DarkPulsar

SL securelist.com/darkpulsar/88199/



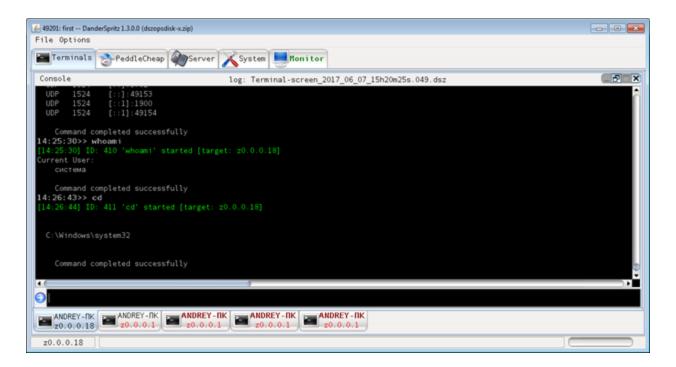
Authors

- Expert Andrey Dolgushev
 Dmitry Tarakanov
- Expert Vasily Berdnikov

In March 2017, the ShadowBrokers published a chunk of stolen data that included two frameworks: DanderSpritz and FuzzBunch.

DanderSpritz consists entirely of plugins to gather intelligence, use exploits and examine already controlled machines. It is written in Java and provides a graphical windows interface similar to botnets administrative panels as well as a Metasploit-like console interface. It also

includes its own backdoors and plugins for not-FuzzBunch-controlled victims.



DanderSprit interface

Fuzzbunch on the other hand provides a framework for different utilities to interact and work together. It contains various types of plugins designed to analyze victims, exploit vulnerabilities, schedule tasks, etc. There are three files in the plugin set from the FuzzBunch framework:

%pluginName%-version.fb

This is the utility file of the framework. It duplicates the header from XML and includes the plugin's ID.

%pluginName%-version.exe

This executable file is launched when FuZZbuNch receives the command to do so.

%pluginName%-version.xml

This configuration file describes the plugin's input and output parameters – the parameter name, its type and description of what it's responsible for; all of these can be shown in FuzzBunch as a prompt. This file also contributes a lot to the framework's usability, as it supports the specification of default parameters.

One of the most interesting Fuzzbunch's categories is called ImplantConfig and includes plugins designed to control the infected machines via an implant at the post-exploitation stage. **DarkPulsar** is a very interesting administrative module for controlling a passive

backdoor named 'sipauth32.tsp' that provides remote control, belonging to this category.

It supports the following commands:

- Burn
- RawShellcode
- EDFStagedUpload
- DisableSecurity
- EnableSecurity
- UpgradeImplant
- PingPong

Burn, RawShellcode, UpgradeImplant, and *PingPong* remove the implant, run arbitrary code, upgrade the implant and check if the backdoor is installed on a remote machine, respectively. The purpose of the other commands is not that obvious and, to make it worse, the leaked framework contained only the administrative module to work with DarkPulsar's backdoor, but not the backdoor itself.

While analyzing the administrative module, we noticed several constants that are used to encrypt the traffic between the C&C and the implant:

```
(TcLog) (v2, 5, "[+] - Performing crypto session setup\n");
v3 = v1[1];
sub 402B70(pbBuffer, 4u);
*&pbBuffer[4] = 0x3BA6814F - *pbBuffer;
v4 = *pbBuffer ^ (0x3BA6814F - *pbBuffer);
v5 = *v1;
*(\varepsilon v 28 + 1) = 4;
HIBYTE(v27) = 5;
*(&v27 + 3) ^= v4;
*(&v28 + 3) = v4 ^ 0xAA64F13D;
v21 = 16;
v20 = 16;
v22 = pbBuffer;
v6 = (*(*v5 + 8))(&v20, &v23);
v7 = v6;
if ( v6 && v6 != 0x90312 )
Ł
  TcLog(v1[2], 3, "[%s] - CDPProtocolHandler::SendRecv Failed (0x%x)\n",
        "CDPClient::PerformSetupSession", v6);
}
else
₹.
  v8 = v25;
  if ( (v25 || v23) && v23 >= 16 )
  {
    v9 = *v25;
    v16 = v25;
    if ( *v25 + v25[1] == 0xA13C82E )
```

We thought that probably these constants should also appear in the backdoor, so we created a detection for them. Several months later we found our mysterious DarkPulsar backdoor. We later were able to find both 32- and 64-bit versions.

