


‘Scattered Spider’ group launches ransomware attacks while expanding targets in hospitality, retail

 therecord.media/scattered-spider-ransomware-attacks-hospitality-retail



Jonathan Greig

September 18th, 2023

Hackers connected to a group known to researchers by names like "Scattered Spider," "Oktapus," and UNC3944 have moved beyond targeting telecommunication firms and tech companies into attacks on hospitality, retail, media and financial services.

The group made waves last week for its alleged role in a ransomware attack on MGM Resorts that caused chaos at several hotels in Las Vegas and drew the attention of not only federal law enforcement agencies but even the White House.

In a report late last week, security experts at cybersecurity firm and Google subsidiary Mandiant spotlighted the group's evolution from relatively aimless — yet high-profile — data theft incidents on major tech firms to sophisticated ransomware attacks on a wide range of industries.

The researchers — who refer to the group as UNC3944 — said that since 2022, the hackers' calling card has been “phone-based social engineering and SMS phishing campaigns (smishing) to obtain credentials to gain and escalate access to victim organizations.” They

initially focused on SIM swapping attacks that likely supported secondary criminal operations.

Yet by the middle of 2023, the group began to deploy ransomware in victim environments, “signaling an expansion in the group’s monetization strategies.”

“These changes in their end goals signal that the industries targeted by UNC3944 will continue to expand; Mandiant has already directly observed their targeting broaden beyond telecommunication and business process outsourcer (BPO) companies to a wide range of industries including hospitality, retail, media and entertainment, and financial services,” the researchers said.

“At least some UNC3944 threat actors appear to operate in underground communities, such as Telegram and underground forums, which they may leverage to acquire tools, services, and/or other support to augment their operations.”

UNC3944 initially made a name for itself with several high-profile attacks, including one on [Coinbase](#) in February. The group, which is allegedly made up of U.S. and U.K.-based hackers, has shown skill with social-engineering techniques.

Group-IB calls the group “Oktapus” because it targets users of tech company Okta’s identity and access management services. Typically it sends victims to lookalike pages to steal Okta credentials.

Does Scattered Spider seem to be everywhere? The scope of their intrusions since March 2022 from a [@CrowdStrike](#) perspective is pretty broad. They use social engineering, living off the land, and RMM tools before deploying ransomware or conducting extortion. pic.twitter.com/fP3Z1Mj0mW

— adam_cyber (@Adam_Cyber) [September 15, 2023](#)

“The methods used by this threat actor are not special, but the planning and how it pivoted from one company to another makes the campaign worth looking into,” said Rustam Mirkasymov, head of cyber threat research at Group-IB Europe.

“Oktapus shows how vulnerable modern organizations are to some basic social engineering attacks and how far-reaching the effects of such incidents can be for their partners and customers.”

Focus on data theft

Mandiant said the group has shown a consistent focus in stealing large amounts of sensitive data for extortion purposes and has a knack for understanding the contours of U.S. and European business practices, aiding their efforts in siphoning as much money as possible from victims.

UNC3944 also rely heavily on publicly available tools, legitimate software and malware that they purchase on underground forums.

Their most tried and true methods involve SMS phishing campaigns and calls to IT help desks, where they try to get password resets or bypass codes.

“The threat actors operate with an extremely high operational tempo, accessing critical systems and exfiltrating large volumes of data over a course of a few days. The tempo and volume of systems UNC3944 accesses can overwhelm security response teams,” Mandiant explained.

“Once obtaining a foothold, UNC3944 often spends significant time searching through internal documentation, resources, and internal chat logs to surface information that could help facilitate escalating privileges and maintaining presence within victim environments. UNC3944 often achieves privilege escalation by targeting password managers or privileged access management systems.”

During ransomware attacks examined by Mandiant, the hackers tend to target specific virtual machines and other systems that will cause significant impact to victims and force them to pay ransoms.

In the past, they have contacted company executives and employees with threatening messages, even infiltrating communication channels being used by victims to respond to incidents in some instances.

Mandiant said in the majority of cases where they identified the initial point of access, the hackers obtained credentials after a smishing attack.

Using the stolen credentials, the hackers impersonated employees during calls with help desk officials, who provided MFA codes or password resets.

They managed to obtain personal information about the employee being impersonated that allowed them to answer security questions posed by help desk officials.

“In one incident, UNC3944 social engineered the IT help desk to get the MFA token reset for account credentials that may have been exposed on a laptop used by an IT outsourcing company contracted by the victim organization,” the researchers said.

“Mandiant determined that RECORDSTEALER credential theft malware was installed on this laptop through a fake software download only a few weeks prior. UNC3944 typically uses stolen credentials to then establish a foothold on victim environments.”

The hackers also use their access to internal systems to create phishing pages that look like legitimate single sign-on pages or service pages, fooling other employees into handing over even more credentials.

In addition to their skilled use of impersonation, Mandiant said it has identified three phishing kits that allow the hackers to send stolen credentials to a Telegram channel controlled by the actors, deploy remote management software onto a victim device and more.

UNC3944 has been seen using other credential theft tools, infostealers and data miners to move laterally within victim networks

“A common hallmark of UNC3944 intrusions has been their creative, persistent, and increasingly effective targeting of victims’ cloud resources,” Mandiant said.

“This strategy allows the threat actors to establish a foothold for their later operations, perform network and directory reconnaissance, and to access many sensitive systems and data stores while having minimal interaction with what some organizations would traditionally consider their internal corporate network.”

Mandiant warned that the hackers continue to evolve their skill set and take advantage of internal system tools to perpetrate their attacks. The researchers said defenders should expect that these hackers will continue to improve their tradecraft and may expand their relationships with other groups for more support.

Its initial success is likely what emboldened it to expand to attacks that are more disruptive and profitable, Mandiant said, noting that the expansion into ransomware and extortion was likely to lead to the use of other strains and methods of monetization to maximize profits.

AlphV dispute

A [report](#) from cybersecurity company Group-IB said a recent phishing campaign by the group resulted in 9,931 accounts from more than 136 organizations being compromised — including [Riot Games](#), [Reddit](#) and [Twilio](#). While UNC3944 was initially identified as involved only in data theft, in recent months they allegedly have coordinated with the BlackCat/AlphV ransomware gang — with several recent victims [showing up on the group’s leak site](#).

Members of the group spoke to the [Financial Times](#) and [TechCrunch](#) last week, claiming their original goal was to attack MGM’s slot machines only and use paid mules to slowly milk the devices. But when that failed, they turned to their tried-and-true methods of attack, eventually encrypting the company’s systems.

According to Telegram conversations with both outlets, the hackers were able to exploit remote login software and leaked VPN account information from MGM employees to move throughout the company’s system.

AlphV has since [come out](#) to dispute these claims and deny that anyone connected to them spoke to news outlets – causing confusion and igniting claims that the gang was either attempting to take credit for the MGM attack back from UNC3944 or attempting to draw law

enforcement scrutiny away from the hackers.

- [Cybercrime](#)
- [Industry](#)
- [News](#)

Get more insights with the
Recorded Future

Intelligence Cloud.

[Learn more.](#)

No previous article

No new articles

Jonathan Greig



Jonathan Greig is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.