

Threat Update: Industroyer2 | Splunk

By Splunk Threat Research Team

Published: 2022-06-23 · Archived: 2026-04-05 19:07:36 UTC

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 Splunk Threat Research Team (STRT) continues to monitor new relevant payloads to the ongoing conflict in Eastern Europe. One of these new payloads was found by the [Ukrainian CERT](#) named “Industroyer2.” The name of this new payload references the original “[Industroyer](#)” malicious payload used against the country of Ukraine's power grid in 2016 and allegedly was able to affect [a fifth of the power capacity of the city of](#) Kyiv.

According to the recent [Ukraine CERT](#) and [ESET](#) report, Industroyer2 resembles the former Industroyer in functionality and is also targeting the electric grid containing commands targeting high-voltage electrical substations. It was reported that Industroyer2 was also used along with [CaddyWiper](#), another payload recently addressed by the Splunk Threat Research Team. This payload — in combination with previous featured destructive payloads — targets [CPEs](#). These customer premise devices such as modems, cable modems, and internet gateways are devices that provide connectivity to the great majority of commercial and residential customers, and speak to the attacker’s intention of overwhelming or degrading the victim's infrastructure.

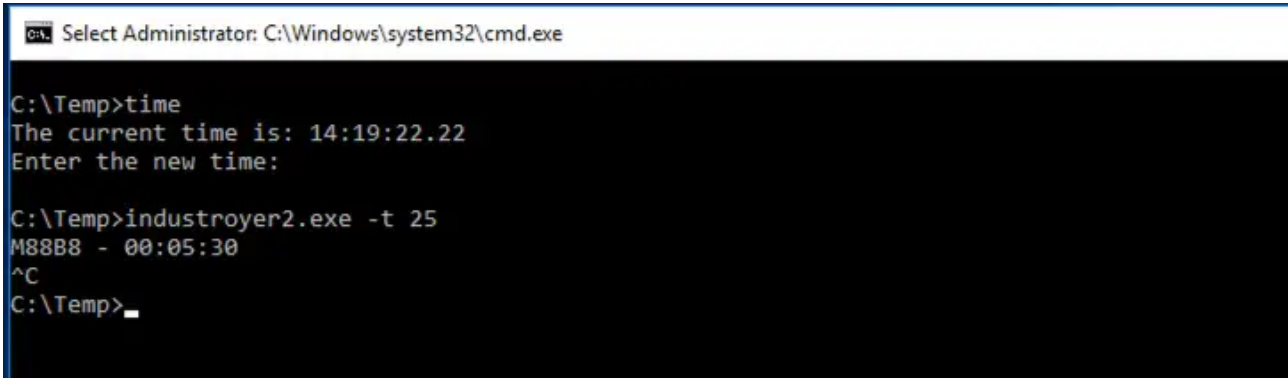
The following is an analysis of relevant detection opportunities of this payload and observed [TTPs](#) during the deployment of this payload.

Parameter Check

The first part of its code is checking parameters that can execute some of its features related to timing and logging. Below is the code screenshot of this checking with its 2 parameters.

```
if ( hMem )
{
  if ( pNumArgs )
  {
    str_minute_timer = (LPCWCH)mw_check_param((int)hMem, (int *)hMem + pNumArgs, (char)L"-t");
    if ( str_minute_timer )
    {
      v1 = mw_get_system_time_and_create_timer(v3, str_minute_timer);
      wrap_WaitForMultipleObjectsEx((int)v1);
      wrap_CloseHandle(v3);
    }
    if ( sub_403B60((int)hMem, (int)hMem + 4 * pNumArgs, (char)L"-o" ) )
    {
      v11 = mw_check_param((int)hMem, (int *)hMem + pNumArgs, (char)L"-o");
      if ( v11 )
      {
        wrap_InitializeCriticalSection_0();
        mw_generate_logs(v11);
      }
      v2 = wrap_InitializeCriticalSection_0();
      mw_write_console_logs((int)v2, "%d\n", 22);
    }
  }
}
```

The first parameter is “-t” which will trigger a waiting timer relative to the current minute of the system time. For example, if your system time is 14:19:22 PM and you use this parameter with a value of 25 as the third parameter, it means it will wait 5 mins before it executes its code like the screenshot below.



