Scattered Spider Attack Analysis

reliaquest.com/blog/scattered-spider-attack-analysis-account-compromise/

November 21, 2023

Table of Contents

In early September, an automated retroactive indicator of compromise (IoC) threat hunt identified an indicator of compromise (IoC) in the environment of one of our customers. The detected IP address, 144.76.136[.]153, was previously used by the cybercrime group Scattered Spider to perform exfiltration via the domain *transfer.sh*. Following a thorough investigation using additional information provided by the customer not known to ReliaQuest at the time of the attack, we uncovered additional evidence of intrusion, involving tools previously associated with Scattered Spider, but also techniques, tactics, and procedures (TTPs) that were new to the group. Based on this evidence, our team concluded with high confidence that Scattered Spider was responsible for the attack, which spanned multiple days across cloud and on-premises environments. This blog presents our findings from the investigation.

Click here to download a copy of this report.

Key Points

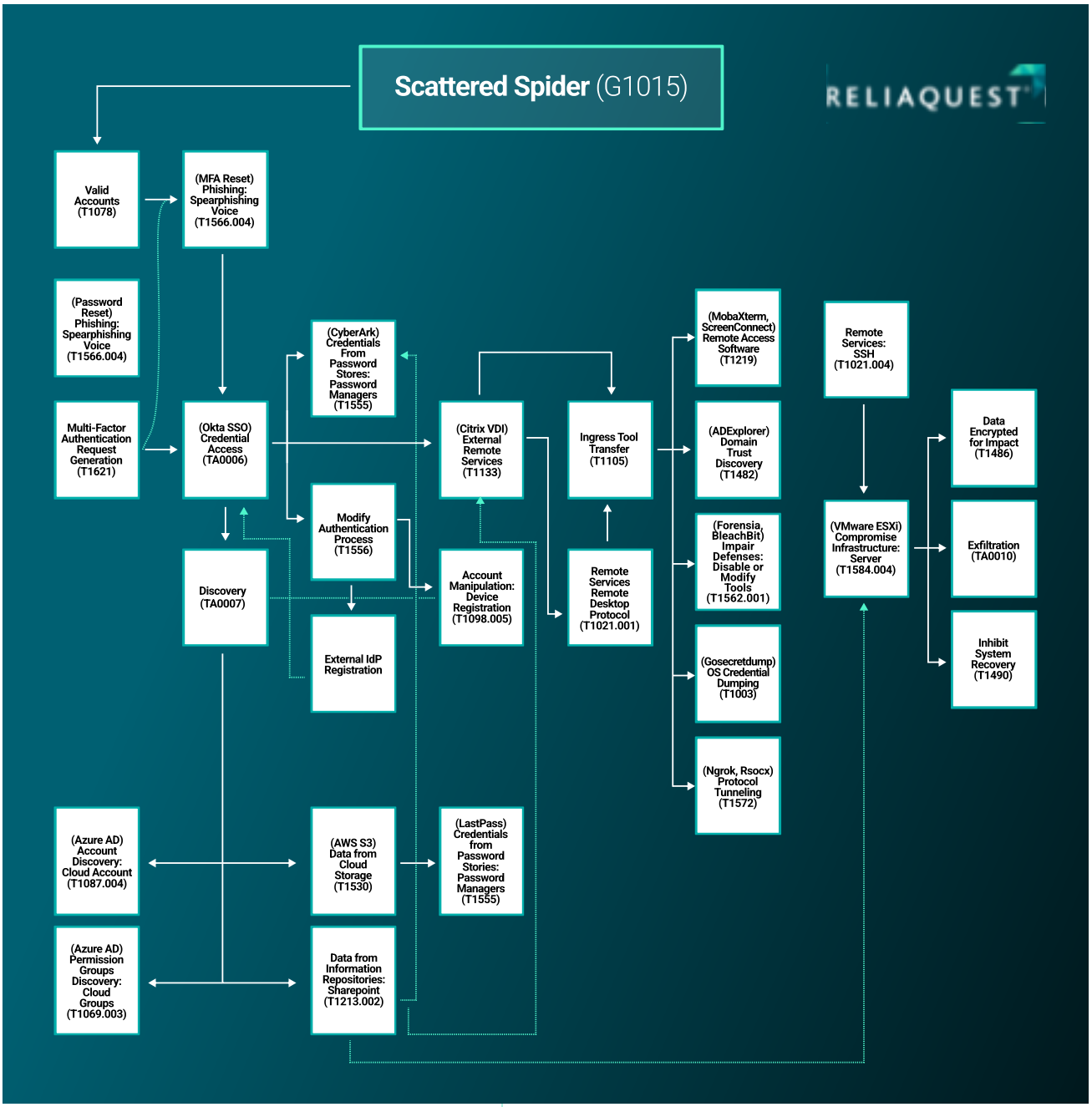
- ReliaQuest recently observed an abuse of access to a customer's internal IT documentation, and a lateral move from the customer's identity-as-a-service (IDaaS) provider to their on-premises assets in less than one hour. We determined, with high confidence, that the highly capable "Scattered Spider" cybercrime group perpetrated the attack.
- Scattered Spider, an "ALPHV"/"BlackCat" ransomware affiliate, infiltrates cloud and on-premises environments via social engineering. The recent compromise revealed remarkable sophistication when infiltrating cloud services and speed in pivoting to the on-premises environment: evidence that the group is extremely knowledgeable about how to abuse common enterprise applications.
- Scattered Spider and similar malicious actors will continue to pose a high threat to entities in various sectors and regions. Mitigation recommendations include MFA fatigue rules, help-desk challenge-response policies, and privileged identity management.