We found around 50 victims located in Russia, Iran and Egypt, typically infecting Windows 2003/2008 Server. Targets were related to nuclear energy, telecommunications, IT, aerospace and R&D.

DarkPulsar technical highlights

The DarkPulsar implant is a dynamic library whose payload is implemented in exported functions. These functions can be grouped as follows:

- 1. Two nameless functions used to install the backdoor in the system.
- 2. Functions with names related to TSPI (Telephony Service Provider Interface) operations that ensure the backdoor is in the autorun list and launched automatically.
- 3. A function with a name related to SSPI (Security Support Provider Interface) operations. It implements the main malicious payload.

The implementations of the SSPI and TSPI interfaces are minimalistic: the functions that are exported by DarkPulsar have the same names as the interface functions; however, they include malicious code instead of the phone service.

The implant is installed in the system by the nameless exported function. The backdoor is launched by calling Secur32.AddSecurityPackage with administrator privileges with the path to its own library in the parameter, causing lsass.exe to load DarkPulsar as SSP/AP and to call its exported function *SpLsaModeInitialize* used by DarkPulsar to initialize the backdoor. In this way AddSecurityPackage is used to inject code into lsass.exe. It also adds its library name at HKLM\Software\Microsoft\Windows\CurrentVersion\Telephony\Providers

This is loaded at start by the Telephony API (TapiSrv) launched alongside the Remote Access Connection Manager (RasMan) service, setting startup type as "Automatic". When loading the telephony service provider's library, TapiSrv calls *TSPI_lineNegotiateTSPIVersion* which contains the AddSecurityPackage call to make the inject into Isass.exe.

DarkPulsar implements its payload by installing hooks for the SpAcceptLsaModeContext – function responsible for authentication. Such injects are made in several system authentication packets within the process lsass.exe and allow Darkpulsar to control authentication process based on the following protocols:

- Msv1_0.dll for the NTLM protocol,
- Kerberos.dll for the Kerberos protocol,
- Schannel.dll for the TLS/SSL protocols,
- Wdigest.dll for the Digest protocol, and
- Lsasrv.dll -for the Negotiate protocol.

After this, Darkpulsar gets ability to embed malware traffic into system protocols. Since this network activity takes place according to standard system charts, it will only be reflected in the System process – it uses the system ports reserved for the above protocols without hindering their normal operation.

