The Diamond Model of Intrusion Analysis: Twilio Breach

Jairo Carbonell
jcarbonell9@gatech.edu

***Abstract*—**Technological advances in automated phishing, AI-driven deception, and adoption of remote work worldwide have significantly increased identity-based cyberattacks. According to the CrowdStrike 2024 Global Threat Report, three out of every four attacks now rely on valid credentials rather than malicious software.[1] This paper analyzes the Scattered Spider hacking group and precisely how its subdivision, oktapus, executed a targeted phishing operation against Twilio by using SMS-based schemes to obtain employee credentials through social engineering. We use the diamond model to understand better the adversary tactics, the victim's (Twilio's) vulnerabilities, and the social-political and technical environment facilitating the attack. Additionally, this analysis delves into a policy assessment to highlight the need for industry-level policy change to provide a safer, interconnected digital world.

1 INCIDENT DESCRIPTION

Starting mid-July 2022, current and former Twilio employees received smishing text messages on their mobile phones from malicious actors. These actors pretended to be Twilio IT administrators, asking users to click on a link for fake reasons such as the user's password expiring or their schedule changing.

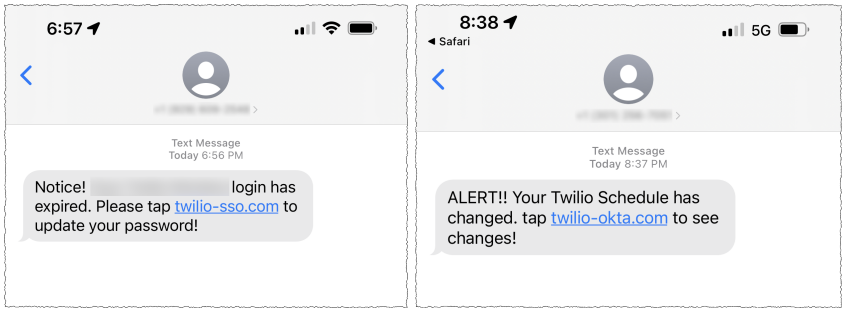

***Figure 1*—**From Twilio's Incident Report

1 Forbes article referencing CrowdStrike 2024 Global Threat Report

The links led to fake Okta login pages that mirrored Twilio's legitimate Okta login page. These fake Okta login pages were hosted on domains created by the malicious actors, such as twilio-sso.com, twilio.net, twilio.org, sendgrid-okta.org, twilio-okta.net, and twilio-okta.com.[2] Then, some of Twilio's employees fell for the trick and entered their username, password, and MFA code, which the malicious actors used to access internal Twilio administrative tools to pivot and launch subsequent supply chain attacks.

Based on Twilio's Incident Report findings, Twilio was first aware of the unauthorized access on August 4, 2022, and the last observed unauthorized activity in Twilio's systems was on August 9, 2022. It was discovered that the malicious actors accessed Authy, an MFA provider owned by Twilio, where 93 users had their accounts accessed and additional devices registered by the malicious actors.[3] These actors also accessed Twilio's customer support console connected to hundreds of services like Signal, meaning that approximately 1,900 users had their phone numbers revealed as being registered to a Signal account or had their SMS verification code used to register with Signal revealed.[4] Out of those 1,900 users, the malicious actors only searched for three numbers, and the affected customers confirmed that only one of those three users had their accounts re-registered.

Okta's Defensive Cyber Operations analysis discovered these actors looked up 38 unique phone numbers in the Twilio customer support console, almost all linked to a single targeted customer.[5] After reviewing the logs, Okta concluded that these actors were looking to expand their access into the targeted customer's Okta tenant by using previously stolen customer credentials to trigger SMS-based MFA challenges and then using Twilio systems to retrieve the one-time MFA passcode sent. Okta's analysis confirms that the remaining exposed phone numbers and one-time MFA passcodes outside the targeted activity were not used and considered incidental. In this paper, we'll continue to review how oktapus successfully breached Twilio systems. But with the rise of identity-based attacks across the industry, all organizations should take this as a warning of what can happen despite all of the security controls you can place within an organization, and industry-level changes need to happen to safeguard our identity and data.

