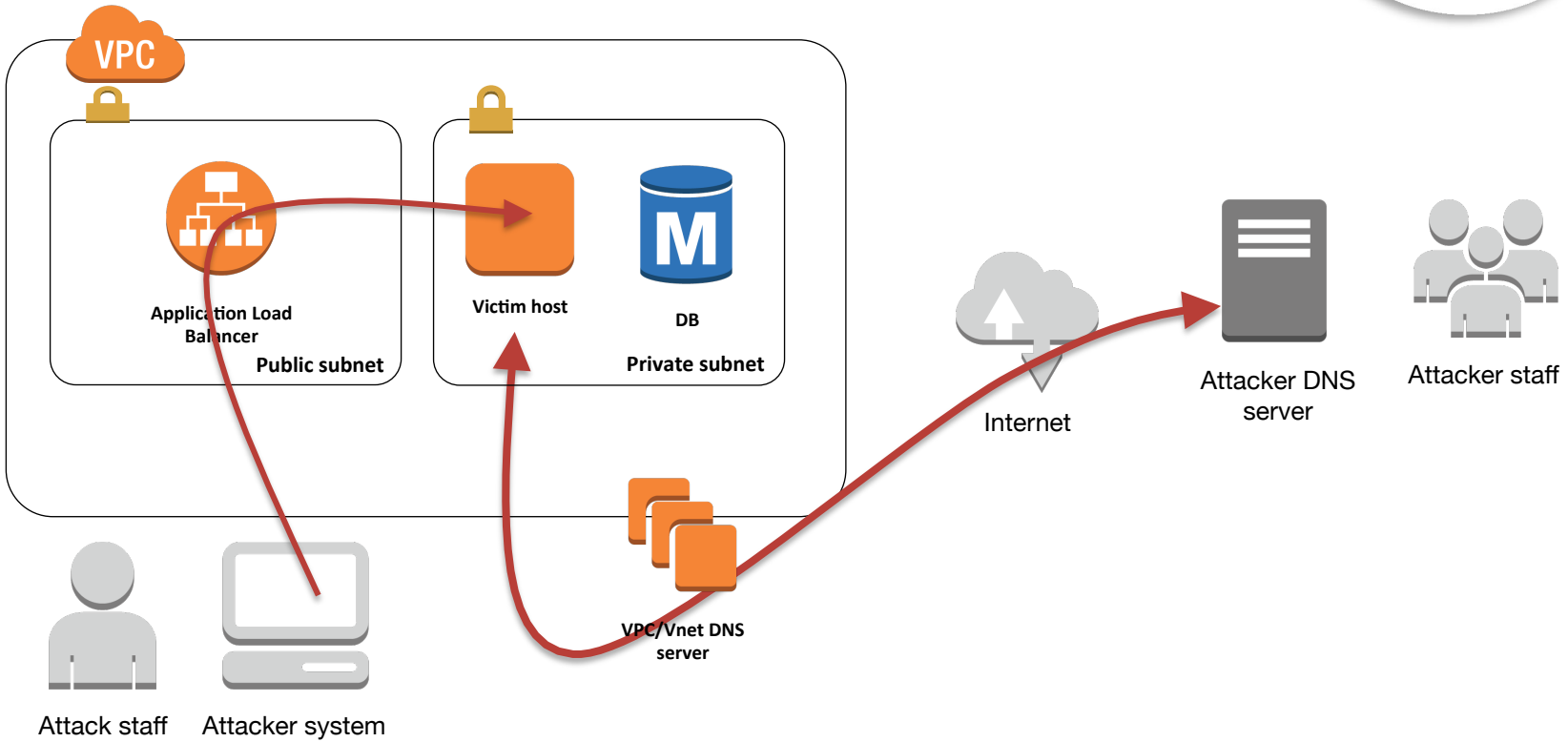
Hypothetical victim

- CatSwap.io - the leading startup for trading cats
- Databases
  - Celebrity cat demographic info (PII)
  - Credentials & payment info
- Files
  - Private cat photos
- API keys

Attack #1 overview

- Blind code injection to vulnerable Struts web server (CVE-2017-5638)
- Downloads `dnscat2` over VPC DNS server
- `dnscat2` creates tunnel for C2 and exfiltration
- Runs a few reconnaissance commands
- Dump data from cat user database
- Exfiltrate through DNS tunnel

