PwndLocker Ransomware Now Comes With A Fixed New Version Dubbed "ProLock"

Recently, a freshly modified version of the PwndLocker ransomware dubbed "ProLock" has been detected to go after a few servers belonging to corporate networks.

What is ProLock?

ProLocker ransomware has originated from PwndLocker that was discovered in early March 2020, infecting the networks of Lasalle County in Illinois i.e. a government body from which the attacker demanded a ransom of 50 bitcoins for a decryption key, and the city of Novi Sad in Serbia.

Why did the attackers create a new version of PwndLocker?

Attackers reproduced PwndLocker by fixing an encryption flaw that was allowing victims to get their data back by using a free decryption tool without paying the ransom amount.

How do the attackers infiltrate target networks?

It is believed that the threat actors behind ProLock ransomware are breaking into target networks, most probably, via unprotected Remote Desktop services.

How is ProLock distributed?

The ProLock ransomware is being delivered by embedding the ransomware executable inside a BMP image file that is saved in the path C:\ProgramData as "WinMgr.bmp".

When this BMP file is viewed in an image viewer, all the user sees are some dots in the upper right corner of the screen as a result of which he might not get apprehensive. However, the image comes embedded with some binary data that is later reassembled by a PowerShell script and injected directly into the memory of the target device.

How does the use of a BMP file facilitate the attack process?

Since the crooks install their malware all over the victim network using PSExec or PowerShell Empire, embedding the ransomware payload inside a BMP image file is a measure taken to dodge detection from anti-virus solutions.

What is the encryption routine?

1. To start with, ProLocker deletes the infected system's Shadow Volume Copies before moving forward with its encryption routine.
2. Its encryption process is similar to that used by its predecessor PwndLocker during which, ProLocker encrypts its victim's files with the "RSA-2048" encryption algorithm and appends the ".proLock" extension to the name of each encrypted file. It, however, does not encrypt files with extensions such as '.exe', '.dll', '.lnk', '.ico', '.ini',

'.msi', '.chm', '.sys', '.hlf', '.lng', '.inf', '.ttf', '.cmd', '.bat', '.vhd', '.bac', '.bak', '.wbc', '.bkf', '.set', '.win', '.dsk', and files residing in operating system and common application folders.

3. Post encryption, the ransomware drops a ransom note titled "[HOW TO RECOVER FILES].TXT" in every folder scanned for files. The note instructs the victim about the mode of connection to a Tor to receive information regarding the ransom payment.

4. The ransom demand varies from victim to victim based on the ProLock ransomware executable delivered to him. The demands are quite high i.e. in the range of 80 bitcoins.

Any other threat?

To worsen the situation, cybercriminals claim to have gathered highly sensitive information regarding the victim and threaten to publicize the same if their ransom demand is not fulfilled within one month during which they will store the decryption keys.

Any protective measures?

The following basic security practices should be essentially maintained in order to protect against ProLock ransomware:

1. Ransomware infections like ProLock primarily keep data as hostage. Therefore, practicing regular backup of critical data can save the business in the event of such outbreaks. Also please ensure to maintain offline backups.

2. It is crucial to install an active instance of a reputed multi-layered anti-malware solution updated with latest signatures in all endpoint devices which will help reduce the gravity of such attacks.

3. All operating systems and applications should be kept updated on a regular basis. Virtual patching can be considered for protecting legacy systems and networks. This measure hinders cybercriminals from gaining easy access to any system through vulnerabilities in outdated applications and software. Avoid applying updates / patches available in any unofficial channel.

4. Deployment of application control and whitelisting and behavior monitoring can be considered as an easy and affordable method for mitigating unauthorized access and privilege by preventing suspicious applications or processes from executing.

5. Enabling and deploying firewalls and intrusion detection and prevention systems will aid in better monitoring and scanning of traffic traversing the network i.e. these measures may block the communication of ProLock ransomware with its controllers.

6. Monitoring all outbound traffic especially the traffic that is destined to newly-registered domains or belongs to the category: “Uncategorized” should be inspected closely or blocked.

7. As the threat actors behind ProLock claim to steal data from compromised systems, using DLP can enhance data protection by highlighting policy violations, or by preventing any data transmission in question.

8. Network / endpoints should be monitored for the presence of PSEXEC tool. If this tool is not utilized for any business purposes, then a positive presence of PSEXEC in the network will require further investigation.

9. Usage of RDP should be closely regulated, monitored, and controlled.

10. Any deployed remote systems (accessible via Internet using RDP) should be reachable over a list of approved IPs. Access should be restricted on port 3389 (RDP).

11. Proper account lockout policies should be established to make it difficult for accounts to be brute forced over Remote Desktop Services.

12. Audit of network for systems using RDP for remote communication should be carried out.

13. Post analysis of the various samples identified in the wild, a list of indicators has been prepared, which is advised to be monitored via endpoint solutions to detect any early signs of compromise.