RSA Conference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: AIR-R05F

Cloud Attacks Illustrated: Insights from the cloud provider

Craig Nelson

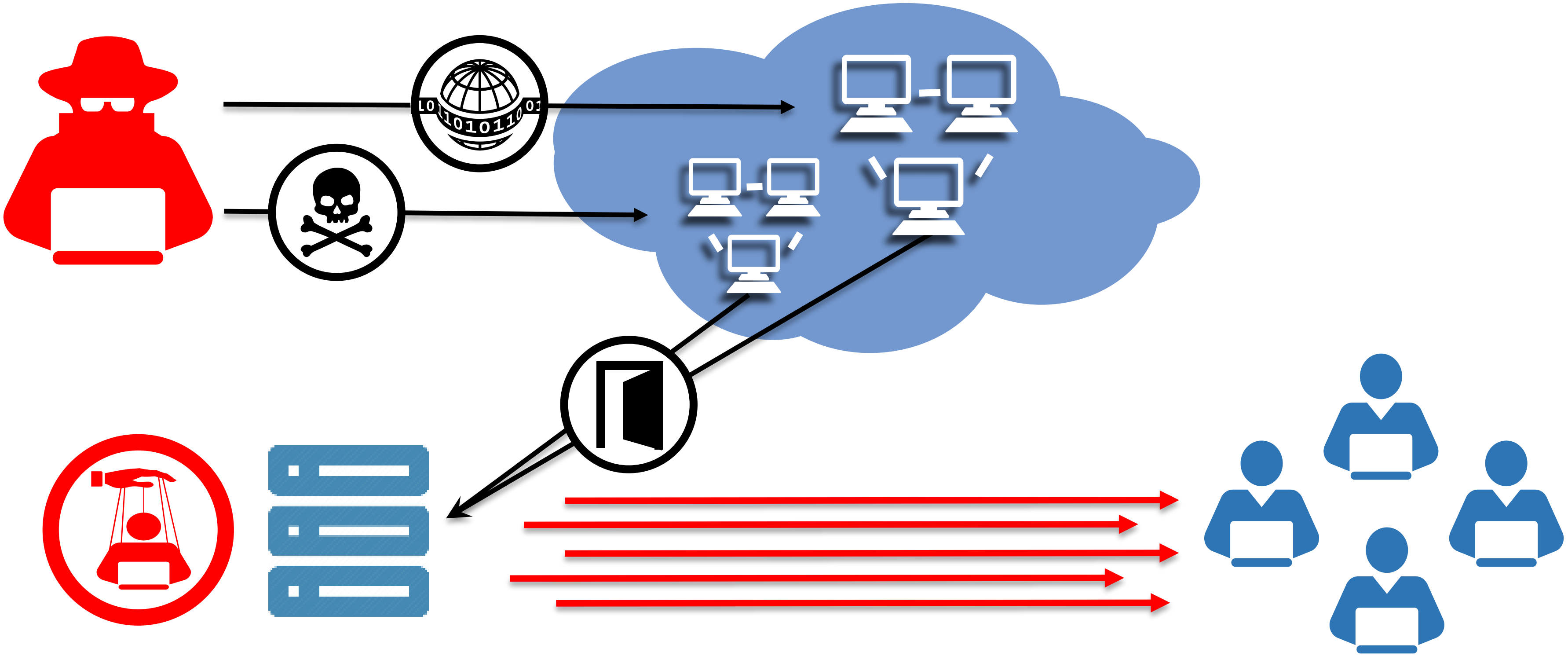
Security Software Engineering Manager
Microsoft, MSRC (Azure)
@ath0nocarrier

Tomer Teller

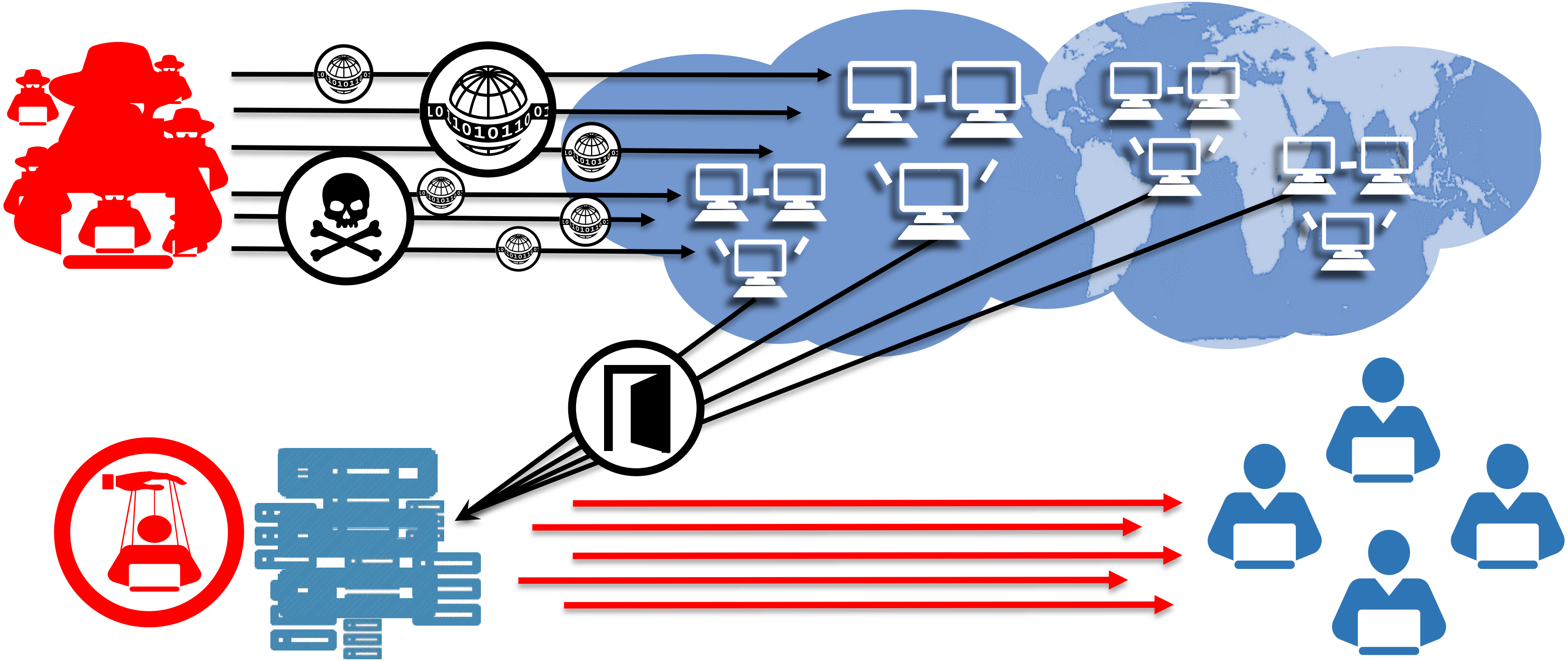
Azure Security Research PM
Microsoft
@djteller

