DarkSide Ransomware Behavior and Techniques

blogs.keysight.com/blogs/tech/nwvs.entry.html/2021/05/18/darkside_ransomware-QfsV.html

2021-05-18 | 5 min read

A modern ransomware, DarkSide offers their ransomware-as-a-service to other cyber-criminal groups for a percentage of the profits. Both Windows and Linux versions of the ransomware have been found in the wild. It encrypts files using the lightweight Salsa20 encryption algorithm with an RSA-1024 public key. Victims are presented with Bitcoin and Monero wallets to pay the cyber-criminal sums varying from two thousand to two million dollars for the decryption key. According to TrendMicro, the actor behind this ransomware family is believed to be Eastern European.

Groups leveraging DarkSide have recently been targeting manufacturing, insurance, healthcare, and energy organizations. Multiple strains of the ransomware were released either to attack specific high-value targets or to hamper the detection effort. Following the attack on Colonial Pipeline, another DarkSide strain also managed to successfully infected a Toshiba Tech business unit in France. Meanwhile, another eastern-European ransomware (calling themselves Conti) has infected the Ireland's national health service.

DarkSide uses phishing, weak credentials, and exploitation of known vulnerabilities (such as CVE-2021-20016, a SQL injection in the SonicWall SMA100 SSL VPN product) as tactics to gain system access.

Keysight's Application and Threat Intelligence (ATI) research team has released a DarkSide kill chain assessment, simulating the malware's behavior. In this blog post, we'll walk you through what happens when the DarkSide malware infects a system, in terms of MITRE ATT&CK techniques.

T1082 - System Information Discovery

The malware checks whether its process is being debugged by a user-mode debugger. If that is the case, then the malware will exit. It is a common malware anti-debugging mechanism.

```
push    50h
mov     [ebp+var_270], eax
lea     eax, [ebp+var_58]
push    0
push    eax
call    sub_40A3D0
mov     eax, [ebp+4]
add     esp, 0Ch
mov     [ebp+var_58], 40000015h
mov     [ebp+var_54], 1
mov     [ebp+var_4C], eax
call    ds:IsDebuggerPresent
push    0               ; lpTopLevelExceptionFilter
lea     ebx, [eax-1]
neg     ebx
lea     eax, [ebp+var_58]
mov     [ebp+ExceptionInfo.ExceptionRecord], eax
lea     eax, [ebp+var_324]
sbb     bl, bl
mov     [ebp+ExceptionInfo.ContextRecord], eax
inc     bl
call    ds:SetUnhandledExceptionFilter
```

Other WIN APIs associated with system information discovery that this malware showcases include:

- **GetSystemInfo**: Used to return the processor count. This API can be used to determine if the malware is being run in a virtualized environment.
- **CheckRemoteDebuggerPresent**: Used to determine if a remote process is being debugged.
- **GetSystemDefaultUILanguage**, **GetUserDefaultLangID**: Used to detect the configured language on the system. The malware will not infect the host if the following languages are installed:

Russian - 419	Azerbaijani (Latin) - 42C	Uzbek (Latin) - 443	Uzbek (Cyrillic) - 843
Ukranian - 422	Georgian - 437	Tatar - 444	Arabic (Syria) - 2801
Belarusian - 423	Kazakh - 43F	Romanian (Moldova) - 818	
Tajik - 428	Kyrgyz (Cyrillic) - 440	Russian (Moldova) - 819	
Armenian - 42B	Turkmen - 442	Azerbaijani (Cyrillic) - 82C	

T1543.003: Create or Modify System Process: Windows Service

The malware will attempt to attain persistence by calling the CreateServiceA WIN API that creates a system service pointing to the malware executable file, which will start automatically after restart:

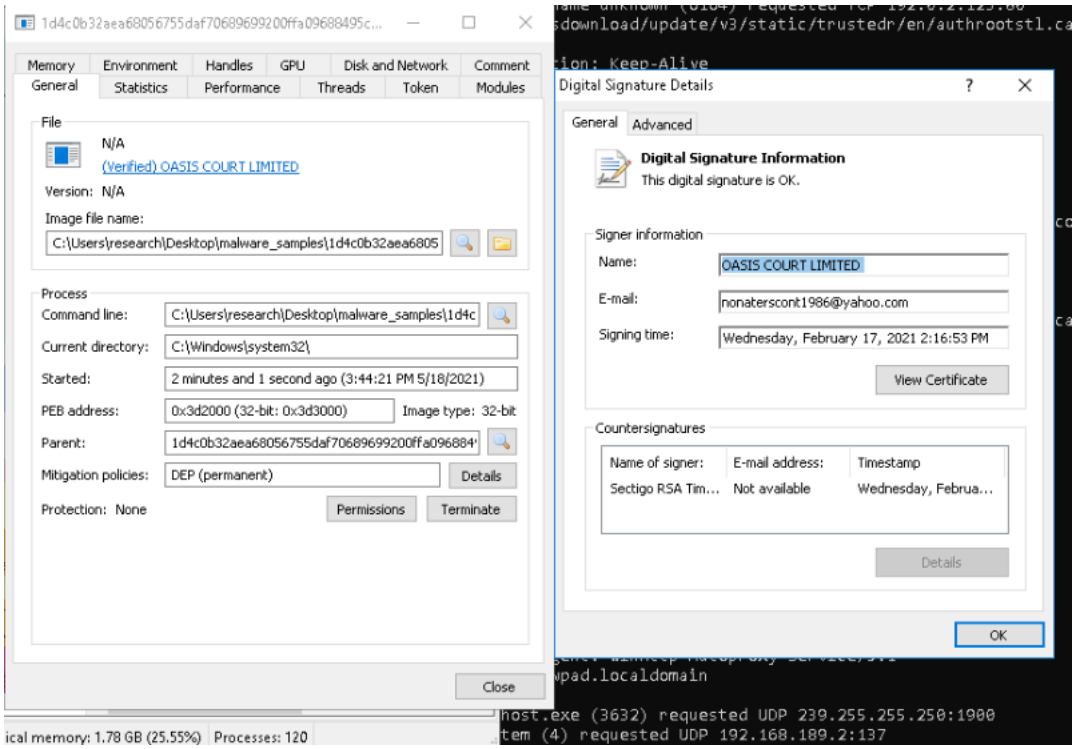
The malicious service hides itself using the name .021e895b, a pseudo-random string of eight lowercase hexadecimal characters, generated based on either the system's MAC address or MachineGuid registry value.

T1548.002: Abuse Elevation Control Mechanism, Bypass User Account Control

If the operating system is Windows 10 or newer, the malware attempts a UAC bypass through a CMSTPLUA COM interface. A proof of concept is available here.

T1553.002: Subvert Trust Controls, Code Signing

To be able to run on systems where only signed code is allowed to execute, the malware is signed with Cobalt Strike stager's certificate.