Attack #1 - CatSwap.io web server & DNS



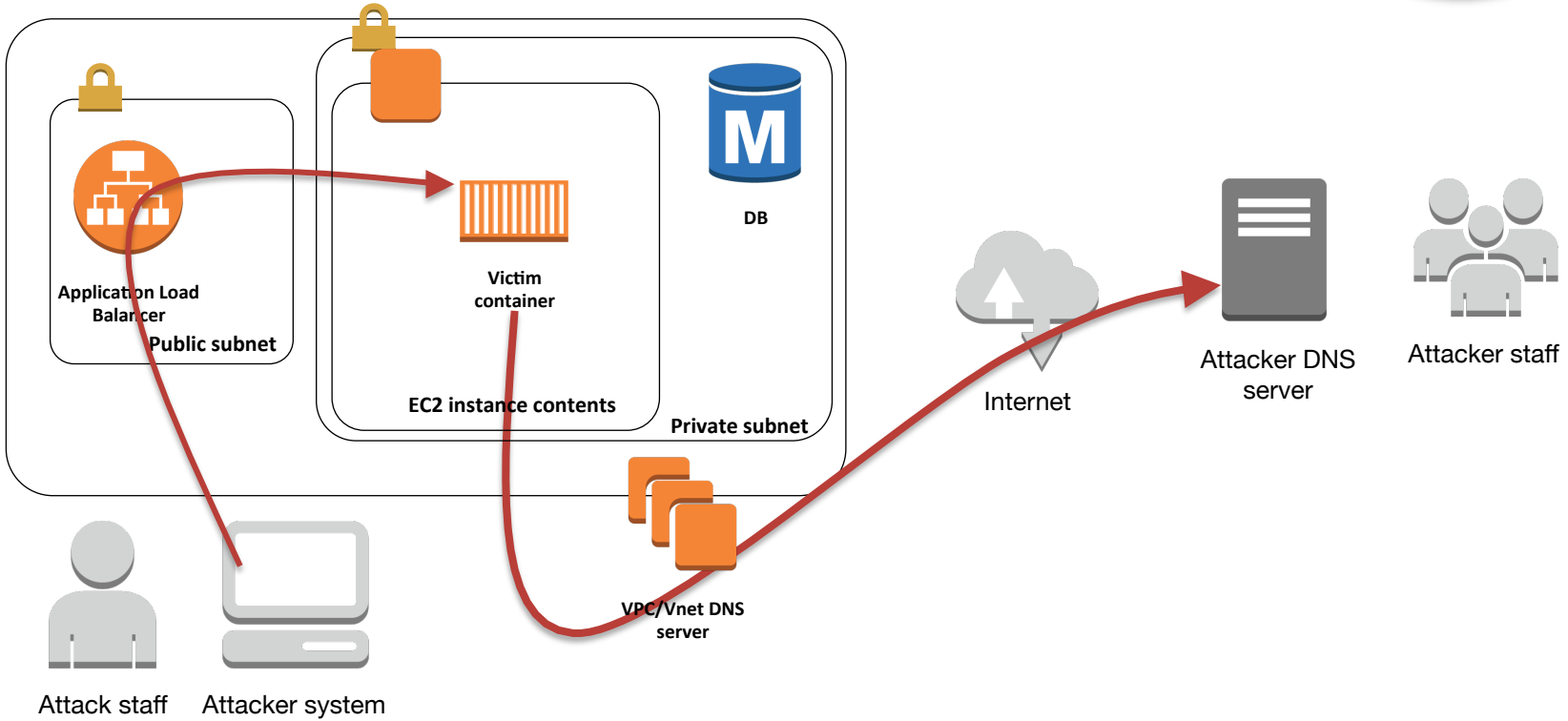
Attack #1 demo

Recap – Demo #1 VPC DNS

- Security groups did not stop the traffic – that is normal
- AWS VPC flow logs did not register anything – that is normal
- Attack utilities were downloaded over DNS by the attackers
  - AWS
  - Azure
  - GCP
- Simulated demographic info was exfiltrated without a trace at the cloud infrastructure level.

