

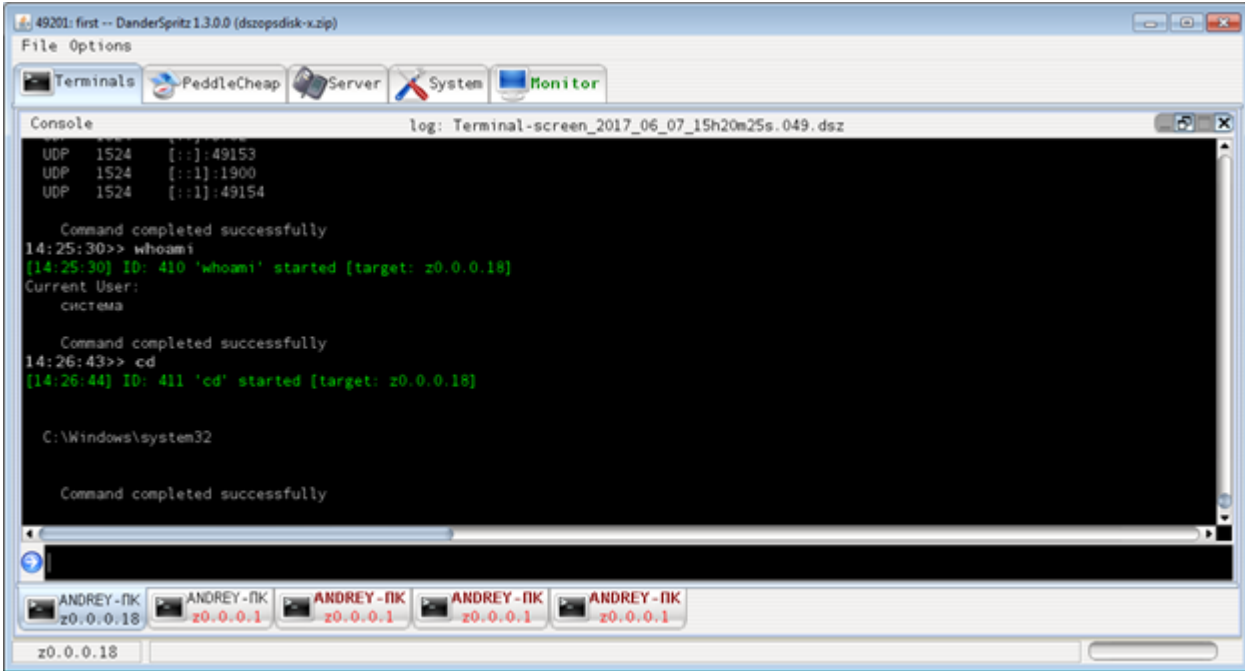
## “黑暗恒星”事件分析

[s小胖不吃饭](#) / 2018-10-20 10:36:55 / 浏览数 2408 [技术文章](#) [技术文章](#) [顶\(1\)](#) [踩\(0\)](#)

■■■■■■■■■■■■■■■■■■■■https://securelist.com/darkpulsar/88199/

在2017年3月，ShadowBrokers发表了一大部分被盗数据，其中包含两种构架：DanderSpritz 和 FuzzBunch。

DanderSpritz完全由插件组成，用于收集情报，使用漏洞并检查已经被控制的机器。它是用Java编写的，提供了类似于僵尸网络管理面板的图形窗口界面以及类似Metasploit



在另一方面DanderSprit

接口Fuzzbunch为不同的实用程序提供了一个交互和协同工作的框架。它包含各种类型的插件，用于分析受害者，利用漏洞，计划任务等。FuzzBunch框架的插件集中有三

