Defender Experts Chronicles: A Deep Dive into Storm-0867

techcommunity.microsoft.com/t5/microsoft-security-experts-blog/defender-experts-chronicles-a-deep-dive-into-storm-0867/ba-p/3911769

Aug 28 2023 10:04 AM

BACKGROUND

At Microsoft, we are always on the lookout for advanced and emerging threats that could compromise the security of our customers. This has pushed our Defender Experts for XDR team to constantly stay vigilant, monitoring and responding to incidents with speed and efficiency. In late May 2023 (See Fig. 1), we encountered a surge in cases involving highly sophisticated adversary-in-the-middle (AiTM) attacks. This attack involves an attacker intercepting and manipulating the communication between two parties, such as a user and a server. The team quickly unmasked the face behind these attacks: Storm-0867, a threat actor that per Microsoft Threat Intelligence has been active since 2012 and has targeted various industries and regions with different tactics, techniques, and procedures (TTPs). Our team reacted swiftly in triaging and prioritizing the cases related to Storm-0867, with the aim of protecting our customers from this adversary.

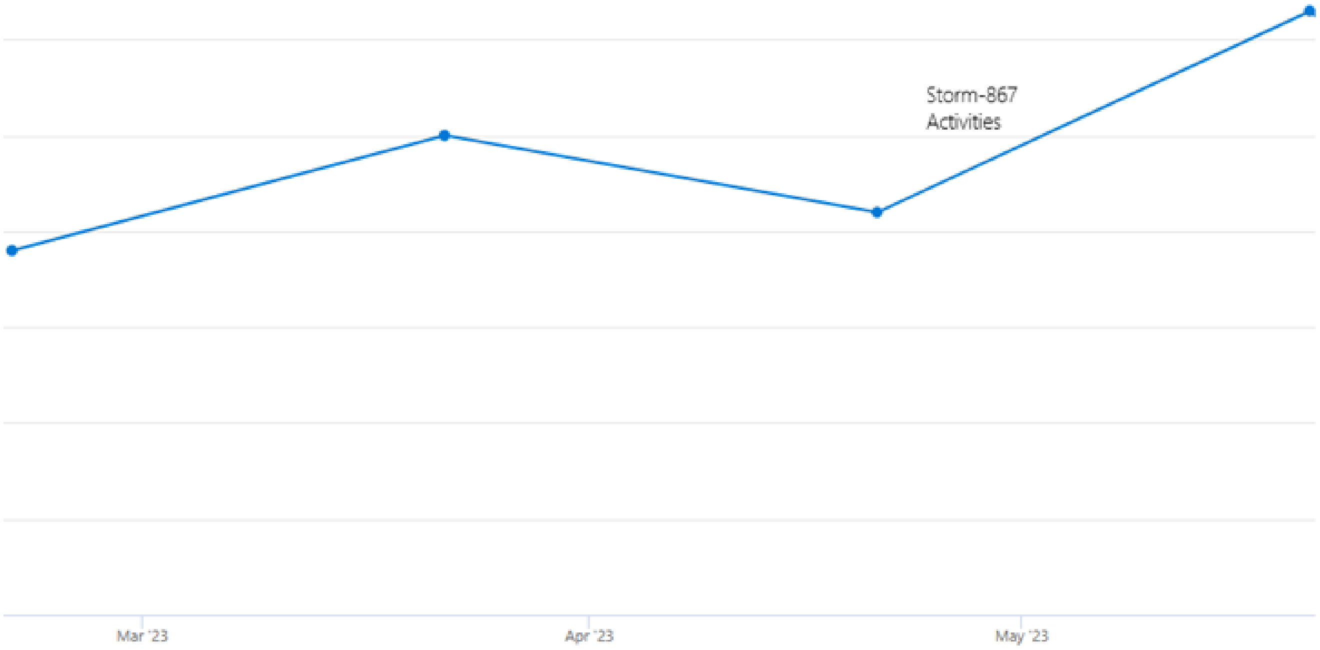

Figure 1: Significant uptick in Storm-867 activities

THE ADVERSARY

Storm-0867 has been launching sophisticated phishing campaigns for years. By employing various social engineering techniques and malicious infrastructure, the adversary tricks and manipulates its victims. Based on Microsoft’s intelligence, the Defender Experts for XDR team was aware of the potential damage this threat could cause for our customers. Storm-0867’s deceptive tactics, along with its use of the phishing as a service (PhaaS) platform called Caffeine, allowed it to carry out a multitude of AiTM-based attacks. These attacks involved intercepting and altering the communication between users and legitimate services, such as email providers or cloud applications. By doing so, Storm-0867 was able to steal passwords, hijack sign-in sessions, bypass multifactor authentication (MFA), and modify MFA methods. Such successful campaigns have caused financial losses and reputational harm across different sectors, including banking and financial services.

TRIAGE AND INVESTIGATION

The experts started the triage process by reviewing the associated triggered alerts. Each alert was meticulously examined to comprehend the adversary’s tactics, techniques, and procedures (TTPs). The team inspected the attack chains to extract the malicious URLs and the rest of the adversary infrastructure used in the attack.