Eth	ame 6: 204 bytes on wire (1632 bits), 204 bytes cap hernet II, Src: PcsCompu_90:44:d2 (08:00:27:90:44:d	
	ternet Protocol Version 4, Src: 192.168.56.104, Dst	
	ansmission Control Protocol, Src Port: 1502, Dst Po	rt: 445, Seq: 138, Ack: 132, Len: 150
	tBIOS Session Service	
	B (Server Message Block Protocol)	
	SMB Header	
-	Session Setup AndX Request (0x73)	
	Word Count (WCT): 12	
	AndXCommand: No further commands (0xff)	
	Reserved: 00	
	AndXOffset: 59	
	Max Buffer: 4356	
	Max Mpx Count: 10	
	VC Number: 25	
	Session Key: 0x0000000	
	Security Blob Length: 16	
	Reserved: 00000000	
	Capabilities: 0x800000d4, Unicode, NT SMBs, N	Status Codes, Level 2 Oplocks, Extended Security
	Byte Count (BCC): 87	
	a lo al la collectere de la case a la lai ana a las	
	Security Blob: 04d647334bab5e084a7d1d3b728c7d91	
	Security Blob: 04d647334bab5e084a7d1d3b728c7d91 Native OS: Windows 2000 2195	
	Native OS: Windows 2000 2195	
	Native OS: Windows 2000 2195	
0000	Native OS: Windows 2000 2195	's '.DE.
	Native OS: Windows 2000 2195 Native LAN Manager: Windows 2000 5.0	's '.DE.).@n8h
0010 0020	Native OS: Windows 2000 2195 Native LAN Manager: Windows 2000 5.0 08 00 27 73 f8 81 08 00 27 90 44 d2 08 00 45 00 00 be 29 ab 40 00 80 06 de 6e c0 a8 38 68 c0 a8 38 67 05 de 01 bd 14 0d fc 59 39 4c 5a 50 50 18).@n8h 8gY9LZPP.
0010 0020 0030	Native OS: Windows 2000 2195 Native LAN Manager: Windows 2000 5.0 08 00 27 73 f8 81 08 00 27 90 44 d2 08 00 45 00 00 be 29 ab 40 00 80 06 de 6e c0 a8 38 68 c0 a8 38 67 05 de 01 bd 14 0d fc 59 39 4c 5a 50 50 18 fa 6d 9e 0e 00 00 00 00 00 92 ff 53 4d 42 73 00).@sh 8gY9LZPP. .mSMBs.
0010 0020 0030 0040	Native OS: Windows 2000 2195 Native LAN Manager: Windows 2000 5.0 08 00 27 73 f8 81 08 00 27 90 44 d2 08 00 45 00 00 be 29 ab 40 00 80 06 de 6e c0 a8 38 68 c0 a8 38 67 05 de 01 bd 14 0d fc 59 39 4c 5a 50 50 18 fa 6d 9e 0e 00 00 00 00 00 92 ff 53 4d 42 73 00 00 00 00 18 07 c8 00 00 00 00 00 00 00 00 00 00).@
0010 0020 0030 0040 0050	Native OS: Windows 2000 2195 Native LAN Manager: Windows 2000 5.0 08 00 27 73 f8 81 08 00 27 90 44 d2 08 00 45 00 00 be 29 ab 40 00 80 06 de 6e c0 a8 38 68 c0 a8 38 67 05 de 01 bd 14 0d fc 59 39 4c 5a 50 50 18 fa 6d 9e 0e 00 00 00 00 00 92 ff 53 4d 42 73 00 00 00 00 18 07 c8 00 00 00 00 00 00 00 00 00 00 00 00 00).@
0010 0020 0030 0040 0050 0060	Native OS: Windows 2000 2195 Native LAN Manager: Windows 2000 5.0 08 00 27 73 f8 81 08 00 27 90 44 d2 08 00 45 00 00 be 29 ab 40 00 80 06 de 6e c0 a8 38 68 c0 a8 38 67 05 de 01 bd 14 0d fc 59 39 4c 5a 50 50 18 fa 6d 9e 0e 00 00 00 00 00 92 ff 53 4d 42 73 00 00 00 00 18 07 c8 00 00 00 00 00 00 00 00 00 00 00 00 00).@
0010 0020 0030 0040 0050 0060 0060	Native OS: Windows 2000 2195 Native LAN Manager: Windows 2000 5.0 08 00 27 73 f8 81 08 00 27 90 44 d2 08 00 45 00 00 be 29 ab 40 00 80 06 de 6e c0 a8 38 68 c0 a8 38 67 05 de 01 bd 14 0d fc 59 39 4c 5a 50 50 18 fa 6d 9e 0e 00 00 00 00 00 22 ff 53 4d 42 73 00 00 00 08 18 07 c8 00 00 00 00 00 26 ff 53 4d 42 73 00 00 00 00 08 ff fe 00 00 40 00 00 00 00 00 00 00 00 00 00).@sh 8gSMBs.