DEMO SETUP #2 – DNS TUNNELING IN CLOUD-BASED CONTAINERS

Attack #2 - CatSwap.io container design



Attack #2 demo

Recap – Demo #2: DNS Tunnels in Containers

- Sensitive data was taken through the same channels as in Demo #1
- Not substantially different from instances/virtual machines model
- Containers can make it easier to deny attackers to the commands they need to set up subsequent stages of attack

Applying – containers (and hosts)

- Reduce attackers' ability to "live off the land" from stock images
  - Remove/block DNS utilities like: host, dig, nslookup, getent
  - Remove/block cloud utilities: AWS CLI/Boto, Google Cloud SDK, Azure CLI/SDK
- Use read-only disks, or minimize local writable storage (noexec)
- Recycle containers before attackers can gain a foothold
- Many endpoint security & container security options

Applying what you have learned - DNS

- Focus on limiting full egress first
- In AWS, Azure and GCP:
  - Block & detect DNS traffic to unauthorized (not built-in) servers if possible
  - Host-based query logging is an option;
  - Advanced Endpoint Protection, WAFs, and other host controls can compensate
  - Application performance monitoring may be able to aid detection
- In AWS:
  - Consider building sensitive VPCs without `EnableDnsSupport`
  - Be aware of the many implications of doing this
- Configure your environment to use a DNS firewall or DNS filtering services

EXFILTRATION AND C2 THROUGH SERVICE ENDPOINTS

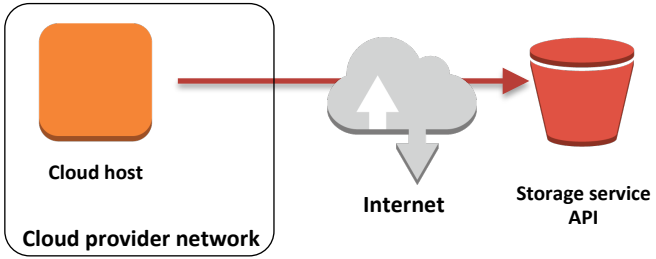
Exploiting Service Endpoints

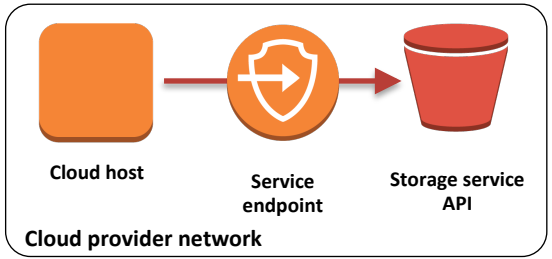
- Many interesting services in IaaS beyond cloud servers
- Hosts access these IaaS APIs via public IP space
  - Not just a simple network range
  - Uncontrolled access to public IP space is how data is stolen
- Private service endpoints avoid the need to expose outbound access

aws
VPC Endpoints

Google Cloud Platform
Private Google Access

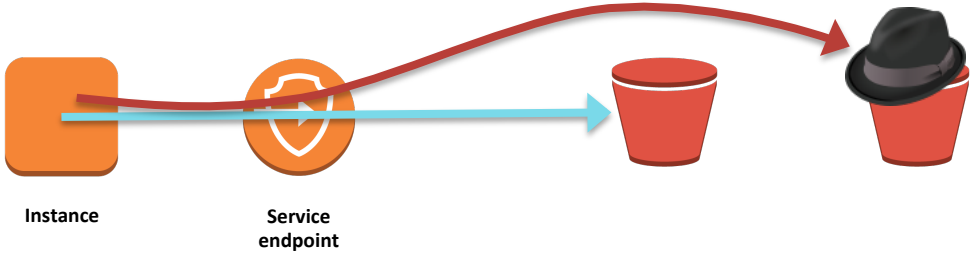
Microsoft Azure
Virtual Network Service Endpoints





Exploiting Service Endpoints

- Attackers can use service endpoints in your environment… to access services in their environment
  - AWS VPC endpoint policies can be used narrow use of service endpoints
- Mostly, policy capabilities prevent attackers from accessing victim resources – not vice versa