Scattered Spider Overview

Scattered Spider recently emerged as a significant cybercrime group focused on compromising large enterprises. This blog highlights the scale and operations of the group, which have spanned various sectors and regions. The group has also demonstrated the ability to abuse resources in compromised environments, discovering additional attack vectors to infiltrate deeper.

Scattered Spider's TTPs are highly significant to the wider threat landscape, as attacks are being aided by gaps in identification and insufficient help-desk user verification policies. Scattered Spider pivots and targets applications with remarkable precision, using access to internal IT documentation for extremely efficient lateral movement. As other threat actors become more sophisticated and learn from successful patterns, they will be able to exploit similar TTPs. Considering the high threat posed by Scattered Spider and similarly sophisticated/skilled groups—and the potential severe consequences—organizations should take appropriate measures to protect themselves, including those recommended later in this blog.

Attack Path


Scattered Spider (G1015)
RELIAQUEST
Valid Accounts (T1078)
(MFA Reset) Phishing: Spearphishing Voice (T1566.004)
(Password Reset) Phishing: Spearphishing Voice (T1566.004)
Multi-Factor Authentication Request Generation (T1621)
(Okta SSO) Credential Access (TA0006)
(CyberArk) Credentials From Password Stores: Password Managers (T1555)
Modify Authentication Process (T1556)
Discovery (TA0007)
External IdP Registration
(Citrix VDI) External Remote Services (T1133)
Account Manipulation: Device Registration (T1098.005)
Ingress Tool Transfer (T1105)
Remote Services Remote Desktop Protocol (T1021.001)
(MobaXterm, ScreenConnect) Remote Access Software (T1219)
(ADExplorer) Domain Trust Discovery (T1482)
(Forensia, BleachBit) Impair Defenses: Disable or Modify Tools (T1562.001)
(Gosecretdump) OS Credential Dumping (T1003)
(Ngrok, Rsocx) Protocol Tunneling (T1572)
Remote Services: SSH (T1021.004)
(VMware ESXi) Compromise Infrastructure: Server (T1584.004)
Data Encrypted for Impact (T1486)
Exfiltration (TA0010)
Inhibit System Recovery (T1490)
(Azure AD) Account Discovery: Cloud Account (T1087.004)
(Azure AD) Permission Groups Discovery: Cloud Groups (T1069.003)
(AWS S3) Data from Cloud Storage (T1530)
Data from Information Repositories: Sharepoint (T1213.002)
(LastPass) Credentials from Password Stories: Password Managers (T1555)

Following the release of additional information by the customer that was not known to ReliaQuest at the time of the attack, we were able to determine that the intrusion began in the customer's cloud environment, where the group gained access to an IT administrator's account, via Okta single sign-on (SSO). During the investigation, the initial access vector was unclear, but weeks later, the customer reported that the intrusion was attributed to a social-engineering attack, in which the user's credentials were reset by the attackers. This tactic of social engineering strongly aligns with Scattered Spider's previous TTPs, which are used to elicit valid account credentials from a target. We are highly confident that the group attained the IT administrator's credentials that way.

