Scattered Spider laying new eggs

blog.sekoia.io/scattered-spider-laying-new-eggs/

22 February 2024

Log in

Whoops! You have to login to access the Reading Center functionalities!

Forgot password?

Pierre-Antoine D., Quentin Bourgue, Livia Tibirna and TDR (Threat Detection & Research)

February 22 2024
545 0

Read it later Remove

19 minutes reading

Introduction

Scattered Spider (aka UNC3944, Scatter Swine, Muddled Libra, Octo Tempest, Oktapus, StarFraud) is a **lucrative intrusion set** active since at least May 2022, primarily engaged in social engineering, ransomware, extortion campaigns and other advanced techniques.

The intrusion set employs state-of-the-art techniques, particularly related to **social engineering**, such as impersonation of IT personnel to deceive employees for targeted phishing, SIM swapping, leverage of MFA fatigue, and contact with victims' support teams. Scattered Spider also conducted high-profile network intrusions and ransomware attacks as a BlackCat ransomware affiliate since mid-2023.

The intrusion set attracted significant media coverage several times with the compromise of Twilio in August 2022 and the campaign against the casino chains Caesars Entertainment and MGM Resorts International in the summer of 2023.

This report provides an **overview of the Scattered Spider evolution**, its modus operandi and the toolset leveraged over the past years. Additionally, it delves into the Scattered Spider **Techniques, Tactics and Procedures** (TTPs), as well as the **latest ongoing campaigns, including their current targets**.

Background

Tracing the threads: the history of naming “Scattered Spider”

Since mid-2022, **Scattered Spider’s modus operandi** has been documented under numerous aliases by various sources. It is reported **overlapping** with the activity of intrusion sets known as **0ktapus** (Group-IB), **Scatter Swine** (Okta), **UNC3944** (Mandiant), **Octo Tempest** (previously Storm-0875, Microsoft), **Muddled Libra** (Unit42) and others.

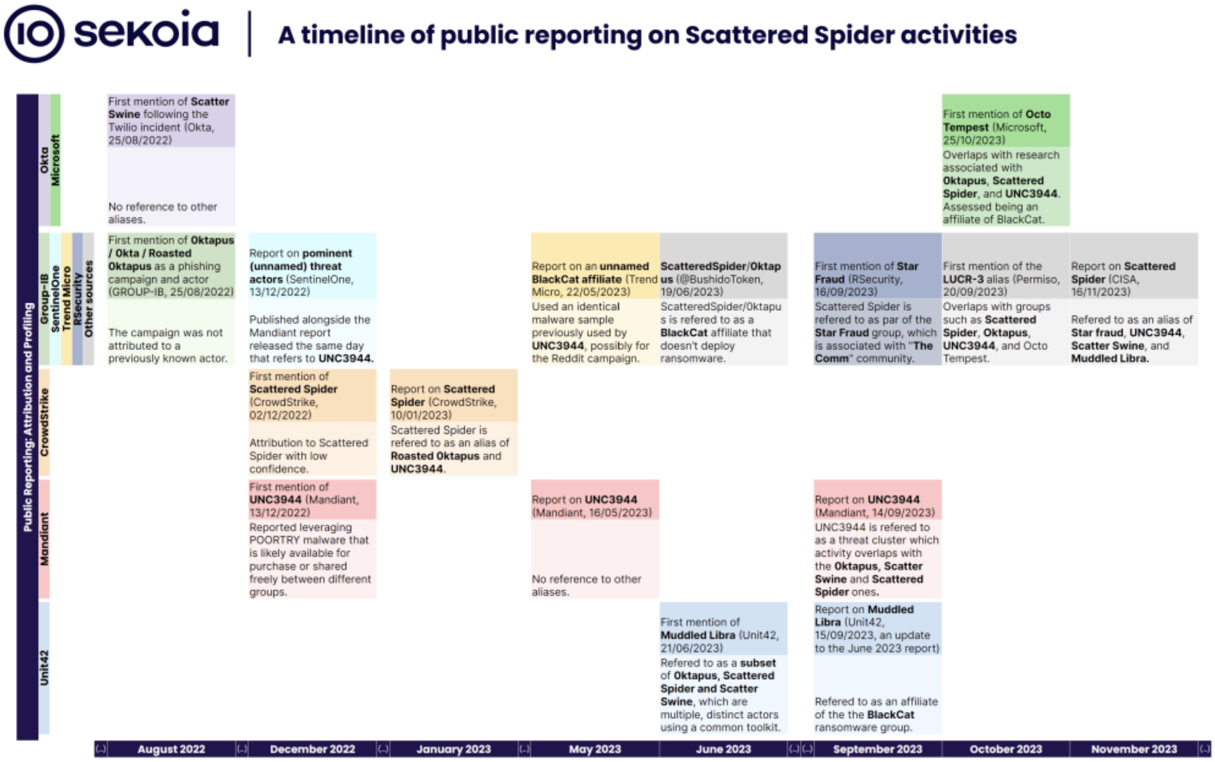
SentinelOne associates Scattered Spider with the “**Star Fraud**” group, which is likely part of a larger cybercrime ecosystem of disparate and sometimes rival subgroups that refers to itself as “The Community” (aka “The Com.” and “The Comm”). This long-running online community is reported to be the cyber threat with the greatest impact in 2023 as per SentinelOne. While, Coveware links with a low level of confidence Scattered Spider to Rhysida ransomware activity, we could not cross-reference this information.

While most vendors use the above-mentioned aliases interchangeably, RedCanary analysts assess with high confidence that Scattered Spider, UNC3944, Oktapus, and Muddled Libra are not exact overlaps. Those subgroups are likely multiple actors using a **common toolkit**, according to Unit42.

Sekoia.io Threat Detection & Research (TDR) team monitors Scattered Spider as a **cluster of all the above-mentioned intrusion-sets** that are highly likely subsets of a larger umbrella. So, we encompass all the related activities under the Scattered Spider intrusion set.