2 Twilio's Incident Report
3 Cyber Security Hub Article
4 Signal's Incident Report
5 Okta's Defensive Cyber Operations

2 DIAMOND MODEL ANALYSIS

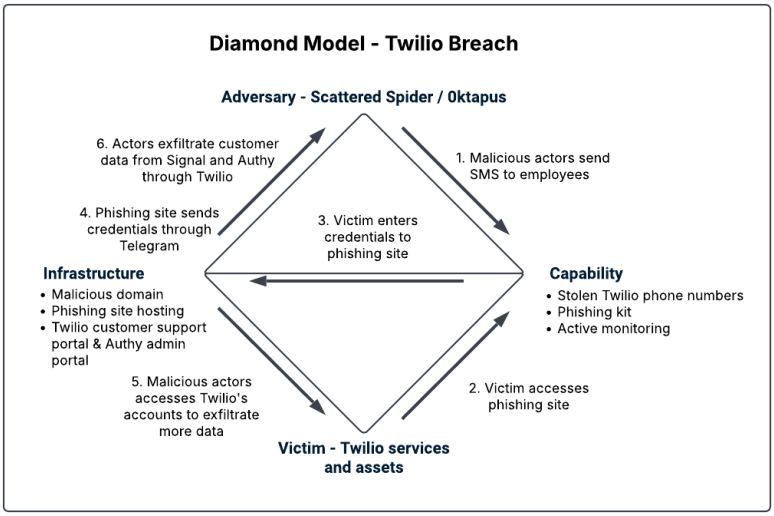

Figure 2—A diamond model diagram for the Twilio breach

2.1 Adversary

After further investigation and with the assistance of Group-IB Threat Intelligence, the adversary operator was discovered and codenamed oktapus by Group-IB researchers.[6] Group-IB produced a list of phishing domains and organizations oktapus had attacked. Despite the attack using low-skill methods, oktapus got its tentacles inside many well-known organizations alongside Twilio.

In the following years, law enforcement has been trying to close in on the hacker group, and those in the cybersecurity industry have noticed oktapus members overlapping other data breaches using different methods, which eventually grouped oktapus under the umbrella group of hackers called Scattered Spider.[7] Since the group was very active and successful, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the FBI issued an advisory in late 2023 with details of the group's latest activities, techniques, and provides recommendations to lessen the amount of organization getting breached by malicious actors.[8]

It took until November 20, 2024, for law enforcement to unseal criminal charges against five alleged Scattered Spider members aged 20-25. United States Attorney

6 Group-IB oktapus Research
7 CrowdStrike Scattered Spider Research
8 Joint Cybersecurity Advisory - Scattered Spider

Martin Estrada said, "... this group of cybercriminals perpetrated a sophisticated scheme to steal intellectual property and proprietary information worth tens of millions of dollars".[9] The FBI is still investigating these matters as the case is being prosecuted, and if convicted, each member will face jail time.

The discovery of younger malicious actors, even minors, being recruited into the hacking group has led to the realization that Scattered Spider did not start alone. While, for the most part, Scattered Spider can be considered both the adversary operator and customer in recent attacks, there have been some members with relationships to the more extensive adversary customer, The Com, of approximately 1,000 individuals responsible for directing different hacking group operators.[10] Scattered Spider has since evolved out of The Com after successfully developing identity-based intrusion techniques to conduct multiple high-profile breaches. Despite the investigation of key members, we still see Scattered Spider techniques being used in attacks today.

2.2 Victim

As Scattered Spider conducted a widespread smishing campaign and supply chain attack, various targeted victims existed throughout the attack lifecycle. For this paper, we'll explore the attack on Twilio and its effects.

