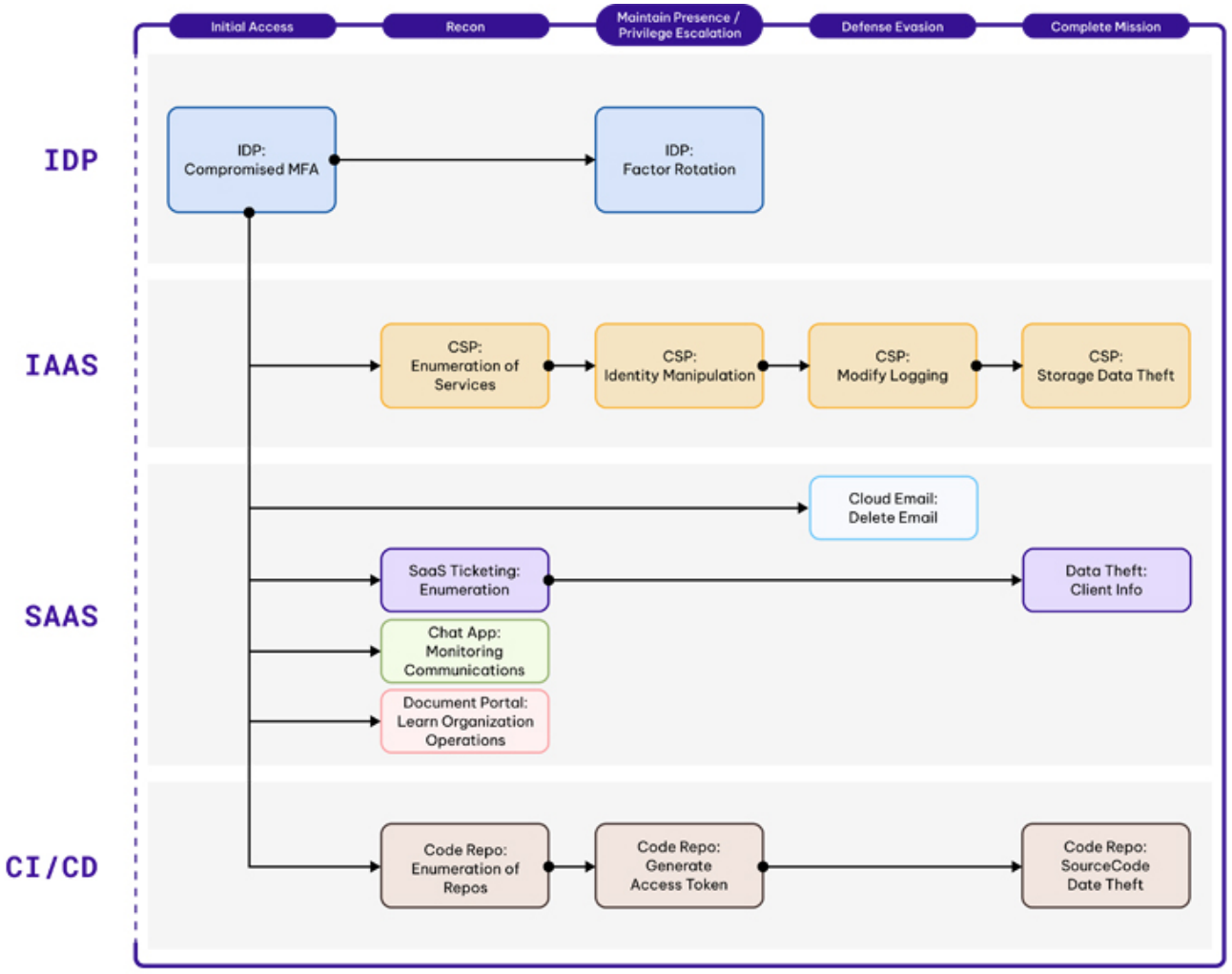
LUCR-3: Scattered Spider Getting SaaS-y in the Cloud

By The Hacker News

Published: 2023-10-02 · Archived: 2026-04-02 12:07:43 UTC

LUCR-3 overlaps with groups such as Scattered Spider, Oktapus, UNC3944, and STORM-0875 and is a financially motivated attacker that leverages the Identity Provider (IDP) as initial access into an environment with the goal of stealing Intellectual Property (IP) for extortion. LUCR-3 targets Fortune 2000 companies across various sectors, including but not limited to Software, Retail, Hospitality, Manufacturing, and Telecoms.