According to public reporting, Scattered Spider is an intrusion set of 17-22 years old, **native English-speaking** individuals that reside primarily in Western countries. Intel471 refers to its members as mid-to-lower-level skilled actors with a small subset of highly technically capable members.

Of note, a threat actor specialised in wire fraud and identity theft, reported in open sources as a Scattered Spider affiliate, was arrested in early 2024.



A timeline of public reporting on Scattered Spider activities

Public Reporting: Attribution and Profiling

	August 2022	December 2022	January 2023	May 2023	June 2023	September 2023	October 2023	November 2023
Okta Microsoft	First mention of **Scatter Swine** following the Twilio incident (Okta, 25/08/2022) No reference to other aliases.						First mention of **Octo Tempest** (Microsoft, 25/10/2023) Overlaps with research associated with **Oktapus**, **Scattered Spider**, and **UNC3944**. Assessed being an affiliate of BlackCat.	
Group-IB SentinelOne Trend Micro RSecurity Other sources	First mention of **Oktapus / Okta / Roasted Oktapus** as a phishing campaign and actor (GROUP-IB, 25/08/2022) The campaign was not attributed to a previously known actor.	Report on **pominent (unnamed) threat actors** (SentinelOne, 13/12/2022) Published alongside the Mandiant report released the same day that refers to **UNC3944.**		Report on an **unnamed BlackCat affiliate** (Trend Micro, 22/05/2023) Used an identical malware sample previously used by **UNC3944**, possibly for the Reddit campaign.	**ScatteredSpider/Oktapus** (@BushidoToken, 19/06/2023) ScatteredSpider/Oktapus is refered to as a **BlackCat** affiliate that doesn't deploy ransomware.	First mention of **Star Fraud** (RSecurity, 16/09/2023) Scattered Spider is refered to as par of the **Star Fraud** group, which is associated with "**The Comm**" community.	First mention of the **LUCR-3** alias (Permiso, 20/09/2023) Overlaps with groups such as **Scattered Spider**, **Oktapus**, **UNC3944**, and Octo Tempest.	Report on **Scattered Spider** (CISA, 16/11/2023) Refered to as an alias of **Star fraud**, **UNC3944**, **Scatter Swine**, and **Muddled Libra.**
CrowdStrike		First mention of **Scattered Spider** (CrowdStrike, 02/12/2022) Attribution to Scattered Spider with low confidence.	Report on **Scattered Spider** (CrowdStrike, 10/01/2023) Scattered Spider is refered to as an alias of **Roasted Oktapus** and **UNC3944**.					
Mandiant		First mention of **UNC3944** (Mandiant, 13/12/2022) Reported leveraging POORTRY malware that is likely available for purchase or shared freely between different groups.		Report on **UNC3944** (Mandiant, 16/05/2023) No reference to other aliases.		Report on **UNC3944** (Mandiant, 14/09/2023) UNC3944 is refered to as a threat cluster which activity overlaps with the **Oktapus, Scatter Swine** and **Scattered Spider** ones.		
Unit42					First mention of **Muddled Libra** (Unit42, 21/06/2023) Refered to as a **subset** of **Oktapus, Scattered Spider and Scatter Swine**, which are multiple, distinct actors using a common toolkit.	Report on **Muddled Libra** (Unit42, 15/09/2023, an update to the June 2023 report) Refered to as an affiliate of the the **BlackCat** ransomware group.		

Figure 1. A timeline of public reporting on Scattered Spider activities. Sources: see the External References section.

Unravelling the threads: Scattered Spider's web profile

Over the past years, Scattered Spider compromised numerous **high-profile organisations**, mainly located in the **United States**. In mid-2022, a wide-scale social engineering campaign aiming at stealing employee credentials was reported impacting technology companies, telecommunications providers, and cryptocurrency-related individuals and organisations. The campaign targeted Twilio and Cloudflare employees among others, and was attributed to the Scattered Spider intrusion set.

The intrusion set was **highly prolific** since its first appearance, as it had allegedly compromised over 130 unique organisations between March and July 2022 only. Since 2022 and throughout 2023, attacks targeting the social news website Reddit, the hospitality and entertainment giant MGM Resorts International were also attributed to the intrusion set in open sources.

Moreover, the campaigns attributed to Scattered Spider are **continuously persistent**. In a 2022 campaign targeting T-Mobile customers, Scattered Spider and two additional intrusion sets engaged in SIM swapping accessed victim's systems 100 times across seven months.

The intrusion set persistently conducts **phishing campaigns** to gain access to a company's network. Scattered Spider is reported to leverage **advanced, targeted, mainly phone-based social engineering techniques**. This includes tailored phishing domains, SIM swapping, phishing phone calls and targeted SMS.

The intrusion set's proficiency in phishing is highly likely due to their **comprehensive understanding of their targets' environment**, allowing them to successfully impersonate a victim's employee. Indeed, Scattered Spider is known to meticulously plan their campaigns, consistently gathering intelligence on corporate hierarchies, specific employees, and the IT support infrastructure of their targets.

According to Microsoft, if initial attempts fail, Scattered Spider members leverage personal information such as residential addresses and relatives' names, coupled with threats of physical harm, to **coerce victims into revealing login credentials for corporate systems**.

Upon gaining unauthorised access, the intrusion set frequently reviewed internal documents detailing processes and procedures, using this information to expand their reach further and secure an extensive access to sensitive systems and data.

While conducting advanced and targeted campaigns, Scattered Spider is reported as being exclusively **financially-motivated**. The latest monetisation strategy adopted by Scattered Spider consists of deploying ransomware in victims' environments. Indeed, the intrusion set conducts **double extortion campaigns** leveraging the **BlackCat ransomware** since mid-2023, after several months of exfiltrating files without encryption.

TTPs leveraged by Scattered Spider for high-profile attacks

A spider's web expansion: from access broker to BlackCat ransomware affiliate

Since mid-2022, Scattered Spider evolving activities have been documented by multiple sources, outlining the various techniques adopted by the intrusion set over time.