#RSAC

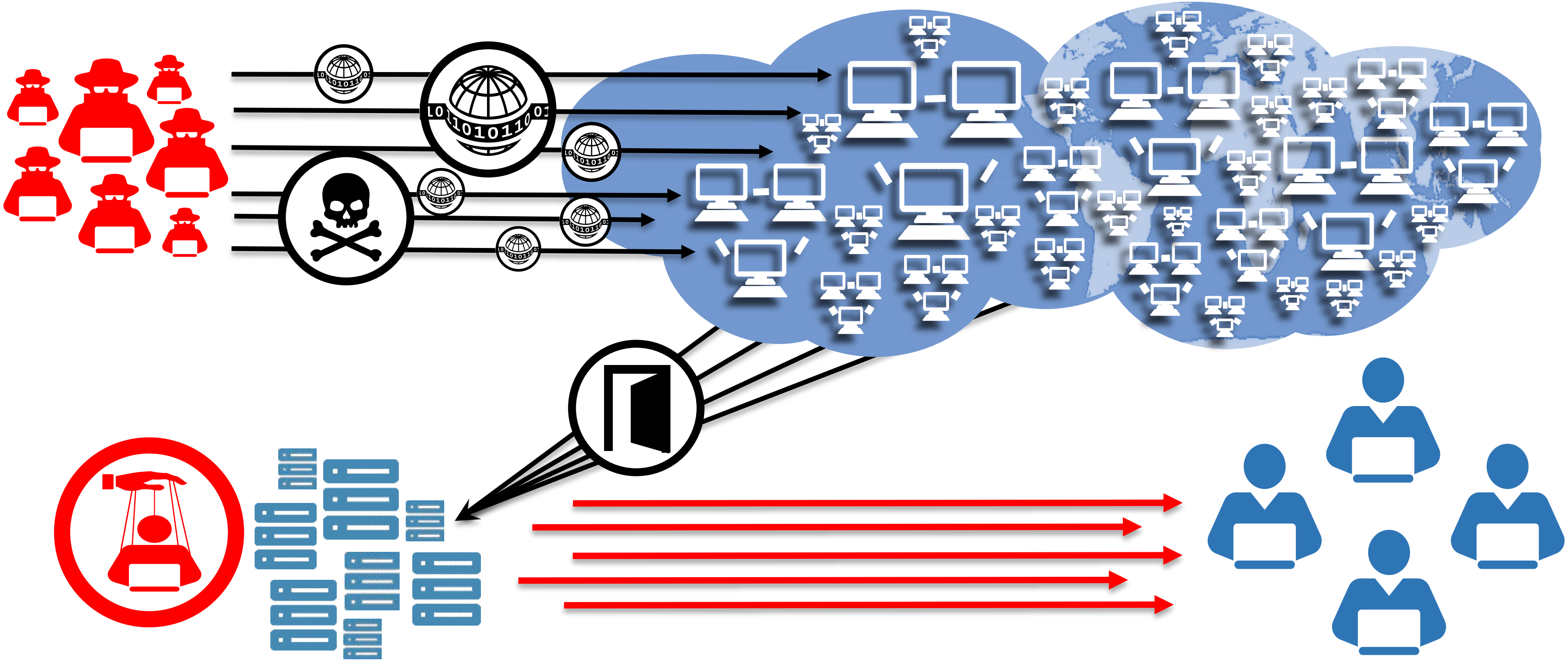
Cloud Weaponization



Cloud Weaponization

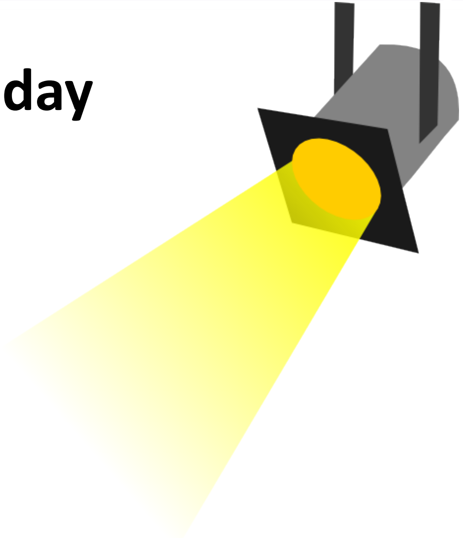


Cloud Weaponization



Setting the Stage

- We are going to talk about what is **happening today**
- This information is **immediately applicable**



Which attacks should I expect?

How to prevent them?

How to detect them?

How to respond to them?