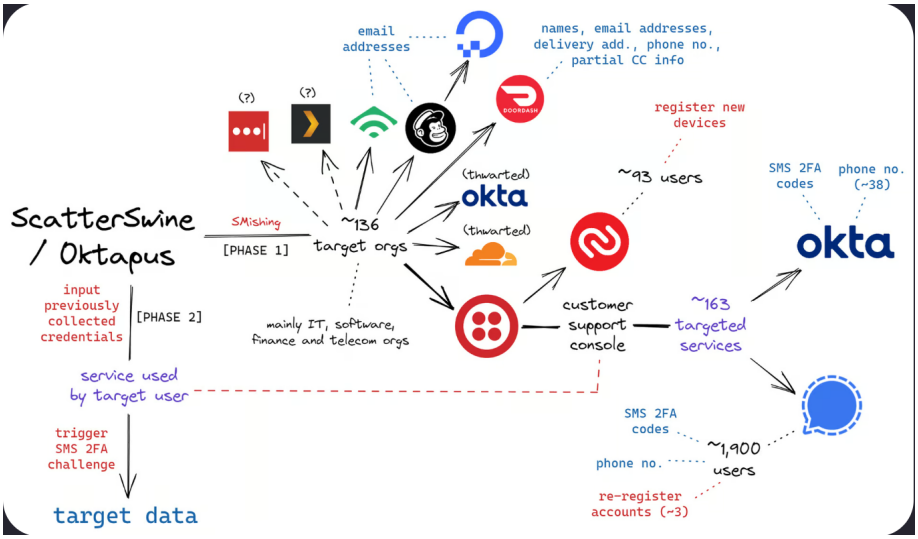

Figure 3—From Wiz's Twilio Incident Review

9 U.S. Attorney Press Release

10 Defending Against SCATTERED SPIDER and The Com with Cybercrime Intelligence

2.2.1 *Victim Persona*

Scattered Spider targeted Twilio, a customer engagement platform used by over 300,000 global enterprises and digital disruptors, plus more than 10 million developers worldwide, to build unique, personalized experiences for their customers.[11]

The malicious actors also targeted other victim personas' through Twilio using internal applications and services. For example, Authy, owned by Twilio, had 93 compromised accounts. Through Twilio's customer support portal, they could target an additional 163 services, but only Signal and an undisclosed customer's Okta tenant were explored in the attack.

2.2.2 *Victim Asset*

The main asset that the adversary directed their capabilities to was the phone numbers of Twilio's current and former employees. The successful breach of Twilio led the adversary to target Twilio's customers through internal assets such as Twilio's customer support console and Authy.[12] This led to more asset discovery where 93 Authy accounts had the malicious actors' devices registered, 1900 Signal phone numbers and SMS verification codes were exposed, and 38 unique numbers tied to a specific customer were searched in the Twilio support console in attempts to capture the Okta SMS MFA passcode sent through Twilio.

2.2.3 *Victim Susceptibilities*

The attack on Twilio was successful due to the lack of user training around social engineering and detecting phishing domains, which led to employees disclosing their credentials to malicious actors. Also, the lack of stricter security controls, such as preventing untrusted networks from accessing internal applications and the lack of phishing-resistant MFA, allowed the attackers to reach far more with Twilio than other organizations breached by Scattered Spider.

2.3 Capabilities

Scattered Spider techniques do not take much skill to deploy, but their success relied on having real phone numbers of active employees to smish. It is still unknown how the actors could obtain active employee mobile numbers, as there is

11 Twilio Research Center

12 Twilio Incident Report

no direct evidence that the group orchestrated a breach to get the phone numbers prior. In the months leading up to the attack, a separate hacker was able to exfiltrate Twitter data, stealing email addresses and phone numbers tied to celebrities and companies.[13] Therefore, Scattered Spider were capable of locating or having enough money to buy stolen data from other breaches to use in their own attacks.

The actors were capable of stealing stolen credentials through the use of phishing kits. Group-IB located a copy of the phishing kit through Virustotal as a member of the hacker group scanned the link of where they uploaded the phishing kit to a file hosting service, Pomf.cat, which Group-IB was able to retrieve to analyze the kit.[14] Group-IB discover the stolen credentials were being sent to a Telegram channel. This meant these actors were actively monitoring communication channels to be capable of breaching accounts before the MFA code expired.

2.4 Infrastructure

Scattered Spider used physical and logical communication structures to deliver and maintain control of capabilities. First, through service providers like domain and hosting resellers, the actors were able to register malicious domains with Twilio's name and keywords like SSO and MFA in the domain. Then, the actors pointed the domains to their phishing site location, obtained from hosting resellers, and sent stolen credentials through Telegram.[15] These type 2 infrastructures allowed the malicious actors to compromise Twilio's employee accounts to pivot further into the supply chain attack.