The **evolution of Scattered Spider's TTPs** and the reported victimology illustrates a **significant shift** in their operational strategy. Initially functioning as an access broker, the intrusion set targeted high-value organisations across the telecommunications and technology sectors, as well as individuals linked to cryptocurrency. Over time, Scattered Spider's tactics evolved into those of a ransomware affiliate, including data exfiltration and ransomware deployment for extortion.

Starting from mid-2022, Scattered Spider conducted campaigns to **gain initial access to organisation's accounts through social engineering**, leveraging SMS, phone calls or Telegram to impersonate IT personnel and direct victims to a credential harvesting site. Such attacks led to further smishing campaigns and account takeovers of high-net-worth individuals. Microsoft assesses that Scattered Spider **monetised intrusions by selling access to other criminals** at that time.

By late 2022, the intrusion set expanded its targeting to business process outsourcing (BPO) intending to gain **further access to mobile carrier networks** from a Telco or BPO environment. For this purpose, Scattered Spider established persistence using VPN access or Remote Monitoring and Management (RMM) tools. The intrusion set innovates to gain an initial foothold within the victims' environment, by targeting corporate assets through stolen Azure credentials and exploiting vulnerabilities. Microsoft assesses that Scattered Spider **monetised intrusions by extorting organisations with stolen data**.

In mid-2023, Scattered Spider **allegedly joined the BlackCat ransomware operation and began deploying the ransomware payload** on Windows and Linux systems, and later on VMWare ESXi servers.

BlackCat (aka ALPHV) Ransomware as a Service (RaaS) distributes its malware since late 2021 and was among the Top 3 most prolific ransomware operations in 2023, according to Sekoia.io observations. BlackCat representatives declare cooperating with Russian-speaking affiliates only. Therefore, Scattered Spider joining this RaaS as an affiliate is likely indicative of a constantly evolving Russian-speaking RaaS group, driven by the maximisation of financial gain, whose main condition for recruiting affiliates likely remains to avoid attacking within the Commonwealth of Independent States (CIS) organisation.

The intrusion set **continuously expanded its arsenal of tools, malware and techniques**, for establishing persistence and reconnaissance on networks, escalating privileges, removing, disabling and bypassing security tools, as well as exfiltrating data. These evolutions, as well as the ever-extended targeting, are indicative of a relatively advanced, increasingly persistent and well-established intrusion set.

Based on open-source reporting (see the External References section), Sekoia.io analysts compiled the techniques employed by Scattered Spider over time and the targeted sectors, as shown in the table below:

	Scattered Spider’s techniques	Targeted sectors
Mid-2022 Roasting 0ktapus (Group-IB, August 2022 – Twilio, August 2022 – Cloudflare, August 2022) Scatter Swine (Okta, August 2022)	– Gathered mobile phone numbers of employees from commercially available data aggregation services – Targeted employees with phishing, including smishing and voice phishing. – Harvested credentials through targeted phishing pages – Relayed One Time Password (OTP) through phishing pages – Distributed the commercial RMM tool AnyDesk – Used anonymising proxy services – Took over user accounts – Conducted further smishing attacks	– Technology – Telecommunications – Individuals linked to cryptocurrency
Late 2022 Scattered Spider (CrowdStrike, December 2022) UNC3944 (Mandiant, December 2022)	– Gathered mobile phone numbers of employees – Targeted employees with phishing, including smishing, Telegram message and phone calls – Impersonated IT personnel for phishing – Accessed Azure account using stolen credentials – Exploited CVE in ForgeRock OpenAM application server – Distributed various RMM tools – Persisted using VPN access, AWS key theft and IAM manipulation – Exploited the Bring Your Own Vulnerable Driver (BYOD) technique to bypass endpoint security – Deployed the Remote Access Trojan (RAT) RattyRAT – Conducted further smishing attacks – Gained access to mobile carrier network and SIM card information – Exfiltrated data using transfer[.]sh – Performed SIM swapping	– Telecommunications – Business process outsourcing

Mid-2023 UNC3944 (Mandiant, September 2023) Muddled Libra (Unit42, September 2023)	– Purchased stolen credentials from cybercriminal market – Gathered mobile phone numbers of employees – Targeted employees with phishing, including smishing and phone calls – Used phone-based social engineering – Leveraged MFA bombing – Performed SIM swapping – Used the commercial residential proxy services NSOCKS and TrueSocks – Distributed various RMM tools – Created publicly accessible virtual machines inside victims' environments – Deployed commodity malware (infostealers, reconnaissance, privilege escalation) – Targeted VMware vCenters servers using the open-source bedevil Linux rootkit – Achieved privilege escalation by resetting password or modifying multi-factor authentication (MFA) – Performed reconnaissance and credential dump using public tools – Enumerated the internal documentation and resources – Achieved privilege escalation by targeting password managers or IAM – Disabled security products – Exfiltrated data using Rclone, MEGAsync, FileZilla or DropBox – Deleted shadow copies, disabled security tools – Deployed BlackCat ransomware – Engaged aggressive communications with victims for persuasion	– Telecommunications – Business process outsourcing – Hospitality – Retail – Media – Entertainment – Financial services

Late 2023 Octo Tempest (Microsoft, October 2023) Scattered Spider (CISA, November 2023)	– Purchased stolen credentials from cybercriminal market – Targeted employees with phishing, including smishing and phone calls – Harvested credentials through targeted AiTM phishing pages – Used phone-based social engineering – Distributed various RMM tools – Used reverse shells – Deployed commodity malware (infostealers, reconnaissance, privilege escalation) – Targeted VMware vCenters servers using the open-source bedevil Linux rootkit – Achieved privilege escalation by resetting password or modifying multi-factor authentication (MFA) – Performed reconnaissance and credential dump using public tools – Enumerated the internal documentation and resources – Disabled security products – Modified mailbox rules to delete emails from security vendors, and exfiltrate emails – Exfiltrated data using MEGAsync, Gofile, shz[.]al, Storj, Temp[.]sh, Paste[.]ee, Backblaze, and AWS S3 buckets – Deployed BlackCat ransomware – Engaged aggressive communications with victims for persuasion	– Natural resources – Gaming – Hospitality – Consumer products – Retail – Managed services providers – Manufacturing – Law – Technology – Financial services