0010 0020 0030 0040 0050 0060 0060 0070 0080	Native OS: Windows 2000 2195 Native LAN Manager: Windows 2000 5.0 08 00 27 73 f8 81 08 00 27 90 44 d2 08 00 45 00 00 be 29 ab 40 00 80 06 de 6e c0 a8 38 68 c0 a8 38 67 05 de 01 bd 14 0d fc 59 39 4c 5a 50 50 18 fa 6d 9e 0e 00 00 00 00 00 92 ff 53 4d 42 73 00 00 00 00 18 07 c8 00 00 00 00 00 00 00 00 00 00 00 00 00).@
0010 0020 0030 0040 0050 0060 0060 0070 0080 0090	Native OS: Windows 2000 2195 Native LAN Manager: Windows 2000 5.0 08 00 27 73 f8 81 08 00 27 90 44 d2 08 00 45 00 00 be 29 ab 40 00 80 06 de 6e c0 a8 38 68 c0 a8 38 67 05 de 01 bd 14 0d fc 59 39 4c 5a 50 50 18 fa 6d 9e 0e 00 00 00 00 00 92 ff 53 4d 42 73 00 00 00 00 ff fe 00 00 00 00 00 cf fo0 3b 00 04 11 0a 00 19 00 00 00 00 00 00 00 00 00 00 00 00 00).@sh 8gSMBs.
0010 0020 0030 0040 0050 0060 0070 0080 0090 0080	Native OS: Windows 2000 2195 Native LAN Manager: Windows 2000 5.0 08 00 27 73 f8 81 08 00 27 90 44 d2 08 00 45 00 00 be 29 ab 40 00 80 06 de 6e c0 a8 38 68 c0 a8 38 67 05 de 01 bd 14 0d fc 59 39 4c 5a 50 50 18 fa 6d 9e 0e 00 00 00 00 00 92 ff 53 4d 42 73 00 00 00 00 18 07 c8 00 00 00 00 02 ff 53 4d 42 73 00 00 00 00 18 07 c8 00 00 00 00 00 c0 00 00 00 00 00 00 00 00 ff fe 00 00 00 00 00 00 00 00 00 00 00 00 00).@
0010 0020 0030 0040 0050 0060 0070 0080 0090 0080 0080	Native OS: Windows 2000 2195 Native LAN Manager: Windows 2000 5.0 08 00 27 73 f8 81 08 00 27 90 44 d2 08 00 45 00 00 be 29 ab 40 00 80 06 de 6e c0 a8 38 68 c0 a8 38 67 05 de 01 bd 14 0d fc 59 39 4c 5a 50 18 fa 6d 9e 00 00 00 00 00 00 00 00 00 00 00 00 00).@
0010 0020 0030 0040 0050 0060 0070 0080 0090 0080 0080	Native OS: Windows 2000 2195 Native LAN Manager: Windows 2000 5.0 08 00 27 73 f8 81 08 00 27 90 44 d2 08 00 45 00 00 be 29 ab 40 00 80 06 de 6e c0 a8 38 68 c0 a8 38 67 05 de 01 bd 14 0d fc 59 39 4c 5a 50 50 18 fa 6d 9e 0e 00 00 00 00 00 00 2 ff 53 4d 42 73 00 00 00 00 01 18 07 c8 00 00 00 00 00 00 00 00 00 00 00 41 10 a0 19 00 00 00 00 00 00 00 00 00 00 00 00 00).@
0010 0020 0030 0040 0050 0060 0070 0080 0090 0080 0080	Native OS: Windows 2000 2195 Native LAN Manager: Windows 2000 5.0 08 00 27 73 f8 81 08 00 27 90 44 d2 08 00 45 00 00 be 29 ab 40 00 80 06 de 6e c0 a8 38 66 c0 a8 38 67 05 de 01 bd 14 0d fc 59 39 4c 5a 50 50 18 fa 6d 9e 0e 00 00 00 00 00 92 ff 53 4d 42 73 00 00 00 00 ff fe 00 00 00 00 00 c0 00 2 ff 53 4d 42 73 00 00 00 00 60 ff fe 00 00 00 00 00 00 00 00 00 00 00 00 00).@sh 8gyuzpp. .m
0010 0020 0030 0040 0050 0060 0070 0080 0090 0080 0080	Native OS: Windows 2000 2195 Native LAN Manager: Windows 2000 5.0 08 00 27 73 f8 81 08 00 27 90 44 d2 08 00 45 00 00 be 29 ab 40 00 80 06 de 6e c0 a8 38 68 c0 a8 38 67 05 de 01 bd 14 0d fc 59 39 4c 5a 50 50 18 fa 6d 9e 0e 00 00 00 00 00 00 2 ff 53 4d 42 73 00 00 00 00 01 18 07 c8 00 00 00 00 00 00 00 00 00 00 00 41 10 a0 19 00 00 00 00 00 00 00 00 00 00 00 00 00).@sh 8gyuzpp. .msMBs.

