Mphasis
The Next Applied

Dark Power Ransomware Advisory

Severity: Medium

Date: 27th March 2023

Description

New ransomware gang named Dark Power is in the wild hacking various organizations globally for an affordable ransom demand. The Dark Power gang has over 10 victims listed on its dark net website already waiting to leak their data!

Researchers note Dark Power is slightly typical by using a least-known programming language and spreading two variants to hit the victims accordingly.

The Dark Power ransomware is using NIM, a cross-platform programming language with several speed-related advantages making it apt for ransomware operations. NIM is a relatively new language, most of the security solutions fail to detect it.

How it works

According to the researchers the ransomware group creates a randomized 64-character long ASCII string for starting the encryption process, with a unique key on each execution.

Further, it proceeds to terminate specific services and processes on the victim's system to free up files for encryption, while also deleting the shadow copies of data to make recovery hard later. This gets even much harder with the ransomware gang wiping out the console and Windows system logs in the process.

The Dark Power ransomware targets specific services on the victim's machine. It stops the following services: VEEAM, MEMTAS, SQL, MSSQL, BACKUP, VSS, SOPHOS, and MEPOCS. By disabling these services, the ransomware makes it difficult for the victim to recover their files, as the services free file like databases, which allows the ransomware to encrypt them. Additionally, the Volume Shadow Copy Service (VSS) is stopped, which is common for ransomware to do, all the other back-up and anti-malware services are stopped.

Encrypted files are renamed with the ".DARK POWER" extension, with certain file types like DLLs, LIBs, INIs, CDMs, LNKs, BINs, MSIs excluded from encryption to keep the infected system operational and allow the victim to view the ransom note and contact them.

The ransomware runs the below query to terminate the process from the Windows Management Instrumentation (WMI).

Query:

“winmgmts: & {impersonationLevel=impersonate}!.\root\cimv2” with the query “select * from win32_process”

The table below contains the terminated processes and services

taskmgr.exe	sqbcoreservice.exe	oracle.exe	thunderbird.exe
agntsvc.exe	outlook.exe	isqlplussvc.exe	msaccess.exe
synctime.exe	mydesktopqos.exe	excel.exe	visio.exe
encsvc.exe	dbeng50.exe	mydesktopservice.exe	dbsnmp.exe
mspub.exe	sql.exe	ocssd.exe	wordpad.exe
infopath.exe	ocautoupds.exe	winword.exe	xfssvccon.exe
powerpnt.exe	tbirdconfig.exe	firefox.exe	thebat.exe
onenote.exe	ocomm.exe	steam.exe	

Targeted Industries

- Education
- Technology
- Healthcare
- Manufacturing
- Food production

Indicators of compromise

SHA 256 Values.

- 33c5b4c9a6c24729bb10165e34ae1cd2315cfce5763e65167bd58a57fde9a389
- 11ddebd9b22a3a21be11908feda0ea1e1aa97bc67b2dfefe766fcea467367394

Reference Links

https://www.trellix.com/en-us/about/newsroom/stories/research/shining-light-on-dark-power.html

https://www.darkreading.com/vulnerabilities-threats/dark-power-ransomware-extorts-10-targets-less-than-a-month