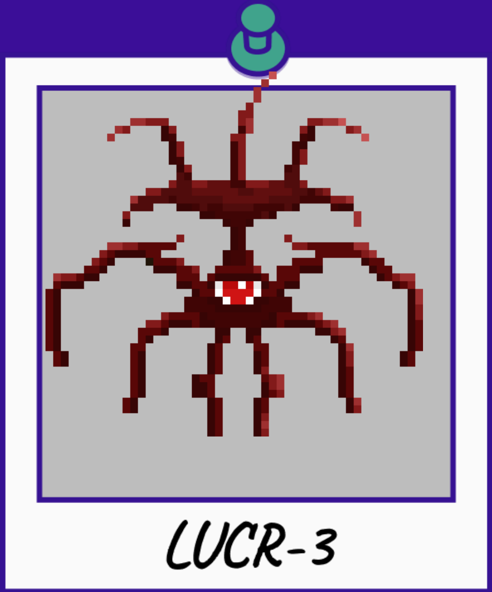
PERMISO

LUCR-3

Cloud Clepto & SaaS-y Scattered Spider shenanigans



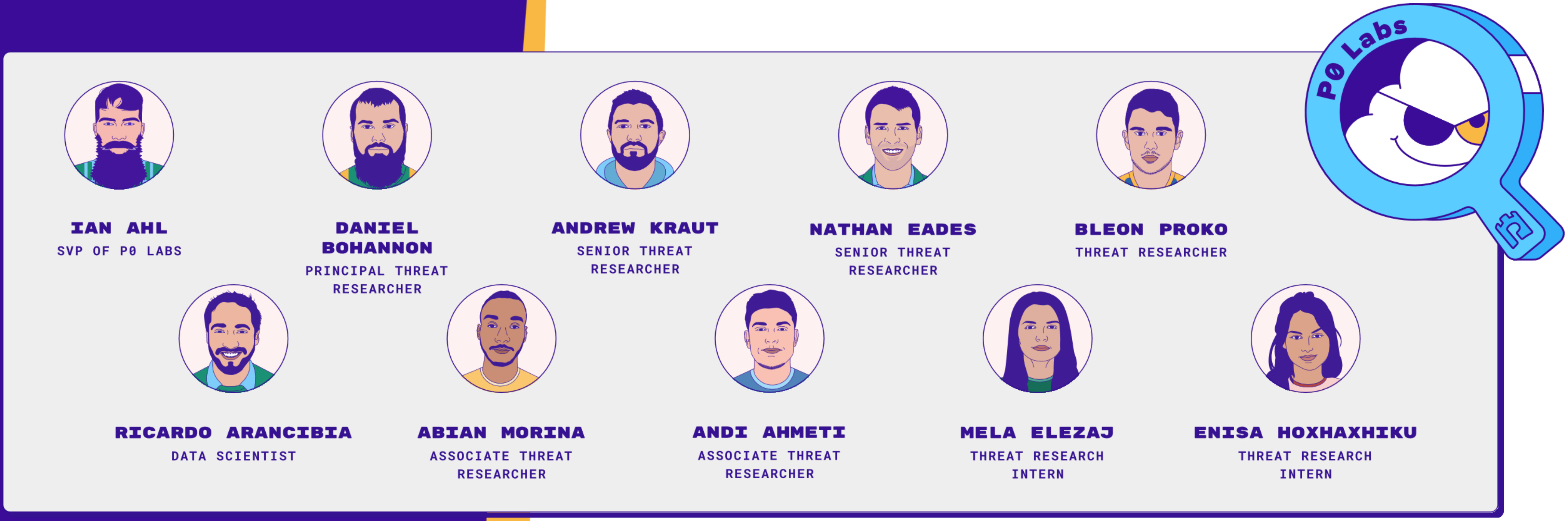
AKAs:

SCATTERED SPIDER
UNC3944
Roasted 0ktapus
STORM-0875 (Octo Tempest)

https://permiso.itch.io/permiso-survivors

Ian Ahl, SVP of Permiso's P0 Labs

- Mandiant 10'ish Years
  - Advanced Practices Lead
  - Incident Response
- @TekDefense
- USMC



IAN AHL
SVP OF P0 LABS

DANIEL BOHANNON
PRINCIPAL THREAT RESEARCHER

ANDREW KRAUT
SENIOR THREAT RESEARCHER

NATHAN EADES
SENIOR THREAT RESEARCHER

BLEON PROKO
THREAT RESEARCHER

RICARDO ARANCIBIA
DATA SCIENTIST

ABIAN MORINA
ASSOCIATE THREAT RESEARCHER

ANDI AHMETI
ASSOCIATE THREAT RESEARCHER

MELA ELEZAJ
THREAT RESEARCH INTERN

ENISA HOXHAXHIKU
THREAT RESEARCH INTERN

Understanding LUCR-3

Who

- AKAs: Scattered Spider, UNC3944, Roasted Oktapus, STORM-0875
- Attribution Difficulties (BlackCat)