Cloud Basic Terminology

Customer

Subscription

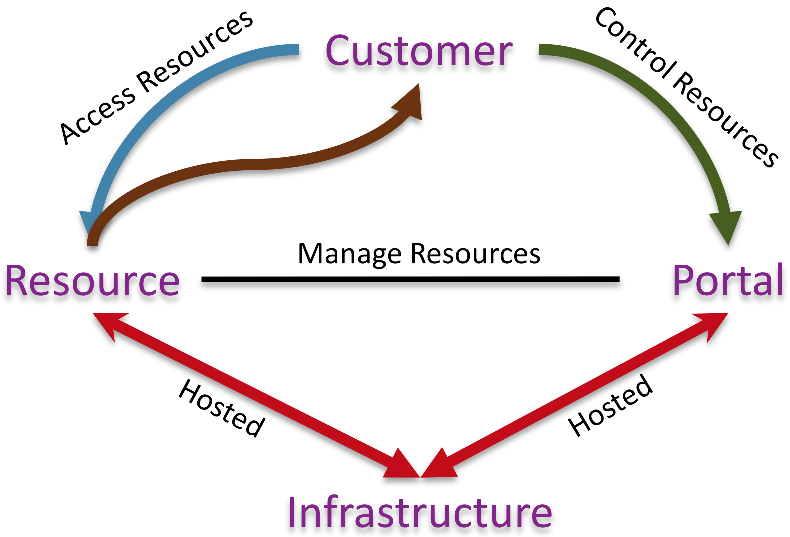
Resource Group

Resource

Cloud Attack Surface (Partial)

Buffer overflow
SQL Injection
Privilege escalation

Certificate spoofing
Phishing
Drive-By-Download

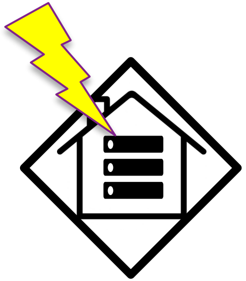


Side channel
DDoS
Data integrity

Brute Force
Password reset
Impersonation

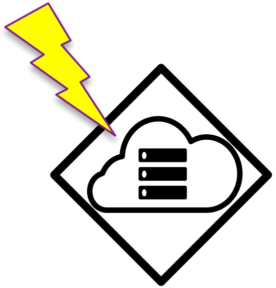
Types of Attacks

On-Prem



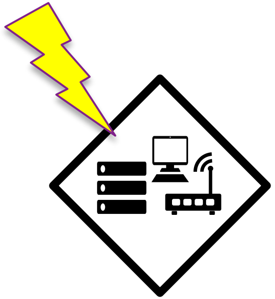
Direct Indirect

Cloud Resource



Fraud Exploit

Infrastructure

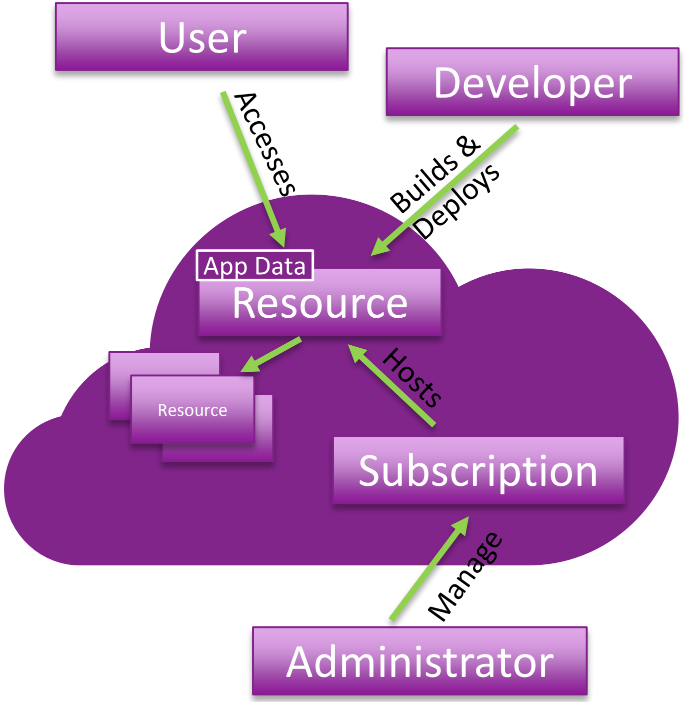


DoS LPE

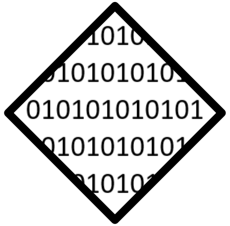
Perspectives on the cloud

Who are the targets?

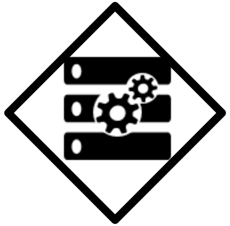
- **User**
  Impersonate the user, Take the user's data
- **Developer**
  Compromise services, bypass controls, plant backdoors
- **Resource**
  Take data, logic bomb, surveil transactions, subvert auditing
- **Subscription**
  Complete control of cloud resources
- **Administrator**
  Pivot attack to on-prem resources
- **Cloud Provider**
  Complete dominion of multiple tenant



Why does the cloud appeal to attackers?



Data

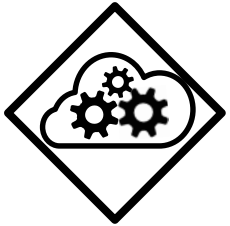


Technology

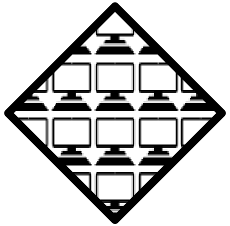
Multitenant

Free Trials

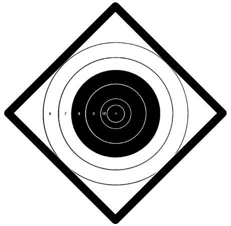
Anonymity



Horse Power



Heterogeneous



Attack Surface

Cloud Services – Shared Responsibility

On Premises	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
🟦 Applications	🟦 Applications	🟦 Applications	🟩 Applications
🟦 Data	🟦 Data	🟦 Data	🟩 Data
🟦 Runtime	🟦 Runtime	🟩 Runtime	🟩 Runtime
🟦 Middleware	🟦 Middleware	🟩 Middleware	🟩 Middleware
🟦 O/S	🟦 O/S	🟩 O/S	🟩 O/S
🟦 Virtualization	🟩 Virtualization	🟩 Virtualization	🟩 Virtualization
🟦 Servers	🟩 Servers	🟩 Servers	🟩 Servers
🟦 Storage	🟩 Storage	🟩 Storage	🟩 Storage
🟦 Networking	🟩 Networking	🟩 Networking	🟩 Networking

Managed by:

- 🟦 Customer
- 🟩 Provider

What are the risks for the provider?