While the “-o” parameter is a feature to redirect its console logs to a debug log file you inputted as the 3rd parameter.

Console Logs

Upon executing this malware, it outputs some console logs with a customized code structure that tells something about what features it executes. Some of it will be discussed further in the next subheadings. Below is an example of the console logs during its execution.

```
12:13:36:0049> T281 00006800
12:13:36:0098> RNM 0015
12:13:36:0113> T65 00006800
12:13:36:0113> 10 [REDACTED]: 2404: 3
12:13:36:0130> 10 [REDACTED] M68B0 SGCNT 44
12:13:36:0130> RNM 0015
12:13:36:0145> T113 00006800
12:13:36:0145> 192 [REDACTED]: 2404: 2
12:13:36:0161> 192 [REDACTED] M68B0 SGCNT 8
12:13:36:0161> RNM 0015
12:13:36:0191> 192 [REDACTED]: 2404: 1
12:13:36:0222> 192 [REDACTED] M68B0 SGCNT 16
12:13:51:0159> 10 [REDACTED] M6812
12:13:51:0191> 192 [REDACTED] M6812
12:13:51:0268> 192 [REDACTED] M6812
```

Terminate Process and Rename Process File Path

This function enumerates all running processes in the targeted host and looks for the process named “PServiceControl.exe” and also the process name stated in its config data. It will also look for the file path of that process in a specific folder that is in the config file and rename it with “.MZ” file extension.

The code screenshot below shows the process termination and renaming of process file path. We can see in the code snippet the code “RNM” plus the last error code after the call MoveFileA() function that will be displayed in its console logs after executing this part of the code. You can see that in the console log screenshot earlier.

```
for ( dwProcessId = mw_EnumProcess((int)"PServiceControl.exe"); dwProcessId; dwProcessId = mw_EnumProcess(a1 + 0x10047) )
{
    hProcess = OpenProcess(1u, 0, dwProcessId);
    TerminateProcess(hProcess, 0);
}
while ( 1 )
{
    dwProcessId = mw_EnumProcess(a1 + 0x10047);
    if ( !dwProcessId )
        break;
    v4 = OpenProcess(1u, 0, dwProcessId);
    TerminateProcess(v4, 0);
}
if ( *(_BYTE *) (a1 + 0x10154) && a1 != 0xFFFEFEAB )
{
    lpExistingFileName = (const CHAR *)wrap_heapAlloc(0x100u);
    lpNewFileName = (const CHAR *)wrap_heapAlloc(0x100u);
    lpMem = wrap_heapAlloc(0x100u);
    sub_402540(lpExistingFileName, 256);
    sub_402540(lpNewFileName, 256);
    sub_402540(lpMem, 256);
    sub_401A10(lpExistingFileName, a1 + 65877);
    sub_401A10(lpNewFileName, a1 + 65877);
    sub_405360(lpExistingFileName, "\\");
    sub_405360(lpNewFileName, "\\");
    sub_405360(lpExistingFileName, a1 + 65607);
    sub_405360(lpNewFileName, a1 + 65607);
    sub_405360(lpNewFileName, ".MZ");
    MoveFileA(lpExistingFileName, lpNewFileName);
    v3 = GetLastError();
    v1 = wrap_SleepAndInit();
    mw_prepare_console_logs((int)v1, " RNM %04x \n", v3);
    mw_memsetHeap(lpExistingFileName);
    mw_memsetHeap(lpNewFileName);
    mw_memsetHeap(lpMem);
}
return 1;
```

