ANNOUNCEMENT

Executive Intelligence Update – Oct. 31, 2023

Published: 30 Oct 2023 22:21:44 UTC

Intel 471's Executive Intelligence Update gives CISOs and security teams insight into trends, threats, risks and regulations. In this issue:

- Scattered Spider Makes Graphic, Violent Threats
- Okta Customers Concerned After Another Breach
- Targeting Supply Chains Could be More Lucrative for Ransomware
- Android Malware Looks to Defeat Anti-Fraud Controls

1. Scattered Spider Makes Graphic, Violent Threats

What's happening: Scattered Spider, a spooky group of English-speaking threat actors that use social engineering and short message service (SMS) phishing to gain access, combines its ransomware and extortion campaigns with intimidating harassment and threats of violence.

Family members threatened: Scattered Spider is also known as Octo Tempest, 0ktapus, Roasted 0ktapus, UNC3944 and Scattered Swine. The group has attacked more than 100 organizations since 2022, conducting SMS phishing attacks and duping information technology (IT) help desks into reassigning multifactor authentication (MFA) tokens to new devices, removing MFA and other account-related manipulations. The group elevated its attacks by aligning with the ALPHV aka BlackCat ransomware-as-a-service (RaaS) group, recently conducting attacks against MGM Resorts International and Caesars Entertainment. In an extensive new Microsoft report, the company says the group resorts to fearmongering in rare instances and targets "specific individuals through phone calls and texts. These actors use personal information, such as home addresses and family names, along with physical threats to coerce victims into sharing credentials for corporate access." In a screenshot of one message within the blog post, a Scattered Spider member threatens that if a victim doesn't reveal their credentials, the group will send a "shooter" to the person's house. The next message warns: "Ur wife is gonna get shot if u dont fold it. Lmk. [let me know]." Researchers have documented a worrying progression of some threat actors particularly in the subscriber identity module (SIM) swapping-cryptocurrency theft scene moving to real-life physical attacks, including brickings and firebombings.

Intel 471's view: It's not unusual for threat actors to use other tactics to increase the pressure on ransomware or extortion victims in order to achieve a payout. Ransomware groups exfiltrate sensitive information such as payroll and human resources (HR) data, which often means they have the phone numbers of top executives and their email addresses. Threat actors have sent WhatsApp messages to executives, and if the organizations didn't pay, released screenshots of those messages. Employees have also received direct threats concerning their family members. These actions take these attacks to a highly personal, unnerving angle, and organizations should expect this to happen and incorporate it into their tabletop exercises. Scattered Spider relies heavily on the success of its social engineering. We hear much about its successes, but the group fails a lot, too. Its attempts can be defeated by strong processes: requiring a video call, for example, before an MFA token is reset on a super admin Okta account. As Microsoft notes in its report, one of the sources for the group's initial access is initial access brokers (IABs). By monitoring underground advertisements for access, organizations can potentially reset account credentials before threat groups such as Scattered Spider can buy the access and start lateral movement within systems. Organizations can also warn their employees that actors may target them directly and use harassment to get them to reveal login credentials.

2. Okta Customers Concerned After Another Breach

What's happening: Identity and access giant Okta suffered a breach that compromised session tokens for several of its customers. The breach shows the extent to which threat actors are going to understand customer support processes used by identity vendors and spotting opportunities for novel supply chain intrusions.

Not-so-hardy HAR: This is yet another Scattered Spider-like tale of threat actors wedging themselves deep in systems to gain access. In this case, threat actors gained access to an Okta customer support system. If a bug occurs, Okta asks its customers to upload HTTP Archive (HAR) files for troubleshooting. HAR files are a recording of a web browser's interaction with a service, and the data includes session tokens and cookies. After a BeyondTrust employee shared a HAR file with Okta, just 30 minutes later a threat actor tried to create an admin account on BeyondTrust's Okta with the Okta session token in that HAR file (BeyondTrust's post-mortem is here). 1Password was affected. 1Password writes that the same day the HAR file was uploaded, the attacker stole the uploaded session token and tried several

actions, including updating an identity provider (IDP) tied to 1Password's production environment. The attacker requested a report about admin users, but that triggered an email to someone on the company's IT team, and 1Password started to unwind what had occurred from there. Cloudflare was also affected, posting a sassy after-action review titled "How Cloudflare mitigated yet another Okta compromise." Cloudflare described this latest breach (it was impacted by an Okta incident in January 2022) as "troubling," but wrote that none of its customers' information was affected. Okta's position is that customers should be excising cookies and session tokens before uploading the HAR files.