Compromise infrastructure

Impact to provider

Cloud Weaponization

Impact to target

Compromise tenant

Impact to cloud adoption

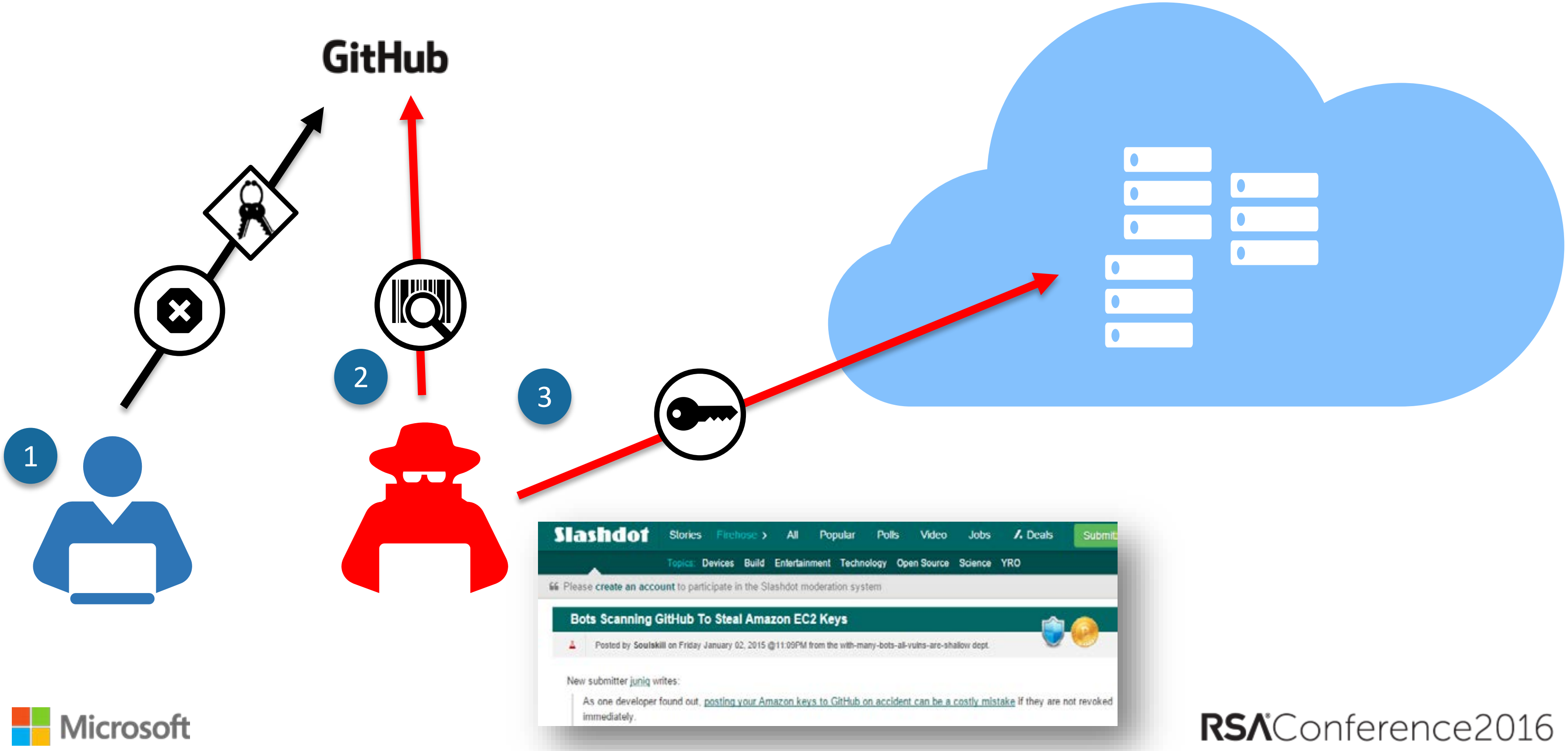
Cloud attack case studies

“Public Secrets” Attacker Profile

“LOW”
SOPHISTICATION

“LOW”
FOCUS

"Public Secrets" – Attacks Against Tenants



Slashdot Stories Firehose › All Popular Polls Video Jobs Deals Submit

Topics: Devices Build Entertainment Technology Open Source Science YRO

Please **create an account** to participate in the Slashdot moderation system

Bots Scanning GitHub To Steal Amazon EC2 Keys

Posted by **Soulskill** on Friday January 02, 2015 @11:09PM from the with-many-bots-all-vulns-are-shallow dept.

New submitter juniq writes:

> As one developer found out, posting your Amazon keys to GitHub on accident can be a costly mistake if they are not revoked immediately.