Network traffic during successful connection to DarkPulsar implant

The second advantage of controlling authentication processes is ability to bypass entering a valid username and password for obtaining access to objects that require authentication such as processes list, remote registry, file system through SMB. After Darkpulsar's DisableSecurity command is sent, backdoor's hooks on the victim side will always returns in the SpAcceptLsaModeContext function that passed credentials are valid. Getting that, system will provide access to protected objects to client.

Working with DarkPulsar

Darkpulsar-1.1.0.exe is the administrative interface working under the principle of "one command – one launch". The command to be executed must be specified either in the configuration file Darkpulsar-1.1.0.9.xml or as command line arguments, detailing at least:

- whether the target machine uses a 32-bit or 64-bit system;
- protocol (SMB, NBT, SSL, RDP protocols are supported) to deliver the command and port number
- private RSA key to decrypt the session AES key

Darkpulsar-1.1.0 was not designed as a standalone program for managing infected machines. This utility is a plugin of the Fuzzbunch framework that can manage parameters and coordinate different components. Here is how DisableSecurity command in Fuzzbunch looks like:

```
C:\Python26\python.exe
                                                                                                                              - - X
fb ImplantConfig (Darkpulsar) > set ImplantAction DisableSecurity
[+] Set ImplantAction => DisableSecurity
fb ImplantConfig (Darkpulsar) > execute
 Preparing to Execute Darkpulsar
Redirection OFF
 [*] Configure Plugin Local Tunnels
[*] Local Tunnel - local-tunnel-1
[?] Destination IP [127.0.0.1]:
[?] Destination Port [445]:
[*] (TCP) Local 127.0.0.1:445
 Configure Plugin Remote Tunnels
Module: Darkpulsar
                                         Value
Name
                                                                                                                                                Ξ
TargetIp
SspMTU
                                         127.0.0.1
TargetPort
                                         445
NetworkTimeout
                                         60
SSPFragmentSize
PrivateKeyInputType
PrivateKeyFile
                                         0
                                         File
                                         C:\Users\Andrey\Desktop\fuzzbunch-master\private.k
                                         ey
DisableSecurity
ImplantAction
Protocol
UseNTLMSSPHeader
                                         SMB
                                         False
Architecture
                                         ×86
[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] - Performing crypto session setup
[+] - Performing crypto session setup
[+] Darkpulsar Succeeded
fb ImplantConfig (Darkpulsar) >
```

Below is an example of Processlist after DisableSecurity, allowing to execute any plugin without valid credentials and operating via regular system functions (remote registry service):

		exe			
	Processli				
ane		Value			
 etworkTi argetIp argetPor ogFile sername redentia uthLevel redentia	∿t 1	60 127.0.0.1 445 processlist.txt 416e64726579 416e64726579 None UnicodeCreds			
😫 Execu	ıting Plu	n? [Yes] : gin st >>>			
"" [+] "T [+] "T [+] "N [+] "U [+] "C [*] Init	argetIp" argetPor letworkTi lsername" Credentia talizing	t" 445 meout" 60 416e6472657 1" 416e6472657 Network	29	Andrey Andrey	
[*] Perf [+] Co	forming P Innected	rocess List to the Registry Ser	vice		
ystem Na ystem Up	ume otime (H:	rocess List to the Registry Ser : ANDREY-494 M:S>: 10:00:07	∾ice :017 15:34:25 GMT		
ystem Na ystem Up ystem Ti	ume otime (H:	rocess List to the Registry Ser : ANDREY-494 M:S>: 10:00:07		Handles	Threads
ystem Na ystem Up ystem Ti	ume otime (H: ime	rocess List to the Registry Ser : ANDREY- ¹¹ Я ¹¹ Ъ M:S>: 10:00:07 : Wed, 07 Jun 2	017 15:34:25 GMT	Handles 0	Threads 1
ystem Na ystem Up ystem Ti	ume otime (H: ime PPID	rocess List to the Registry Ser : ANDREY-UAU M:S>: 10:00:07 : Wed, 07 Jun 2 Process Name	017 15:34:25 GMT		
ystem Na ystem Up ystem Ti ID	ome otime <h: ime PPID O</h: 	rocess List to the Registry Ser : ANDREY- ^{UAU} b M:S>: 10:00:07 : Wed, 07 Jun 2 Process Name 	017 15:34:25 GMT	0	1
ystem Na ystem Up ystem Ti ID 	ame otime <h: ime PPID 0 0</h: 	rocess List to the Registry Ser : ANDREY-4944 M:S>: 10:00:07 : Wed, 07 Jun 2 Process Name Idle System	2017 15:34:25 GMT Runtime	0 416	1 86
ystem Na ystem Up ystem Ti ID 	ume otime (H: ime PPID 0 0 4	rocess List to the Registry Ser : ANDREY-UAUb M:S>: 10:00:07 : Wed, 07 Jun 2 Process Name Idle System smss	017 15:34:25 GMT Runtime 	0 416 29	1 86 2
ystem Na ystem Up ystem Ti ID 64 36	nne otime <h: PPID 0 0 4 328</h: 	rocess List to the Registry Ser : ANDREY-UAU M:S>: 10:00:07 : Wed, 07 Jun 2 Process Name Idle Systen smss csrss	2017 15:34:25 GMT Runtime 121:00:15 121:00:15	0 416 29 530	1 86 2 9
ystem Na	nne otime (H: PPID 0 0 4 328 328	rocess List to the Registry Ser : ANDREY-UAU M:S>: 10:00:07 : Wed, 07 Jun 2 Process Name Idle System smss csrss wininit	017 15:34:25 GMT Runtime 121:00:15 121:00:15 121:00:15	0 416 29 530 74	1 86 2 9 3

DanderSpritz

DanderSpritz is the framework for controlling infected machines, different from FuZZbuNch as the latter provides a limited toolkit for the post-exploitation stage with specific functions such as DisableSecurity and EnableSecurity for DarkPulsar.

