Tracking the Expansion of ShinyHunters-Branded SaaS Data Theft

By Mandiant

Published: 2026-01-30 · Archived: 2026-04-05 13:19:20 UTC

Introduction

Mandiant has identified an expansion in threat activity that uses tactics, techniques, and procedures (TTPs) consistent with prior ShinyHunters-branded extortion operations. These operations primarily leverage sophisticated voice phishing (vishing) and victim-branded credential harvesting sites to gain initial access to corporate environments by obtaining single sign-on (SSO) credentials and multi-factor authentication (MFA) codes. Once inside, the threat actors target cloud-based software-as-a-service (SaaS) applications to exfiltrate sensitive data and internal communications for use in subsequent extortion demands.

Google Threat Intelligence Group (GTIG) is currently tracking this activity under multiple threat clusters (UNC6661, UNC6671, and UNC6240) to enable a more granular understanding of evolving partnerships and account for potential impersonation activity. While this methodology of targeting identity providers and SaaS platforms is consistent with our prior observations of threat activity preceding ShinyHunters-branded extortion, the breadth of targeted cloud platforms continues to expand as these threat actors seek more sensitive data for extortion. Further, they appear to be escalating their extortion tactics with recent incidents including harassment of victim personnel, among other tactics.

This activity is not the result of a security vulnerability in vendors' products or infrastructure. Instead, it continues to highlight the effectiveness of social engineering and underscores the importance of organizations moving towards phishing-resistant MFA where possible. Methods such as FIDO2 security keys or passkeys are resistant to social engineering in ways that push-based or SMS authentication are not.

Mandiant has also published a comprehensive guide with proactive hardening and detection recommendations, and Google published a detailed walkthrough for operationalizing these findings within Google Security Operations.

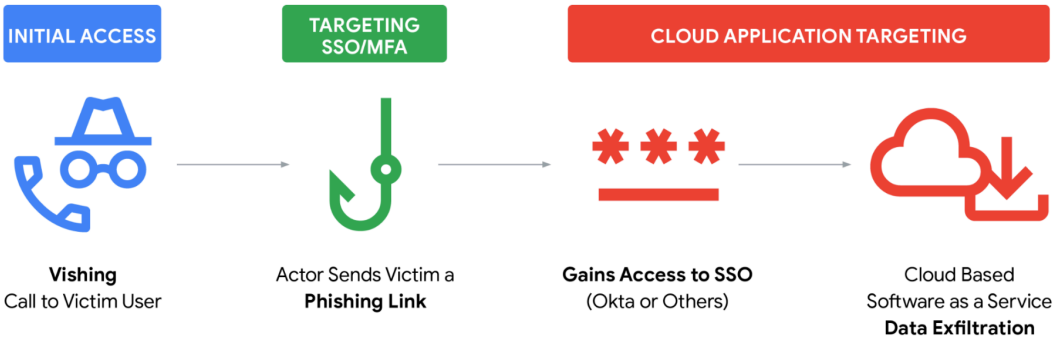

Figure 1: Attack path diagram

UNC6661 Vishing and Credential Theft Activity

In incidents spanning early to mid-January 2026, UNC6661 pretended to be IT staff and called employees at targeted victim organizations claiming that the company was updating MFA settings. The threat actor directed the employees to victim-branded credential harvesting sites to capture their SSO credentials and MFA codes, and then registered their own device for MFA. The credential harvesting domains attributed to UNC6661 commonly, but not exclusively, use the format <companyname>sso.com or <companyname>internal.com and have often been registered with NICENIC.

In at least some cases, the threat actor gained access to accounts belonging to Okta customers. Okta published a report about phishing kits targeting identity providers and cryptocurrency platforms, as well as follow-on vishing attacks. While they associate this activity with multiple threat clusters, at least some of the activity appears to overlap with the ShinyHunters-branded operations tracked by GTIG.

After gaining initial access, UNC6661 moved laterally through victim customer environments to exfiltrate data from various SaaS platforms (log examples in Figures 2 through 5). While the targeting of specific organizations and user identities is deliberate, analysis suggests that the subsequent access to these platforms is likely opportunistic, determined by the specific permissions and applications accessible via the individual compromised SSO session. These compromises did not result from security vulnerabilities in the vendors' products or infrastructure.