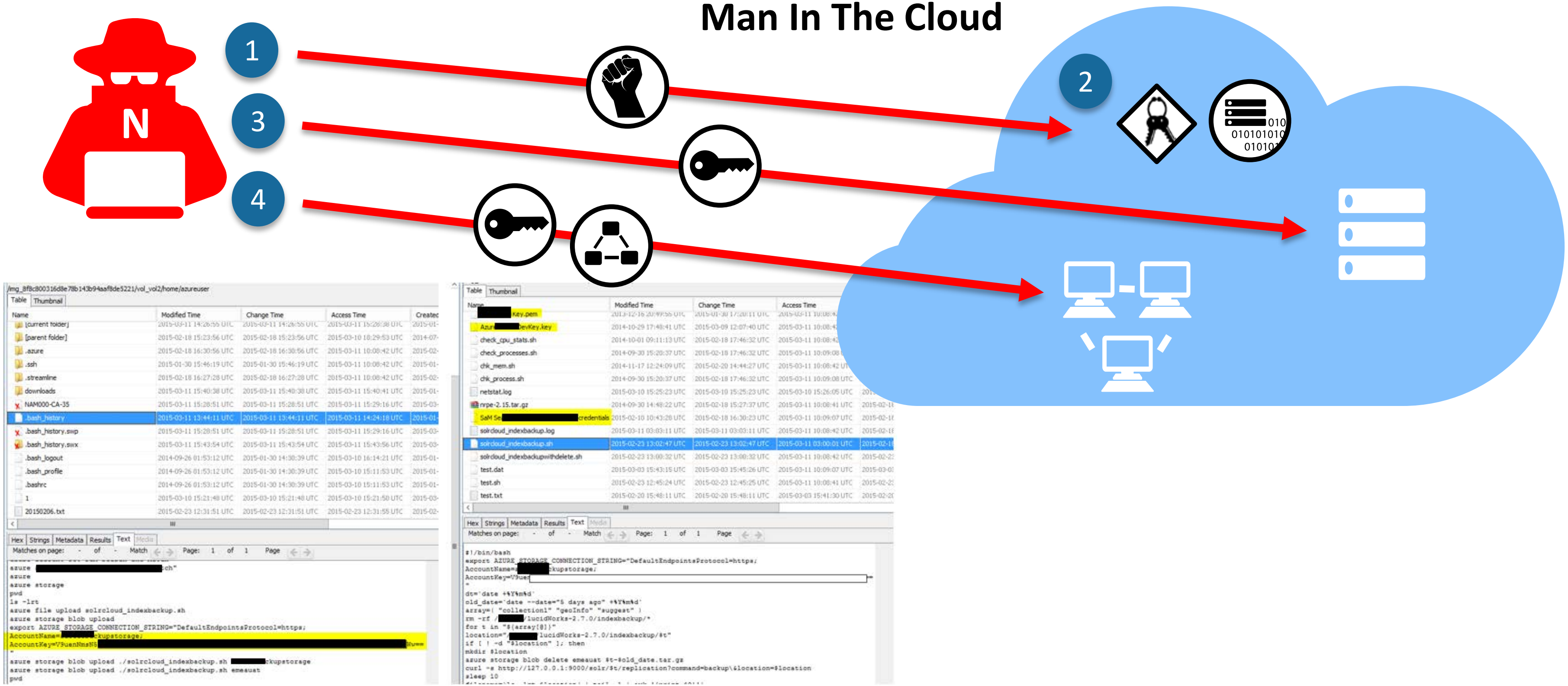
“Deep Impact” Attacker Profile

“MEDIUM”
SOPHISTICATION

“HIGH”
FOCUS

“Deep Impact” – Attacks Against Tenants

Man In The Cloud



/img_8f8c800316d8e78b143b94aaf8de5221/vol_vol2/home/azureuser

Table | Thumbnail

Name	Modified Time	Change Time	Access Time	Created
[current folder]	2015-03-11 14:26:55 UTC	2015-03-11 14:26:55 UTC	2015-03-11 15:28:38 UTC	2015-01-
[parent folder]	2015-02-18 15:23:56 UTC	2015-02-18 15:23:56 UTC	2015-03-10 18:29:53 UTC	2014-07-
.azure	2015-02-18 16:30:56 UTC	2015-02-18 16:30:56 UTC	2015-03-11 10:08:42 UTC	2015-02-
.ssh	2015-01-30 15:46:19 UTC	2015-01-30 15:46:19 UTC	2015-03-11 10:08:42 UTC	2015-01-
.streamline	2015-02-18 16:27:28 UTC	2015-02-18 16:27:28 UTC	2015-03-11 10:08:42 UTC	2015-02-
downloads	2015-03-11 15:40:38 UTC	2015-03-11 15:40:38 UTC	2015-03-11 15:40:41 UTC	2015-01-
NAM000-CA-35	2015-03-11 15:28:51 UTC	2015-03-11 15:28:51 UTC	2015-03-11 15:29:16 UTC	2015-03-
.bash_history	2015-03-11 13:44:11 UTC	2015-03-11 13:44:11 UTC	2015-03-11 14:24:18 UTC	2015-01-
.bash_history.swp	2015-03-11 15:28:51 UTC	2015-03-11 15:28:51 UTC	2015-03-11 15:29:16 UTC	2015-03-
.bash_history.swx	2015-03-11 15:43:54 UTC	2015-03-11 15:43:54 UTC	2015-03-11 15:43:56 UTC	2015-03-
.bash_logout	2014-09-26 01:53:12 UTC	2015-01-30 14:30:39 UTC	2015-03-10 16:14:21 UTC	2015-01-
.bash_profile	2014-09-26 01:53:12 UTC	2015-01-30 14:30:39 UTC	2015-03-10 15:11:53 UTC	2015-01-
.bashrc	2014-09-26 01:53:12 UTC	2015-01-30 14:30:39 UTC	2015-03-10 15:11:53 UTC	2015-01-
1	2015-03-10 15:21:48 UTC	2015-03-10 15:21:48 UTC	2015-03-10 15:21:50 UTC	2015-03-
20150206.txt	2015-02-23 12:31:51 UTC	2015-02-23 12:31:51 UTC	2015-02-23 12:31:55 UTC	2015-02-

Hex | Strings | Metadata | Results | Text | Media

Matches on page: - of - Match Page: 1 of 1 Page

```
azure [redacted]ch"
azure
azure storage
pwd
ls -lrt
azure file upload solrcloud_indexbackup.sh
azure storage blob upload
export AZURE_STORAGE_CONNECTION_STRING="DefaultEndpointsProtocol=https;
AccountName=[redacted]ckupstorage;
AccountKey=V9uenNmsN5[redacted]Nw==
"
azure storage blob upload ./solrcloud_indexbackup.sh [redacted]ckupstorage
azure storage blob upload ./solrcloud_indexbackup.sh emeauat
pwd
```