HardCoded Configuration Data

This malware contains hardcoded configuration files that will be parsed with the help of CommandLineToArgvW() function and put in a structure that will be used later in its code. Below is the screenshot of the parsing function.

```
lp_cmd_argvW = CommandLineToArgvW(lpCmdLine, &pNumArgs);
if ( lp_cmd_argvW )
{
    *(_DWORD *)ctr = 0;
    while ( *(_DWORD *)ctr < (unsigned int)pNumArgs )
    {
        if ( mw_parse_ip_addr_in_cfg(*((LPCWCH *)lp_cmd_argvW + *(_DWORD *)ctr)) )
        {
            lpMem = wrap_heap_alloc(0x48u);
            if ( lpMem )
            {
                lpParameter = wrap_heap_alloc(0x10D70u);
                v28 = 1;
                *lpMem = wrap_wide_to_multi_bytes(*((LPCWCH *)lp_cmd_argvW + *(_DWORD *)ctr)); // ip_addr
                if ( ++*(_DWORD *)ctr < (unsigned int)pNumArgs && v28 )
                {
                    lpMem[1] = wrap_wide_to_multi_bytes(*((LPCWCH *)lp_cmd_argvW + *(_DWORD *)ctr)); // port
                    ++*(_DWORD *)ctr;
                }
            }
        }
        else
    }
```

The config data contains values and checks that this payload uses through its execution. We saw four main components of its three configuration data settings that are hardcoded to its data section like the screenshot below: The first component is the IP address of devices where it tries to communicate via IEC-104 protocol, the next one is the port number (2404), third is the process name (PService_PPD.exe) it tries to kill aside from “PServicecontrol.exe” and a file path (D:\OIK\DevCounter) where it locates the process file path it tries to kill to rename it with .MZ file extension.

```

00409190 a10824010524043: ; DATA XREF: .data:off 40B000↓o
00409190 text "UTF-16LE", '10. [redacted] 5 2404 0 0 1 1 PService_PPD.exe 1 "D:\OI
00409190 text "UTF-16LE", 'K\DevCounter" 0 1 0 0 1 0 0 44 130202 1 0 1 1 160
00409190 first config data text "UTF-16LE", '921 1 0 1 1 2 160923 1 0 1 1 3 160924 1 0 1 1 4 160
00409190 text "UTF-16LE", '925 1 0 1 1 5 160927 1 0 1 1 6 160928 1 0 1 1 7 190
00409190 text "UTF-16LE", '202 1 0 1 1 8 260202 1 0 1 1 9 260901 1 0 1 1 10 26
00409190 text "UTF-16LE", '0902 1 0 1 1 11 260903 1 0 1 1 12 260904 1 0 1 1 13
00409190 text "UTF-16LE", ' 260905 1 0 1 1 14 260906 1 0 1 1 15 260907 1 0 1 1
00409190 text "UTF-16LE", ' 16 260908 1 0 1 1 17 260909 1 0 1 1 18 260910 1 0
00409190 text "UTF-16LE", ' 1 1 19 260911 1 0 1 1 20 260912 1 0 1 1 21 260914 1
00409190 text "UTF-16LE", ' 0 1 1 22 260915 1 0 1 1 23 260916 1 0 1 1 24 26091
00409190 text "UTF-16LE", ' 8 1 0 1 1 25 260920 1 0 1 1 26 290202 1 0 1 1 27 33
00409190 text "UTF-16LE", '8501 1 0 1 1 28 1401 0 0 0 1 29 1402 0 0 0 1 30 140
00409190 text "UTF-16LE", ' 3 0 0 0 1 31 1404 0 0 0 1 32 1301 0 0 0 1 33 1302 0
00409190 text "UTF-16LE", ' 0 0 1 34 1303 0 0 0 1 35 1304 0 0 0 1 36 1201 0 0
00409190 text "UTF-16LE", '0 1 37 1202 0 0 0 1 38 1203 0 0 0 1 39 1204 0 0 0 1
00409190 text "UTF-16LE", ' 40 1101 0 0 0 1 41 1102 0 0 0 1 42 1103 0 0 0 1 43
00409190 text "UTF-16LE", ' 1104 0 0 0 1 44 ',0
00409814 a1: ; DATA XREF: sub_403E50+19E↑o
00409814 text "UTF-16LE", '1',0
00409818 a1921681222404: ; DATA XREF: .data:0040B004↓o
00409818 2nd config data text "UTF-16LE", '[redacted] 2 2404 2 0 1 1 PService_PPD.exe 1 "D:\O
00409818 text "UTF-16LE", 'IK\DevCounter" 0 1 0 0 1 0 0 8 1104 0 0 0 1 1105
00409818 text "UTF-16LE", '0 0 0 1 2 1106 0 0 0 1 3 1107 0 0 0 1 4 1108 0 0 0
00409818 text "UTF-16LE", ' 1 5 1101 0 0 0 1 6 1102 0 0 0 1 7 1103 0 0 0 1 8 ',0
004099AE align 10h
004099B0 a19216812122404: ; DATA XREF: .data:0040B008↓o
004099B0 3rd config data text "UTF-16LE", '[redacted] 2 2404 1 0 1 1 PService_PPD.exe 1 "D:\O
004099B0 text "UTF-16LE", 'IK\DevCounter" 0 1 0 0 1 0 0 16 1258 0 0 0 1 1259
004099B0 text "UTF-16LE", ' 0 0 0 1 2 1260 0 0 0 1 3 1261 0 0 0 1 4 1262 0 0 0
004099B0 text "UTF-16LE", ' 1 5 1265 0 0 0 1 6 1252 0 0 0 1 7 1253 0 0 0 1 8 1
004099B0 text "UTF-16LE", '254 0 0 0 1 9 1255 0 0 0 1 10 1256 0 0 0 1 11 1257
004099B0 text "UTF-16LE", '0 0 0 1 12 1263 0 0 0 1 13 1264 0 0 0 1 14 1250 0 0
004099B0 text "UTF-16LE", ' 0 1 15 1251 0 0 0 1 16 ',0