In some cases, they have appeared to target specific types of information. For example, the threat actors have conducted searches in cloud applications for documents containing specific text including "poc," "confidential," "internal," "proposal," "salesforce," and "vpn" or targeted personally identifiable information (PII) stored in Salesforce. Additionally, UNC6661 may have targeted Slack data at some victims' environments, based on a claim made in a ShinyHunters-branded data leak site (DLS) entry.

```
{
 "AppAccessContext": {
   "AADSessionId": "[REDACTED_GUID]",
   "AuthTime": "1601-01-01T00:00:00",
   "ClientAppId": "[REDACTED_APP_ID]",
   "ClientAppName": "Microsoft Office",
   "CorrelationId": "[REDACTED_GUID]",
   "TokenIssuedAtTime": "1601-01-01T00:02:56",
   "UniqueTokenId": "[REDACTED_ID]"
 },
 "CreationTime": "2026-01-10T13:17:11",
 "Id": "[REDACTED_GUID]",
 "Operation": "FileDownloaded",
 "OrganizationId": "[REDACTED_GUID]",
 "RecordType": 6,
 "UserKey": "[REDACTED_USER_KEY]",
 "UserType": 0,
 "Version": 1,
 "Workload": "SharePoint",
 "ClientIP": "[REDACTED_IP]",
 "UserId": "[REDACTED_EMAIL]",
 "ApplicationId": "[REDACTED_APP_ID]",
 "AuthenticationType": "OAuth",
 "BrowserName": "Mozilla",
 "BrowserVersion": "5.0",
 "CorrelationId": "[REDACTED_GUID]",
 "EventSource": "SharePoint",
 "GeoLocation": "NAM",
 "IsManagedDevice": false,
 "ItemType": "File",
 "ListId": "[REDACTED_GUID]",
 "ListItemUniqueId": "[REDACTED_GUID]",
 "Platform": "WinDesktop",
 "Site": "[REDACTED_GUID]",
 "UserAgent": "Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.20348.4294",
 "WebId": "[REDACTED_GUID]",
 "DeviceDisplayName": "[REDACTED_IPV6]",
 "EventSignature": "[REDACTED_SIGNATURE]",
 "FileSizeBytes": 31912,
 "HighPriorityMediaProcessing": false,
 "ListBaseType": 1,
 "ListServerTemplate": 101,
 "SensitivityLabelId": "[REDACTED_GUID]",
 "SiteSensitivityLabelId": "",
 "SensitivityLabelOwnerEmail": "[REDACTED_EMAIL]",
 "SourceRelativeUrl": "[REDACTED_RELATIVE_URL]",
```

```
  "SourceFileName": "[REDACTED_FILENAME]",
  "SourceFileExtension": "xlsx",
  "ApplicationDisplayName": "Microsoft Office",
  "SiteUrl": "[REDACTED_URL]",
  "ObjectId": "[REDACTED_URL]/[REDACTED_FILENAME]"
}
```


Figure 2: SharePoint/M365 log example


```
"Login","20260120163111.430","SLB:[REDACTED]","[REDACTED]","[REDACTED]","192","25","/index.jsp","","1jVcuDh1VI
```


Figure 3: Salesforce log example


```
{
 "Timestamp": "2026-01-21T12:5:2-03:00",
 "Timestamp UTC": "[REDACTED]",
 "Event Name": "User downloads documents from an envelope",
 "Event Id": "[REDACTED_EVENT_ID]",
 "User": "[REDACTED]@example.com",
 "User Id": "[REDACTED_USER_ID]",
 "Account": "[REDACTED_ORG_NAME]",
 "Account Id": "[REDACTED_ACCOUNT_ID]",
 "Integrator Key": "[REDACTED_KEY]",
 "IP Address": "73.135.228[.]98",
 "Latitude": "[REDACTED]",
 "Longitude": "[REDACTED]",
 "Country/Region": "United States",
 "State": "Maryland",
 "City": "[REDACTED]",
 "Browser": "Chrome 143",
 "Device": "Apple Mac",
 "Operating System": "Mac OS X 10",
 "Source": "Web",
 "DownloadType": "Archived",
 "EnvelopeId": "[REDACTED_ENVELOPE_ID]"
}
```