Mission

- Financial Gain through
  - Ransom
  - Extortion
  - CryptoMining

Victimology

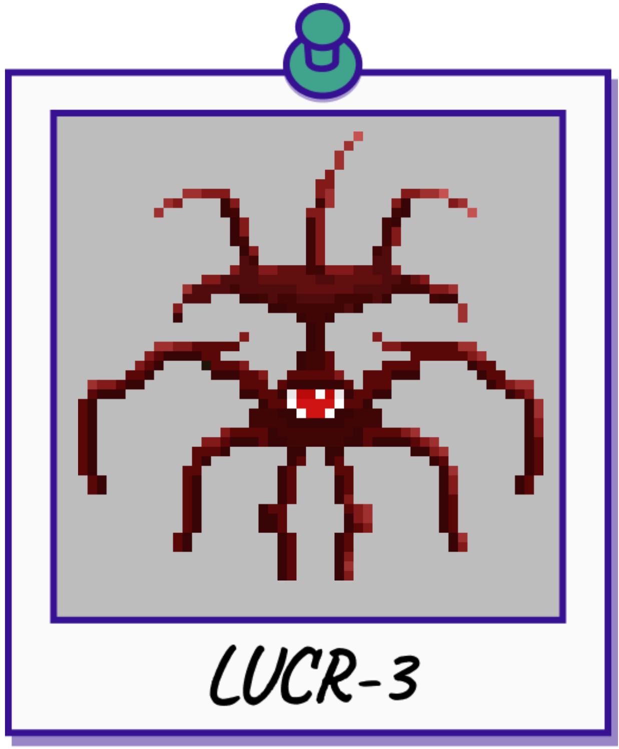
- Telecom
- Software/Technology
- Heavy Expansion

Impacted Environments

- On Prem
- Cloud
- SaaS
- CI/CD

Consistent Themes

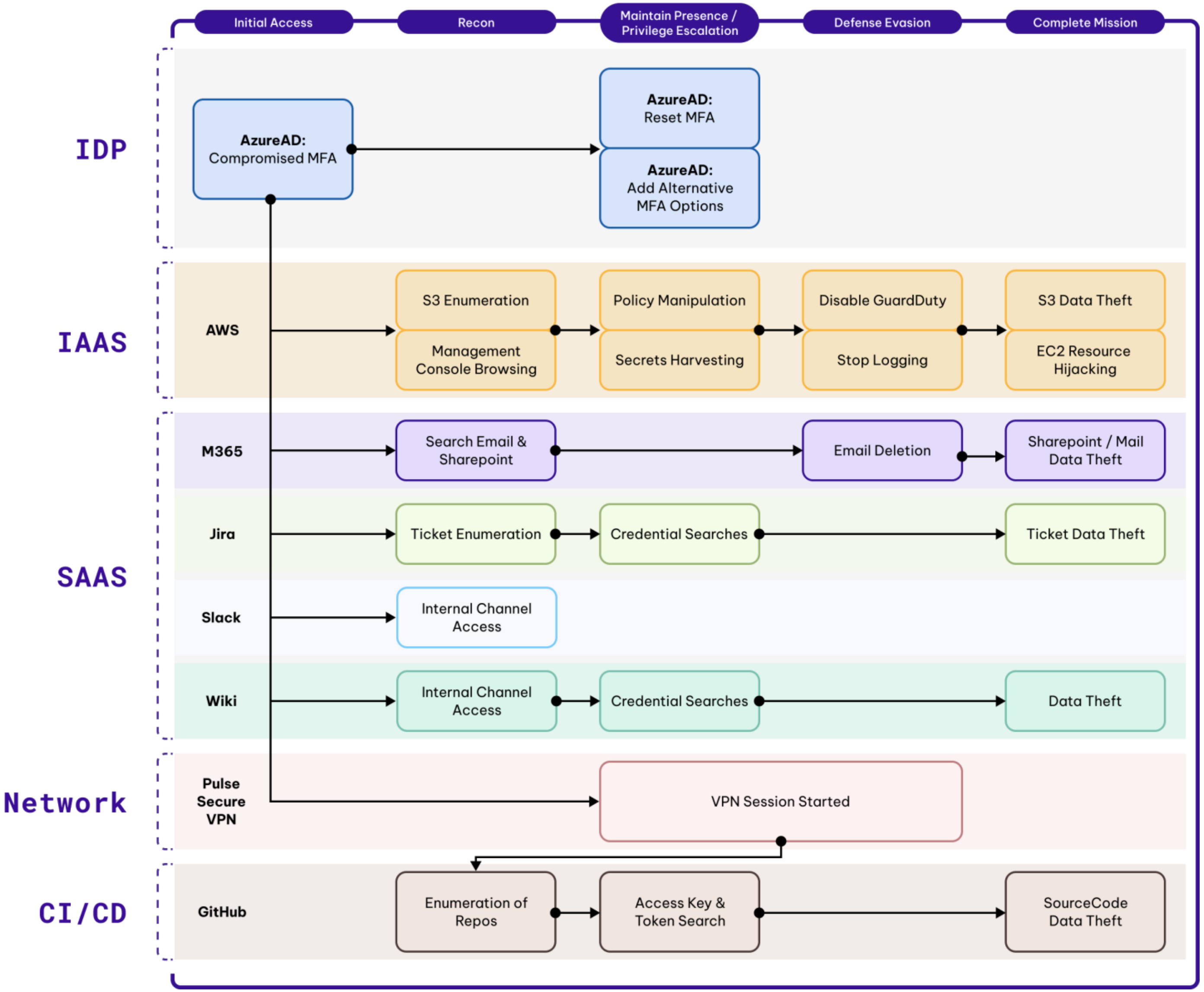
- Targeted personas
- Pick up the phone
- GUI tooling
- Very little malware used
- Opportunistic
- Watchers



