Oct 28 2023

NETMANAGEIT

Intelligence Report

Hacktivism in the Israel-Hamas Conflict | Citizen Data Leakage Using Old Malware

d2f321fb9e5150f231d8...
RedLine
uses
[T1027] Obfuscated Files or...
[T1041] Exfiltration Over C2...
Israel

Table of contents

Overview

Entities

Observables

External References

Overview

Description

So far, the use of novel malware/scareware and tools such as Redline Stealer and PrivateLoader by these threat actors continue to target Israeli citizens, businesses, and critical sector entities, causing data leaks and widespread disruptions.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Attack-Pattern

Name
Obfuscated Files or Information
ID
T1027
Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

Exfiltration Over C2 Channel

ID

T1041

Description

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

Country

Name
Israel

Malware

Name
RedLine

StixFile

Value
d2f321fb9e5150f231d82d0fb0fbf52350cf2edd131ab960601d9b6832a7e248

External References

- https://otx.alienvault.com/pulse/653aa8fa78a4252d596a65be
- https://www.sentinelone.com/blog/hacktivism-in-the-israel-hamas-conflict-citizen-data-leaked-using-old-malware/