For DanderSpritz works for a larger range of backdoors, using PeedleCheap in the victim to enable operators launching plugins. PeddleCheap is a plugin of DanderSpritz which can be used to configure implants and connect to infected machines. Once a connection is established all DanderSpritz post-exploitation features become available.

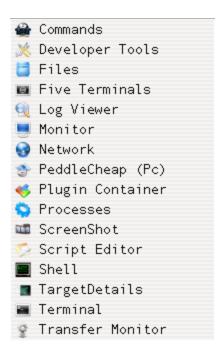
This is how DarkPulsar in EDFStagedUpload mode provides the opportunity to infect the victim with a more functional implant: PCDIILauncher (Fuzzbunch's plugin) deploys the PeddleCheap implant on the victim side, and DanderSpritz provides a user-friendly post-

exploitation interface. Hence, the full name of PCDIILauncher is 'PeddleCheap DLL Launcher'.

The complete DanderSpritz usage scheme with the plugin PeddleCheap via FuZZbuNch with the plugins DarkPulsar and PCDIILauncher consists of four steps:

- Via FuZZbuNch, run command EDFStagedUpload to launch DarkPulsar.
- In DanderSpritz, run command pc_prep (PeedelCheap Preparation) to prepare the payload and the library to be launched on the implant side.
- In DanderSpritz, run command pc_old (which is the alias of command pc_listen -reuse nolisten -key Default) this sets it to wait for a socket from Pcdllauncher.

 Launch Pcdlllauncher via FuZZbuNch and specify the path to the payload that has been prepared with the command pc_prep in the ImplantFilename parameter.



DanderSpritz

	PeddleCheap	Server	System	Monitor				
0.0.0.11	📑 🕨 🖾 C: 🕨							
0.0.0.12	Name	Alt	Name	Size		Created	Modified	Accessed
	SRecycle.Bin				<dir></dir>	7/14/2009 2:36	3/10/2017 3:57	3/10/2017 3:57
.0.0.15	Documents an				<dir></dir>	7/14/2009 4:53	7/14/2009 4:53	7/14/2009 4:53
.0.0.16	. i go				<dir></dir>	6/1/2017 5:31:	6/1/2017 5:31:	6/1/2017 5:31:
0.0.18	Logs				<dir></dir>	5/25/2017 10:4	12:26:14 PM	12:26:14 PM
7.0.0.1	PerfLogs				<dir></dir>	7/14/2009 2:37	7/14/2009 2:37	7/14/2009 2:37
	prjs				<dir></dir>	6/2/2017 10:39	6/2/2017 10:39	6/2/2017 10:39
	Program Files				<dir></dir>	7/14/2009 2:37	5/24/2017 3:35	5/24/2017 3:35
	ProgramData				<dir></dir>	7/14/2009 2:37	5/24/2017 3:35	5/24/2017 3:35
	Python26				<dir></dir>	5/24/2017 3:44	5/24/2017 3:47	5/24/2017 3:47
	Python27				<dir></dir>	5/24/2017 3:06	5/24/2017 3:41	5/24/2017 3:41
	Recovery				<dir></dir>	3/10/2017 3:56	3/10/2017 3:56	3/10/2017 3:56
	System Volum				<dir></dir>	3/10/2017 3:52	1:26:14 PM	1:26:14 PM
	.i temp				<dir></dir>	5/24/2017 3:47	5/24/2017 3:47	5/24/2017 3:47
	Users				<dir></dir>	7/14/2009 2:37	3/10/2017 3:56	3/10/2017 3:56
	Windows				<dir></dir>	7/14/2009 2:37	3/29/2017 12:5	3/29/2017 12:5
	autoexec.bat				24	7/14/2009 2:04	6/10/2009 9:42	7/14/2009 2:04
	config.sys				10	7/14/2009 2:04	6/10/2009 9:42	7/14/2009 2:04
	두 mda.txt				0	4/14/2017 6:03	4/14/2017 6:03	4/14/2017 6:03
	pagefile.sys			375	7629440	3/10/2017 3:52	6/2/2017 2:18:	3/10/2017 3:52

File System plugin

Conclusions

The FuzzBunch and DanderSpritz frameworks are designed to be flexible and to extend functionality and compatibility with other tools. Each of them consists of a set of plugins designed for different tasks: while FuzzBunch plugins are responsible for reconnaissance and attacking a victim, plugins in the DanderSpritz framework are developed for managing already infected victims.