- %pluginName%-version.fb

这是框架的实用程序文件。它从XLM复制标头并包含插件的ID。

- %pluginName%-version.exe

当FuZZbuNch收到执行此命令的命令时，将启动此可执行文件。

- %pluginName%-version.xml

此配置文件描述了插件的输入和输出参数—参数名称，其类型和对其负责的描述；所有这些可以在FuzzBunch中显示为提示。该文件也为框架的可用性做出了很大贡献，因为

最有趣的Fuzzbunch类别之一称为ImplantConfig，其中包含旨在通过植入后控制受感染机器的插件。DarkPulsar是一个非常有意思的管理模块，用于控制名为“sipauth32.ts”

它支持以下命令：

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

Burn, RawShellcode, UpgradeImplant和PingPong移除植入物, 运行任意代码, 升级植入物并检查后门是否分别安装在远程机器上。

其他命令的目的并不那么明显，更糟糕的是，泄漏的框架只包含管理模块来处理DarkPulsar的后门，而不是后门本身。

在分析管理模块时，我们注意到几个常量用于加密C&C和植入物之间的流量：

```

(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;
*(&v28 + 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 )
{
    TcLog(v1[2], 3, "[%s] - CDPPProtocolHandler::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 )

```

我们认为可能这些常量也应该出现在后门中，因此我们为它们创建了一个检测器。几个月后，我们发现了神秘的DarkPulsar后门。后来我们能够找到32位和64位版本。

我们发现大约50名受害者位于俄罗斯，伊朗和埃及，通常感染Windows 2003/2008服务器。目标涉及核能，电信，IT，航空航天和R&D研发。

#### DarkPulsar 技术亮点

DarkPulsar植入体是一个动态库，其有效载荷在导出的函数中实现。这些功能可以分组如下：

- 1.两个无名函数用于在系统中安装后门。
- 2.名称与TSPI（电话服务提供程序接口）操作相关的函数，用于确保后门位于自动运行列表中并能够自动启动。
- 3.具有与SSPI（安全支持提供程序接口）操作相关的名称的函数。它承载了主要的恶意负载。

SSPI和TSPI接口的实现是简洁的：DarkPulsar导出的函数与接口函数的名称相同；但是，它们包含恶意代码而不是电话服务。

植入物通过无名导出功能安装在系统中。通过调用具有管理员权限的Secur32.AddSecurityPackage以及参数中它自己的库的路径来启动后门，导致lsass.exe将DarkPulsar / AP，并由DarkPulsar初始化后门来调用其导出的函数SpLsaModeInitialize。这样，AddSecurityPackage用于将代码注入lsass.exe。它还在HKLM\Software\Microsoft\Windows\CurrentVersion\Telephony\Providers添加了库名。

这是在远程访问连接管理器（RasMan）服务旁边启动的Telephony

API（TapiSrv）开始加载，将启动类型设置为“自动”。加载由电话服务提供商的库时，TapiSrv调用TSPI\_lineNegotiateTSPIVersion，其中包含AddSecurityPackage调用以

DarkPulsar通过为SpAcceptLsaModeContext（负责身份验证的函数）安装钩子来实现其有效负载。此类注入在进程lsass.exe中的多个系统身份验证数据包中生成，并允许

- Msv1\_0.dll – 用于NTLM协议，
- Kerberos.dll – 用于Kerberos协议，
- Schannel.dll – 用于TLS / SSL协议，
- Wdigest.dll – 用于摘要协议，
- Lsasrv.dll – 用于谈判协议。

在此之后，Darkpulsar能够将恶意软件流量嵌入到系统协议中。由于此网络活动是根据标准系统图表进行的，因此它只会反映在系统进程中，它使用为上述协议保留的系统

Wireshark · Packet 6 · success attack

```

    > Frame 6: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits) on interface 0
    > Ethernet II, Src: PcsCompu_90:44:d2 (08:00:27:90:44:d2), Dst: PcsCompu_73:f8:81 (08:00:27:73:f8:81)
    > Internet Protocol Version 4, Src: 192.168.56.104, Dst: 192.168.56.103
    > Transmission Control Protocol, Src Port: 1502, Dst Port: 445, Seq: 138, Ack: 132, Len: 150
    > NetBIOS Session Service
    > SMB (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: 0x00000000
          Security Blob Length: 16
          Reserved: 00000000
          > Capabilities: 0x800000d4, Unicode, NT SMBs, NT Status Codes, Level 2 Oplocks, Extended Security
          Byte Count (BCC): 87
          > Security Blob: 04d647334bab5e084a7d1d3b728c7d91
            Native OS: Windows 2000 2195
            Native LAN Manager: Windows 2000 5.0
  