```

Detections

Below are the detections related to the Industroyer2 malware and other components found during the attack that was mentioned in the [ESET blog](#) and [CERT-UA blog](#).

Linux Adding Crontab Using List Parameter

This analytic identifies a suspicious cron jobs modification using crontab list parameters. This command line parameter can be abused by malware like Industroyer2, adversaries, and red teamers to add a crontab entry to their malicious code to execute to the schedule they want.

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime from datamodel=I
```

```
where Processes.process_name = "crontab" Processes.process= "*" -[*]"
```

```
by Processes.parent_process_name Processes.process_name Processes.process Processes.process_id Processes.pa
```

```
| `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 = "crontab" Processes.process= "* -l*"
by Processes.parent_process_name Processes.process_name Processes.process Processes.process_id Processes.parent_process_id Processes.dest Processes.user
| `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

✓ 2 events (22/04/2022 08:53:13.000 to 22/04/2022 09:08:13.000) No Event Sampling ▾

Events Patterns **Statistics (2)** Visualization

20 Per Page ▾ Format Preview ▾

parent_process_name ↕	process_name ↕	process ↕	process_id ↕	parent_process_id ↕	dest ↕
sudo	crontab	crontab -l	2269	2268	sysmonlinux
sudo	crontab	crontab -l	2289	2288	sysmonlinux

Linux Deleting Critical Directory Using RM Command

This analytic identifies a suspicious deletion of a critical folder in Linux machine using rm command. This technique was seen in Industroyer2 campaign to wipe or destroy energy facilities of a targeted sector.

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime from datamodel=
```

```
where Processes.process_name =rm AND Processes.process= "* -rf *" AND Processes.process IN ("*/boot/*", "*/va
```

```
by Processes.parent_process_name Processes.process_name Processes.process Processes.process_id Processes.parc
```

```
| `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 =rm AND Processes.process=* -rf * AND Processes.process IN ("%boot/*", "%home/*", "%var/log/*", "%etc/*")
by Processes.parent_process_name Processes.process_name Processes.process Processes.process_id Processes.parent_process_id Processes.process_guid Processes.dest Processes.user
| `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
    
```

✓ 2 events (22/04/2022 08:37:00.000 to 22/04/2022 12:37:57.000) No Event Sampling ▾

Events Patterns **Statistics (2)** Visualization

20 Per Page ▾ Format Preview ▾

parent_process_name	process_name	process	process_id	parent_process_id	process_guid
bash	rm	rm -rf /etc/systemd/system	5164	5122	{ec230001-9b48-6262-7043-69efe1550000}
bash	rm	rm -rf /home --no-preserve-root rm -rf /etc/systemd/system	5166	5122	{ec230001-9b48-6262-7093-0e114e560000}

Linux Disable Services

This analytic identifies events that attempt to disable a service. This is typically identified in parallel with other instances of service enumeration of attempts to stop a service and then delete it.