The identification of the URLs, their patterns, and the redirections leading to the final phishing sites enabled the team to recognize the tactics employed by the actor. Additionally, by delving deep into the telemetry data of the URLs that were clicked or accessed by potential victims, the team unraveled the affected entities and the initial attack vectors that led to the compromise.

The experts then mined the telemetry and scoped the incident to understand the impact at the organization level.

Armed with key insights from Microsoft's intelligence, the experts verified the findings against known patterns of Storm-0867's activities. In parallel, they employed advanced techniques for deep-dive investigations. They explored network and endpoint telemetries, observed impacted users’ behaviors and their authentication activities, correlated these findings, and sought additional traces or footprints of the adversary’s movements. Each piece of data played a pivotal role in forming a comprehensive understanding of the attack chain.

Throughout the investigation, real-time data analysis and sharing of threat intelligence among team members enhanced our collaborative approach to triaging the incidents and solving the puzzle.

Our experts worked carefully to evaluate each case, utilizing a systematic triaging approach to promptly recognize the most pressing incidents that required immediate attention. Prioritizing cases based on risk, severity, and potential impact ensured that the team's efforts remained focused on dissecting and addressing the most prominent threats to our customers.

FINDINGS

The team was quick to assess that the attack flow was in fact associated with Storm-0867's phishing campaigns. The consistent usage of the Caffeine platform, which allows Storm-0867 to create dynamic and customized phishing pages that mimic the appearance of legitimate websites, was a significant indicator.

Storm-0867’s phishing campaigns follow a multi-stage attack flow, as shown in Figure 2. The first stage involves sending emails containing deceptive links enticing them to view seemingly innocuous documents. Once clicked, the links redirect users to the phishing pages powered by Caffeine. The second stage involves stealing the user’s session cookies or capturing credentials when they enter them on the phishing pages.

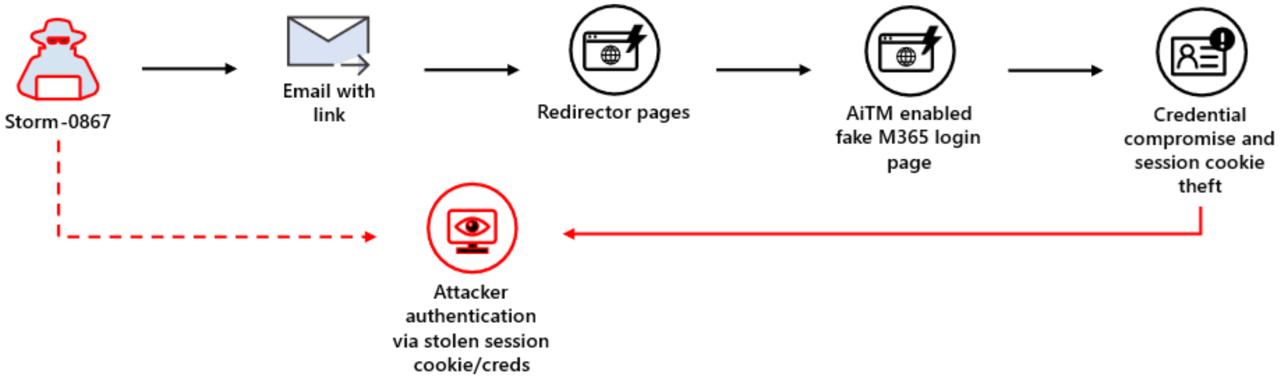
Storm-0867
Email with link
Redirector pages
AiTM enabled fake M365 login page
Credential compromise and session cookie theft
Attacker authentication via stolen session cookie/creds

