BLUE MOCKING BIRD

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON BLUE MOCKINGBIRD :ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Blue Mockingbird is the name given to a cluster of similar activity involving Monero cryptocurrency-mining payloads in dynamic-link library (DLL) form on Windows systems by Red Canary.

II. TARGETS

Thousands of enterprise systems are believed to have been infected with a cryptocurrency-mining malware operated by a group tracked under the codename of Blue Mockingbird. esearchers say Blue Mockingbird attacks public-facing servers running ASP.NET apps that use the Telerik framework for their user interface (UI) component.

III. METHODS USED

Hackers exploit the CVE-2019-18935 vulnerability to plant a web shell on the attacked server. They then use a version of the Juicy Potato technique to gain admin-level access and modify server settings to obtain (re)boot persistence.Once they gain full access to a system, they download and install a version of XMRRig, a popular cryptocurrency mining app for the Monero (XMR) cryptocurrency.
Red Canary experts say that if the public-facing IIS servers are connected to a company's internal network, the group also attempts to spread internally via weakly-secured RDP (Remote Desktop Protocol) or SMB (Server Message Block) connections.

IV. CAMPAIGNS

- This is a fairly new apt which was discovered in may 2020 by malware analysts from cloud security firm Red Canary, the Blue Mockingbird group is believed to have been active since December 2019.

- This threat, in particular, has affected a very small percentage of the organizations whose endpoints Red canary monitor. However, they observed roughly 1,000 infections within those organizations, and over a short amount of time

AX1AL

V. IOCS

SHA 256 FOR XMRIG MINER DLLS

d388c309a540d4619169a07a4b64707f4c44953511875b57ad7cfa3e097115af
14e3c16ca940244bea9b6080fa02384ebb4818572cef7092f90d72ae210b330d
5377c69c05817a0e18f7b0ebbeed420f9ab8d1e81b439f439b42917fbe772dfb
c957d007824ee8173c67122a1843c979c818614eeed7db03dea3ba7fede43eba
5d7116f04e10e968de64c4201fc7374fa84b364e90f8e4eba0fbc41afeaf468c
1d30d3cafdcc43b2f9a593983ad096c2c3941025fb4e91257e2dcf0919ed24ba
968b324be2b89f1a8ee4743d946723c1ffdca16ccfbbbbb68e5b9f60e0bff4c9
018a02fd0dbc63e54656b8915d71cd8a2ce4409608ae4dff6ec196ffa8743ba1b3
1f7152a547fa41c31f9c96177b2cd7131a93f7c328bf6da360dc1586ba18dc

TTP's

Execution with rundll32.exe explicitly calling the DLL export fackaaxv.
Execution using regsvr32.exe using the /s command-line option.
Execution with the payload configured as a Windows Service DLL.

VI. REFRENCES

https://www.zdnet.com/article/thousands-of-enterprise-systems-infected-by-new-blue-mockingbird-malware-gang/

https://redcanary.com/blog/blue-mockingbird-cryptominer/
https://securityaffairs.co/wordpress/103020/cyber-crime/blue-mockingbird-campaign.html