Table 1. TTPs leveraged by Scattered Spider between 2022 and 2023

Eggspedition: Scattered Spider’s exfiltration tactics

By late 2022, a notable development in Scattered Spider’s tactics emerged with the employment of the file sharing service transfer[.]sh to facilitate **data exfiltration**. In 2023, the intrusion set further **expanded its data exfiltration capabilities**, incorporating new tools such as **Rclone, MEGAsync, DropBox**, and subsequently, Gofile, shz[.]al, Storj, Tem[.].sh, Paste[.]ee, Backblaze and AWS S3 buckets, as reported by Mandiant and Microsoft.

Ransomware affiliates frequently use such file-hosting services to **exfiltrate large volumes of data** from compromised networks onto anonymous infrastructures. Once they obtain sensitive data from victims, attackers typically coerce victims into paying the ransom by threatening publication. Since 2020, this tactic, known as double extortion ransomware, has become widespread among ransomware gangs, including BlackCat and its affiliate, Scattered Spider.

While some ransomware affiliates or groups use **customised exfiltration tools** (*e.g.* ExMatter, StealBit, Grixba) to exfiltrate data to their own infrastructures, many operators tend to leverage **legitimate, open source tools** (*e.g.* FileZilla, MEGAsync, Rclone, WinSCP) to remain stealthy, as they are widely used in corporate environments. Also, ransomware actors frequently leverage anonymous infrastructures (*e.g.* transfer[.]sh, MEGA, DropBox) for data hosting and sharing, **allowing attackers to avoid burning their infrastructure during the exfiltration stage**.

One such example is the **cloud storage MEGA** (also known as mega[.]nz or mega[.]io) and its associated client MEGAsync. Created in 2013 by Kim Dotcom, MEGA provides **privacy and security-focused storage** boasting "zero-knowledge encryption" at an attractive price compared to competitors. Moreover, **MEGA accepts Bitcoin as payment**, enabling cybercriminals to capitalise on anonymity, decentralisation, and difficulty in tracking associated with cryptocurrency transactions. The MEGA service provides end-to-end encryption with restricted access to user data and account information, enhancing anonymity and reducing the risk of exposure or interception of exfiltrated data.

The **MEGAsync client is an open-source, cross-platform exfiltration tool available on GitHub**, enabling ransomware affiliates to deploy the tool across Windows, Linux and macOS distributions.

For **Scattered Spider and numerous other ransomware intrusion sets** – like LockBit, BlackCat, Trigona, INC, Vice Society, and Monti – **MEGA and MEGAsync stand out as one of the preferred solutions for the data exfiltration stage**, owing it to their protective measures for identity and data.

With similar intentions, cybercriminals rely on a wide range of legitimate services, tools and technologies, prioritising privacy, anonymisation and data protection. It includes cryptocurrencies, VPNs, VPS, proxy services, the Tor network, various messaging services (*e.g.* Telegram, Tox, Session, Jabber), and email providers (*e.g.* ProtonMail, Tutanota, Onion Mail).

Spider's web: phishing traps unveiled

Target webs: where cyber spiders aim their digital threads

SilentPush recently reported on the advanced **Scattered Spider** intrusion set deploying a **new phishing kit** since September 2023, along with sharing the intrusion set registrars and Autonomous System Numbers (ASN) details.

Following this article, Sekoia.io TDR analysts initiated a dedicated infrastructure tracking, resulting in new tracking heuristics for our Sekoia.io C2 Tracker project.

In January 2024, our tracker got new matches, indicating that **a new campaign** was underway. Instead of using the usual ASN, Scattered Spider switched to **another registrar**: **“registrar[.]eu”**. Subsequently, all domains registered since then use the same combination as of mid-February 2024.

Based on TDR observations, the **phishing pages** designed by Scattered Spider have **short online lifespans**, often lasting only several days or even a few hours, which is consistent with previous reports by other security companies. For example, the domain “linkedinsso[.]com” was registered on 19 January 2024, it became active immediately and ceased operations two days later. On 8 February, after a one-week break, the phishing infrastructure went live again, with new registered domains and, subsequently, new targets.