High Level Overview

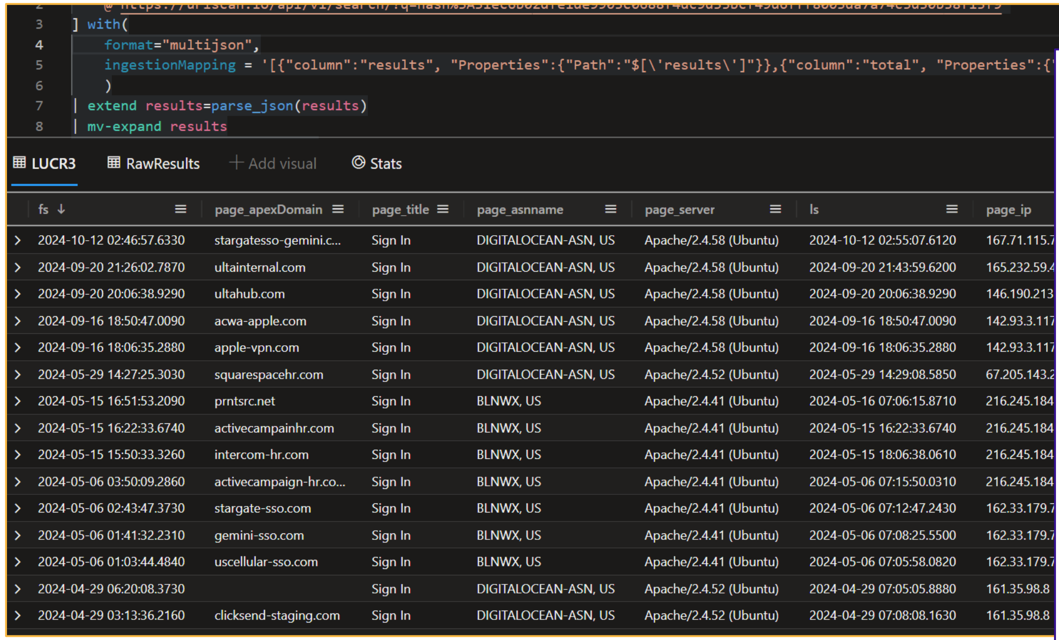
Highlights

- **Initial Access** via SIM Swapping, and push fatigue in the **IDP**
- **IAAS** for **credential harvesting** and **Data Theft**
- **SaaS** to **learn enough** about your environment to carry out their mission
- **CI/CD** to perform **Source Code Theft**, Code Signing Certs