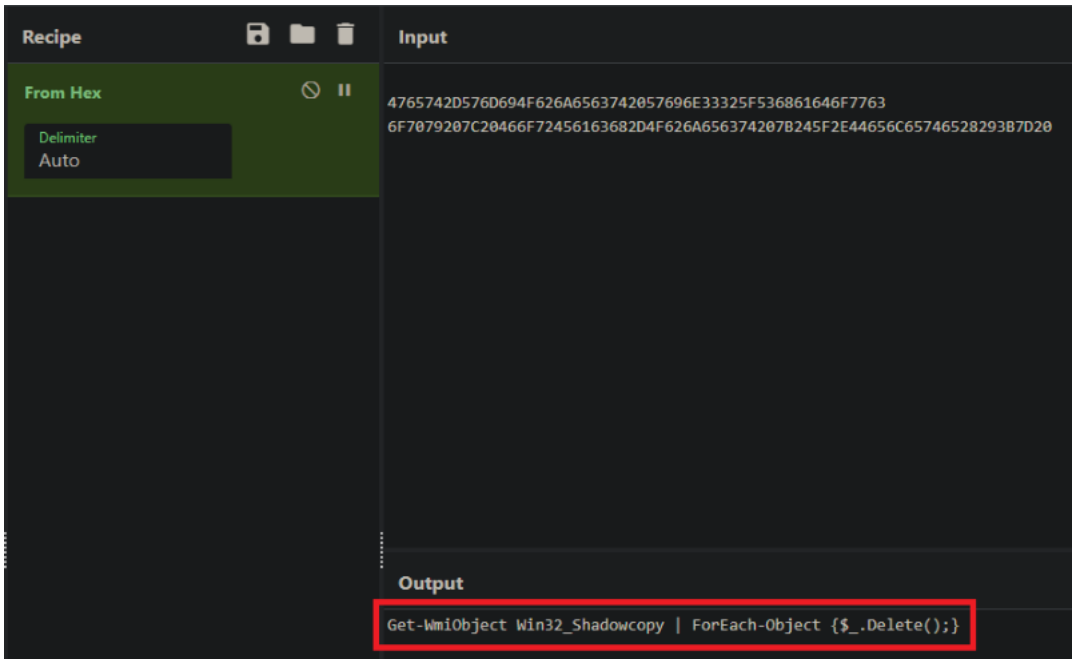


T1490: Inhibit System Recovery

Before encrypting the files on the system, the ransomware uses the **CreateProcess** API to execute the following command:

```
powershell -ep bypass -c "(0..61)|%{$s+=[char][byte]
('0x'+'4765742D576D694F626A6563742057696E33325F536861646F77636F7079207C20466F72456163682D4F626A656374207B245F2E44656C657
$s"
```

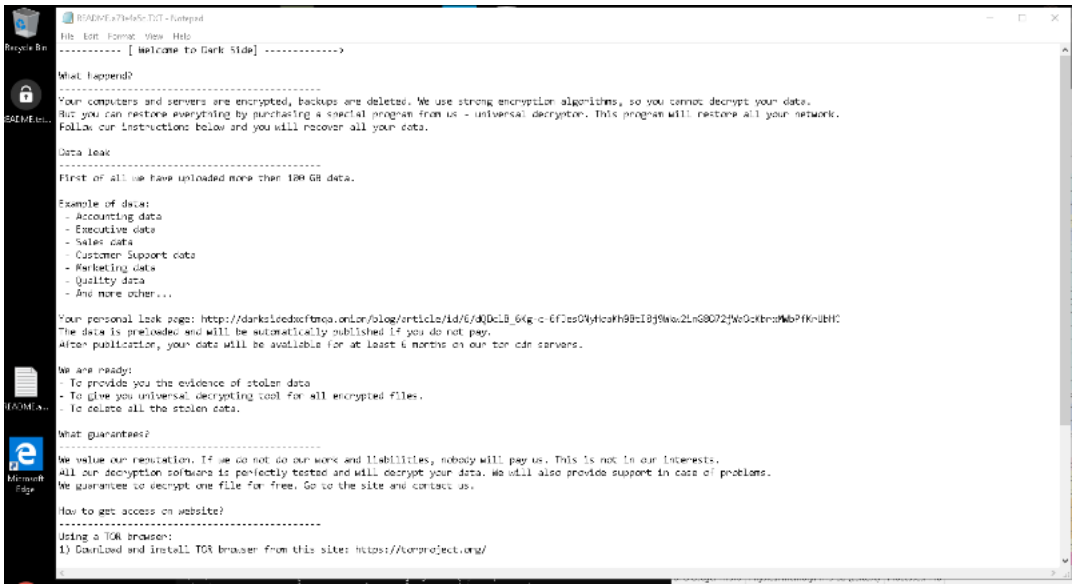
By decoding the content of the byte stream, we obtain:



The PowerShell command is querying the WMI to obtain the list of the system's shadow copies and deletes them before encrypting the user files, thus avoiding post-infection system recovery.

T1486: Data Encrypted for Impact

The found system files are encrypted using the lightweight Salsa20 encryption algorithm. Each key is encrypted using the embedded RSA-1024 public key. In each traversed directory, the malware writes the ransom note shown below.



Conclusion

Darkside has above-average anti-VM/anti-debugging protections. Written in C and highly modular, it was released in different versions, with multiple packers, which made it hard to pin down with signature-based detection. For more details, please inspect joint CISA-FBI cybersecurity advisory on the DarkSide ransomware.

Using the knowledge gleaned from reverse engineering, we have released a complete Darkcloud killchain assessment for our Threat Simulator customers. Now you can test your endpoint and network security controls for coverage of this and many other threats in your production environment safely.