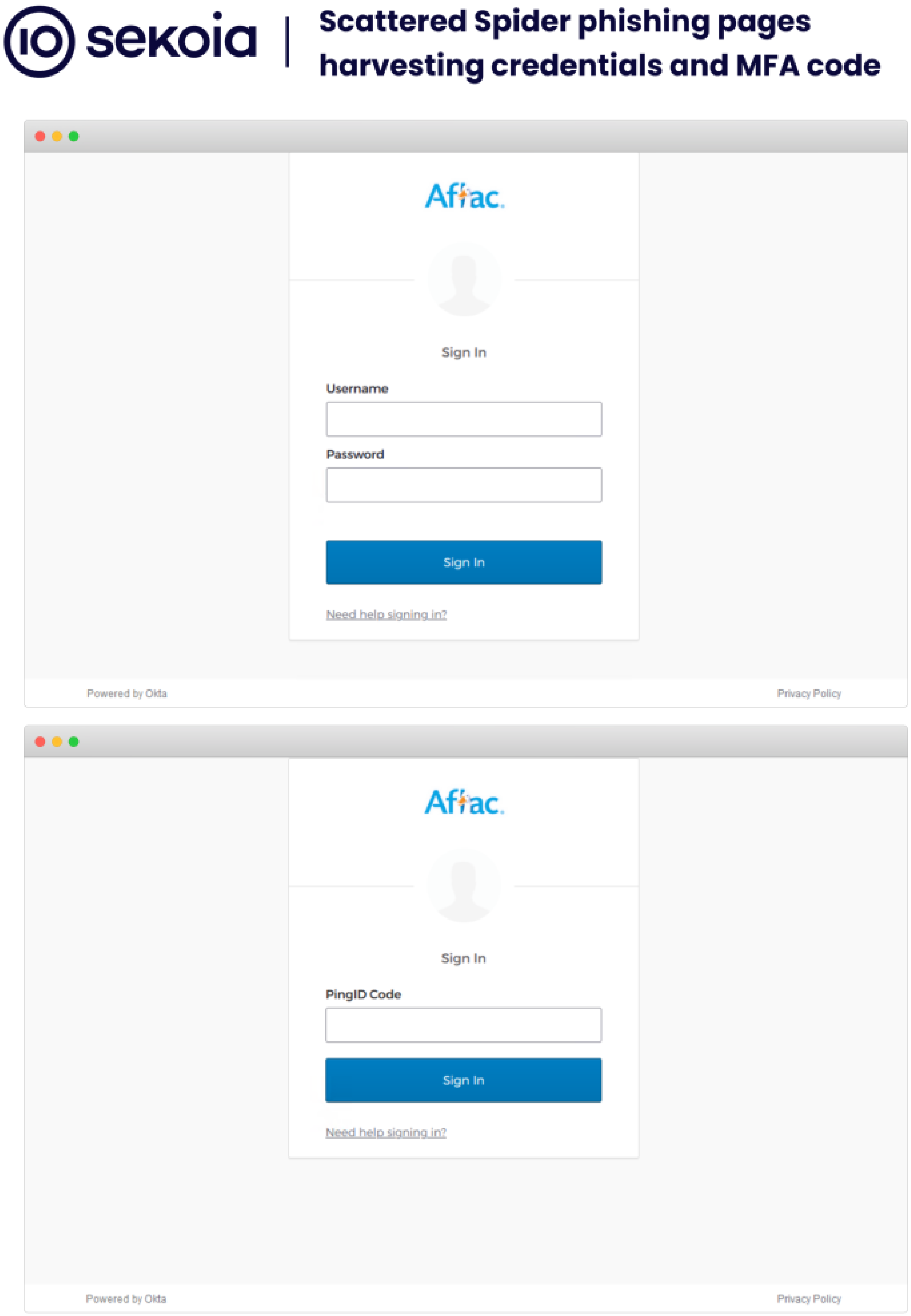


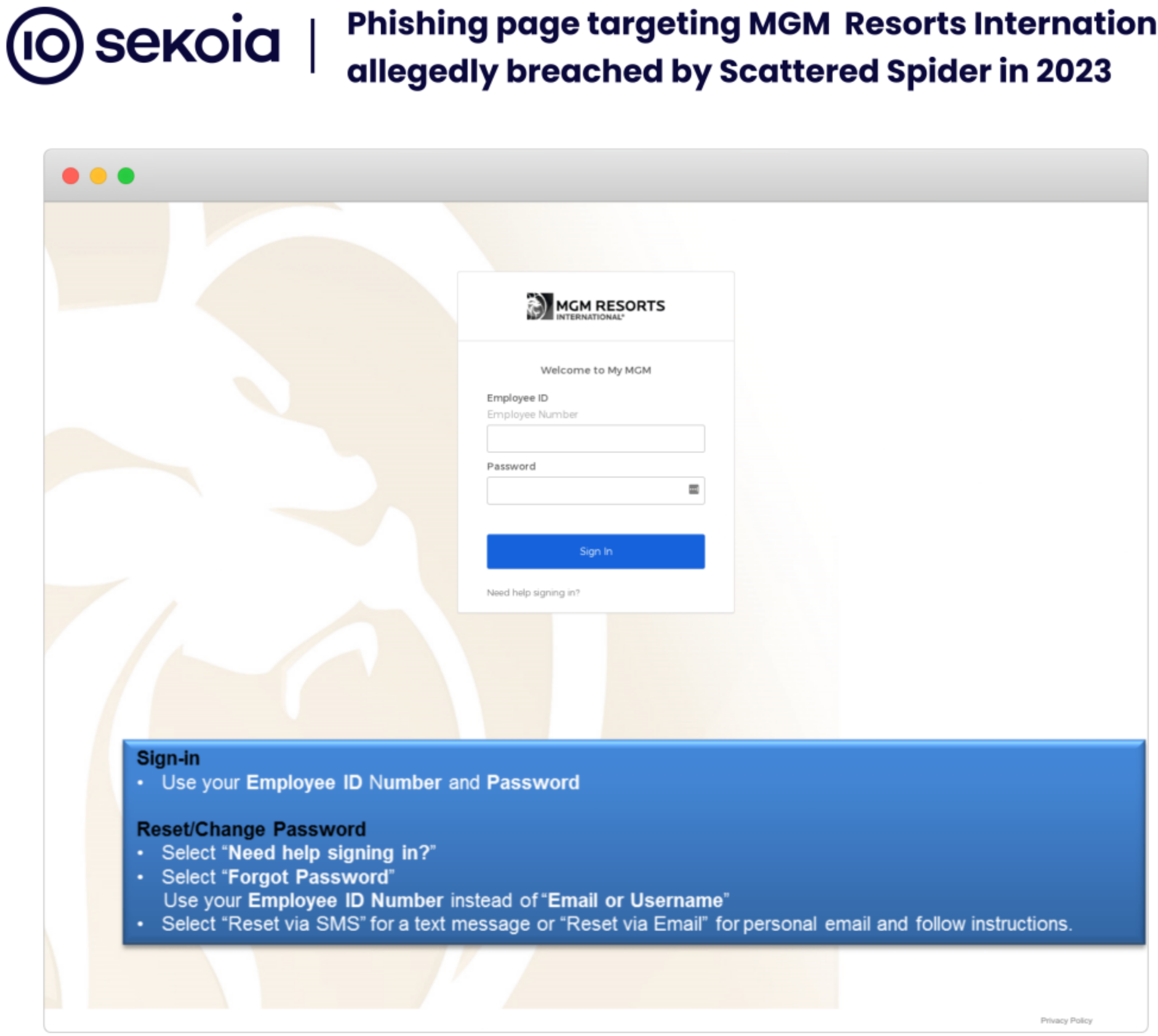
Figure 2. Scattered Spider phishing pages harvesting credentials and MFA code targeting a United States insurance company in February 2024.