```

| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Processes
where Processes.process_name IN ("systemctl", "service", "svcadm") Processes.process = "* disable*"
by Processes.parent_process_name Processes.process_name Processes.process Processes.process_id Processes.parent_process_id Processes.process_guid Processes.dest Processes.user
| `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 IN ("systemctl", "service", "svcadm") Processes.process = "* disable*"
by Processes.parent_process_name Processes.process_name Processes.process Processes.process_id Processes.parent_process_id Processes.process_guid Processes.dest Processes.user
| `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
    
```

✓ 1 event (22/04/2022 10:09:38.000 to 22/04/2022 10:24:38.000) No Event Sampling ▾

Events Patterns **Statistics (1)** Visualization

20 Per Page ▾ Format Preview ▾

parent_process_name	process_name	process	process_id	parent_process_id	process_guid	dest
sudo	systemctl	systemctl disable apache2	4380	4379	{ec230001-81c1-6262-d0dc-b9e65e550000}	sys

Linux Shred Overwrite Command

This analytic identifies a shred process to overwrite files in a linux machine. Shred Linux application is designed to overwrite a file to hide its contents or make the deleted file unrecoverable.

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint
```

```
where Processes.process_name =shred AND Processes.process IN ("*-n*", "*-u*", "*-z*", "*-s*")
```

```
by Processes.parent_process_name 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)`
```

NEW SEARCH

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Processes
where Processes.process_name =shred AND Processes.process IN ("*-n*", "*-u*", "*-z*", "*-s*")
by Processes.parent_process_name Processes.process_name Processes.process Processes.process_id Processes.parent_process_id Processes.process_guid Processes.dest Processes.user
| `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

5 events (22/04/2022 08:35:00.000 to 22/04/2022 12:35:07.000) No Event Sampling

Events Patterns **Statistics (5)** Visualization

20 Per Page Format Preview

parent_process_name	process_name	process	process_id	parent_process_id	process_guid
bash	shred	shred -n 1 -x -z /boot	5169	5122	{ec230001-9b48-6262-50df-8eb5f1550000}
bash	shred	shred -n 1 -x -z /usr/lib/systemd/system	5165	5122	{ec230001-9b48-6262-50ef-678624560000}
bash	shred	shred -n 1 -x -z /usr/lib/systemd/system	5167	5122	{ec230001-9b48-6262-50df-5cdb6e550000}
sudo	shred	shred -n 1 -x -z /boot	5200	5199	{ec230001-9be1-6262-50cf-aa2c0b560000}
sudo	shred	shred -n 1 -x -z /boot	5224	5223	{ec230001-9c75-6262-50df-1d86bc550000}

Linux Stop Services

This analytic identifies events that attempt to stop or clear a service.

This is typically identified in parallel with other instances of service enumeration of attempts to stop a service and then delete it.

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint
```

```
where Processes.process_name IN ("systemctl", "service", "svcadm") Processes.process = "*stop*"
```

```
by Processes.parent_process_name Processes.process_name Processes.process Processes.process_id Processes.parent_process_id
```

```
Processes.process_guid Processes.dest Processes.user
```

```
| `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 IN ("systemctl", "service", "svcadm") Processes.process = "*stop*"
by Processes.parent_process_name Processes.process_name Processes.process Processes.process_id Processes.parent_process_id
Processes.process_guid Processes.dest Processes.user
| `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

✓ 1 event (22/04/2022 09:41:00.000 to 22/04/2022 10:41:53.000) No Event Sampling ▾