Figure 4: Docusign log example

In at least one incident where the threat actor gained access to an Okta customer account, UNC6661 enabled the ToogleBox Recall add-on for the victim's Google Workspace account, a tool designed to search for and permanently delete emails. They then deleted a "Security method enrolled" email from Okta, almost certainly to prevent the employee from identifying that their account was associated with a new MFA device.

```
{
 "Date": "2026-01-11T06:3:00Z",
 "App ID": "[REDACTED_ID].apps.googleusercontent.com",
 "App name": "ToogleBox Recall",
 "OAuth event": "Authorize",
 "Description": "User authorized access to ToogleBox Recall for specific Gmail and Apps Script scopes.",
 "User": "user@[REDACTED_DOMAIN].com",
 "Scope": "https://www.googleapis.com/auth/gmail.addons.current.message.readonly, https://www.googleapis.com/au
 "API name": "",
 "Method": "",
 "Number of response bytes": "0",
 "IP address": "149.50.97.144",
 "Product": "Gmail, Apps Script Runtime, Apps Script Api, Identity, Unspecified",
 "Client type": "Web",
 "Network info": "{\n  \"Network info\": {\n    \"IP ASN\": \"201814\",\n    \"Subdivision code\": \"\",\n    \
}
```


Figure 5: ToogleBox Recall auth log entry example

In at least one case, after conducting the initial data theft, UNC6661 used their newly obtained access to compromised email accounts to send additional phishing emails to contacts at cryptocurrency-focused companies. The threat actor then deleted the outbound emails, likely in an attempt to obfuscate their malicious activity.

GTIG attributes the subsequent extortion activity following UNC6661 intrusions to UNC6240, based on several overlaps, including the use of a common Tox account for negotiations, ShinyHunters-branded extortion emails, and Limewire to host samples of stolen data. In mid-January 2026 extortion emails, UNC6240 outlined what data they allegedly stole, specifying a payment amount and destination BTC address, and threatening consequences if the ransom was not paid within 72 hours, which is consistent with prior extortion emails (Figure 6). They also provided proof of data theft via samples hosted on Limewire. GTIG also observed extortion text messages sent to employees and received reports of victim websites being targeted with distributed denial-of-service (DDoS) attacks.

Notably, in late January 2026 a new ShinyHunters-branded DLS named "SHINYHUNTERS" emerged listing several alleged victims who may have been compromised in these most recent extortion operations. The DLS also lists contact information (shinycorp@tutanota[.]com, shinygroup@onionmail[.]com) that have previously been associated with UNC6240.

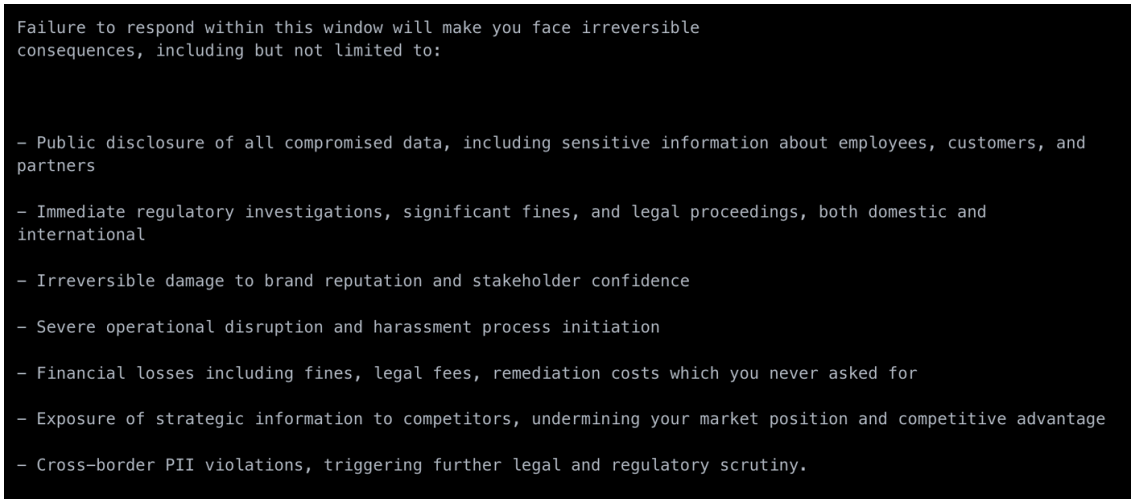

Figure 6: Ransom note extract

Similar Activity Conducted by UNC6671

Also beginning in early January 2026, UNC6671 conducted vishing operations masquerading as IT staff and directing victims to enter their credentials and MFA authentication codes on a victim-branded credential harvesting site. The credential harvesting domains used the same structure as UNC6661, but were more often registered using Tucows. In at least some cases, the threat actors have gained access to Okta customer accounts. Mandiant has also observed evidence that UNC6671 leveraged PowerShell to download sensitive data from SharePoint and OneDrive. While many of these TTPs are consistent with UNC6661, an extortion email stemming from UNC6671 activity was unbranded and used a different Tox ID for further contact. The threat actors employed aggressive extortion tactics following UNC6671 intrusions, including harassment of victim personnel. The extortion tactics and difference in domain registrars suggests that separate individuals may be involved with these sets of activity.

