OMΞGΛ

Threat Actor Report – Initial Findings

Malware Distributor Storm-0324

Date: 9/13/23

Prepared by: Omega Consulting

Email: intel@omegablack.io

Table of Contents

Executive Summary

A threat actor currently being referred to as Storm-0324 is a threat actor that acts as a ransomware access broker. They have recently switched to Microsoft Teams to perform their phishing attacks in order to breach corporate networks. Once Storm-0324 has access to a corporate network they then provide that access to other cybercriminal groups such as FIN7, which has deployed Clop ransomware. Due to the use of teams by our organization as well as it's widespread use across the corporate landscape it is important to be aware of this threat in order to prevent our systems and client systems becoming vulnerable to this group.

Introduction

Storm-0324 is a temporary named assigned by Microsoft to this threat actor. This means that Microsoft does not have high confidence about the origin or identity of the actor behind these operations. Storm-0324 has been around for 8 years. During that time, they used exploit kits and email-based vectors to deliver malware payloads. These payloads include banking trojans (Gootkit, Dridex), information-stealing malware (IcedID, Gozi), ransomware (Sage, GandCrab), and Trickbot.

However, as of July 2023 Storm-0324 has begun using phishing lures sent over Microsoft Teams. These lures contain malicious links that lead to a malicious SharePoint-hosted file. As an access broker Storm-0324 hands off access to breached networks to other threat actors.

Analysis

Recommendations and Conclusion

Some ways to defend against Storm-0324 attacks are as follows:

- Deploy phishing-resistant authentication methods for users.
- Specify trusted Microsoft 365 organization in order to define which external domains are allowed to chat and meet.
- Enable Microsoft 365 auditing enabled so that audit records can be investigated.
- Educate users about social engineering and phishing attacks.

Overall, Storm-0324's latest use of Microsoft Teams as a vector of attack is problematic due to the use of teams within the organization and widespread use across the corporate world. They also are a precursor to more dangerous attacks from other malicious actors. However, due to Storm-0324 being an access broker, identifying and preventing Storm-0324 activity can prevent follow-up attacks, such as ransomware, from groups that Storm-0324 provides access to.

References

https://www.microsoft.com/en-us/security/blog/2023/09/12/malware-distributor-storm-0324-facilitates-ransomware-access/

https://www.bleepingcomputer.com/news/security/ransomware-access-broker-steals-accounts-via-microsoft-teams-phishing/

https://www.helpnetsecurity.com/2023/09/13/ransomware-microsoft-teams-phishing/