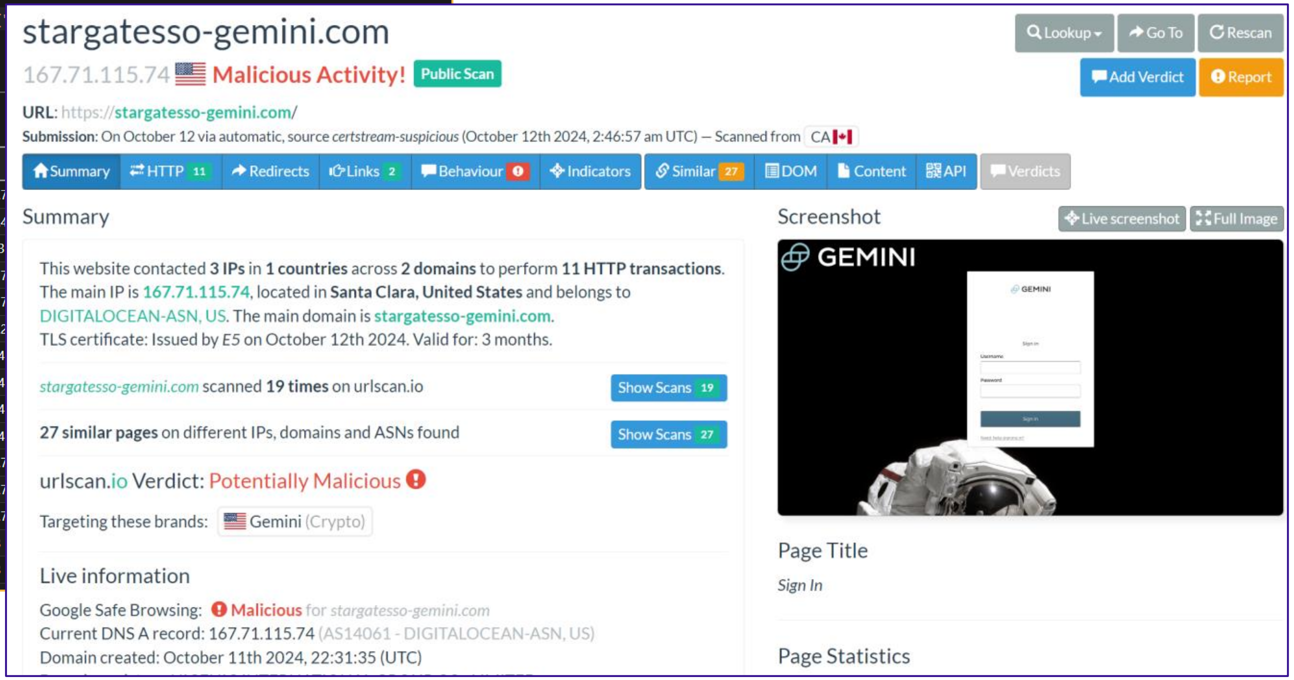
		Initial Access	Recon	Maintain Presence / Privilege Escalation	Defense Evasion	Complete Mission
IDP		**AzureAD:** Compromised MFA		**AzureAD:** Reset MFA **AzureAD:** Add Alternative MFA Options		
IAAS	AWS		S3 Enumeration Management Console Browsing	Policy Manipulation Secrets Harvesting	Disable GuardDuty Stop Logging	S3 Data Theft EC2 Resource Hijacking
SAAS	M365		Search Email & Sharepoint		Email Deletion	Sharepoint / Mail Data Theft
	Jira		Ticket Enumeration	Credential Searches		Ticket Data Theft
	Slack		Internal Channel Access			
	Wiki		Internal Channel Access	Credential Searches		Data Theft
Network	Pulse Secure VPN			VPN Session Started		
CI/CD	GitHub		Enumeration of Repos	Access Key & Token Search		SourceCode Data Theft

Phishing Infrastructure



```
] with(
    format="multijson",
    ingestionMapping = '[{"column":"results", "Properties":{"Path":"$[\'results\']"}},{"column":"total", "Properties":{'
    )
| extend results=parse_json(results)
| mv-expand results
```

fs	page_apexDomain	page_title	page_asnname	page_server	ls	page_ip
2024-10-12 02:46:57.6330	stargatesso-gemini.c...	Sign In	DIGITALOCEAN-ASN, US	Apache/2.4.58 (Ubuntu)	2024-10-12 02:55:07.6120	167.71.115.7
2024-09-20 21:26:02.7870	ultainternal.com	Sign In	DIGITALOCEAN-ASN, US	Apache/2.4.58 (Ubuntu)	2024-09-20 21:43:59.6200	165.232.59.4
2024-09-20 20:06:38.9290	ultahub.com	Sign In	DIGITALOCEAN-ASN, US	Apache/2.4.58 (Ubuntu)	2024-09-20 20:06:38.9290	146.190.213
2024-09-16 18:50:47.0090	acwa-apple.com	Sign In	DIGITALOCEAN-ASN, US	Apache/2.4.58 (Ubuntu)	2024-09-16 18:50:47.0090	142.93.3.117
2024-09-16 18:06:35.2880	apple-vpn.com	Sign In	DIGITALOCEAN-ASN, US	Apache/2.4.58 (Ubuntu)	2024-09-16 18:06:35.2880	142.93.3.117
2024-05-29 14:27:25.3030	squarespacehr.com	Sign In	DIGITALOCEAN-ASN, US	Apache/2.4.52 (Ubuntu)	2024-05-29 14:29:08.5850	67.205.143.2
2024-05-15 16:51:53.2090	prntsrc.net	Sign In	BLNWX, US	Apache/2.4.41 (Ubuntu)	2024-05-16 07:06:15.8710	216.245.184
2024-05-15 16:22:33.6740	activecampainhr.com	Sign In	BLNWX, US	Apache/2.4.41 (Ubuntu)	2024-05-15 16:22:33.6740	216.245.184
2024-05-15 15:50:33.3260	intercom-hr.com	Sign In	BLNWX, US	Apache/2.4.41 (Ubuntu)	2024-05-15 18:06:38.0610	216.245.184
2024-05-06 03:50:09.2860	activecampaign-hr.co...	Sign In	BLNWX, US	Apache/2.4.41 (Ubuntu)	2024-05-06 07:15:50.0310	216.245.184
2024-05-06 02:43:47.3730	stargate-sso.com	Sign In	BLNWX, US	Apache/2.4.41 (Ubuntu)	2024-05-06 07:12:47.2430	162.33.179.7
2024-05-06 01:41:32.2310	gemini-sso.com	Sign In	BLNWX, US	Apache/2.4.41 (Ubuntu)	2024-05-06 07:08:25.5500	162.33.179.7
2024-05-06 01:03:44.4840	uscellular-sso.com	Sign In	BLNWX, US	Apache/2.4.41 (Ubuntu)	2024-05-06 07:05:58.0820	162.33.179.7
2024-04-29 06:20:08.3730		Sign In	DIGITALOCEAN-ASN, US	Apache/2.4.52 (Ubuntu)	2024-04-29 07:05:05.8880	161.35.98.8
2024-04-29 03:13:36.2160	clicksend-staging.com	Sign In	DIGITALOCEAN-ASN, US	Apache/2.4.52 (Ubuntu)	2024-04-29 07:08:08.1630	161.35.98.8