Service endpoints types & exfiltration options

AWS		Azure	GCP
Interface	*Gateway*		
EC2 & ELB	DynamoDB🔒	Blob Storage	Cloud Storage
Key Management Svc	S3🔒	SQL Database	Pub/Sub
Service Catalog		SQL Data Warehouse	Cloud Spanner & BigQuery
System Manager (SSM & ec2messages)			Bigtable & Cloud Datastore
Kinesis Data Streams			[…]

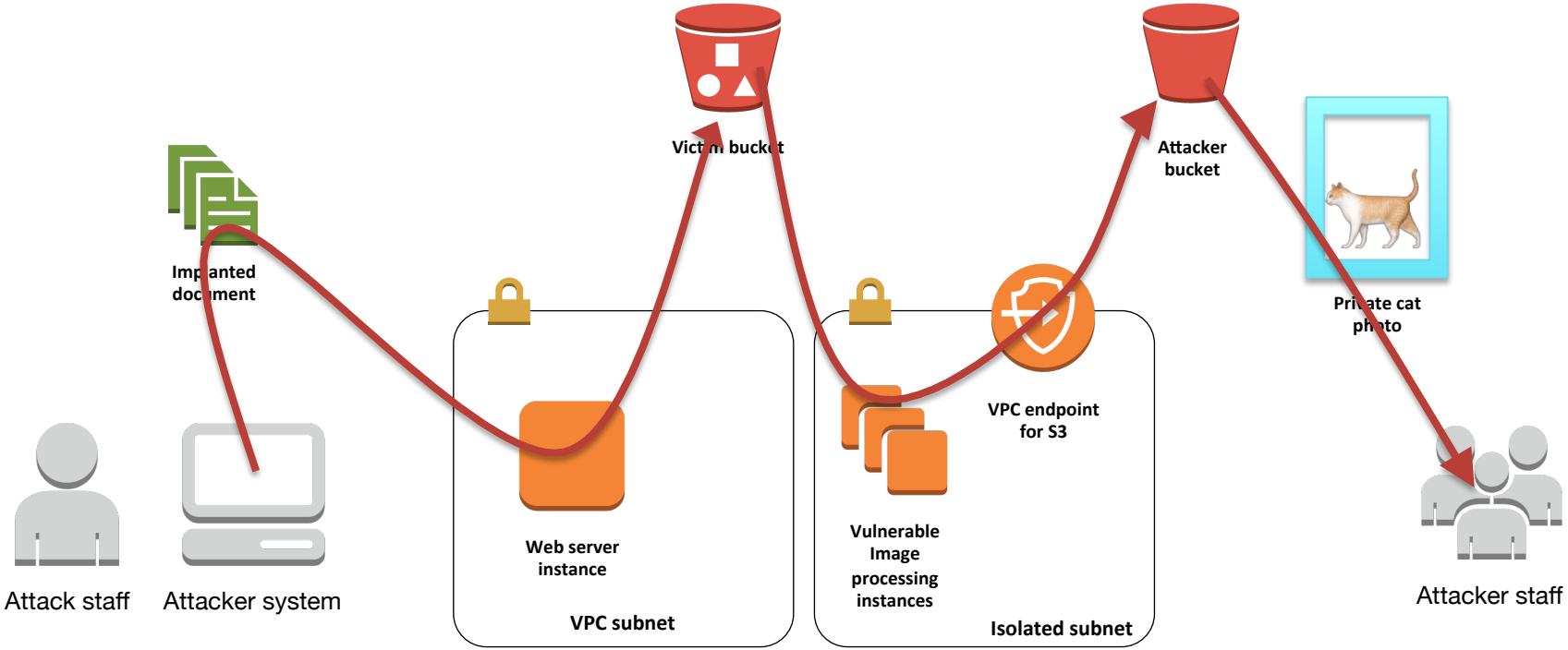
🔒 – support policies to restrict accounts & resources used through the endpoint

DEMO SETUP #3 – EXFILTRATION THROUGH STORAGE SERVICE ENDPOINT

Attack #3 overview

- CatSwap.io uses an image processing pool to handle cat photos
- Cluster has no access to the Internet except for storage service (S3) via service endpoint
- Attacker injects malicious image - vulnerable ImageMagick runs the implant
- C2 and exfiltration through objects in attacker's storage
- Attacker retrieves targeted assets from victim storage and uploads to attacker storage