With valid account credentials acquired, the group conducted an MFA fatigue attack, attempting four MFA challenges within two minutes. The last challenge resulted in successful authentication, with a "new device sign-in" being observed from IP address 99.25.84[.]9 (Florida, US). This IP address was later published as an IoC in an Okta article that highlighted cross-tenant impersonation. In this case, the group used a US-based IP address not connected to VPN infrastructure. We believe the threat actor exhibited a strong sense of operational security, used to evade typical rules that raise alerts of risky sign-ons or anomalous location sign-ons. In this event, Okta did not flag the sign-on as a suspected threat, even though the Okta enriched security data would denote numerous indicators as anomalous. Once Scattered Spider gained access to the account, the group enrolled a new MFA device.

The Okta authentication log (with enriched information) details are as follows.


```
"threatSuspected":"false","url":"/idp/idx/identify?","logOnlySecurityData":"
{\"risk\":
{\"reasons\":\"AnomalousLocation,AnomalousDevice\",\"level\":\"HIGH\"},\"beha
viors\":{\"NewGeo-
Location\":\"POSITIVE\",\"NewDevice\":\"POSITIVE\",\"NewIP\":\"POSITIVE\",\"N
ewState\":\"POSITIVE\",\"NewCountry\":\"NEGATIVE\",\"Velocity\":\"POSITIVE\",
\"NewCity\":\"POSITIVE\"}}"}},"legacyEventType":null,"transaction":
{"type":"WEB","id":[Redacted]"detail":{}},"uuid":
[Redacted]"","version":"0","request":{"ipChain":
[{"ip":"99.25.84.9","geographicalContext":
{"city":"Orlando","state":"Florida","country":"UnitedStates","postalCode":"32
804","geolocation":
{"lat":28.5759,"lon":81.3957}},"version":"V4","source":null}]},"target":
[{"id":"":
[Redacted]"","type":"AppInstance","alternateId":"OktaDashboard","displayName"
:"OktaDashboard","detailEntry":
{"signOnModeType":"OPENID_CONNECT","signOnModeEvaluationResult":"AUTHENTICATE
D"}},{"id":"":
[Redacted]"","type":"Rule","alternateId":"unknown","displayName":"SignInRule"
```

,"detailEntry":null},{"id":"":
[Redacted]"","type":"Rule","alternateId":"unknown","displayName":"OktaDashboa
rdRule","detailEntry":null}]}

File Discovery and Lateral Movement

The group used the Okta SSO Dashboard to access Microsoft 365 and Microsoft Azure AD. As the IT administrator's account accessed Microsoft 365 resources, several file-access events indicated file and directory discovery in the organization's SharePoint platform. These resources gave the attackers enough information to pivot deeper into the environment, via documents on:

- Accessing VDIs
- Implementing privileged IAM
- Virtualization servers (including asset inventory spreadsheets)
- Network architecture diagrams
- Password management solutions
- Cybersecurity planning and budgeting

SharePoint file and directory discovery details are as follows:

"Operation": "FileAccessed","OrganizationId": "":[Redacted],"","RecordType":
6,"UserKey": "i:0h.f|membership|":"[Redacted]","","UserType": 0, "Version":
1, "Workload": "SharePoint","ClientIP": "99.25.84.9","ObjectId":
"https://CUSTOMER.sharepoint.com/sites/GenericITDocuments/Shared
Documents/Documents/Documents on accessing VDIs.docx","UserId": "
[Redacted]","AuthenticationType": "FormsCookieAuth",

Citrix VDI Abuse

From here, Scattered Spider authenticated to Citrix Workspace via the IT administrator's Okta SSO credentials. They were prompted to complete MFA, but the prompt was sent to the newly registered device under the group's control. After accessing Citrix Workspace, there is evidence that the group conducted additional actions on objective in the on-premises environment.

The Citrix session disconnect event details are as follows.