Remediation and Hardening

Mandiant has published a comprehensive guide with proactive hardening and detection recommendations.

Outlook and Implications

This recent activity is similar to prior operations associated with UNC6240, which have frequently used vishing for initial access and have targeted Salesforce data. It does, however, represent an expansion in the number and type of targeted cloud platforms, suggesting that the associated threat actors are modifying their operations to gather more sensitive data for extortion operations. Further, the use of a compromised account to send phishing emails to cryptocurrency-related entities suggests that associated threat actors may be building relationships with potential victims to expand their access or engage in other follow-on operations. Notably, this portion of the activity appears operationally distinct, given that it appears to target individuals instead of organizations.

Indicators of Compromise (IOCs)

To assist the wider community in hunting and identifying activity outlined in this blog post, we have included indicators of compromise (IOCs) in a free GTI Collection for registered users.

Phishing Domain Lure Patterns

Threat actors associated with these clusters frequently register domains designed to impersonate legitimate corporate portals. At time of publication all identified phishing domains have been added to Chrome Safe Browsing. These domains typically follow specific naming conventions using a variation of the organization name:

Pattern	Examples (Defanged)
Corporate SSO	<companyname>sso[.]com, my<companyname>sso[.]com, my-<companyname>sso[.]com
Internal Portals	<companyname>internal[.]com, www.<companyname>internal[.]com, my<companyname>internal[.]com
Support/Helpdesk	<companyname>support[.]com, ticket-<companyname>[.]support, support-<companyname>[.]com
Identity Providers	<companyname>okta[.]com, <companyname>azure[.]com, on<companyname>zendesk[.]com
Access Portal	<companyname>access[.]com, www.<companyname>access[.]com, my<companyname>acess[.]com

Network Indicators

Many of the network indicators identified in this campaign are associated with commercial VPN services or residential proxy networks, including Mullvad, Oxylabs, NetNut, 9Proxy, Infatica, and nsocks. Mandiant recommends that organizations exercise caution when using these indicators for broad blocking and prioritize them for hunting and correlation within their environments.

IOC	ASN	Association

24.242.93[.]122	11427	UNC6661
23.234.100[.]107	11878	UNC6661
23.234.100[.]235	11878	UNC6661
73.135.228[.]98	33657	UNC6661
157.131.172[.]74	46375	UNC6661
149.50.97[.]144	201814	UNC6661
67.21.178[.]234	400595	UNC6661
142.127.171[.]133	577	UNC6671
76.64.54[.]159	577	UNC6671
76.70.74[.]63	577	UNC6671
206.170.208[.]23	7018	UNC6671
68.73.213[.]196	7018	UNC6671
37.15.73[.]132	12479	UNC6671
104.32.172[.]247	20001	UNC6671
85.238.66[.]242	20845	UNC6671

199.127.61[.]200	23470	UNC6671
209.222.98[.]200	23470	UNC6671
38.190.138[.]239	27924	UNC6671
198.52.166[.]197	395965	UNC6671

Google Security Operations

Google Security Operations customers have access to these broad category rules and more under the Okta, Cloud Hacktool, and O365 rule packs. A walkthrough for operationalizing these findings within the Google Security Operations is available in Part Three of this series. The activity discussed in the blog post is detected in Google Security Operations under the rule names:

- Okta Admin Console Access Failure
- Okta Super or Organization Admin Access Granted
- Okta Suspicious Actions from Anonymized IP
- Okta User Assigned Administrator Role
- O365 SharePoint Bulk File Access or Download via PowerShell
- O365 SharePoint High Volume File Access Events
- O365 SharePoint High Volume File Download Events
- O365 Sharepoint Query for Proprietary or Privileged Information
- O365 Deletion of MFA Modification Notification Email
- Workspace ToogleBox Recall OAuth Application Authorized

```
$e.metadata.product_name = "Okta"
  $e.metadata.product_event_type = /\.(add|update_|(policy.rule|zone)\.update|create|register|(de)?activate|gr
  (
       $e.security_result.detection_fields["anonymized IP"] = "true" or
       $e.extracted.fields["debugContext.debugData.tunnels"] = /\"anonymous\":true/
  )
  $e.security_result.action = “ALLOW”
```