LUCR-3 does not rely heavily on malware or even scripts; instead, LUCR-3 expertly uses victims' own tools, applications, and resources to achieve their goals. At a high level, Initial Access is gained through compromising existing identities in the IDP (Okta: Identity Cloud, Azure AD / Entra, Ping Identity: PingOne). LUCR-3 uses SaaS applications such as document portals, ticketing systems, and chat applications to learn how the victim organization operates and how to access sensitive information. Using the data they gained from reconnaissance within the SaaS applications, they then carry out their mission of data theft. Data theft is typically focused on IP, Code Signing Certificates, and customer data.

Attacker Attributes

Highlights

- LUCR-3 attribution is difficult. Many of us in the Cyber Intelligence community have even begun to track the individual personas separately. Further confusing attribution, some LUCR-3 personas appear to be affiliates of ALPHV with access to deploy BlackCat ransomware.
- Much like LUCR-1 (GUI-Vil), LUCR-3 tooling, especially in Cloud, SaaS, and CI/CD, mostly uses web browsers and some GUI utilities such as S3 Browser. Leveraging the native features of applications, just like any employee would do, to carry out their goal.

- LUCR-3 heavily targets the IDPs for Initial Access. Buying creds from common marketplaces and bypassing MFA via SIM swapping, social engineering, and push fatigue.
- LUCR-3 does its homework on its initial access victims, choosing identities that will have elevated privileges and even ensuring they source from similar geolocation as their victim identities to avoid impossible travel (geo disparity) alerts.
- LUCR-3 will utilize the victim organizations software deployment solutions, such as SCCM, to deploy specified software to target systems.

Mission

LUCR-3 is a financially motivated threat actor that uses data theft of sensitive data (IP, Customer data, Code Signing Certificates) to attempt extortion. While extortion demands do vary, they are often in the tens of millions of dollars. Some personas within LUCR-3 will often collaborate with ALPHV to carry out the extortion phase of the attack.