<13>Jan 1 00:00:00 GenericCitrixAPPServer.customer.com AgentDevice=WindowsLog
AgentLogFile=Security PluginVersion=[Redacted] Source=Microsoft-Windows-
Security-Auditing Computer= GenericCitrixAPPServer.customer.com
OriginatingComputer=[Redacted] User= Domain= EventID=4779 EventIDCode=4779
EventType=8 EventCategory=12551 RecordNumber= [Redacted] TimeGenerated=
[Redacted] TimeWritten= [Redacted] Level=Log Always Keywords=Audit Success
Task=SE_ADT_LOGON_OTHERS Opcode=Info Message=A session was disconnected from
a Window Station. Subject: Account Name: [Redacted] Account Domain: customer

```
Logon ID: [Redacted] Session: Session Name: ICA-CGP#100 Additional
Information: Client Name: HTML-1234-56789 Client Address: 0.0.0.0 This event
is generated when a user disconnects from an existing Terminal Services
session, or when a user switches away from an existing desktop using Fast
User Switching.
```

Time to Lateral Movement

The surprisingly swift transition from the cloud environment to the on-premises environment is a unique attack path, indicating the group members' advanced knowledge of both environments. As threat intelligence on Scattered Spider shows, this in-depth understanding stems from a combination of pre-existing knowledge and additional information gleaned from files and documents during the intrusion. The time it took the group to pivot from the customer's cloud environment to their on-premises environment was less than one hour.

Scattered Spider hijacked active Citrix VDI sessions on the host *GenericCitrixAPPServer.CUSTOMER.com* to perform Active Directory (AD) discovery. In these sessions, the group downloaded AD Explorer from the Sysinternals website and executed it. Despite our lack of visibility into these VDI hosts, we correlated the download and execution of AD Explorer to session disconnect events on the host *GenericCitrixAPPServer.CUSTOMER.com*: These events cited ICA-CGP#XXX as the session, which is the protocol used by Citrix desktop and application sessions. Furthermore, it cited the client name HTML-1234-56789, which corresponds to the attackers accessing Citrix Workspace via a browser. This also means active Citrix VDI sessions were hijacked.

Palo Alto log download event details for ADExplorer.exe are as follows:

```
<13>Jan 1 00:00: GenerticPAFirewall.customer.com LEEF:1.0|Palo Alto
Networks|PAN-OS Syslog Integration| [Redacted] |Windows Executable (EXE)
(52020)|ReceiveTime= [Redacted] |SerialNumber= [Redacted]
|cat=THREAT|Subtype=file|devTime= [Redacted] T|src=[Redacted]|dst= [Redacted]
|srcPostNAT=0.0.0.0|dstPostNAT=0.0.0.0|RuleName=General
WebAccess|usrName=customer\user|SourceUser=
customer\user|DestinationUser=|Application=web-browsing|VirtualSystem=
[Redacted] |SourceZone= [Redacted] |DestinationZone= [Redacted]
|IngressInterface=ethernet1/24|EgressInterface=ethernet1/23|LogForwardingProf
ile= [Redacted] G|SessionID=
[Redacted]|RepeatCount=1|srcPort=64875|dstPort=443|srcPostNATPort=0|dstPostNA
TPort=0|Flags=0x1002000|proto=tcp|action=alert|Miscellaneous="ADExplorer.exe"
|ThreatID=Windows Executable (EXE)(52020)|URLCategory=low-
risk|sev=2|Severity=low|Direction=server-to-client|sequence= [Redacted]
|ActionFlags= [Redacted] |SourceLocation=
[Redacted]|DestinationLocation=United
States|ContentType=|PCAP_ID=0|FileDigest=|Cloud=|URLIndex=1|RequestMethod=|Su
bject=|DeviceGroupHierarchyL1= [Redacted]|DeviceGroupHierarchyL2= [Redacted]
```

```
|DeviceGroupHierarchyL3= [Redacted]|DeviceGroupHierarchyL4=
[Redacted]|vSrcName=|DeviceName= [Redacted] |SrcUUID=|DstUUID=|TunnelID=
[Redacted]|MonitorTag=|ParentSessionID=0|ParentStartTime= [Redacted]
|TunnelType=N/A|ThreatCategory=unknown|ContentVer=AppThreat-8745-8229
```