The root page of the phishing domain attempts to lure users into providing their Okta credentials. Upon clicking on the “Sign In” button, the collected information is sent to the “**fuckyou.php**” page before being redirected to the “**factor.html**” page, which prompts the user for what we assess to be a 2FA code.

The information submitted in the 2FA form is then sent to “**factor.php**”, which, after a brief delay, redirects users to the legitimate public website of the targeted company.

Of note, during our infrastructure investigation, we came across several old domains targeting MGM Resorts International, a major casino brand targeted by Scattered Spider in a ransomware and extortion campaign in the summer of 2023. The following two of the observed domains were registered and were active in August 2022:

- mgmresorts-okta[.]com
- schedule.mgmresorthotels[.]com



Phishing page targeting MGM Resorts International, allegedly breached by Scattered Spider in 2023

Sign-in
- Use your **Employee ID** Number and **Password**

Reset/Change Password
- Select “**Need help signing in?**”
- Select “**Forgot Password**”
  Use your **Employee ID Number** instead of “**Email or Username**”
- Select “Reset via SMS” for a text message or “Reset via Email” for personal email and follow instructions.

Figure 3. Fake MGM Resorts International login page.

Sekoia.io analysts assess with high confidence that these phishing domains were set up by Scattered Spider, given their modus operandi, the ASN and the registrar they leveraged at that time.

Furthermore, most of Scattered Spider’s phishing pages contain an invisible list with a distinctive URL in the HTML code, *e.g.*:

```
<li>
  <a href="hxxps://nigga.okta[.]com/help/login" data-se="help-link" class="link js-help-link" rel="noopener noreferrer" target="_blank">Help</a>
</li>
```

Table 2. Characteristic URL in the HTML code

This element aligns with the “colourful” language used by the intrusion set, as reported by Group-IB researchers in August 2022. Their investigation uncovered a Telegram channel used to exfiltrate data from Scattered Spider’s former phishing kit, whose administrator was named “ Bored Niggas INC ”.

Through the eyes of the spider: focused targeting in the digital jungle

Since mid-2022, Scattered Spider was publicly reported as actively **targeting** a wide **range of industries**, including telecommunication providers, software and technology, business process outsourcing providers, cryptocurrency platforms, food delivery services, and organisations in the hospitality, banking, manufacturing, retail as well as customer relationship management, marketing and legal sectors.

Sekoia.io’s tracking of the intrusion set’s phishing infrastructure yielded a list of **new phishing domain names** (see the IoCs section) allegedly targeting employees of specific companies based on the design of the authentication pages and their redirection to targets’ official websites.

On this basis and regarding the previously reported Scattered Spider’s victimology, we assess with high confidence that the intrusion set does target those organisations in **an ongoing campaign.**

As of February 2024, we gathered the following list of **targeted organisations**:

- True Corporation
- Zendesk
- Squarespace
- Walmart
- Linkedin
- Costco
- Cellular Sales

- Grubhub
- Samsung
- Gitlab
- Fireblocks
- Sinch
- Roblox
- Us Cellular
- Apple
- Binance
- Verizon
- Aflac
- Bell
- Allstate
- Athene

