The Scattered Spider Ransomware Group's Secret Weapons? Social Engineering and Fluent English

ransomware.org/blog/the-scattered-spider-ransomwares-secret-weapons-social-engineering-and-fluent-english/

September 28, 2023

In a matter of weeks, a ransomware group with the unusual name "Scattered Spider" has become the hot threat group of the moment.

Also known as "UNC3944," **"**Scatter Swine," and "Muddled Libra" (cybersecurity companies identify groups independently so, confusingly, they end up assigning them different names), this blog recently covered the group's handiwork in the extraordinary extortion raid on Las Vegas casinos belonging to MGM Resorts International.

But who is Scattered Spider and why is the group interesting beyond a few sensational headlines?

Initial Aim of Attack

A new claim has since emerged in the *Financial Times (FT)* newspaper that the initial aim of the MGM Resorts attack was not extortion but to manipulate slot machine software directly for gain. Mules were to be recruited to visit the casinos where they would gamble and win money against the house on these modified machines. This proved harder than expected so the group fell back on the traditional playbook of encryption, date exfiltration, and extortion.

An odd turn for ransomware, perhaps, but combined in-person and malware attacks have been used to target ATM cash machines in the past. As for remote manipulation, criminals have regularly used this concept to skim card numbers from retail point-of-sale terminals.

What's more intriguing is that Scattered Spider came up with such a wacky idea in the first place. It was never likely to work—casinos are famously paranoid about unusual patterns of winning by customers—but it is possible to detect cunning lateral thinking in its ambition.

Social Engineering

But the most notable aspect of Scattered Spider's tactics is the aggressive use of social engineering. For most of the time since it was first noticed in 2022, Scattered Spider looked like any other successful ransomware group, targeting a mixture of software vulnerabilities, password exploits, and phishing to get behind defenses. More recently, however, the group seems to have shifted to voice phishing (or "vishing," a tactic used in the MGM Resorts attack), SMS phishing (also known as "smishing"), SIM swapping, and to targeting multifactor authentication (MFA) and the Okta identity management platform.

There is even evidence that Scattered Spider has started tricking victims into installing remote monitoring and management (RMM) tools in the style of fake online support scams. All of these human-targeted tactics are clever because they can't easily be detected using conventional security layers.

And yet the most ominous innovation of all is one that's easily missed—group members appear to speak fluent English.

Speaking Fluently

The English language has never been a strong point of the average (often Russian) threat group. Scattered Spider, it seems, is the exception. The most likely reason? Perhaps the group is running bad English through ChatGTP. Alternatively., some of its members might really be native speakers from countries such as the United States or the United Kingdom. Good English communication doesn't make Scattered Spider's attacks more dangerous, but it does perhaps bring them closer to home. We've grown used to associating ransomware with Russia and its satellite countries. If that's changing, this suggests the criminal mindset behind it might be spreading out of sight.