Attack #3 - CatSwap.io image cluster design



Attack #3 demo

Recap – Demo #3: Storage Service Endpoint

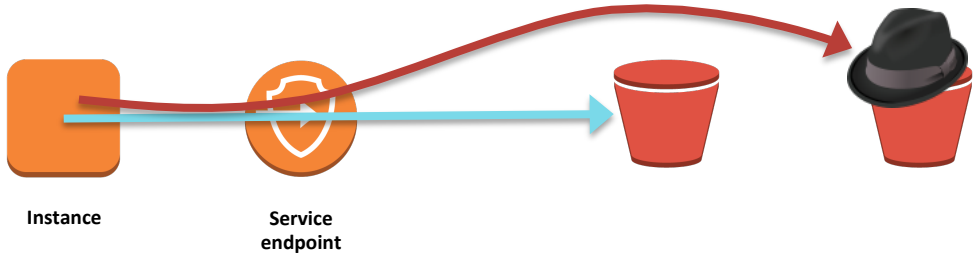
- Security groups did not stop the traffic – as expected
- AWS: Private cat photos were taken from the victim's S3 bucket and uploaded to the attacker's S3 bucket
- Once the AWS VPC Endpoint Policy was modified, the attack was thwarted as the attacker's S3 bucket could not be reached

Applying – Service Endpoints

- Be aware of how Service Endpoints can be used to reach hostile resources
- In AWS, configure policies so that only intended resources, not attacker resources, can be accessed
  - Currently available for: S3, DynamoDB
- In AWS, Azure & GCP, consider isolating service endpoints from sensitive hosts by subnet and filtering traffic by proxy
- As always, watch for new feature announcements from the cloud providers

Key Takeaways

- Simply blocking outbound traffic with network security groups generally does not prevent outbound DNS traffic
  - Hosts with airtight egress rules are not isolated from the Internet
- Hosts which can communicate with trusted cloud-based storage and databases can potentially be made to communicate with malicious cloud-based storage and databases



What to do tomorrow

- Harden your critical cloud-based networks
  - Check your most critical hosts/subnets for unrestricted outbound access
  - Don't allow it
  - Don't allow access to unauthorized DNS servers
- Harden your hosts & containers
  - Potentially block/remove DNS and Cloud API utilities from them
  - Keep instance/container lifetimes short; use read-only disks
  - Many advanced endpoint and container security solutions available
- Log and analyze DNS queries
  - Ask your cloud provider what their plans are for giving you logs
- View rules that allow traffic to cloud service APIs as liabilities
  - Tighten VPC endpoints with endpoint policies where possible

Final thoughts

- Each individual “cloud shadow” will shift & drift along with enhancements from IaaS providers
- Just as some changes will help defenders, other changes may be exploited by attackers
- Attackers are dissolving into the background using the same cloud providers and services as their victims

RESOURCES

Resources

- Struts vulnerability exploitation - https://github.com/tahmed11/strutsy
- Vulnerable application docker images
  - https://hub.docker.com/r/bharghav9/apachestrutscve-vuln-2017-5638/
  - https://github.com/craighurley/docker-imagetragick
- dnscat2 - https://github.com/iagox86/dnscat2

References & Further Reading

- Ed Skoudis on DNS tunneling - https://blogs.sans.org/pen-testing/files/2012/03/RSA-2012-EXP-108-Skoudis-Ullrich.pdf
- Greg Farnham, Detecting DNS tunneling - https://www.sans.org/reading-room/whitepapers/dns/detecting-dns-tunneling-34152
- DNSPerf - https://www.nominum.com/measurement-tools/
- DNS firewalls in Azure: https://azure.microsoft.com/en-us/blog/dns-security-appliances-in-azure/
- DNS analytics in Azure: https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-dns
- Using S3 for C2: https://rhinosecuritylabs.com/aws/hiding-cloudcobalt-strike-beacon-c2-using-amazon-apis/
- DNS tunneling in AWS with Iodine: https://dejandayoff.com/using-dns-to-break-out-of-isolated-networks-in-a-aws-cloud-environment/
- AWS Hybrid Cloud DNS white paper: https://d1.awsstatic.com/whitepapers/hybrid-cloud-dns-options-for-vpc.pdf

- Thanks: Tim S, Julia, Darren, Suresh :)