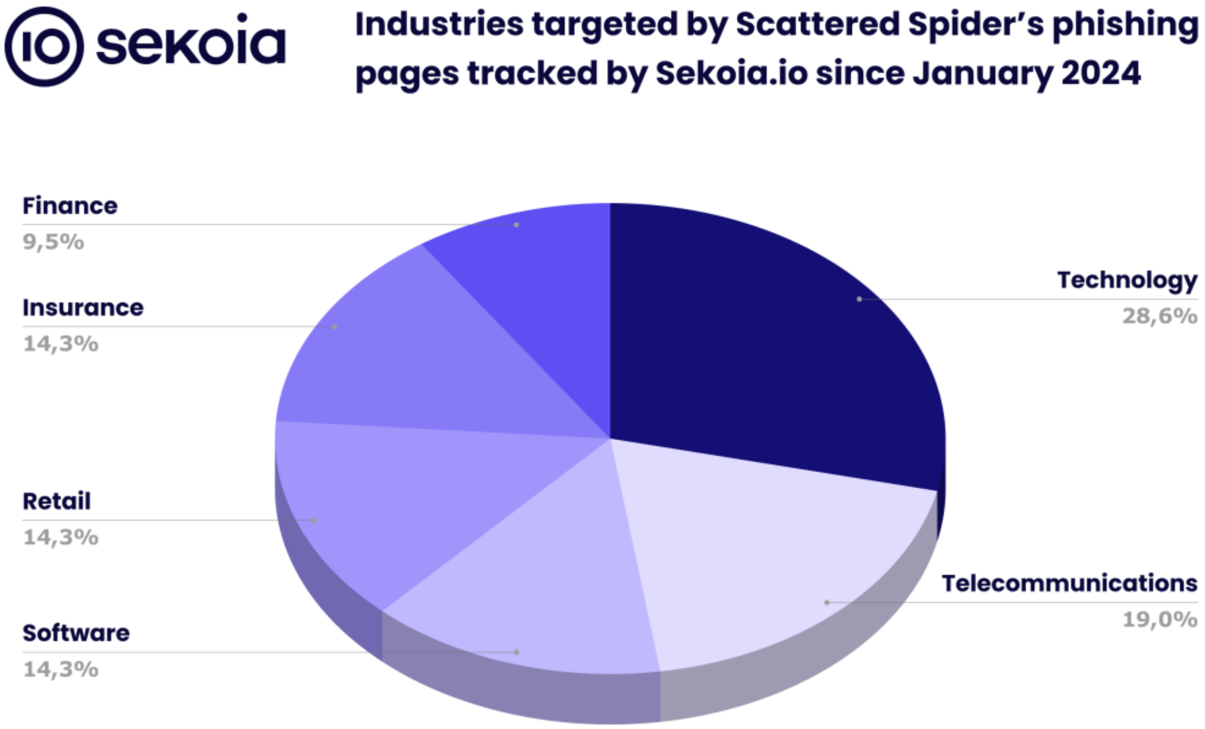
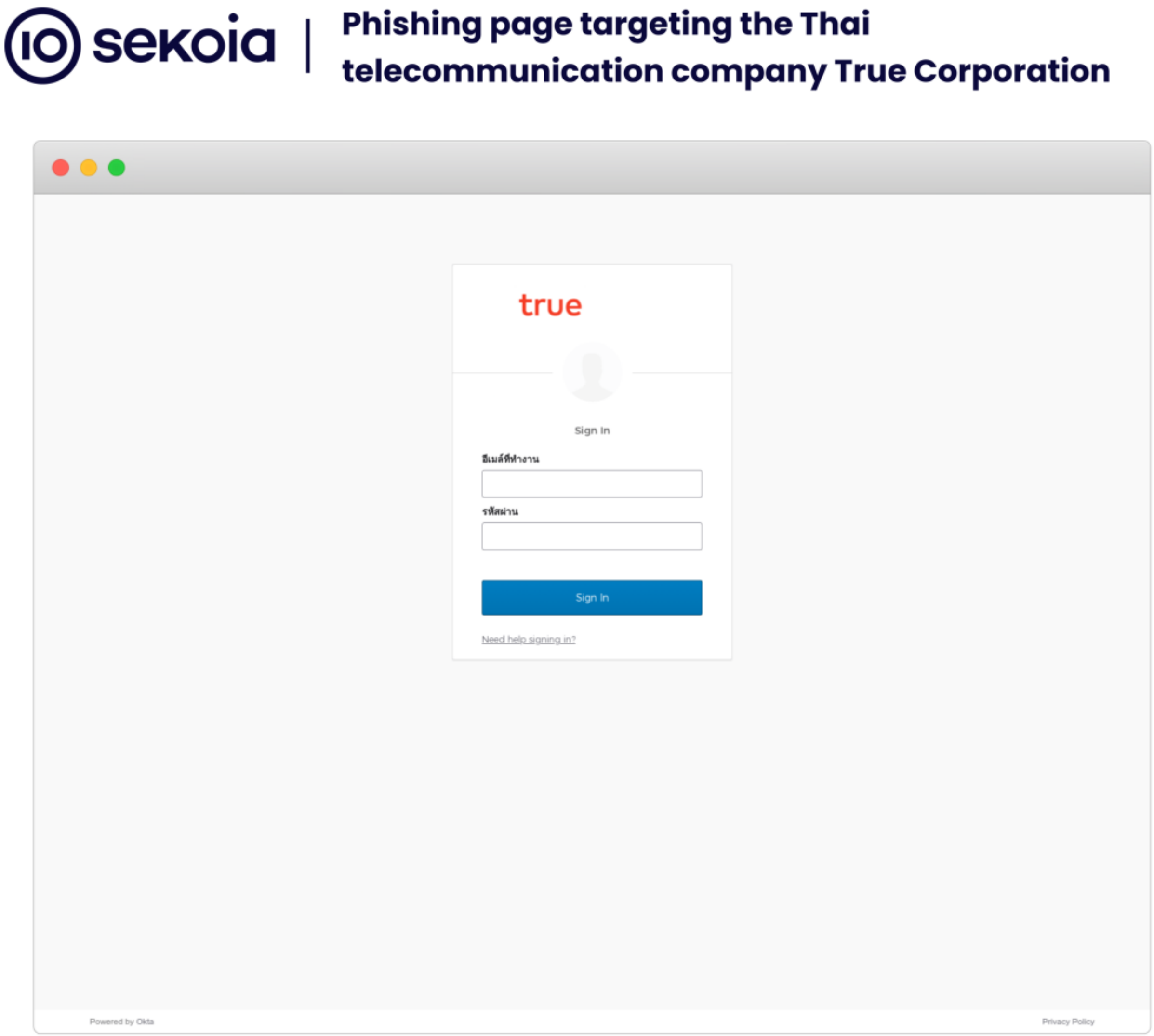


Figure 4. Industries targeted by Scattered Spider's phishing pages tracked by Sekoia.io in January 2024.

Scatter Spider primarily targets organisations based in the **United States**. While some of the newly unveiled targets are based in other regions of the world, the majority of them do maintain offices in the United States.

Yet, of particular interest are True Corporation and Bell companies, based in **Thailand** and **Canada**, respectively. While their industry-related targeting aligns with Scattered Spider's usual campaigns aimed at organisations within the telecommunication sector, this is likely indicative of **new targeted regions**.



Phishing page targeting the Thai telecommunication company True Corporation

Figure 5. Fake True Corporation login page

After expanding their list of targeted sectors over time and switching to Big Game Hunting (BGH) attacks to maximise their profits by increasing extorted amounts, Scattered Spider is likely also expanding their list of targeted locations. Our assumption relies on analysing their phishing pages impersonating novel organisations. As of mid-February 2024, there have been no reported incidents involving victims outside the United States linked to Scattered Spider.

Sekoia.io TDR remains committed to actively monitoring the Scattered Spider activities to anticipate and evaluate further evolutions.

Conclusion

Scattered Spider is a **financially-motivated intrusion set engaging in highly lucrative cybercrime activities** aimed at theft of sensitive data, cryptocurrency stealing, data exfiltration and ransomware deployment for extortion. We assess Scattered Spider’s techniques progressively evolve towards an advanced modus operandi, indicative of a group, or at least of some of its members, with a relatively high level of expertise.

Over the past years, the intrusion set expanded its activities from being an **access broker** specialising in phishing and social engineering to becoming a **ransomware affiliate, enhancing its TTPs, its arsenal of tools and malware, and adjusting its targeting**.