Table | Thumbnail

Name	Modified Time	Change Time	Access Time	
[redacted]Key.pem	2013-12-16 20:49:55 UTC	2015-01-30 17:20:11 UTC	2015-03-11 10:08:4	
Azur[redacted]DevKey.key	2014-10-29 17:48:41 UTC	2015-03-09 12:07:40 UTC	2015-03-11 10:08:4	
check_cpu_stats.sh	2014-10-01 09:11:13 UTC	2015-02-18 17:46:32 UTC	2015-03-11 10:08:4	
check_processes.sh	2014-09-30 15:20:37 UTC	2015-02-18 17:46:32 UTC	2015-03-11 10:09:08	
chk_mem.sh	2014-11-17 12:24:09 UTC	2015-02-20 14:44:27 UTC	2015-03-11 10:08:42 UT	
chk_process.sh	2014-09-30 15:20:37 UTC	2015-02-18 17:46:32 UTC	2015-03-11 10:09:08 UTC	
netstat.log	2015-03-10 15:25:23 UTC	2015-03-10 15:25:23 UTC	2015-03-10 15:26:05 UTC	201
nrpe-2.15.tar.gz	2014-09-30 14:48:22 UTC	2015-02-18 15:27:37 UTC	2015-03-11 10:08:41 UTC	2015-02-1
SaM Se[redacted]credentials	2015-02-10 10:43:28 UTC	2015-02-18 16:30:23 UTC	2015-03-11 10:09:07 UTC	2015-02-1
solrcloud_indexbackup.log	2015-03-11 03:03:11 UTC	2015-03-11 03:03:11 UTC	2015-03-11 10:08:42 UTC	2015-02-1
solrcloud_indexbackup.sh	2015-02-23 13:02:47 UTC	2015-02-23 13:02:47 UTC	2015-03-11 03:00:01 UTC	2015-02-1
solrcloud_indexbackupwithdelete.sh	2015-02-23 13:00:32 UTC	2015-02-23 13:00:32 UTC	2015-03-11 10:08:42 UTC	2015-02-2
test.dat	2015-03-03 15:43:15 UTC	2015-03-03 15:45:26 UTC	2015-03-11 10:09:07 UTC	2015-03-0
test.sh	2015-02-23 12:45:24 UTC	2015-02-23 12:45:25 UTC	2015-03-11 10:08:41 UTC	2015-02-2
test.txt	2015-02-20 15:48:11 UTC	2015-02-20 15:48:11 UTC	2015-03-03 15:41:30 UTC	2015-02-2

Hex | Strings | Metadata | Results | Text | Media

Matches on page: - of - Match Page: 1 of 1 Page

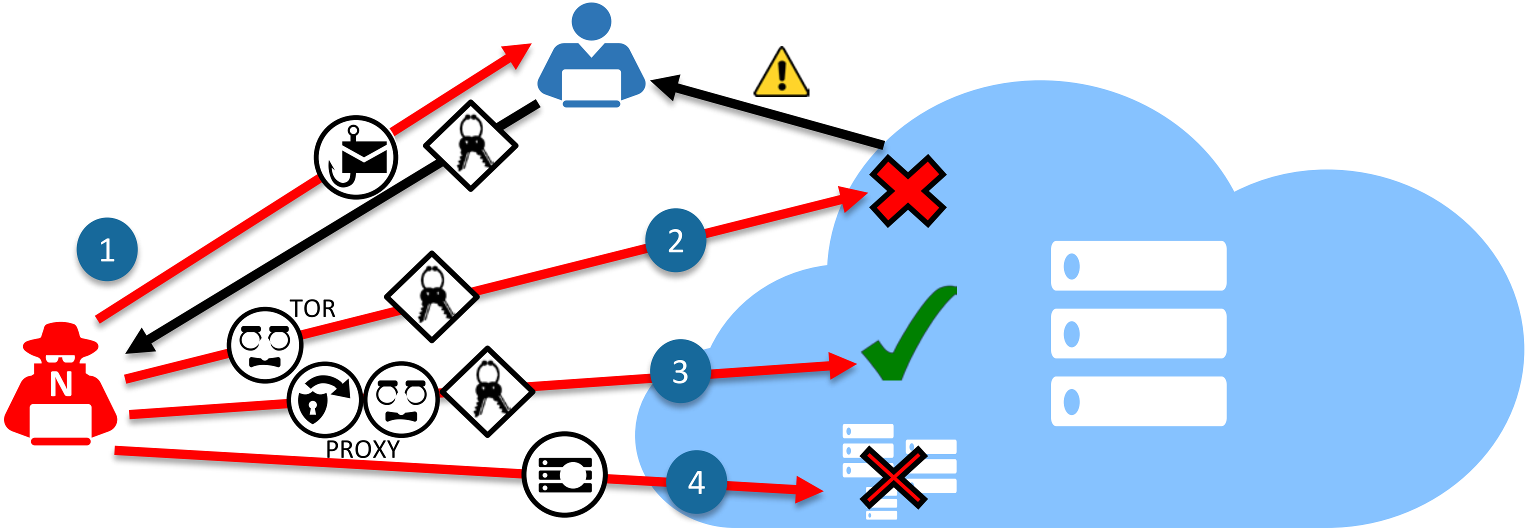
```
#!/bin/bash
export AZURE_STORAGE_CONNECTION_STRING="DefaultEndpointsProtocol=https;
AccountName=[redacted]ckupstorage;
AccountKey=V9ue[redacted]=
"
dt=`date +%Y%m%d`
old_date=`date --date="5 days ago" +%Y%m%d`
array=( "collection1" "geoInfo" "suggest" )
rm -rf /[redacted]/lucidWorks-2.7.0/indexbackup/*
for t in "${array[@]}"
location="/[redacted]/lucidWorks-2.7.0/indexbackup/$t"
if [ ! -d "$location" ]; then
mkdir $location
azure storage blob delete emeauat $t-$old_date.tar.gz
curl -s http://127.0.0.1:9000/solr/$t/replication?command=backup\&location=$location
sleep 10
```