stargatesso-gemini.com

167.71.115.74 Malicious Activity! Public Scan

URL: https://stargatesso-gemini.com/

Submission: On October 12 via automatic, source *certstream-suspicious* (October 12th 2024, 2:46:57 am UTC) — Scanned from CA

Summary

This website contacted **3 IPs** in **1 countries** across **2 domains** to perform **11 HTTP transactions**. The main IP is **167.71.115.74**, located in **Santa Clara, United States** and belongs to DIGITALOCEAN-ASN, US. The main domain is **stargatesso-gemini.com**.
TLS certificate: Issued by *E5* on October 12th 2024. Valid for: 3 months.

stargatesso-gemini.com scanned **19 times** on urlscan.io — Show Scans 19

27 similar pages on different IPs, domains and ASNs found — Show Scans 27

urlscan.io Verdict: Potentially Malicious

Targeting these brands: Gemini (Crypto)

Live information

Google Safe Browsing: Malicious for *stargatesso-gemini.com*
Current DNS A record: 167.71.115.74 (AS14061 - DIGITALOCEAN-ASN, US)
Domain created: October 11th 2024, 22:31:35 (UTC)

Screenshot

Page Title

Sign In

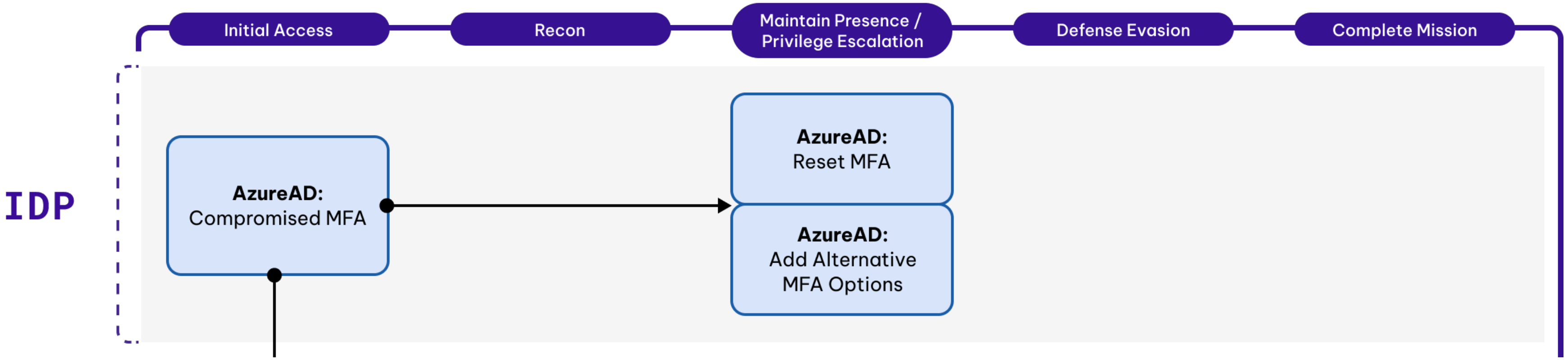
Page Statistics

Commonalities

- Cloudflare and Like services
- DigitalOcean, Choopa(Vultr), and BLNWX
- -sso, -auth, -okta,m –logon, -hr, -support

💡 Pro Tip: Defensive domain registrations will make LUCR-3 and other attackers have to work harder. We recommend defensively registering popular typo squatting versions of your domain. To demonstrate, for example.com, we would recommend registering `examplehr`, `example-hr`, `hr-example`, `hrexample`, `example-sso`, `example-logon`, `example-okta`, etc.

You down with IDP?