Once the actors were inside Twilio's system, they were able to use Twilio's internal assets, Authy and Twilio's customer support portal, as type 2 infrastructures to continue their attack into targeted services like Signal and Okta. After they found vulnerable accounts to compromise, the actors registered their own devices, type 1 infrastructure, to Authy and Signal accounts to maintain persistent access.[16] Twilio had to contact affected users and reset all devices linked to compromised accounts.

13 5.4 million Twitter accounts reportedly on sale
14 Group-IB oktapus Research
15 Group-IB oktapus Research
16 Twilio Incident Report

3 SOCIAL-POLITICAL META-FEATURE

To better understand the adversary-victim relationship between Scattered Spider and Twilio, we can compare cyber-economic gain and influence in the hacker communities. As we noted earlier, these actors were aged 20-25, generally when one does not have much money and is susceptible to more experienced peers. Since the hacking techniques used can alert security systems and can be remediated through stricter security controls such as blocking external VPN network connections and enforcing phishing resistance MFA, the adversaries used a semi-persistent approach, employing smash-and-grab tactics to register malicious devices to accounts and exfiltrate as much data as possible before security teams put an end to it. Twilio and similar organizations were targeted due to its popularity and use across the industry in digital communications. Twilio's direct integrations with customers' environments make them a lucrative victim. Organizations using Okta that integrate with customers are in the same shared threat space, and the same techniques can be used to exfiltrate data if an organization is not adequately protected or if users are not trained to detect these types of attacks.

4 TECHNOLOGY META-FEATURE

Since Scattered Spider targeted many organizations, we can learn how the technology meta-feature played a pivotal role in the Twilio breach, as it bridges the adversary's capabilities with the operational infrastructure used to execute the attack. For example, using SMS allowed adversaries to bypass standard email security controls to reach targets directly and exploit users' trust in mobile devices. Service providers enable this infrastructure with domain registration and web hosting technologies. Scatter Spider rapidly changed IPs, domain names, and hosting providers to ensure phishing kits had enough time to capture credentials while avoiding immediate detection and takedown. Because stolen MFA codes can expire if the actors are not actively monitoring, they are likely using automation and AI to test for valid credentials.

5 POLICY ASSESSMENT AND RECOMMENDATIONS

The attacks by Scattered Spider around the world demonstrate the sophisticated nature of emerging cyber threats, especially identity-based intrusions through social engineering techniques. While we are seeing policy changes at the national and transnational level, and key members of the Scattered Spider group are being

prosecuted, we are still seeing the same techniques used in many attacks today due to members joining other hacking groups like the RansomHub RaaS group as noted by GuidePoint Security.[17] To best address this problem, we need policy changes at the industry level, rated at 8.5 on the governance scale, given the shared threat space across organizations worldwide, which necessitates a unified response to mitigate such threats effectively.

To combat these risks effectively, we must first implement a comprehensive framework for SMS similar to the DMARC and DKIM frameworks for email security. For example, Apple unveiled the upgraded iMessage with PQ3, a groundbreaking post-quantum cryptographic protocol that advances the state of the art of end-to-end secure messaging.[18] This improvement also includes individually signing each message to ensure the receiving device verifies the mapping between the sender's identifier and the public key used for signature verification. This means that if both users have the feature enabled, their devices can confirm if the incoming text is from a legitimate contact. However, because not everyone has an iPhone or has the feature enabled, it will take time before the industry catches up to Apple.

A more feasible recommendation is to push for industry-wide adoption of phishing-resistant authenticators such as Okta FastPass or YubiKeys with passwordless authentication through biometrics. These solutions offer stronger protection and a more user-friendly experience, reducing human error and the risk of phishing.[19] However, recognizing that not all organizations have the resources to harden their security posture, it all comes down to service providers such as domain and hosting resellers taking more responsibility to prevent malicious actors from using their services. It is not enough to simply state in the provider's terms of agreement to avoid using services for malicious activity. Even then, a Trend Micro Research report found official resellers with legitimate clientele advertising services in underground forums to cater to cybercriminals, either with or without the provider's knowledge.[20] While the world is moving in the right direction to combat the latest identity-based threat, we will continue to see these attacks without policy changes at the industry level.