“Big Target” Attacker Profile

“HIGH”
SOPHISTICATION

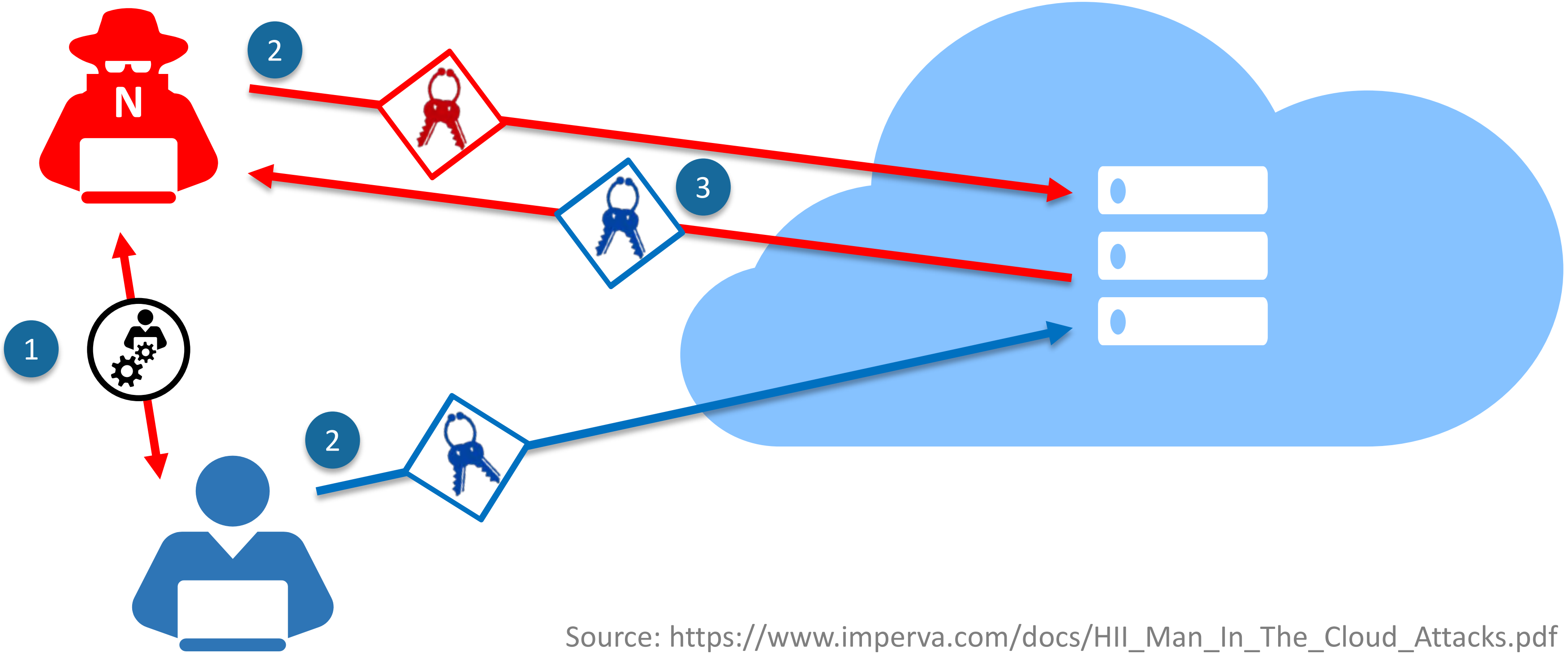
“HIGH”
FOCUS

"Big Target" – Attacks Against Tenants



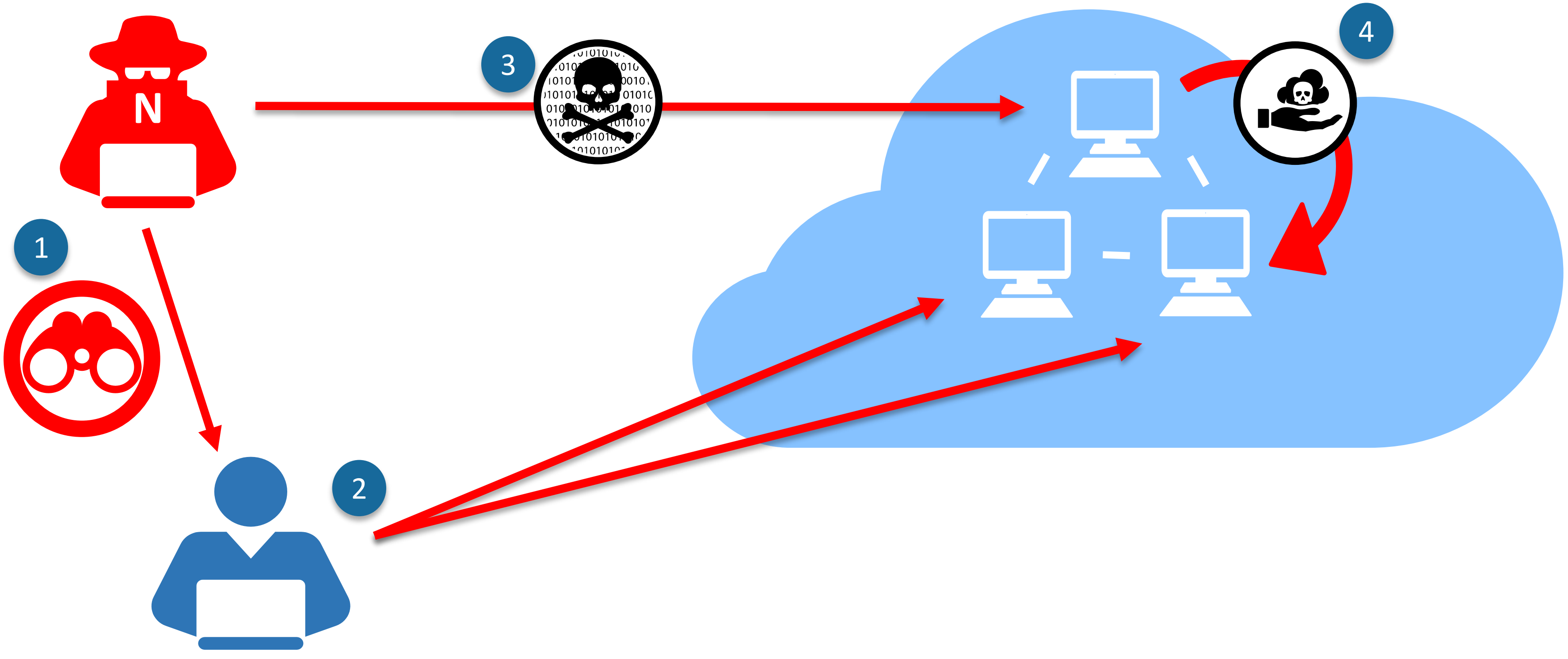
Threats on the horizon

“Man In The Cloud” – In-Direct Tenant Attacks



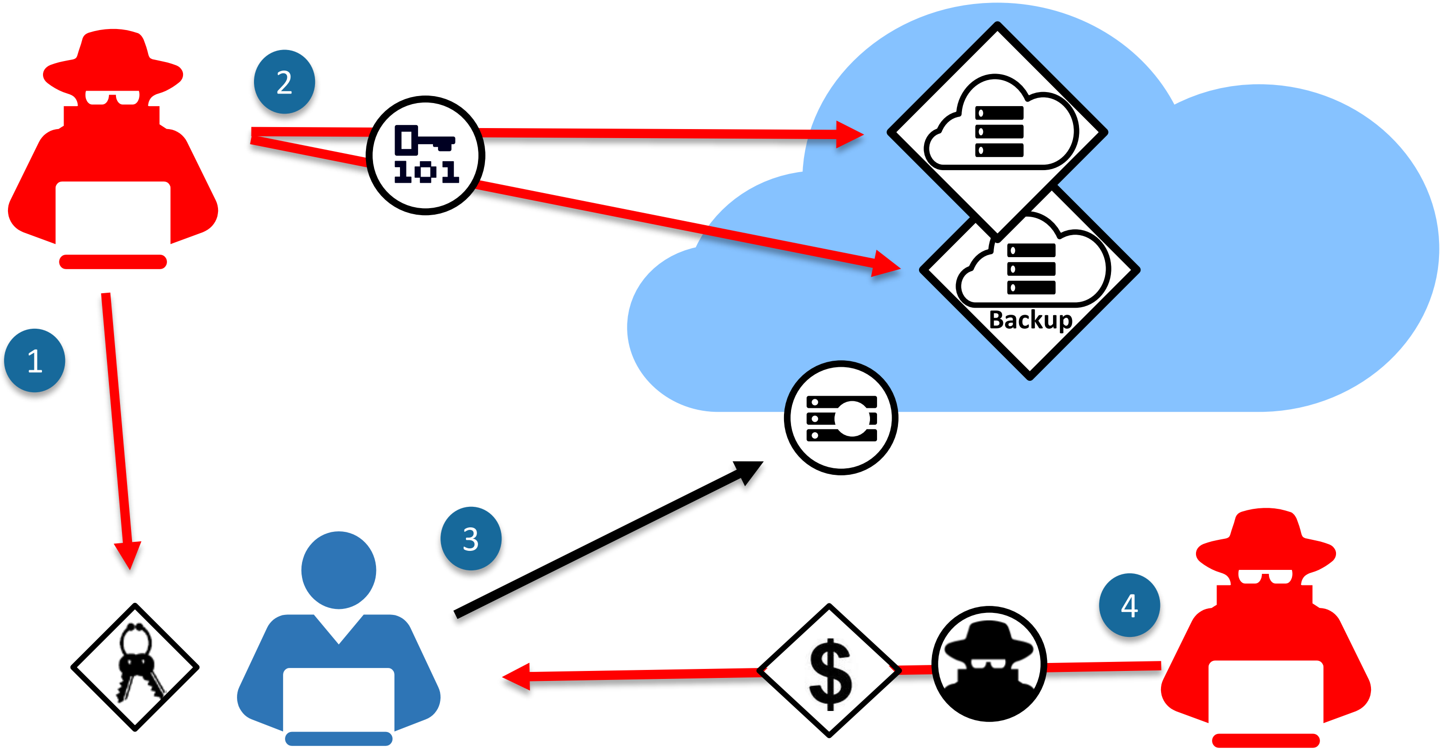
Source: https://www.imperva.com/docs/HII_Man_In_The_Cloud_Attacks.pdf

“Side Channel” – Indirect Tenant Attacks



Source: http://cseweb.ucsd.edu/~hovav/dist/cloudsec.pdf

"Resource Ransom" – Direct Tenant Attacks



Kill Chain Differences

Phase	On-premises	Public Cloud*
Active Recon	HUMINT, OSINT (Users)	Foot printing (Services)
Delivery	Browser, Mail, USB (User Interaction)	Hacking (No User Interaction)
Exploitation	Client-Side vulnerabilities	Server-Side vulnerabilities
Persistence	File System Based	Memory Based
Internal Recon	Custom Tools	Built-in Admin Tools
Lateral Movement	Machine Pivot	Resource Pivot

** Cloud environments add new attack vectors on top of the regular enterprise attack vectors*

Cloud Clean Chain

...or how to not become a case study

Apply - Prevention

For the developer:

- ✓ Remember the SDL
- ✓ Never check Shared Secrets and Private Keys into source control
- ✓ Track, monitor, and review who has access to your subscription
- ✓ Enable and validate logging on Cloud resources