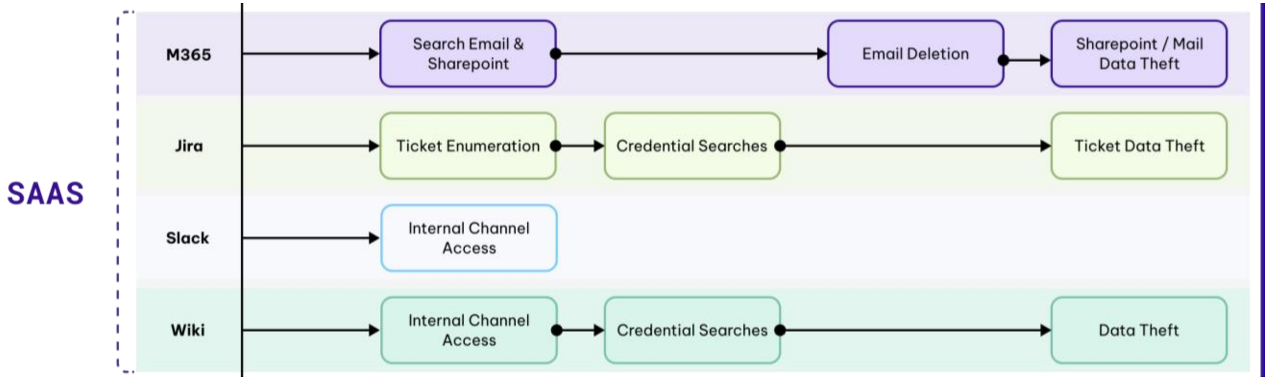
Attacker Actions

- Source from Residential Proxies
- Stolen or coerced creds
- SIM Swap and Push Fatigue
- Register their own MFA
- Downgrade to SMS
- Add new email for password rest

Hunts

- How many users have more than one phone?
- How often do people switch platforms?
- How often do people downgrade phones?
- How many people share phones?
- Downgrade factor?

Feeling SaaS-y?



SAAS

M365: Search Email & Sharepoint → Email Deletion → Sharepoint / Mail Data Theft

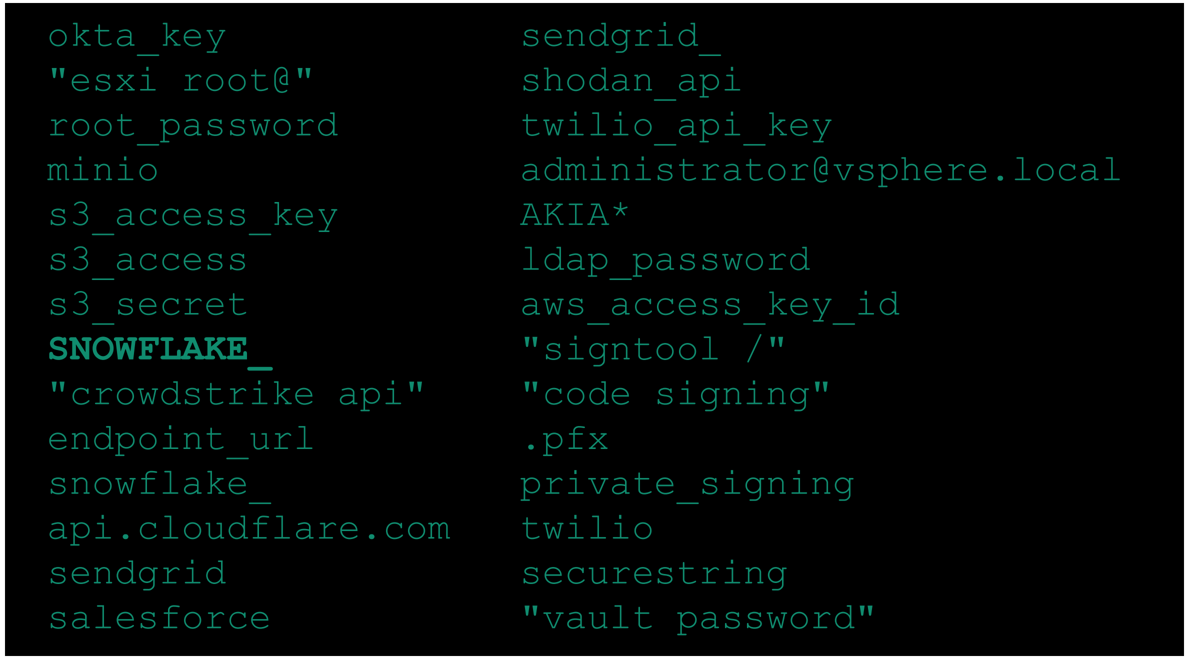
Jira: Ticket Enumeration → Credential Searches → Ticket Data Theft

Slack: Internal Channel Access

Wiki: Internal Channel Access → Credential Searches → Data Theft

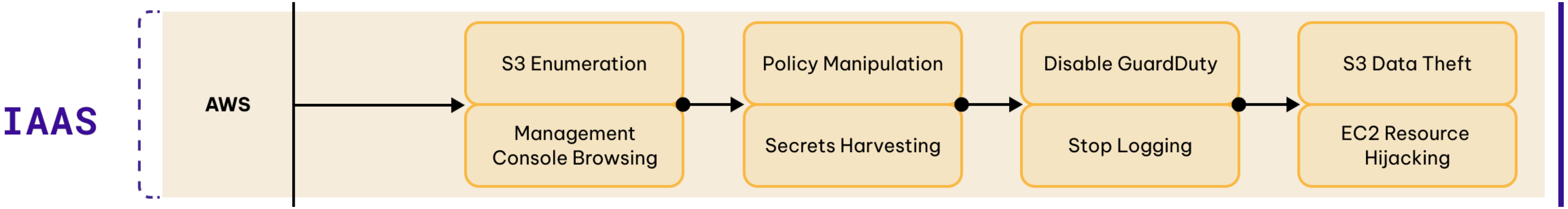
Attacker Actions

- Search knowledge apps
- Search ticket apps
- Search chats
- Search Document stores
- A little defense evasion in 365



```
okta_key                    sendgrid_
"esxi root@"                shodan_api
root_password               twilio_api_key
minio                       administrator@vsphere.local
s3_access_key               AKIA*
s3_access                   ldap_password
s3_secret                   aws_access_key_id
SNOWFLAKE_                  "signtool /"
"crowdstrike api"           "code signing"
endpoint_url                .pfx
snowflake_                  private_signing
api.cloudflare.com          twilio
sendgrid                    securestring
salesforce                  "vault password"
```