```

0000	08 00 27 73 f8 81 08 00 27 90 44 d2 08 00 45 00	.. 's.... ' .D...E.
0010	00 be 29 ab 40 00 80 06 de 6e c0 a8 38 68 c0 a8	..).@... .n..8h..
0020	38 67 05 de 01 bd 14 0d fc 59 39 4c 5a 50 50 18	8g..... .Y9LZPP.
0030	fa 6d 9e 0e 00 00 00 00 00 92 ff 53 4d 42 73 00	.m..... ...SMBs.
0040	00 00 00 18 07 c8 00 00 00 00 00 00 00 00 00	.....
0050	00 00 00 00 ff fe 00 00 40 00 0c ff 00 3b 00 04	..... @....;..
0060	11 0a 00 19 00 00 00 00 00 10 00 00 00 00 00 d4	.....
0070	00 00 80 57 00 04 d6 47 33 4b ab 5e 08 4a 7d 1d	...W...G 3K.^.J}.
0080	3b 72 8c 7d 91 00 57 00 69 00 6e 00 64 00 6f 00	[r.}.W. i.n.d.o.
0090	77 00 73 00 20 00 32 00 30 00 30 00 30 00 20 00	w.s. .2. 0.0.0. .
00a0	32 00 31 00 39 00 35 00 00 00 57 00 69 00 6e 00	2.1.9.5. ..W.i.n.
00b0	64 00 6f 00 77 00 73 00 20 00 32 00 30 00 30 00	d.o.w.s. .2.0.0.
00c0	30 00 20 00 35 00 2e 00 30 00 00 00	0. .5... 0...

0x3347d604 + 0x085eab4b = 3BA6814F (const for manipulating DaPu )

控制身份验证过程的第二个优点是可以绕过输入有效的用户名和密码，以获取对需要身份验证的对象的访问权限，例如进程列表，远程注册表，通过SMB的文件系统。发送

利用DarkPulsar工作

Darkpulsar-1.1.0.exe是在“一个命令-一次启动”原则下工作的管理界面。要执行的命令必须在配置文件Darkpulsar-1.1.0.9.xml中指定或者作为命令行参数指定，至少详细说

- 目标计算机是使用32位还是64位系统；
- 提供命令和端口号的协议（支持SMB，NBT，SSL，RDP协议）
- 私有RSA密钥，用于解密会话AES密钥

Darkpulsar-1.1.0并非管理受感染机器的独立程序。该实用程序是Fuzzbunch框架的插件，可以管理参数和协调不同的组件。以下是Fuzzbunch中的DisableSecurity命令

```
C:\Python26\python.exe
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
=====
Name                Value
-----
TargetIp             127.0.0.1
SspMTU               60
TargetPort           445
NetworkLineout       0
SSPFfragmentSize     0
PrivateKeyInputType  File
PrivateKeyFile       C:\Users\Andrey\Desktop\fuzzbunch-master\private.ke
y
ImplantAction        DisableSecurity
Protocol             SMB
UseNTLMSspHeader     False
Architecture         x86

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] - Performing crypto session setup
[+] - Performing crypto session setup
[+] Darkpulsar Succeeded

fb ImplantConfig <Darkpulsar> >
```