Figure 2: Storm-0867 attack flow

It can further extend to a third stage where it involves accessing the user’s account and launching further attacks within the organization, such as sending intra-org phishing emails, impersonating the user in business email compromise (BEC) schemes, or exfiltrating sensitive data.

The team’s in-depth analysis of the attack flow revealed significant insights, highlighting the malicious techniques used by the threat actor, as briefly outlined a couple of them below:

1. **Sophisticated Redirection Chains:** Storm-0867's orchestration of redirection chains was a defense evasion technique to trick victims and the underlying detection systems.
2. **Customization through API Calls:** Storm-0867 leverages the capabilities of Caffeine, a PhaaS platform that allows them to create dynamic and customized phishing pages. Caffeine uses API calls to pull content from the target websites and apply them to the phishing pages, creating a realistic-looking login portal. For example, Caffeine can use an API call to get the logo of Microsoft 365 from its official website and display it on the phishing page. This technique makes it difficult for users and detection systems to distinguish between the real and fake pages.

3. **Session Hijacking:** Storm-0867 employs a sophisticated technique called Adversary-in-the-Middle (AiTM), which allows them to hijack the user's session and bypass authentication mechanisms. By intercepting and stealing the user's session cookies, they can access their account without needing their credentials. They can also maintain the session until the user completes the authentication process, avoiding any alerts or notifications. This technique enables them to perform unauthorized actions on behalf of the user, such as sending emails, accessing data, or changing settings.

REMEDIATIONS

Our service was in constant communication with the impacted customers from the time the first incident was generated. The experts contained and remediated the incident by providing the necessary inputs to implement blocklists for the identified phishing infrastructure and other indicators of compromise (IoCs) associated with Storm-0867. This included blocking the malicious URLs, email IDs, and IP addresses that the attackers used to carry out phishing campaigns and access the victims' mailboxes. This proactive measure prevented further access to the attacker-controlled infrastructure and safeguarded our customers' data.

Moreover, our experts provided detailed investigation of the attack and preventive recommendations to the customers. In high impact scenarios, the experts directly reached out to customers via phone calls. The team's active support and guidance ensured that impacted customers remained under close monitoring until the threat was neutralized. This approach effectively sustains the organizations' security posture against Storm-0867.

KEY TAKEAWAYS

The Defender Experts for XDR team was able to successfully detect and mitigate the attack using their expertise. Here are some of the key takeaways from this experience:

1. **Dynamic Threat Landscape:** The threat actor constantly changed their TTPs to evade detection and bypass security controls. They used Caffeine PhaaS to create convincing phishing pages and craftly mimicked legitimate senders and domains. They also used multiple stages of redirection and obfuscation to fool detection systems. This shows that AiTM-enabled attacks are a serious and evolving threat that requires continuous monitoring and adaptive detection mechanisms.
2. **Rapid Managed Response:** The Defender Experts for XDR team quickly came into action to help respond to the affected organizations effectively. The experts provided investigation findings, step-by-step instructions, and one-click remediation actions. By their quick and active response, the Defender Experts for XDR team was able to halt the attack before it could cause more damage.
3. **Context is Key:** Microsoft Threat Intelligence played a pivotal role in providing crucial context to the investigation. Defender Experts for XDR used this context in expanding investigation to ensure comprehensive detection and response.

The Storm-0867 incident unraveled several key insights on how to counter modern cyber threats. We learned that effective and threat intelligence-led triaging, evolving defense strategies, and out-of-band engagements are essential to protect our customers from relentless adversaries. We stand committed to securing the digital future for our customers, undeterred by relentless adversaries.

Learn more about Defender Experts for XDR by visiting **https://aka.ms/DefenderExpertsforXDR**.