17 Worldwide Web: An Analysis of Tactics and Techniques Attributed to Scattered Spider
18 iMessage with PQ3: The new state of the art in quantum-secure messaging at scale
19 Why Phishing-Resistant MFA Is No Longer Optional: The Hidden Risks of Legacy MFA
20 Hacker Infrastructure and Underground Hosting 101

6 REFERENCES

1. *5 Defendants Charged Federally with Running Scheme that Targeted*. (2024, November 25). https://www.justice.gov/usao-cdca/pr/5-defendants-charged-federally-running-scheme-targeted-victim-companies-phishing-text
2. Baker, J., & Baker, J. (2024, October 25). *Worldwide Web: An Analysis of Tactics and Techniques Attributed to Scattered Spider*. GuidePoint Security. https://www.guidepointsecurity.com/blog/worldwide-web-an-analysis-of-tactics-and-techniques-attributed-to-scattered-spider/
3. *Blog - iMessage with PQ3: The new state of the art in quantum-secure messaging at scale - Apple Security Research*. (n.d.). Blog - iMessage With PQ3: The New State of the Art in Quantum-secure Messaging at Scale - Apple Security Research. https://security.apple.com/blog/imessage-pq3/
4. Bradley, T. (2025, February 12). *Data reveals Identity-Based attacks now dominate cybercrime*. Forbes. https://www.forbes.com/sites/tonybradley/2025/02/12/data-reveals-identity-based-attacks-now-dominate-cybercrime/
5. *Detecting Scatter Swine: Insights into a Relentless Phishing Campaign*. (2022, August 25). Okta Security. https://sec.okta.com/articles/scatterswine/
6. Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), & Spider, S. (2023). Joint Cybersecurity Advisory: Scattered Spider Threat Actors Targeting Commercial Facilities Sectors and Subsectors. In *Joint Cybersecurity Advisory* (Vols. AA23–320A, pp. 2–14) [Report]. https://www.cisa.gov/sites/default/files/2023-11/aa23-320a_scattered_spider_0.pdf
7. *Hacker Infrastructure and Underground Hosting 101:Where Are Cybercriminal Platforms Offered?* (n.d.). https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hacker-infrastructure-and-underground-hosting-101-where-are-cybercriminal-platforms-offered
8. Powell, O. (2022a, July 27). 5.4 million Twitter accounts reportedly on sale in hacking forum | Cyber Security Hub. *Cyber Security Hub*. https://www.cshub.com/attacks/news/54-million-twitter-accounts-reportedly-on-sale-in-hacking-forum
9. Powell, O. (2022b, September 1). Oktapus attack on Twilio exposes data of 163 companies | Cyber Security Hub. *Cyber Security Hub*. https://www.cshub.com/attacks/news/oktapus-attack-on-twilio-exposes-data-of-163-companies

10. *Roasting 0ktapus: The phishing campaign going after Okta identity credentials | Group-IB Blog*. (2025, March 26). Group-IB. https://www.group-ib.com/blog/0ktapus/
11. Security. (2024, January 26). *Incident report: Employee and customer account compromise*. Twilio. https://www.twilio.com/en-us/blog/august-2022-social-engineering-attack
12. Team, C. I. (n.d.). *SCATTERED SPIDER Attempts to Avoid Detection with Bring-Your-Own-Driver Tactic*. https://www.crowdstrike.com/en-us/blog/scattered-spider-attempts-to-avoid-detection-with-bring-your-own-vulnerable-driver-tactic/
13. The Hacker News. (n.d.). *Why Phishing-Resistant MFA Is No Longer Optional: The Hidden Risks of Legacy MFA*. https://thehackernews.com/2024/10/why-phishing-resistant-mfa-is-no-longer.html
14. Twilio. (2025, March 26). *What is Twilio? An introduction to the leading customer engagement platform*. Twilio. https://www.twilio.com/en-us/resource-center/what-is-twilio-an-introduction-to-the-leading-customer-engagement-platform
15. *Twilio Incident: What Signal Users Need to Know*. (n.d.). Signal Support. https://support.signal.org/hc/en-us/articles/4850133017242-Twilio-Incident-What-Signal-Users-Need-to-Know
16. Zeltser, L. (2025, January 13). *Defending Against SCATTERED SPIDER and The Com with Cybercrime Intelligence*. https://www.sans.org/blog/defending-against-scattered-spider-and-the-com-with-cybercrime-intelligence/