下面是DisableSecurity之后的Processlist示例，允许执行任何没有有效凭据的插件，并通过常规系统功能（远程注册表服务）进行操作：

```
C:\Python26\python.exe
Module: Processlist
=====
Name                Value
-----
NetworkTimeout      60
TargetIp             127.0.0.1
TargetPort           445
LogFile              processlist.txt
Username             416e64726579
Credential           416e64726579
AuthLevel            None
CredentialType        UnicodeCreds

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
---<<< Process List >>>---

[*] Reading Input Parameters
[+] "TargetIp"          127.0.0.1
[+] "TargetPort"        445
[+] "NetworkTimeout"    60
[+] "Username"          416e64726579      Andrey
[+] "Credential"        416e64726579      Andrey
[*] Initializing Network
[*] Performing Process List
    [+] Connected to the Registry Service

System Name          : ANDREY-мгмб
System Uptime <H:M:S>: 10:00:07
System Time           : Wed, 07 Jun 2017 15:34:25 GMT

PID      PPID      Process Name      Runtime      Handles      Threads
-----
0         0         Idle              0            0            1
4         0         System            416          86
264       4         smss              121:00:15    29           2
336       328      csrss              121:00:15    530          9
384       328      wininit           121:00:15    74           3
392       376      csrss              121:00:15    569          8
440       376      winlogon          121:00:15    109          3
480       384      services          121:00:15    193          7
```

## DanderSpritz

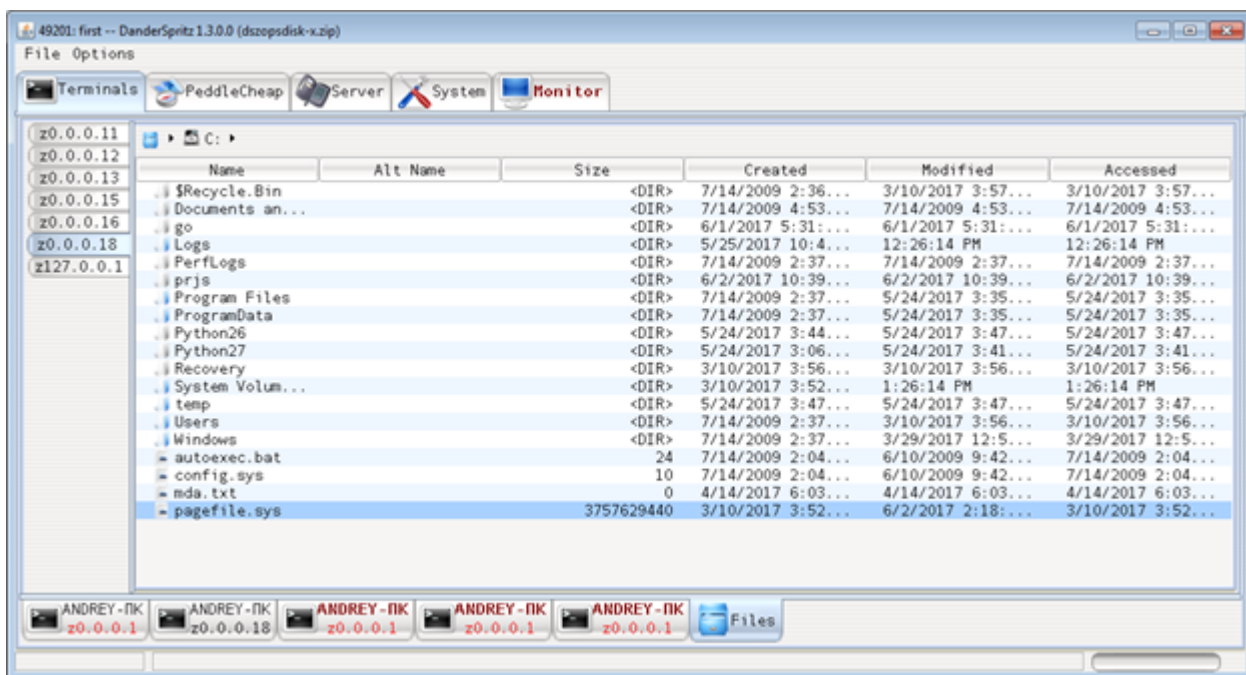
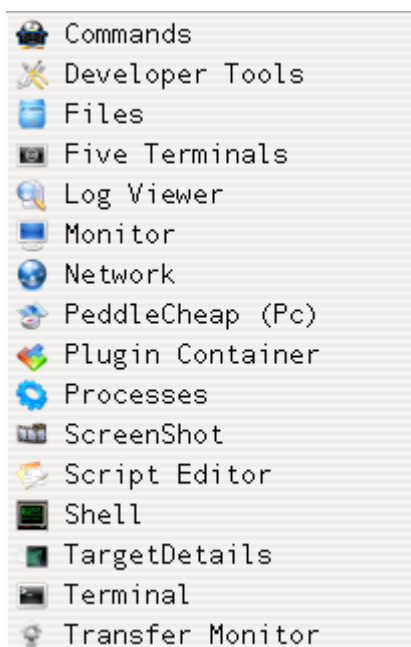
DanderSpritz是用于控制受感染机器的框架，与FuZZbuNch不同，因为后者为具有特定功能的后开发阶段提供了有限的工具包，例如DisableSecurity和DarkSeuls的Enabl