Events Patterns **Statistics (1)** Visualization

20 Per Page ▾ / Format Preview ▾

parent_process_name	process_name	process	process_id	parent_process_id	process_guid	dest	user
sudo	systemctl	systemctl stop apache2	4465	4464	{		

Linux High Frequency Of File Deletion In Boot Folder

This analytic identifies a high frequency of file deletion relative to process name and process id /boot/ folder.

```
| tstats `security_content_summariesonly` values(Filesystem.file_name) as deletedFileNames values(Filesystem.f
```

```
FROM datamodel=Endpoint.Filesystem
```

```
where Filesystem.action=deleted Filesystem.file_path = "/boot/*"
```

```
by _time span=1h Filesystem.dest Filesystem.process_guid Filesystem.action
```

```
| `drop_dm_object_name(Filesystem)`
```

```
|rename process_guid as proc_guid
```

```
|join proc_guid, _time [
```

```
| tstats `security_content_summariesonly` count FROM datamodel=Endpoint.Processes where Processes.parent_pro
```

```
NOT (Processes.parent_process_name IN ("/usr/bin/dpkg", "*usr/bin/python*", "*usr/bin/apt-*", "/bin/rm", "*s
```

```
by _time span=1h Processes.process_id Processes.process_name Processes.process Processes.dest Processes.paren
```

```
| `drop_dm_object_name(Processes)`
```

```
|rename process_guid as proc_guid
```

```
| fields _time dest user parent_process_name parent_process process_name process_path process proc_guid regi:
```

```
| table process_name process proc_guid action _time deletedFileNames deletedFilePath numOfDelFilePath paren
```

```
| where numOfDelFilePath >= 200
```

```
| tstats `security_content_summariesonly` values(Filesystem.file_name) as deletedFileNames values(Filesystem.file_path) as deletedFilePath dc(Filesystem.file_path) as numOfDelFilePath count min(_time) as firstTime max(_time) as lastTime
FROM datamodel=Endpoint.Filesystem
where Filesystem.action=deleted Filesystem.file_path = "/boot/*"
by _time span=1h Filesystem.dest Filesystem.process_guid Filesystem.action
| `drop_dm_object_name(Filesystem)`
|rename process_guid as proc_guid
|join proc_guid, _time [
| tstats `security_content_summariesonly` count FROM datamodel=Endpoint.Processes where Processes.parent_process_name != unknown
NOT (Processes.parent_process_name IN ("/usr/bin/dpkg", "*usr/bin/python*", "*usr/bin/apt-*", "/bin/rm", "*splunkd", "/usr/bin/mandb"))
by _time span=1h Processes.process_id Processes.process_name Processes.process Processes.dest Processes.parent_process_name Processes.parent_process_name Processes.process_path Processes.process_guid
| `drop_dm_object_name(Processes)`
|rename process_guid as proc_guid
| fields _time dest user parent_process_name parent_process process_name process_path process proc_guid registry_path registry_value_name registry_value_data registry_key_name action]
| table process_name process proc_guid action _time deletedFileNames deletedFilePath numOfDelFilePath parent_process_name parent_process process_path dest user
| where numOfDelFilePath >= 200
```

290 events (22/04/2022 11:20:00.000 to 22/04/2022 12:20:10.000) No Event Sampling

Events Patterns **Statistics (1)** Visualization

20 Per Page Format Preview

process_name	process	proc_guid	action	_time	deletedFileNames	deletedFilePath	numOfDelFilePath	parent_process_name	parent_process
rm	rm -rf /boot --no-preserve-root	(ec238801-9ccc-6262-7843-981383568080)	deleted	2022-04-22 12:00:00	915resolution.mod System.map-5.4.0-1071-aws aws acpi.mod adler32.mod affs.mod afs.mod	/boot/System.map-5.4.0-1071-aws /boot/config-5.4.0-1071-aws /boot/grub/default /boot/grub/fonts/unicode.pf2 /boot/grub/gfxblacklist.txt /boot/grub/grub.cfg /boot/grub/grubenv	298	dash	sh

Windows Processes Killed By Industroyer2 Malware

This analytic identifies known processes killed by Industroyer2 malware.