Putting the Awww, in AWS



IAAS

AWS

S3 Enumeration

Management Console Browsing

Policy Manipulation

Secrets Harvesting

Disable GuardDuty

Stop Logging

S3 Data Theft

EC2 Resource Hijacking

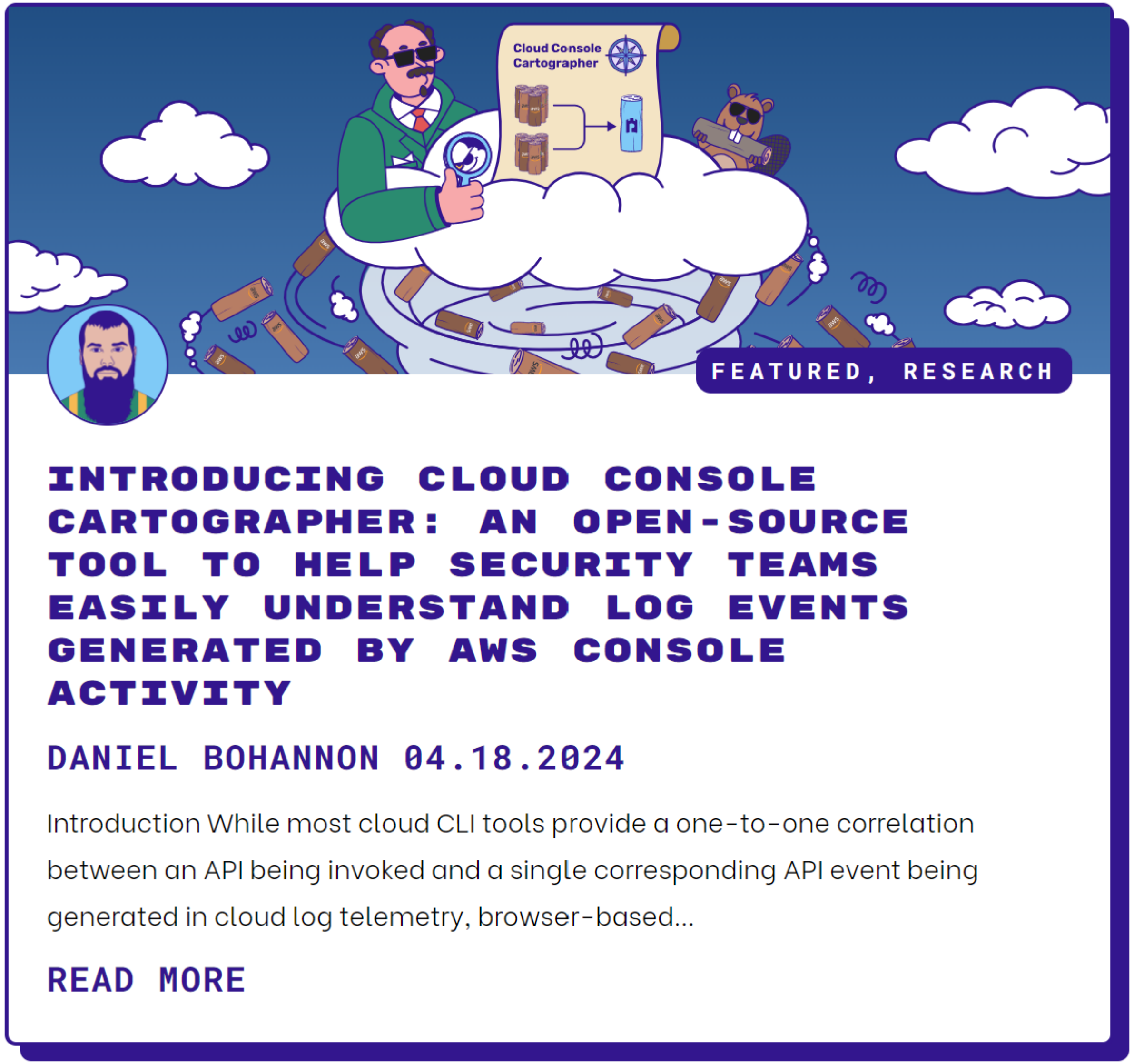
Attacker Actions

- AWS Management Console, S3 Browser, and Cloudshell
- Enumeration via billing, console, SSM
- Credential Harvesting and take over
- Instance Profile replacement
- Disable GuardDuty, StopLogging
- S3 Data Theft

Hunts

- S3 Browser Usage
- * * Policy creation/modifications
- SecretsManager via Cloudshell
- Cloudshell uploads and downloads
- DeleteInvitations
- Serial usage
- Big boxes with Windows!