We identified a concerning series of events originating from the Citrix VDI. The compromised user within the VDI accessed a file located in the organization's AWS S3 bucket, specifically at: *customer.s3.us-east-1.amazonaws.com/lastpass_export%20cleaned.xlsx?X-Amz-Security-Token=[REDACTED]*. The file, lastpass_export cleaned.xlsx, was then downloaded onto the VDI host. Soon after, we noticed web traffic directed toward *lastpass.com*. Upon sandboxing the URLs accessed during this time, we discovered that the threat actor had attempted to access the company's LastPass page. Multiple redirects to the same LastPass login page suggested unsuccessful authentication attempts.

We also observed traffic directed to *lastpass.com/protected.php*, a page that denies login and locks the account after it detects compromised credentials. That page allows a user to reset their master password using their associated email address, and we witnessed an eventual successful web request to the page *lastpass.com/company/*. We are moderately confident that Scattered Spider managed to gain access to the customer's LastPass Vault.

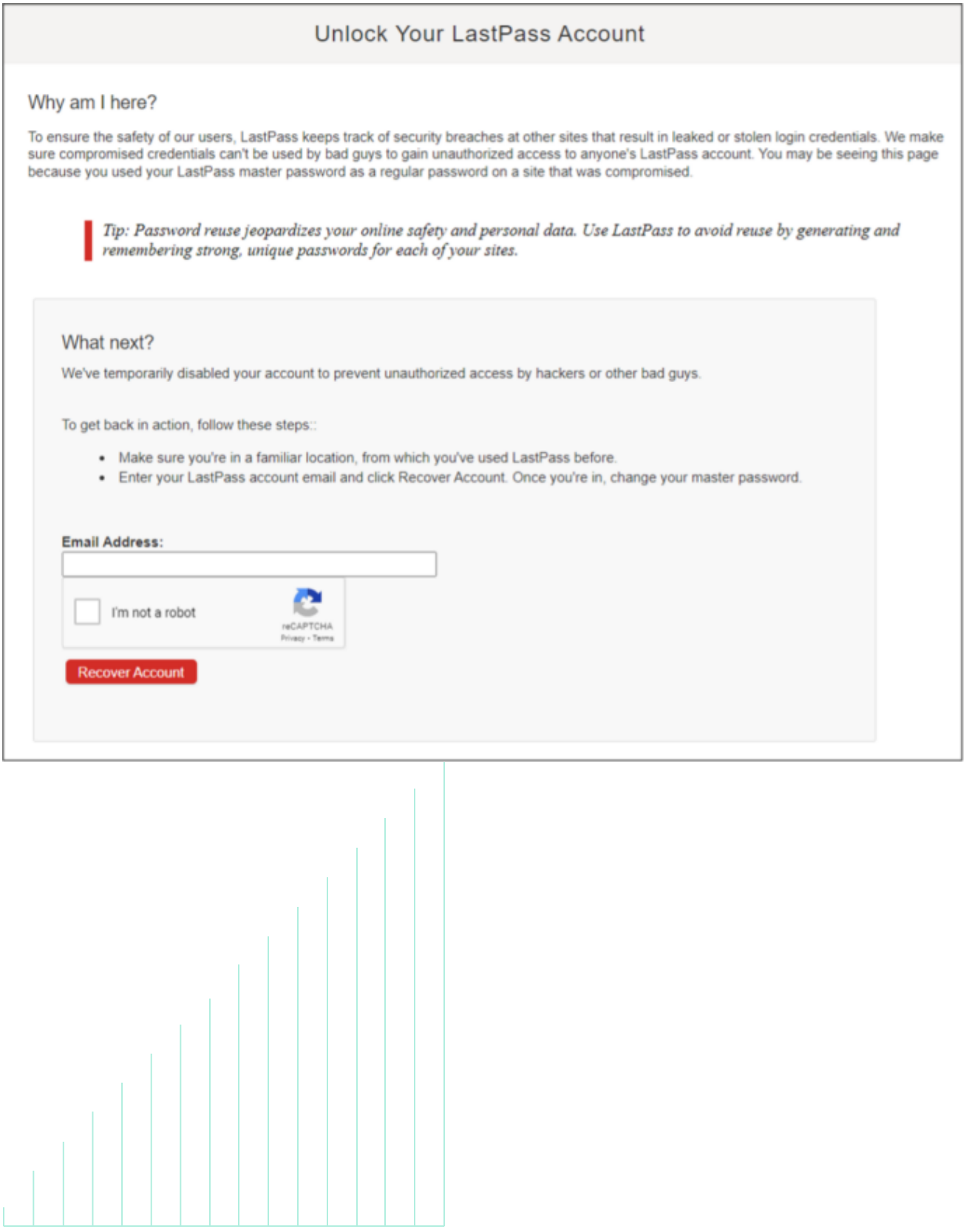


Figure 1: LastPass failed-login page that enables a master password reset

Additionally, we observed a range of malicious process execution events on the Citrix VDI, albeit without complete visibility. The following are relevant critical indicators:

- We observed numerous application crashes during the adversary's presence on the host (C:\PROGRA~1\dynatrace\oneagent\agent\lib64\oneagentdumpproc.exe -> Werfault.exe). This event likely reflect attempts to deploy a beacon on the host.
- Later we found highly suspicious process execution events, such as notepad.exe spawning control.exe, and then notepad spawning mstsc.exe. This potentially indicates process injection into notepad.exe.
- Between these events, we observed the use of RDP for lateral movement to additional hosts. We saw explicit logins using the credentials of two compromised service accounts belonging to Microsoft SQL Data Warehouse (MSSSQLDW-Analysis and MSSSQLDW-Reporting). These accounts were revealed as compromised by events later in the intrusion; they were almost certainly the primary accounts that Scattered Spider used to download malicious tools.