This technique was seen in the Industroyer2 malware attack that tries to kill several processes of windows host machines related to the energy facility network.

```
`sysmon` EventCode=5 process_name IN ("PServiceControl.exe", "PService_PPD.exe")
```

```
| stats min(_time) as firstTime max(_time) as lastTime count by process_name process process_path process_guid
```

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

```
'sysmon' EventCode=5 process_name IN ("PServiceControl.exe", "PService_PPD.exe")
| stats min(_time) as firstTime max(_time) as lastTime count by process_name process process_path process_guid process_id EventCode dest user_id
| `security_content_ctime(firstTime)` | `security_content_ctime(lastTime)`
```

✓ 2 events (before 22/04/2022 14:07:15.000) No Event Sampling ▼

Events Patterns **Statistics (2)** Visualization

20 Per Page ▼ Format Preview ▼

process_name ↕	process ↕	process_path ↕	process_guid ↕	process_id ↕	EventCode ↕
PServiceControl.exe	C:\OIK\Temporary0\PServiceControl.exe	C:\OIK\Temporary0\PServiceControl.exe	{8D845A55-24B5-6260-EB02-00000004402}	5824	5
PService_PPD.exe	C:\OIK\Temporary0\PService_PPD.exe	C:\OIK\Temporary0\PService_PPD.exe	{8D845A55-24BC-6260-ED02-00000004402}	4104	5

Windows Hidden Schedule Task Settings

The following query utilizes Windows Security EventCode 4698. A scheduled task was created to identify suspicious tasks registered on Windows either via schtasks.exe OR TaskService with hidden settings that are unique entry of malware like Industroyer2 or attack that uses lolbin to download other files or payload to the infected machine.

```
`wineventlog_security` EventCode=4698
```

```
| xmlkv Message
```

```
| search Hidden = true
```

```
| stats count min(_time) as firstTime max(_time) as lastTime by Task_Name, Command, Author, Hidden, dest
```

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

New Search

```
`wineventlog_security` EventCode=4698
| xmlkv Message
| search Hidden = true
| stats count min(_time) as firstTime max(_time) as lastTime by Task_Name, Command, Author, Hidden, dest
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

✓ 1 event (25/04/2022 11:00:00.000 to 26/04/2022 11:18:37.000) No Event Sampling ▾

Events Patterns **Statistics (1)** Visualization

20 Per Page ▾  Format Preview ▾

Task_Name	Command	Author	Hidden
\MyTaskname	%~dp0\MyBatch.bat	ATTACKRANGE\administrator	true

Windows Linked Policies In ADSI Discovery

This analytic utilizes PowerShell Script Block Logging (EventCode=4104) to identify the `[Adsisearcher]` type accelerator being used to query Active Directory for domain groups.

```
`powershell` EventCode=4104 ScriptBlockText = "*[adsisearcher]*" ScriptBlockText = "*objectcategory=organizationalunit"
```

```
| stats count min(_time) as firstTime max(_time) as lastTime by EventCode ScriptBlockText Computer user_id
```

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

New Search

Alerts

```
`powershell` EventCode=4104 ScriptBlockText = "*[adsisearcher]*" ScriptBlockText = "*objectcategory=organizationalunit*" ScriptBlockText = "*.findall()*"
| stats count min(_time) as firstTime max(_time) as lastTime by EventCode ScriptBlockText Computer user_id
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

✓ 2 events (24/04/2022 09:00:00.000 to 25/04/2022 09:54:14.000) No Event Sampling ▾