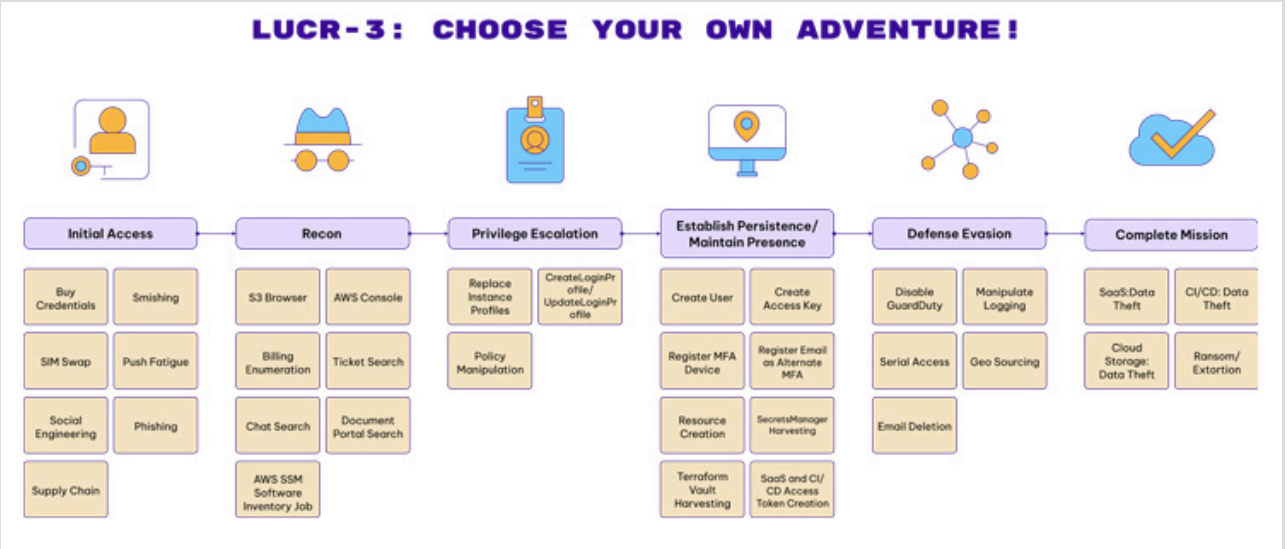
Tooling

LUCR-3 utilizes mostly Windows 10 systems running GUI utilities to carry out their mission in the cloud. Using the native features of SaaS applications such as search, LUCR-3 is able to navigate through an organization without raising any alarms. In AWS, the threat actor routinely leverages the S3 Browser (version 10.9.9) and the AWS management console (via a web browser). LUCR-3 utilizes AWS Cloudshell within the AWS management console to carry out any activity that requires direct interaction with the AWS API.

Victimology

LUCR-3 often targets large (Fortune 2000) organizations that have Intellectual Property (IP) that is valuable enough that victim organizations are likely to pay an extortion fee. Software companies are a common target as they aim to extort a fee related to the theft of source code as well as code signing certificates. LUCR-3 will often target organizations that can be leveraged in a supply chain attack against others. Identity Providers and their outsourced services companies are frequently targeted as a singular compromise of one of these entities will allow for access into multiple other organizations. In recent months, LUCR-3 has expanded its targeting into sectors they haven’t previously focused as much on, such as hospitality, gaming, and retail.

Attacker Lifecycle



AWS Attacker Lifecycle

Initial Recon

LUCR-3 does their homework when deciding on their target victim identities. They ensure they are targeting users that will have the access they need to carry out their mission. This includes but is not limited to Identity Admins, Developers, Engineers, and the Security team.

They have been known to leverage credentials that were available in common deep web marketplaces.

Initial Access (IA)

LUCR-3's initial access into an environment is gained through compromised credentials. They are not performing noisy activities like password spraying to find passwords. When they connect, they already have a legitimate password to use. The typical approach for them is:

1. Identify credentials for the intended victim identity

- Buy credentials from common deepweb marketplaces
- Smishing victims to collect their credentials
- Social engineering help desk personnel to gain access to the credentials

2. Bypass Multi-factor Authentication (MFA)

- SIM Swapping (when SMS OTP is enabled)
- Push Fatigue (when SMS OTP is not enabled)
- Phishing attacks with redirects to legitimate sites where OTP codes are captured and replayed
- Buy or social engineer access from an insider (last resort)

3. Modify MFA settings

- Register a new device
- Add alternative MFA options

When LUCR-3 modifies MFA settings, they often register their own mobile device and add secondary MFA options such as emails. Signals to watch for here are:

- When a user registers a device that is in a different ecosystem than their previous device (Android to Apple as an example)
- When a user registers a new device that is an older model than their previous device
- When a single phone (device ID) is assigned to multiple identities
- When an external email is added as a multi-factor option

Recon (R)

R-SaaS

In order to carry out their goal of data theft, ransom, and extortion, LUCR-3 must understand where the important data is and how to get to it. They perform these tasks much like any employee would. Searching through and viewing documents in various SaaS applications like SharePoint, OneDrive, knowledge applications, ticketing solutions, and chat applications allows LUCR-3 to learn about an environment using native applications without setting off alarm bells. LUCR-3 uses search terms targeted at finding credentials, learning about the software deployment environments, code signing process, and sensitive data.

R-AWS

In AWS, LUCR-3 performs recon in several ways. They will simply navigate around the AWS Management Console into services like Billing, to understand what types of services are being leveraged, and then navigate each of those services in the console. Additionally, LUCR-3 wants to know what packages are running on the compute systems (EC2 instances) in an organization. Leveraging Systems Manager (SSM), LUCR-3 will run the native AWS-GatherSoftwareInventory job against all EC2 instances, returning the software running on the EC2 instances. Lastly, LUCR-3 will leverage the GUI utility S3 Browser in combination with a long-lived access key to view available S3 buckets.