Tooling to Help



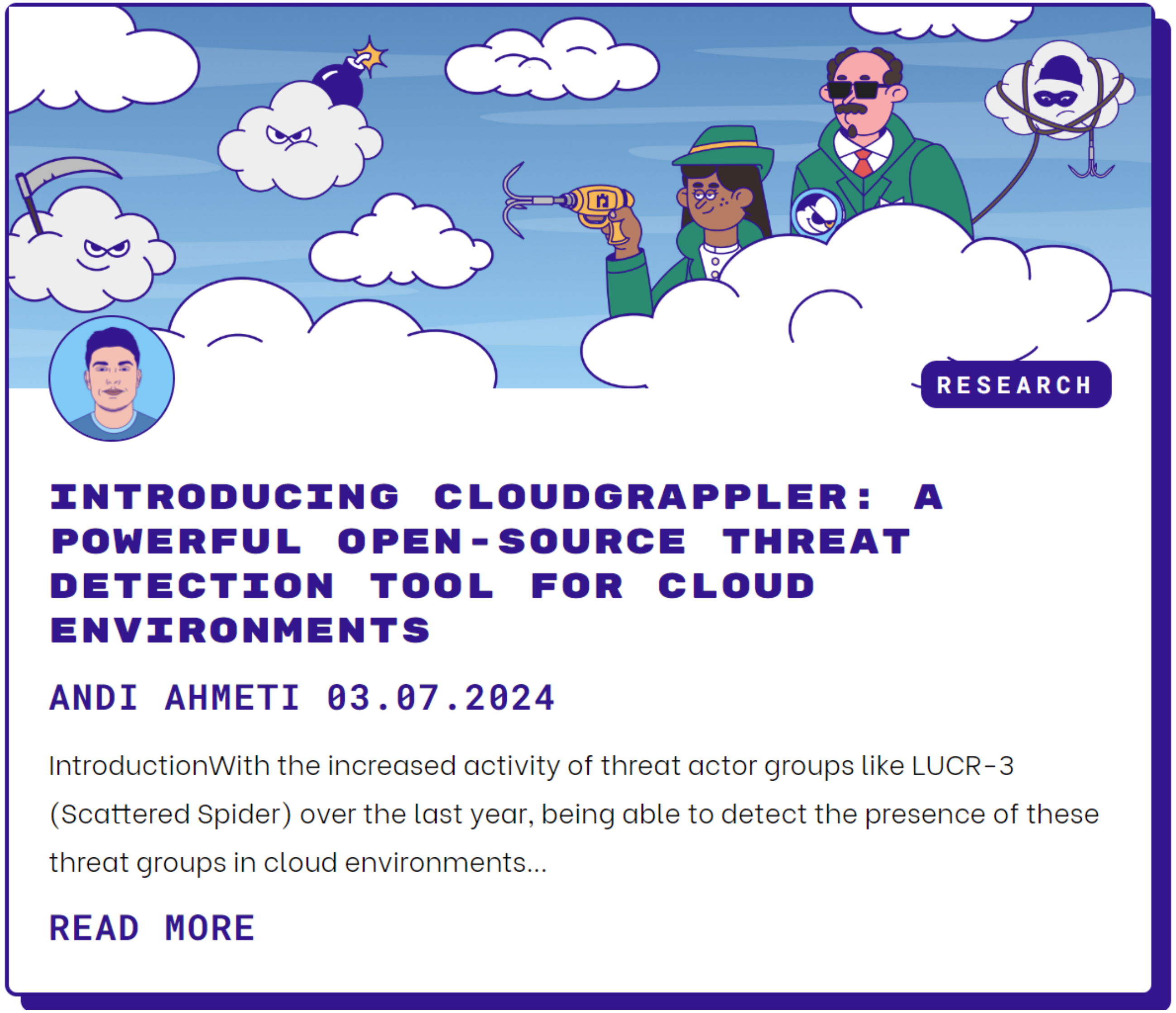
FEATURED, RESEARCH

INTRODUCING CLOUD CONSOLE CARTOGRAPHER: AN OPEN-SOURCE TOOL TO HELP SECURITY TEAMS EASILY UNDERSTAND LOG EVENTS GENERATED BY AWS CONSOLE ACTIVITY

DANIEL BOHANNON 04.18.2024

Introduction While most cloud CLI tools provide a one-to-one correlation between an API being invoked and a single corresponding API event being generated in cloud log telemetry, browser-based...

READ MORE



RESEARCH

INTRODUCING CLOUDGRAPPLER: A POWERFUL OPEN-SOURCE THREAT DETECTION TOOL FOR CLOUD ENVIRONMENTS

ANDI AHMETI 03.07.2024

IntroductionWith the increased activity of threat actor groups like LUCR-3 (Scattered Spider) over the last year, being able to detect the presence of these threat groups in cloud environments...

READ MORE