DanderSpritz适用于更大范围的后门，在受害者中使用PeddleCheap来启动运营商以启动插件。PeddleCheap是DanderSpritz的插件，可用于配置植入物并连接到受感染的

这就是EDFStagedUpload模式中的DarkPulsar如何通过更实用的植入物为受害者提供感染的机会：PCDIIlauncher（Fuzzbunch的插件）在受害者一侧部署PeddleCheap的DLL Launcher'。

完整的DanderSpritz与通过FuZZbuNch 的 PeddleCheap插件及DarkPulsar和PCDIIlauncher插件使用方案包含四个步骤：

- 1.通过FuZZbuNch，运行命令EDFStagedUpload以启动DarkPulsar。
- 2.在DanderSpritz中，运行命令pc\_prep（PeedleCheap Preparation）以准备有效载荷和要在种植体侧启动的库。
- 3.在DanderSpritz中，运行命令pc\_old（这是命令pc\_listen -reuse -nolisten -key Default的别名），这会将其设置为等待来自PcdIIlauncher的套接字。
- 4.通过FuZZbuNch启动PcdIIlauncher并指定使用ImplantFilename参数中的命令pc\_prep准备的有效负载的路径。



## 结论

FuzzBunch和DanderSpritz框架旨在提高灵活性，扩展功能并与其他工具兼容。它们都包含一组专为不同任务设计的插件：虽然FuzzBunch插件负责侦察和攻击受害者，但DarkPulsar后门的发现有助于理解它作为两个泄露框架之间的桥梁的作用，以及它们如何基于DarkPulsar的持久性和隐身性的先进能力，成为同一攻击平台的一部分，这些我们的产品可以完全删除与此攻击恶意软件相关的内容。

## 检测恶意网络活动

在受感染的计算机中执行EDFStagedUpload时，会建立永久连接，这就是出现通过端口445的流量的原因。Isass.exe中还出现一对绑定套接字：



Proc.	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
alg.exe	1692	TCP	work	1027	work	0	LISTENING				
qqs.exe	632	TCP	work	5152	work	0	LISTENING				
lsass.exe	708	UDP	work	isakmp	*	*					
lsass.exe	708	UDP	work	4500	*	*					
lsass.exe	708	TCP	work	1037	localhost	1038	ESTABLISHED				
lsass.exe	708	TCP	work	1038	localhost	1037	ESTABLISHED				
svchost.exe	996	TCP	work	epmap	work	0	LISTENING			20	3,152
svchost.exe	1296	UDP	work	1900	*	*					
svchost.exe	1116	UDP	work	1025	*	*					
svchost.exe	1116	UDP	work	nlp	*	*					
svchost.exe	1296	UDP	work	1900	*	*					
System	4	TCP	work	netbios-ssn	work	0	LISTENING				
System	4	TCP	work	microsoft-ds	work	0	LISTENING				
System	4	UDP	work	netbios-ns	*	*		32	1,807	114	4,350
System	4	UDP	work	netbios-dgm	*	*		19	3,618	30	179
System	4	UDP	work	microsoft-ds	*	*					
System	4	TCP	work	microsoft-ds	andrey-ali	49176	ESTABLISHED	48	6,576	48	9,312

