Report on Darkside Ransomware

1. **What is Ransomware:** Ransomware is an attack that limits the user's access to their assets by encrypting or locking the complete or part of a system and preventing them from accessing the data until a ransom payment is made.

2. **Types of ransomware attacks:** The most common types of ransomware are listed below.

   2.1. **Crypto Ransomware or Encryptors**: Encryptors are the most well-known and harmful kind of ransomware attack. This ransomware encrypts the data and makes it inaccessible without a decryption key. Once the user pays the ransom they give them the description key to access the data.

   2.2. **Lockers** : This is another kind of a ransomware attack. Where an attacker locks the user out of the system completely and data, files and application are inaccessible. A lock screen shows the ransom demand with a countdown or other information to pay the ransom.

   2.3. Scareware : It's a kind of ransom attack where a fake software is used that claims to have detected a virus or other critical issues on the users system and directs users to pay to resolve the problem. This type of ransomware attack doesn't harm the system or files but it simply floods the screen with popup alerts.

   2.4. Doxware or Leakware : In this kind of attacks the attackers threaten the user to distribute the sensitive personal or an organization information online, this makes the user panic and pays the ransom to prevent data from falling into the wrong peoples and entering in the public domain.

   2.5. RaaS (Ransomware as a Service) : Ransomware As a service is a business model between ransomware operators and affiliates in which affiliates pay to launch ransomware attacks developed by operators.

3. Darkside Ransomware attack :

This hacking group adopted the Ransomware-as-a-Service (RaaS) model, which means they rented their software to third parties. The profit was split between the partners, affiliates, and holders, and the group took around 25% of the gains after successful attacks.

DARKSIDE appears first in August 2020. Darkside is a new group but In the short period of time they managed to get a good reputation to operate the group and perform their operation in a more professional and organized way.

The DARKSIDE group claims that they are doing it to make the world better and they only target large profitable organizations and extorted millions of dollars from companies.

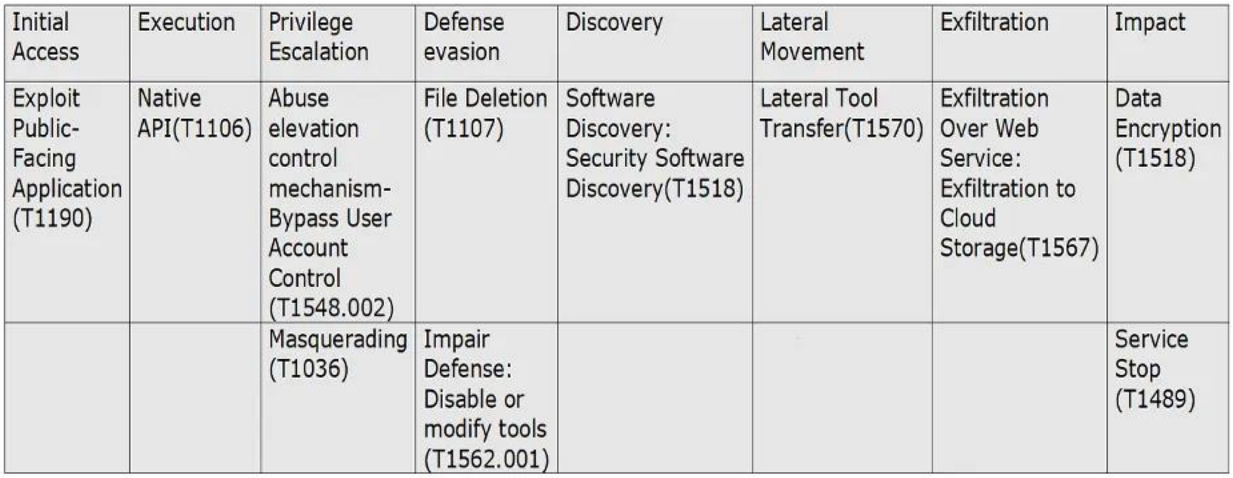
The darkside group is the most organized group and they work in a professional way.
They do have policies for their attacks. Some of them are as follow:
1) They don't target attacks against the countries associated with former Soviet Bloc nations.
2) It prohibits attacks against hospitals, hospices, schools, universities, non-profit organizations and government agencies.

4. How the DarkSide Attacks Worked:

DarkSide groups use various methods for penetrating the networks or systems of their victims, similar to the way other ransomware groups operate. Usually, it combined stolen credentials and manual hacking with different penetration testing tools, some of which were used for the DarkSide gas hack.

Before deploying ransomware, the group identified critical servers, escalated privileges, and disabled and deleted backups. When everything is done, the victim is notified that their systems are immobilized and that they need to pay the ransom if they want their data back.

DarkSide Ransomware TTP Map



Initial Access	Execution	Privilege Escalation	Defense evasion	Discovery	Lateral Movement	Exfiltration	Impact
Exploit Public-Facing Application (T1190)	Native API(T1106)	Abuse elevation control mechanism-Bypass User Account Control (T1548.002)	File Deletion (T1107)	Software Discovery: Security Software Discovery(T1518)	Lateral Tool Transfer(T1570)	Exfiltration Over Web Service: Exfiltration to Cloud Storage(T1567)	Data Encryption (T1518)
		Masquerading (T1036)	Impair Defense: Disable or modify tools (T1562.001)				Service Stop (T1489)

5. DARKSIDE Technical Details:

Phase 1) Initial Access : DarkSide ransomware performs brute force attacks and exploits known vulnerabilities in the remote desktop protocol (RDP) to gain initial access. After initial access DarkSide ransomware does validation on the machines to infect. DarkSide ransomware collects information about computer name and system language in its initial code execution. DarkSide is used to target English-speaking countries.

Phase 2) Privilege Escalation: Privilege Escalation consists of techniques that are used to gain higher-level permissions on a system or network. Privilege escalation attacks can be performed if a malicious user exploits a bug or configuration error in an application or operating system.

Phase 3) Data Exfiltration: DarkSide ransomware identifies data backup applications, exfiltrated data, and then encrypts local files as part of the ransomware deployment.

Phase 4) Delete Volume Shadow Copies: Ransomware campaigns often attempt to delete the volume shadow copies of the files on a given computer so that their victims will not be able to restore file access by reverting to the shadow copies. DarkSide ransomware deletes the volume shadow copies via PowerShell scripts.

Phase 5) Impair Defenses: DarkSide disables security protection services using the Impair Defenses technique to avoid possible detection of their tools and activities. This can take the form of killing security software or event logging processes, deleting Registry keys so that tools do not start at run time, or other methods to interfere with security tools scanning or reporting information.

Phase 6) Ransomware Execution: Ransomware generates the custom file extension based on machine GUID and using API RtlComputeCRC32. File extension generated by using Machine GUID is of 8 characters and will be added to each encrypted file name.

6. Safety Measures to Prevent Ransomware Attack:

- Protect systems from ransomware by backing up important files regularly and keep a recent backup copy offline. Encrypt your backup.
- Always keep your security software (antivirus, firewall, etc.) up to date to protect your computer from new variants of malware.
- Avoid downloading software from untrusted P2P or torrent sites, which often host malicious software.
- Do not provide administrative privileges to users. Do not stay logged in as administrator unless strictly required. In addition, avoid browsing, opening documents, or other regular work activities while logged in as an administrator.
- Establish a lockout policy that prevents the ability to guess credentials.
- Regularly patch and update applications, software, and operating systems to address any exploitable software vulnerabilities.