Privilege Escalation (PE)

LUCR-3 often chooses initial victims who have the type of access necessary to carry out their mission. They do not always need to utilize privilege escalation techniques, but we have observed them do so on occasion in AWS environments.

PE-AWS

LUCR-3 has utilized three (3) main techniques for privilege escalation in AWS:

1. Policy manipulation: LUCR-3 has been seen modifying the policy of existing roles assigned to EC2 instances (*ReplaceIamInstanceProfileAssociation*) as well as creating new ones with a full open policy.
2. *UpdateLoginProfile*: LUCR-3 will update the login profile and, on occasion, create one if it doesn't exist to assign a password to an identity so they can leverage it for AWS Management Console logons.

3. SecretsManager Harvesting: Many organizations store credentials in SecretsManger or Terraform Vault for programmatic access from their cloud infrastructure. LUCR-3 will leverage AWS CloudShell to scrape all credentials that are available in SecretsManager and similar solutions.

Establish Persistence/ Maintain Presence (EP)

LUCR-3, like most attackers, wants to ensure that they have multiple ways to enter an environment in the event that their initial compromised identities are discovered. In a modern cloud world, there are many ways to achieve this goal, and LUCR-3 employs a myriad to maintain its presence.

EP-AzureAD/Okta

After gaining access to an identity in the IDP (AzureAD, Okta, etc.), LUCR-3 wants to ensure they can easily continue to access the identity. In order to do so, they will often perform the following actions:

1. Reset/Register Factor: LUCR-3 will register their own device to ease their ability for continued access. As mentioned previously, watch for ecosystem switches for users as well as single devices that are registered to multiple users.
2. Alternate MFA: Many IDPs allow for alternate MFA options. LUCR-3 will take advantage of these features to register external emails as a factor. They are smart about choosing a name that aligns with the victim's identity.
3. Strong Authentication Type: In environments where the default setting is to not allow for SMS as a factor, LUCR-3 will modify this setting if they are able to. In AzureAD, you can monitor for this by looking for the StrongAuthenticationMethod changing from a 6 (PhoneAppOTP) to a 7 (OneWaySMS)

EP-AWS

To maintain persistence in AWS, LUCR-3 has been observed performing the following:

1. *CreateUser*: LUCR-3 will attempt to create IAM Users when available. They choose names that align with the victim identity they are using for initial access into the environment.
2. *CreateAccessKey*: LUCR-3 will attempt to create access keys for newly created IAM Users as well as existing IAM Users that they can then use programmatically. Like GUI-Vil (LUCR-1), the access keys that are created are often inputted into the S3 Browser to interact with S3 buckets.
3. *CreateLoginProfile* / *UpdateLoginProfile*: LUCR-3, when trying to be more stealthy or when they do not have access to create new IAM users, will attempt to create or update login profiles for existing users. Login profiles are what assign a password to an IAM User and allow for console access. This technique also lets the attacker gain the privileges of the victim's identity.
4. Credential Harvesting: As mentioned previously, LUCR-3 finds great value in harvesting credentials from credential vaults such as AWS SecretsManager and Terraform Vault. These often store credentials not just for the victim organizations but also credentials that may allow access to business partners, technology integrations, and even clients of the victim organization.
5. Resource Creation: Lastly, LUCR-3 will create or take over existing resources, such as EC2 instances that can be leveraged for access back into the environment as well as a staging area for tools and data theft as

needed.

EP-SaaS

LUCR-3 will use all the applications available to them to further their goal. In ticketing systems, chat programs, document stores, and knowledge applications, they will often perform searches looking for credentials that can be leveraged during their attack.

Additionally, many of these applications allow the creation of access tokens that can be used to interact with the SaaS applications API.

EP-CI/CD

LUCR-3 will also generate access tokens for interacting with the APIs of your code repositories, such as GitHub and GitLab.