Okta and Azure AD Abuse

Shortly thereafter, Scattered Spider shifted focus back to Okta and Azure AD. In Okta, we saw an IT infrastructure architect authenticating and passing MFA from the same malicious IP address (99.25.84[.]9). The IT infrastructure architect also served as the organization's virtualization engineer and had a highly privileged account. After the authentication, we observed this user checking out CyberArk credentials for the VMWareVCenterSharedCreds folder. This event proved more notable later in the intrusion.

At the same time, we saw a second IT Administrator ("IT administrator 2") authenticating in Okta from the same malicious IP address and targeting the customer's Okta and Azure AD administrator settings. It remains unclear how the group had valid credentials to this account, but we again observed MFA fatigue attacks, with at least eight MFA attempts sent in bulk. With regard to IT administrator 2, we saw the Okta event system.org.rate_limit.violation for too many challenges in a short timeframe. URL filtering events show evidence of attempts to abuse Okta's delegated authentication with traffic observed to *customer.kerberos.okta.com*. Using IT administrator 2's account, we saw further evidence of access to Okta's system administration pages: *customer-admin.okta.com* and *oinmanager.okta.com*.

IT administrator 2 was also seen performing the following suspicious discovery events in Azure AD.

- Configuring Azure API access
- Making Azure billing changes
- Updating Azure Portal settings
- Enumerating Azure AD Permission
- Performing Azure AD user, group, onPremSync, PIM role, enumeration queries

The following day, the IT infrastructure architect was observed configuring Okta with a secondary identity provider (IdP). As a result of the configuration change, we saw the Okta events system.idp.lifecycle.activate and system.idp.lifecycle.update: the exact event that allows cross-tenant Okta impersonation of a privileged user. In effect, this would allow the attacker to authenticate via their external IdP to access the customer's Okta environment. Such a change would give the attacker the ability to impersonate and use any Okta account through the secondary IdP. The change would also strengthen the group's persistence in the environment.

