CSIS
REST ASSURED

APRIL 18, 2023

MANAGED DETECTION & RESPONSE

Vidar Incident

Info-stealer attack against a leading expert in Microsoft Dynamics 365, Cloud & Data technologies.

THE POWER OF CSIS'S MDR SERVICE

CSIS detected a suspicious file downloaded from a malicious website in the customer's Environment. The executable file and site were posed as legitimate to trick users into installing the malware. The CSIS MDR Analyst Team determined the malware strain, origin, and intent. By acting quickly, the analyst team was able to fully contain and remediate the infection, preventing further spread.

THE ATTACKER'S INTENTION

The main objective of the perpetrators was to trick users into installing the malware and then steal credentials and cookies from the browser. To achieve this, the perpetrators impersonated a legitimate website to trick unsuspecting victims into downloading and installing the malware by posing it as a legitimate tool. The perpetrators abused Google Ads to place multiple sites at the top of search results for legitimate software. These sites also mimicked the legitimate website, making it significantly more challenging to detect deceit.

Bad actors can use stolen credentials to gain access to a company's systems, allowing them to perform whatever attack they desire, such as: deploying Ransomware, exfiltrating confidential data, selling the credentials, social engineering to obtain further access/lateral movement etc.

CSIS IN ACTION

Based on CSIS's constantly evolving detection rules and leveraging Microsoft Defender for Endpoint, the analyst team quickly detected the suspicious file and its execution. CSIS notified the customer immediately through its proprietary Threat Intelligence Portal and a Critical Incident Phone Call.

Continued next page…

Continued from previous page...

CSIS proceeded to take immediate action to ensure both accounts were reset – one being an Administrator-level account – and to isolate the device.

By applying our knowledge of Microsoft Defender, we could accurately determine the behavior of both the user and the malware. Afterwards, we could cross-reference this information with our Threat Intelligence expertise to verify whether any contact was made with the C2 host and whether further malware was downloaded.

CSIS MDR Team obtained the specific malware and determined its exact capabilities through Dynamic Analysis and sandboxing. We provided custom-built Threat Hunting queries to search across the customer environment for further potential infection, lateral movement, and connections to known malicious IPs.

Having assessed the full capabilities of the attack, we performed a forensic investigation using CSIS's proprietary Chronos Collector. We could then fully determine the extent of the attack and its success and verify if any browser credentials had been accessed or exfiltrated.

All required actions were taken rapidly, including blocking the file, resetting user credentials, device isolation, and revoking sessions.

Fortunately, the customer utilized a third-party service for credential storage with encryption and did not rely on browsers to store credentials. It was also confirmed with the customer that no suspicious access of credentials was observed.

OUR HIGHLIGHTS

Info-stealing attacks continue to be prevalent and are one of the most effective ways cybercriminals can compromise an organization. Info-stealing attacks can be extraordinarily well-designed and sophisticated - the biggest challenge is that an attacker only needs one entry point (especially if administrator credentials are obtained) to initiate a severe incident. There is also the challenge of malicious websites being pushed to the top of Google search results, making it seem that the user is accessing a legitimate service. It has been a recent trend for threat actors to use Google Ads to push their malicious or compromised websites to the top of search results to trick users into thinking they are accessing a reliable and authentic website.

Rapid detection and follow-up actions are a must. Info-stealing attacks can become full-blown incidents involving serious damage to an organization, including exfiltrated, destroyed, and leaked data.

It is essential to correctly understand the scale and scope of incidents to ensure that remediation actions are comprehensive and effective.

Utilizing our custom detection rules CSIS was able to rapidly respond and then gain a full understanding of the attack. Furthermore, by exercising CSIS's analyst expertise, we were able to provide additional value by building custom threat-hunting queries tailored specifically to this attack and by performing a forensic examination verifying if any data was compromised.

Find out how we can help your organisation as well

call us +45 8813 6030
or visit www.csis.com/managed-detection-and-response