Sekoia.io analysts view Scattered Spider as an umbrella **encompassing various modus operandi** that are likely to evolve, notably as new threat actors bring their skills, experiences and arsenal by joining the group.

To actively monitor the threat and protect our customers, we focus on monitoring and tracking the **Scattered Spider’s TTPs in time, consistent with those of many ransomware affiliates** and initial access brokers. To provide our customers with actionable intelligence, the TDR team will continue to proactively track Scattered Spider’s phishing infrastructure and investigate new reports outlining the intrusion set operations.

IoCs & Technical Details

Scattered Spider’s IoCs

You can find the IoCs as a CSV file on our Community Github here.

Phishing Domains

bell-hr[.]com	gitlabsso[.]com
allstate-hr[.]com	fireblocks-sso[.]com
uscellular-hr[.]com	sec-sso[.]net
marsh-hr[.]com	cellularsso[.]com
uscellularhr[.]com	connect-sso[.]com
usinfo1[.]net	costsso[.]com
uscchr[.]com	grubhubsso[.]com
aflac-hr[.]com	walmartsso[.]com
www[.]aflac-hr[.]com	linkedinsso[.]com
usccplus[.]com	vz-hr[.]com
sinchdev[.]com	walmartworkspace[.]com
on-sinch[.]com	square-sso[.]com
uscell[.]net	zen-sso[.]com
cellularhr[.]com	zendesklt[.]com
rbxhr[.]net	applesso[.]com
roblox-hrs[.]com	www.truecorphr[.]net
gitlabhr[.]com	truecorphr[.]net
bn-sso[.]com	athene-usa[.]com

Phishing servers

IP address	First seen	Last seen
149.248.14[.]222	2024-02-19	2024-02-19
149.28.105[.]251	2024-02-09	2024-02-10
216.128.128[.]163	2024-02-09	2024-02-09
155.138.227[.]80	2024-02-08	2024-02-09
149.28.41[.]193	2024-02-08	2024-02-09
140.82.29[.]65	2024-02-08	2024-02-09
149.248.12[.]179	2024-02-07	2024-02-09
45.32.66[.]91	2024-01-30	2024-01-31
162.33.178[.]245	2024-01-29	2024-01-29
207.246.106[.]194	2024-01-28	2024-01-28
45.63.54[.]8	2024-01-26	2024-01-26
45.76.65[.]42	2024-01-25	2024-01-28
144.202.114[.]128	2024-01-25	2024-01-25
45.76.172[.]113	2024-01-24	2024-01-25
45.32.64[.]247	2024-01-24	2024-01-25
149.248.0[.]189	2024-01-24	2024-01-25
104.207.153[.]50	2024-01-24	2024-01-25
45.63.53[.]99	2024-01-22	2024-01-23
149.28.66[.]216	2024-01-18	2024-01-21
149.28.80[.]155	2024-01-19	2024-01-20
45.63.52[.]43	2024-01-19	2024-01-20
207.246.102[.]242	2024-01-18	2024-01-20
45.77.120[.]140	2024-01-10	2024-01-12
45.32.84[.]65	2024-01-09	2024-01-11
104.238.141[.]119	2024-01-08	2024-01-09
108.61.86[.]177	2024-01-06	2024-01-08

195.35.10[.]222	2024-01-01	2024-01-02
2a02:4780:b:1342:0:238d:fa59[:]3	2024-01-02	2024-01-03

Annexes

Annex 1 – Malware and tools used by Scattered Spider

Tactics	Malware, tools, services
Reconnaissance	Linkedin
Initial Access	EIGHTBAIT (0ktapus phishing kit)
Persistence	RattyRat, bedevil, AADInternals
Privilege Escalation	LINpeas, aws_consoler, STONESTOP, POORTRY, KDMapper, HashiCorp Vault, Trufflehog, GitGuardian, Jecretz, pacu
Defense Evasion	privacy.sexy
Credential Access	Mimikatz, ProcDump, DCSync, LAPSToolkit, LaZagne, gosecretsdump
Discovery	RustScan, ADRecon, ADExplorer, PingCastle, MicroBurst, Advanced Port Scanner, Angry IP Scanner, Angry Port Scanner, SharpHound, CIMplant, ManageEngine, LANDESK, PDQ Inventor, Govnomi, PureStorage FlashArray
Lateral Movement	Impacket, CitrixReceiver, CitrixWorkspaceApp, mobaxterm, ngrok, OpenSSH, proxifier, PuTTY, socat, Wstunnel, RDP, Cloudflare Tunnel client, Chrome Remote Desktop, PsExec, Sshimpanzee
Collection	Atomic, Vidar, Meduza, Raccoon, Snaffler, Hekatomb, Lumma, DBeaver, MongoDB Compass, Azure SQL Query Editor, Cerebrata, FiveTran, AveMaria
Command and Control	RMM tools (listed below), rsocx, NSOCKS, TrueSocks, Twingate
Exfiltration	Telegram, Rclone, MEGAsync, Storage Explorer
Impact	BlackCat ransomware

Annex 2 – RMM tools

AnyDesk	RemotePC
ASG Remote Desktop	Rport
BeAnywhere	RSAT
ConnectWise	Rsocx
Domotz	RustDesk
DWService (DWAgent)	ScreenConnect
FixMe.IT	Socat
FleetDeck	Splashtop
GetScreen	SSH RevShell and RDP Tunnelling via SSH
ITarian Endpoint Manager	Tailscale
Level.io (Level RMS)	Tactical RMM
LogMeIn	TeamViewer
ManageEngine	TightVNC
Mesh	TrendMicro Basecamp
N-Able	Twingate
Ngrok	Sorillus
Parsec	WsTunnel
Pulseway	ZeroTier
Remote Server Administration Tools (RSAT)	ZohoAssist

External references

Feel free to read other Sekoia TDR (Threat Detection & Research) analysis here :

Comments are closed.