The discovery of the DarkPulsar backdoor helped in understanding its role as a bridge between the two leaked frameworks, and how they are part of the same attacking platform designed for long-term compromise, based on DarkPulsar's advanced abilities for persistence and stealthiness. The implementation of these capabilities, such as encapsulating its traffic into legitimate protocols and bypassing entering credentials to pass authentication, are highly professional.

Our product can completely remove the related to this attack malware.

Detecting malicious network activity

When EDFStagedUpload is executed in an infected machine, a permanent connection is established, which is why traffic via port 445 appears. A pair of bound sockets also appears in lsass.exe:

I A → [•										
	1											
100 /	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rovd Packet	s Rovd Bytes	
alg.exe	1692 632	TOP	work.	1027	work.	0	LISTENING					
qs.exe	632	TCP	work.	5152	work.	0	LISTENING					
Isacs.exe	708	UDP	work.	isakmp								
loacs.exe	708	UDP	work.	4500								
Isass.exe	708 708 708	UDP TCP TCP	work.	1037	locahost	1038	ESTABLISHED					
Isass.exe	708	TCP	work.	1038	locahost	1037	ESTABLISHED					
sychost.exe	996	TCP	work.	epmap	work.	0	LISTENING					
sychost.exe	1296	UDP	work.	1900							20	3,152
sychost.exe	1116	UDP	work.	1025								
sychost.exe	1116	UDP	work.	nlp		-						
sychost.exe	1116	UDP	work.	n/p 1900								
sychost.exe	1296	UDP	work.	1900								
System	4	TCP	work.	netbico-ssn	work.	0	LISTENING					
System	4	TOP	work.	microsoft-da	work.	0	LISTENING					
System	4	UDP	work.	netbico-na					32 19	1.007	114 30	4,350
System	4	UDP	work.	netbios-dgm					19	3.618	30	173
System	4	UDP	work.	microsoft-da								
		TOP	work	microsoft-ds	andrey-Ne	49176	ESTABLISHED		48	6.576	48	9,312

When DanderSpritz deploys PeddleCheap's payload via the PcDIILauncher plugin, network activity increases dramatically:

alg.exe 1 iqs.exe 6 isass.exe 7	PID 1692 632	Photocol TOP	Local Address work	Local Port	Remote Address	Remote Port	State	Sent Packets	00		
alg.exe 1 iqs.exe 6 isass.exe 7	1692 632	TOP			Remote Address	Remote Port	Cista				
gs.exe	632	TOP	week			a reprinted in the		Serk Packets	Sent Bytes	Rovd Packets	Rovd Bytes
bass.exe 7	632			1027	work.	0	LISTENING				
Isacs.exe 2		TOP	work.	5152	work.	0	LISTENING				
have not	708	UDP	work.	isakmp							
12002-080	708 708	UDP TOP	work.	4500 1037							
Isass.exe 2	708	TOP	work.	1037	locahost	1038	ESTABLISHED	313	62,494	410	830,153
	708	TOP	work.	1038	locahost	1037	ESTABLISHED	537	840,761	312	62,434
sychost.exe S	996	TOP	work.	epmap	work.	0	LISTENING				
	1296	UDP	work.	1900						32	5,240
	1116	UDP	work.	1025							
	1116	UDP	work.	n/p							
	1116	UDP	work.	n/p 1900							
sychost.exe 1	1296	UDP	work.	1900							
System 4	4	TCP	work.	netbics-ssn	work.	0	LISTENING				
System 4	4	TOP	work.	microsoft-da	work.	0	LISTENING				
System 4	4	UDP	work.	netbico-na				60 22	3.607	240 35	10,650
System 4	4	UDP	work.	netbics-dgm				22	4.229	35	173
System 4 System 4	4	UDP	work.	microsoft-da							
System 4	4	109	work	microsoft-ds	andrey-Ne	49176	ESTABLISHED	1,704	299,816	1,900	1,216,352