Events Patterns **Statistics (2)** Visualization

20 Per Page ▾  Format Preview ▾

EventCode	ScriptBlockText
4104	(([adsisearcher]'LDAP://DC=adsecurity,DC=lab'),([adsisearcher]'(objectcategory=organizationalunit)').findall()).Path %if([[ADSISearcher]].gPlink){Write-Host "[+] OU Path:"([ADSISearcher]).Path;\$a=([ADSISearcher].gPlink) -replace "[;]" -split " ";for(\$i=0;\$i -lt \$a.Length;\$i++){if(\$a[\$i]){Write-Host "Policy Path[\$i]:"([ADSISearcher].Substring(0,\$a[\$i].length-1)).Path;Write-Host "Policy Name[\$i]:"([ADSISearcher].Substring(0,\$a[\$i].length-1)).DisplayName } ;Write-Output "n" }}
4104	(([adsisearcher]'(objectcategory=organizationalunit)').FindAll()).Path %if([[ADSISearcher]].gPlink){Write-Host "[+] OU Path:"([ADSISearcher]).Path;\$a=([ADSISearcher].gPlink) -replace "[;]" -split " ";for(\$i=0;\$i -lt \$a.Length;\$i++){if(\$a[\$i]){Write-Host "Policy Path[\$i]:"([ADSISearcher].Substring(0,\$a[\$i].length-1)).Path;Write-Host "Policy Name[\$i]:"([ADSISearcher].Substring(0,\$a[\$i].length-1)).DisplayName } ;Write-Output "n" }}

Windows Root Domain Linked Policies Discovery

This analytic utilizes PowerShell Script Block Logging (EventCode=4104) to identify the `[Adsiseacher]` type accelerator being used to query Active Directory for domain groups. Red Teams and adversaries may leverage `[Adsiseacher]` to enumerate root domain linked policies for situational awareness and Active Directory Discovery.

```
`powershell` EventCode=4104 ScriptBlockText = "*[adsiseacher]*" ScriptBlockText = "*.SearchRoot*" ScriptBlock
```

```
| stats count min(_time) as firstTime max(_time) as lastTime by EventCode ScriptBlockText Computer user_id
```

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

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

New Search

```
`powershell` EventCode=4104 ScriptBlockText = "*[adsiseacher]*" ScriptBlockText = "*.SearchRoot*" ScriptBlockText = "*([ADSI]"$_.gplink)"
| stats count min(_time) as firstTime max(_time) as lastTime by EventCode ScriptBlockText Computer user_id
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

✓ 1 event (24/04/2022 10:00:00.000 to 25/04/2022 10:02:31.000) No Event Sampling ▾

Events Patterns **Statistics (1)** Visualization

20 Per Page ▾ Format Preview ▾

EventCode	ScriptBlockText
4104	<pre>(([adsiseacher]`).SearchRoot).Path %{{if([ADSI]"\$_.gplink){Write-Host "[+] Domain Path:"([ADSI]"\$_.Path;\$a=([ADSI]"\$_.gplink) -replace "[[;]" -split "];for(\$i=0;\$i -lt \$a.length;\$i++){if(\$a[\$i]){Write-Host "Policy Path[\$i]:"([ADSI] (\$a[\$i]).Substring(0,\$a[\$i].length-1)).Path;Write-Host "Policy Name[\$i]:"([ADSI](\$a[\$i]).Substring(0,\$a[\$i].length-1)).DisplayName} };Write-Output "n"}}</pre>

* To see a detailed explanation on the different types please refer to [this](#) wiki.

IOC:

Mitigation

Please follow [CISA and NSA Joint advisory](#) on securing Operational Technology (OT).

Learn More

You can find the latest content about security analytic stories on [GitHub](#) and in [Splunkbase](#). [Splunk Security Essentials](#) also has these detections available via push update. In the upcoming weeks, the Splunk Threat Research Team will be releasing a more detailed blog post on this analytic story. Stay tuned!

For a full list of security content, check out the [release notes](#) on [Splunk Docs](#).

Feedback

Any feedback or requests? Feel free to put in an issue on GitHub and we'll follow up. Alternatively, join us on the [Slack](#) channel #security-research. Follow [these instructions](#) If you need an invitation to our Splunk user groups on Slack.

We would like to thank the following for their contributions to this post: Teoderick Contreras, Rod Soto, Jose Hernandez, Patrick Barreiss, Lou Stella, Mauricio Velazco, Michael Haag, Bhavin Patel, and Eric McGinnis

Source: https://www.splunk.com/en_us/blog/security/threat-update-industry2.html