OP Plan #3- Operation Keanu

Completed by:
Team Texas

Members:
Thomas Larkin
Colin Mullican
Graeme Dickerson-Southworth
Ikechukwu Igboemaka

Completed on:
04/17/2024

Overview

In our offensive operation, Operation Keanu, our goal is to exfiltrate Team Illinois's flags. The attack will occur Monday, April 22nd @ 10 PM.

Objective

The objective of this attack is to gain access to Team Illinois's network and exfiltrate flags from their Steel domain file share.

Targeted Systems

We have access to all of Team Illinois's Steel domain systems. The following is a list of all reported systems:

Hostname	IPv4	Operating System
peoria.steel.illinois.tu	172.21.140.118	Windows Server 2019
waukegan.steel.illinois.tu	172.21.140.240	Windows 2019
elgin.steel.illinois.tu	172.21.140.58	Windows Server 2019
schaumburg.steel.illinois.tu	172.21.140.17	Windows Server 2019
springfield.steel.illinois.tu	172.21.140.238	Linux
cicero.steel.illinois.tu	172.21.140.32	Windows 11|10|2022
champaign.steel.illinois.tu	172.21.140.252	Windows

Procedure

The attack will proceed through the following steps, according to the MITRE ATT&CK Framework:

Reconnaissance

Reconnaissance was conducted on Team Illinois and their known systems. Upon reviewing systems to connect to, we decided the optimal system to target is the File Share, containing our target's flags, an important asset to our team. While targeting BIND to steal bank credentials is a potential candidate, due to a recent incident leaving all teams with 0 credits in their bank, we believe targeting the File Share to be more effective.

Resource Development

On April 16th, we were privately sent a list of admin credentials, including plaintext passwords, associated with Team Illinois's Steel domain, from our allies within Team New York. While it is unknown how these credentials were obtained, we as a team plan to use this intel, in the event it is legitimate.

Initial Access

Initial access to each system will be established through SSH, using the acquired credentials. If successful, we will be granted sudo privileges, logged in as admin users within the company (thus achieving privilege escalation). While the scope of this operation is only to target the File Share, we still plan to attempt establishing connection to each system we have credentials for, to use in future operations.

Persistence

Persistence will be achieved through inserting our public SSH key into a logged-on user's authorized_keys files, upon logging onto a Windows machine, or upon opening Terminal on Linux machines. This will be done on Windows through registry key values containing the persistence script, and in Linux through the .bashrc file.

Evasion

Access to the File Share will be done through a valid domain account, under the preexisting user "webclient", a user left behind by our adversaries' previous attacks. Additionally, we plan to wipe system logs ranging from the time of accessing the system, to the time of exiting the system.

Exfiltration

Exfiltrated flags will be sent using an FTP connection from Illinois’s system to our system.