Figure 7: Hunting query for suspicious Okta actions conducted from anonymized IPs

```
$e.metadata.vendor_name = "Google Workspace"
  $e.metadata.event_type = "USER_RESOURCE_ACCESS"
  $e.metadata.product_event_type = "authorize"
  $e.target.resource.name = /ToogleBox Recall/ nocase
```

Figure 8: Hunting query for Google Workspace authorization events for ToogleBox Recall

```
$e.principal.ip_geo_artifact.network.organization_name = /mullvad.vpn|oxylabs|9proxy|netnut|infatica|nsocks/ no
  $e.extracted.fields["debugContext.debugData.tunnels"] = /mullvad.vpn|oxylabs|9proxy|netnut|infatica|nsocks/ n
```

Figure 9: Hunting query for suspicious VPN / proxy services observed in this campaign

```
$e.network.http.user_agent = /Geny\s?Mobile/ nocase
  $event.security_result.action != "BLOCK"
```

Figure 10: Hunting query for suspicious user-agent string observed in this campaign

```
   $e.metadata.log_type = "OFFICE_365"
 ($e.metadata.product_event_type = "FileDownloaded" or $e.metadata.product_event_type = "FileAccessed")
  (
    $e.target.application = "SharePoint" or
    $e.principal.application = "SharePoint"
  )
  $e.network.http.user_agent = /PowerShell/ nocase
```

Figure 11: Hunting query for programmatic file access or downloads from SharePoint where the User-Agent identifies as PowerShell

```
events:
  $e.metadata.log_type = "OFFICE_365"
  $e.metadata.product_event_type = "FileAccessed"
  (
    $e.target.application = "SharePoint" or
    $e.principal.application = "SharePoint"
  )
  $e.target.file.full_path = /\.(doc[mx]?|xls[bmx]?|ppt[amx]?|pdf)$/ nocase
  $file_extension_extract = re.capture($e.target.file.full_path, `\.([^\.]+)$`)
  $event.security_result.action != "BLOCK"
  $session_id = $e.network.session_id

match:
   $session_id over 5m
```

```
outcome:
   $target_url_count = count_distinct(strings.coalesce($e.target.file.full_path))
   $extension_count = count_distinct($file_extension_extract)

condition:
   $e and $target_url_count >= 50 and $extension_count >= 3
```

Figure 12: Hunting query for high volume document file access from SharePoint

```
 events:
   $e.metadata.log_type = "OFFICE_365"
   $e.metadata.product_event_type = "FileDownloaded"
   (
     $e.target.application = "SharePoint" or
     $e.principal.application = "SharePoint"
   )
   $e.target.file.full_path = /\.(doc[mx]?|xls[bmx]?|ppt[amx]?|pdf)$/ nocase
   $file_extension_extract = re.capture($e.target.file.full_path, `\.([^\.]+)$`)
   $event.security_result.action != "BLOCK"
   $session_id = $e.network.session_id

 match:
    $session_id over 5m

outcome:
   $target_url_count = count_distinct(strings.coalesce($e.target.file.full_path))
   $extension_count = count_distinct($file_extension_extract)

condition:
   $e and $target_url_count >= 50 and $extension_count >= 3
```

Figure 13: Hunting query for high volume document file downloads from SharePoint

```
 $e.metadata.log_type = "OFFICE_365"
   $e.metadata.product_event_type = "SearchQueryPerformed"
   $e.additional.fields["search_query_text"] = /\bpoc\b|proposal|confidential|internal|salesforce|vpn/ nocase
```

Figure 14: Hunting query for SharePoint queries for strings of interest

```
 $e.metadata.log_type = "OFFICE_365"
   $e.target.application = "Exchange"
   $e.metadata.product_event_type = /^(SoftDelete|HardDelete|MoveToDeletedItems)$/ nocase
   $e.network.email.subject = /new\s+(mfa|multi-|factor|method|device|security)|\b2fa\b|\b2-Step\b|(factor|metho
```

```
// filtering specifically for new device registration strings
$e.network.email.subject = /enroll|registered|added|change|verify|updated|activated|configured|setup/ nocase

// tuning out new device logon events
$e.network.email.subject != /(sign|log)(-|\s)?(in|on)/ nocase
```

Figure 15: Hunting query for O365 Exchange deletion of MFA modification notification email

Posted in

- Threat Intelligence