When a connection to the infected machine is terminated, network activity ceases, and only traces of the two bound sockets in Isass.exe remain:

TCP word TCP word UDP word UDP word TCP word TCP word TCP word UDP word UDP word UDP word UDP word	ok 5152 ok isálmp ok 4500 ok 1037 ok 1038 ok epmap ok 1900	Remote Address work work * iccelhost localhost work	Remote Port 0 	State USTENING USTENING ESTABUSHED ESTABUSHED	Sent Packets 1,151 1,215	Sent Bytes 246.530 1.166.277	Rovd Packets / 1.078 1.114	Scvd Bytes
TOP word TOP word UDP word UDP word TOP word TOP word TOP word UDP word UDP word UDP word UDP word UDP word	ok. 1027 ok. 5152 ok. isakimp ok. 4500 ok. 1037 ok. 1038 ok. epmap ok. 1900	work. work. * localhost localhost work.	0 0 - 1038 1037	LISTENING LISTENING ESTABUSHED ESTABUSHED	1,151	246.538	1.078	1,149,811
TCP wol UDP wol TCP wol TCP wol TCP wol UDP wol UDP wol	ok. 5152 ok. isalimp ok. 4500 ok. 1037 ok. 1038 ok. epmap ok. 1900	work * localhost localhost work	1038 1037	USTENING ESTABUSHED ESTABUSHED	1.151			
UDP word UDP word TCP word TCP word UDP word UDP word UDP word	ofi. isakmp ofi. 4500 ofi. 1037 ofi. 1038 ofi. epmap ofi. 1900	= = locahost locahost work	1038 1037	ESTABLISHED	1.151			
UDP wor TOP wor TOP wor TOP wor UDP wor UDP wor	ok 4500 ok 1037 ok 1038 ok epnap ok 1900	localhost localhost work	1038 1037	ESTABLISHED	1,151			
TCP wol TCP wol UDP wol UDP wol	ok. 1037 ok. 1038 ok. epnap ok. 1900	localhost work.	1038 1037	ESTABLISHED	1,151			
TCP wol TCP wol UDP wol UDP wol	ok. 1038 ok. epmap ok. 1900	localhost work.	1037	ESTABLISHED	1,151			
TCP wol TCP wol UDP wol UDP wol	ok epmap ok 1900	work.			1.215	1 166 277	1 114	
UDP wor UDP wor	ork. 1900		0			1,100,277	1,114	246,538
UDP wor	ok. 1900			LISTENING				
		-					40	6.632
	ork. 1025							
	ok ntp ok ntp ok 1900	-						
UDP wor	ok. n/p							
UDP wor	ok. 1900	-						
	ofi. netbios-ssn	work.	0					
		work.	0	LISTENING				
					71	4,020	420	19,500
	ok netbios-dgm				24	4,609	38	173
UDP wor	ofk. microsoft-ds							
	TOP w TOP w UDP w UDP w	TCP work netbio-sm TCP work microsoft-dis UDP work netbio-ns UDP work netbio-dgm	TCP work netbionism work TCP work microsoft-ds work UDP work netbioning " UDP work netbioning "	TCP work netbiocissn work 0 TCP work netbiocissn work 0 UDP work netbiocins " UDP work netbiocing "	TCP work netbiostan work 0 USTENING TCP work netbiostan work 0 USTENING UDP work netbiostan " " UDP work netbiostan " "	TCP wolk netbiosan wolk 0 USTENING TCP wolk netbiosan wolk 0 USTENING UDP wolk netbiosan * * 71 UDP wolk netbiosage * 24	TCP wolk netbiossin wolk 0 LISTENING TCP wolk microsoft-da wolk 0 LISTENING UDP wolk netbiosnis " 71 4,020 UDP wolk netbiosdam " 24 4,633	TCP wolk refbicesin wolk 0 USTENING TCP wolk microcold at wolk 0 LISTENING UDP wolk refbicesins 1 71 4,020 420 UDP wolk refbicedge 1 24 4,603 38

implant - 96f10cfa6ba24c9ecd08aa6d37993fe4

File path – %SystemRoot%\System32\sipauth32.tsp

 $Registry-HKLM \verb|Software|Microsoft|Windows|CurrentVersion|Telephony|Providers|$

- <u>APT</u>
- <u>Backdoor</u>
- Shadow Brokers
- <u>Targeted attacks</u>

Authors



Your email address will not be published. Required fields are marked *