Endpoints: 18    Established: 3    Listening: 5    Time Wait: 0    Close Wait: 0

当DanderSpritz通过PcDllLauncher插件部署PeddleCheap的有效负载时，网络活动会急剧增加。

Proc.	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
alg.exe	1692	TCP	work	1027	work	0	LISTENING				
qqs.exe	632	TCP	work	5152	work	0	LISTENING				
lsass.exe	708	UDP	work	isakmp	*	*					
lsass.exe	708	UDP	work	4500	*	*					
lsass.exe	708	TCP	work	1037	localhost	1038	ESTABLISHED	313	62,494	410	830,153
lsass.exe	708	TCP	work	1038	localhost	1037	ESTABLISHED	537	840,761	312	62,494
svchost.exe	996	TCP	work	epmap	work	0	LISTENING				
svchost.exe	1296	UDP	work	1900	*	*				32	5,240
svchost.exe	1116	UDP	work	1025	*	*					
svchost.exe	1116	UDP	work	nlp	*	*					
svchost.exe	1116	UDP	work	nlp	*	*					
svchost.exe	1296	UDP	work	1900	*	*					
System	4	TCP	work	netbios-ssn	work	0	LISTENING				
System	4	TCP	work	microsoft-ds	work	0	LISTENING				
System	4	UDP	work	netbios-ns	*	*		68	3,687	240	10,650
System	4	UDP	work	netbios-dgm	*	*		22	4,229	35	179
System	4	UDP	work	microsoft-ds	*	*					
System	4	TCP	work	microsoft-ds	andrey-ali	49176	ESTABLISHED	1,704	299,816	1,900	1,216,352

Endpoints: 18    Established: 3    Listening: 5    Time Wait: 0    Close Wait: 0

当终止与受感染计算机的连接时，网络活动将停止，并且只保留lsass.exe中两个绑定套接字的跟踪：

Proc.	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
alg.exe	1692	TCP	work	1027	work	0	LISTENING				
qqs.exe	632	TCP	work	5152	work	0	LISTENING				
lsass.exe	708	UDP	work	isakmp	*	*					
lsass.exe	708	UDP	work	4500	*	*					
lsass.exe	708	TCP	work	1037	localhost	1038	ESTABLISHED	1,151	246,538	1,078	1,149,811
lsass.exe	708	TCP	work	1038	localhost	1037	ESTABLISHED	1,215	1,166,277	1,114	246,538
svchost.exe	996	TCP	work	epmap	work	0	LISTENING				
svchost.exe	1296	UDP	work	1900	*	*				40	6,632
svchost.exe	1116	UDP	work	1025	*	*					
svchost.exe	1116	UDP	work	nlp	*	*					
svchost.exe	1116	UDP	work	nlp	*	*					
svchost.exe	1296	UDP	work	1900	*	*					
System	4	TCP	work	netbios-ssn	work	0	LISTENING				
System	4	TCP	work	microsoft-ds	work	0	LISTENING				
System	4	UDP	work	netbios-ns	*	*		71	4,020	420	19,500
System	4	UDP	work	netbios-dgm	*	*		24	4,609	38	179
System	4	UDP	work	microsoft-ds	*	*					

Endpoints: 17    Established: 2    Listening: 5    Time Wait: 0    Close Wait: 0

IOCs

implant - 96f10cfa6ba24c9ecd08aa6d37993fe4

File path - %SystemRoot%\System32\slipauth32.tsp

Registry - HKLM\Software\Microsoft\Windows\CurrentVersion\Telephony\Providers

点击收藏 | 0 关注 | 1

[上一篇：D-Link 850L&645路由...](#) [下一篇：区块链安全一白话parity多签名...](#)

1. 0 条回复

- 动手手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

[热门节点](#)

---

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)