Defense Evasion (DE)

We have observed that LUCR-3 significantly focuses on defense evasion tactics in various environments. This is clearly to avoid detection as long as possible until they are sure they have achieved their mission objectives and are ready to perform ransom and extortion activities. They accomplish this through multiple means depending on the type of environment they are in.

DE-AWS

LUCR-3 employs mostly common defense evasion techniques in AWS, with a couple of unique flares.

1. Disable GuardDuty: LUCR-3 will perform the typical deletion of GuardDuty detectors but also tries to make it harder to add back to the org level by deleting invitations. This is accomplished through the following three commands: *DisassociateFromMasterAccount*, *DeleteInvitations*, *DeleteDetector*
2. Stop Logging: LUCR-3 also attempts to evade AWS detections by performing *DeleteTrail* and *StopLogging* actions.
3. Serial Console Access: This may be giving LUCR-3 too much credit, but we have observed them EnableSerialConsoleAccess for AWS accounts they have compromised and then attempt to use EC2 Instance Connect to *SendSerialConsoleSSHPublicKey* which will attempt to establish a serial connection to a specified EC2 instance. This can be leveraged to avoid network monitoring, as serial connections are hardware-based.

DE-AzureAD/Okta

LUCR-3 clearly understands that one of the more common detections in place for IDPs is to monitor and alert on impossible travel. To avoid these impossible travel detections, LUCR-3 will ensure that they source from a similar geolocation as their victim identity. This seems to be mostly accomplished via the use of residential VPNs.

DE-M365/Google Workspace

Some of LUCR-3's actions in an environment, such as generating tokens and opening up help desk tickets, cause emails to be sent to the victims' mailboxes. LUCR-3, already sitting in those mailboxes, will delete the emails to avoid detection. While email deletion on its own is a very weak signal, looking for email deletions via the web version of Outlook with sensitive terms like OAuth, access token, and MFA might bring to light higher fidelity signals to follow.

Complete Mission (CM)

LUCR-3 has one goal: financial gain. They do this mostly through extortion of sensitive data that they have collected via the native tools of the victim organizations' SaaS and CI/CD applications. In AWS, this is accomplished by data theft in S3 and in database applications such as Dynamo and RDS.

While in the SaaS world, they complete their mission by searching and downloading documents and web pages via a traditional web browser.

On the CI/CD side, LUCR-3 will use the clone, archive, and view raw features of Github and Gitlab to view and download source data.

Indicators

Detections

Permiso clients are protected by the following detections:

Name	Type
P0_AWS_ACCESSKEY_CREATED_1	Alert
P0_AWS_CLOUDTRAIL_LOGGING_STOPPED_1	Alert
P0_AWS_CLOUDTRAIL_TRAIL_DELETED_1	Alert
P0_AWS_EC2_ROOT_USER_SSH_1	Alert
P0_AWS_EC2_SERIAL_CONSOLE_ACCESS_ENABLED_1	Alert
P0_AWS_GUARDDUTY_STATUS_CHANGED_1	Alert
P0_AWS_NEW_USER_CREATED_1	Alert
P0_AWS_S3_BROWSER_USERAGENT_1	Alert
P0_AWS_SM_GETSECRETVALUE_CLOUDSHELL_1	Alert
P0_AZUREAD_MFA_FACTOR_ROTATION_1	Alert
P0_AZUREAD_MFA_FACTOR_ROTATION_BY_ADMIN_1	Alert
P0_GIT_CLONE_ALL	Alert
P0_IDP_MFA_DEVICE_DOWNGRADE	Alert
P0_IDP_MFA_ECOSYSTEM_SWITCH	Alert
P0_IDP_MFA_EXTERNAL_EMAIL	Alert
P0_IDP_MFA_MANYUSERS_1DEVICE	Alert
P0_INTEL_LUCR3	Alert
P0_OKTA_MFA_FACTOR_ROTATION_1	Alert
P0_OKTA_MFA_FACTOR_ROTATION_BY_ADMIN_1	Alert
P0_SAAS_CREDENTIAL_SEARCH	Alert

Found this article interesting? This article is a contributed piece from one of our valued partners. Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.