For the subscription owner & infrastructure engineer:

- ✓ Maintain accurate contact information with your cloud provider
- ✓ Control and monitor management ports exposed to the internet
- ✓ Scrutinize authentication choices, and how secrets are controlled
- ✓ Validate patch processes (for IaaS and containers)
- ✓ Extend mature IT security processes to the cloud

Apply - Detection

For the security IT:

- ✓ Think in graphs, visualize your environment!
- ✓ Enable, collect, monitor logs in all your resources
- ✓ Correlate Network, VM and resource signals
- ✓ Cluster events from the same resource groups
- ✓ Map alerts into kill chain to track movement
- ✓ Deploy external/internal Honeypot to gain insights
- ✓ Leverage Threat Intelligence wherever possible

“Final” Apply Slide

- ✓ Understand your cloud attack surface
- ✓ Review the kill chain differences
- ✓ Follow & implement the cloud clean chain
- ✓ Explore security services provided by your cloud providers

Summary

- Cloud services is a shared responsibility
- Cloud clean chain can help reduce the attack surface
- Don’t reinvent the wheel, extend it!

Q&A

?

Craig Nelson
Security Software Engineering Manager

Microsoft, MSRC (Azure)
@ath0nocarrier

Tomer Teller
Azure Security Research PM

Microsoft, Azure Security
@djteller

Thank You