Activation of external IdP details are as follows.


```
"displayMessage": "Activate an Identity Provider", "eventType":
"system.idp.lifecycle.activate", "outcome": { "result": "SUCCESS", "reason":
null }, "published": "2023-08-19T09:48:43.618Z", "securityContext": {
"asNumber": [Redacted], "asOrg": "customer company inc.", "isp": "customer",
"domain": ".", "isProxy": false }, "severity": "INFO", "debugContext": {
"debugData": { "protocol": "SAML 2.0", "requestId": "[Redacted]","dtHash":"
[Redacted]","requestUri":"/api/v1/idps/0oaaaa12b3cDDD4eF5g6/lifecycle/activat
e","url":"/api/v1/idps/0oaaaa12b3cDDD4eF5g6/lifecycle/activate?" }
```


Later that day, Scattered Spider used the newly created IdP to authenticate as another highly privileged user: a security architect. We correlated authentication user.authentication.auth_via_IDP using the malicious IdP, by tracing back the external IdP ID. In creating that external IdP, the threat group misconfigured how user attributes in the external IdP are matched to the customer's Okta tenant, which would later cause authentication errors when linking corresponding users during authentication.

Authentication errors due to mismatching IdP attributes are detailed as follows.


```
"displayMessage": "Authenticate user via IDP", "eventType":
"user.authentication.auth_via_IDP", "outcome": {"result": "FAILURE","reason":
"Unable to match transformed username"},"published":"
[Redacted]","securityContext": {"asNumber": [Redacted],"asOrg": CUSTOMER
company inc.","isp": "CUSTOMER", "domain": ".","isProxy": false},"severity":
"WARN","debugContext": {"debugData": {"authnRequestId": "
[Redacted]","requestId": " <Redacted","dtHash": " [Redacted]","requestUri":
"/idp/idx/introspect","threatSuspected": "false","transformedUserName":
"generic-admin ","url": "/idp/idx/introspect?"}},"legacyEventType":
"core.user_auth.idp.no_matching_users","transaction": {"type": "WEB","id": "
[Redacted]","detail": {}},"uuid": " [Redacted]","version": "0","request":
{"ipChain": [{"ip": " [Redacted]","geographicalContext": {"city": "
[Redacted]","state": " [Redacted]a","country": "United States","postalCode":
" [Redacted]","geolocation [Redacted] version": "V4","source":
null}]},"target": [{"id":0oaaaa12b3cDDD4eF5g6","type":
"AppInstance","alternateId": " Generic SSO for Desktop","displayName": "SAML
2.0 IdP","detailEntry": null}]}
```

On-Premises Compromise

The attackers pivoted back to the on-premises environment with the previously compromised service accounts for Azure SQL Data Warehouse (MSSSQLDW-Analysis and MSSSQLDW-Reporting). Multiple tools were seen ingressed on different hosts within the environment, including:

- MobaXterm_Portable_v23.2.zip (lateral movement)
- WindowsDefenderATPOffboardingPackage_valid_until_2023-XX-XX.zip (defense evasion)
- sysadminanywhere.exe (privilege escalation)
- gosecretsdump_win_v0.3.1.exe (credential access)
- Forensia.exe (defense evasion)
- BleachBit.exe (defense evasion)

Scattered Spider was also observed ingressing the same tool on more than one occasion on different hosts. In each instance, the adversary chose to re-download the tools from legitimate websites and default GitHub repositories, where they are normally hosted.

To maintain persistence, the group used RMM and reverse proxy solutions; use of Ngrok was shortly followed by a URL request to retrieve Ngrok keys from *paste.ee*. Sandboxing the webpage, while it was still up, showed Ngrok authentication tokens being hosted.

Ngrok authentication tokens from *paste.ee/abcd1234/* were:

```
ngrok config add-authtoken 12345678910qwerty
```

Exfiltration was observed via the IP address 144.76.136[.]153, which was the original IoC picked up by the automated retroactive threat hunt. The exfiltration domain *transfer.sh* is associated with this IP address. The following are persistence tools that Scattered Spider deployed on various hosts in the customer's environment:

- PDQConnectAgent
- ScreenConnect
- fleet.io
- rsocx

CyberArk and vCenter Activity

We also observed Scattered Spider performing discovery of vCenter-based documentation within the customer's SharePoint. This was paired with discovery of CyberArk-based documentation, such as CyberArk_Architecture_Diagrams_v2_0.pdf; the attackers were later seen exploiting CyberArk to check out vCenter-related credentials.