Intel 471's view: What's remarkable is that BeyondTrust, 1Password and Cloudflare each prevented attackers from capitalizing on replaying stolen session tokens due to layered defenses and alerting. We'd encourage identity and access management teams to read the blog posts from those companies, which give detailed insight into what alerted each one to a problem and allowed them to approach Okta with strong clues that the issues were on Okta's side. The posts also have excellent tips for defense. For example, 1Password undertook several actions post-incident, including reducing session times, reducing the number of Okta super admins and beefing up alerts. Stepping back, this incident again shows how certain groups of threat actors are patiently working to understand how they can insert themselves into vulnerable processes. Some have suggested that Okta's advice about redacting HAR files is difficult to accomplish. Perhaps there is another way to solve support tickets without sharing data that includes session tokens.

3. Targeting Supply Chains Could be More Lucrative for Ransomware

What's happening: A study of ransomware attacks on integrated supply chains found that attacks targeting firms that are critical parts of supply chains could generate higher payouts. The conclusion suggests that organizations linked in supply chains may derive more defensive strength from closer collaboration.

Collective defense: The study sought to figure out the maximum ransom that affected firms would be willing to pay as part of a ransomware attack impacting a supply chain. The study doesn't come to a hard figure of what the ransom would be but concludes that ransomware attacks based on the relationships of the suppliers could mean higher payouts. If attackers can only breach one firm in a supply chain, they're best to hit one in a hub-and-spoke relationship – think a vehicle manufacturer with direct suppliers. But if the criminals can breach multiple firms, they're best to target a chain or line network. The study suggests some defense strategies. The authors say that it could make financial sense to actively invest in the cybersecurity of suppliers rather than just take a more passive interest. Another idea might be group insurance policies that cover a whole supply chain, although the authors note that this might incentivise attackers. They also suggest that working to diversify and decouple risks that could occur from a supply chain attack can limit the damage from a breach.

Intel 471's view: Threat actors have long realized there is leverage in compromising supply chains. The breach of one firm can have downstream effects on another firm. Building a threat intelligence program that is capable of monitoring the attack surfaces of partners can mean averting a damaging breach.

4. Android Malware Looks to Defeat Anti-Fraud Controls

What's happening: Developers of Android banking trojans are shifting tactics to lower their development costs and attempt to defeat increasingly effective mobile anti-fraud solutions.

Keyloggers are cheaper: Android malware developers are moving away from the traditional account takeover (ATO) modus operandi, based on web-inject attacks, to using keyloggers instead. A keylogger is a tool or software that records the keystrokes a user makes and can operate without the user's knowledge, remaining hidden in the background. The Android malware SharkBot, for example, cancels the authentication feature in banking apps that allow users to perform a biometric authentication, enabling it to collect login credentials with the keylogger. It's an easier way to conduct ATO, as creating web-inject overlays requires frequent development and tweaking. Another recent trend in the Android malware threat landscape: Threat actors are looking to perform on-device fraud (ODF) to attempt to defeat better anti-fraud controls. Most notable mobile malware strains now are equipped with remote access features. This allows for more automated cyberattacks that streamline the fraud process by using advanced features such as virtual network computing (VNC) and automated transfer systems (ATSs). This indicates an imminent challenge for financial institutions as more malware strains might soon adopt these techniques.

Intel 471's view: Threat actors are relentlessly searching for ways to maximize unauthorized data access while minimizing detection and operational costs. With the adoption of features such as VNC and ATS, the fraud process may become even more streamlined. While ATS adoption is not yet mainstream, the potential of eliminating human intervention suggests we might witness more malware strains using this method. Out-of-band MFA is a first-line defense against keyloggers, and other ways to avoid mobile malware include not downloading applications from third-party services, being stingy with app permissions and updating operating systems (OSs). It's worth financial services companies reinforcing the latter two points with their customer bases. For this full report on Android mobile malware, please contact Intel 471.