The group used CyberArk access for lateral movement, which included SSH access to vCenter hosts, such as CUSTOMERvCenter100. Even with limited visibility, we saw suspicious commands being pushed to vCenter servers that included reverting hosts to their latest snapshot and deleting all snapshots. Shortly thereafter, the adversary deleted some CyberArk files for vCenter-related credentials, seemingly in an attempt to disrupt access to the hosts after earlier actions.

```
<134> [Redacted] customervCenter100 envoy-access - - - [Redacted] info
envoy[[Redacted]] [Originator@1234 sub=Default [Redacted]POST
/ui/actionsService/actions/evaluations?
actionUids=vsphere.core.vm.takeSnapshotAction&actionUids=vsphere.core.vm.mana
geSnapshotsAction&actionUids=vsphere.core.vm.revertToLatestSnapshotAction&act
ionUids=vsphere.core.vm.consolidateSnapshots&actionUids=vsphere.core.vm.delet
eAllSnapshots&actionUids=vsphere.core.vm.actions.snapshots&actionUids=vsphere
.core.vm.suspendAction&skipActionFilteringStage=true HTTP/2 200 via_upstream
- [Redacted]
```

Outcome

Although our analysis reached its conclusion at this point, further reporting by the customer indicates that the attackers successfully accomplished their objectives of data exfiltration and widespread encryption.

In summary, we observed the following TTPs in connection with Scattered Spider: social engineering of help-desk employees, IDaaS cross-tenant impersonation, file enumeration and discovery, abuse of specific enterprise applications, and use of persistence tools. As we concluded our investigation, we determined that several of the TTPs observed had a historical connection to Scattered Spider, leading us to attribute the attack to that group with high confidence.

Forecast

We predict, with high confidence, that attacks from Scattered Spider will persist into the long term (beyond one year). The group's ongoing activity is a testament to the capabilities of a highly skilled threat actor or group having an intricate understanding of cloud and on-premises environments, enabling them to navigate with sophistication.

We recently observed another intrusion that seems to be associated with Scattered Spider. The attacker employed the same social-engineering and file-discovery actions as seen in previous Scattered Spider attacks. Although they were unable to access critical resources, it is evident that as long as Scattered Spider's preferred initial access vectors remain unmitigated, attacks will continue.

Given the consistent threat posed by Scattered Spider and similar malicious actors, organizations should prioritize constant vigilance. By strengthening security protocols, conducting regular assessments, and staying informed about emerging threats, organizations can effectively combat the risk posed by Scattered Spider (more details below), mitigating the impact of any attacks and protecting their invaluable assets.

Recommendations and Best Practices

Logging and Visibility

Considering the potential for compromises to move laterally from the cloud and affect on-premises environments, security teams should centralize logs in a unified location. This enables the deployment of correlation-based detections and facilitates thorough investigations of relevant events. In these complex intrusions, establishing a comprehensive timeline of events is of utmost importance, to accurately assess and address security incidents.

Principle of Least Privilege

The customer intrusion underscored the importance of adhering to the principle of least privilege, particularly given the misuse of Okta super administrator credentials. The super administrator role should be restricted as it grants the potential to alter various settings, such as to register an external IdP or deactivate strong authentication requirements. Users assigned to this role should use a form of MFA that demonstrates substantial resistance to MFA bypass attacks. ReliaQuest recommends that new sign-ons, or the enrollment of an MFA factor for super administrator accounts, be accompanied by a notification.

This recommendation also applies to internal IT documentation. Many organizations do not adequately limit access to internal IT documents or knowledge-base articles, enabling staff to access information related to specific IT processes or sensitive information on network architecture. Such accessibility could inadvertently provide a threat actor with valuable documents, and potentially enable an attacker to glean more information about the environment.

Help-Desk Policies

Help-desk users should adhere to rigorous policies concerning the verification of end users' identities, particularly for procedures involving the reset of credentials or MFA factors. With the growing prevalence of social-engineering tactics, we highly recommend implementing a challenge-response process or mandating user identity confirmation prior to any help-desk action. Additionally, consider using out-of-band communication methods to facilitate these changes (e.g., avoiding password reset requests via email if the user is potentially compromised).

We also recommend a stringent escalation process for resetting credentials belonging to administrators, considering the elevated privileges associated with these accounts. Implement a comprehensive procedure before any such credential resets are permitted. At a minimum, the security team should be alerted to investigate when changes to an administrator account occur.