

# Question 13

You are working as a security administrator. Your company was recently struck by a malware infection.

Here is what the regular users report:

User 1: "A strange black window, I think you nerds called it a terminal. I do not remember installing that"

User 2: "Some of my shareware applications stopped working"

User 3: "This is annoying..."

You were able to capture dada.exe and have a reason to believe that it is the culprit.

1. Perform basic static analysis on this binary. What were we able to learn?
2. Perform basic dynamic analysis on this binary. What were you able to learn?
3. Using the results from static and dynamic analysis write up your conclusion about what this malware does and support your results with screenshots. Please be sure to first describe the conclusion in crisply terms accessible to your bosses (who are non-technical individuals) and then provide a technical description suitable for the senior IT experts. An example of a real-world model malware analysis report can be found [here \(Links to an external site.\)](#)

.

Dada-1.

8  
1/67

7  
Community Score

8 security vendors flagged this file as malicious

ab134874ae49a4f1dcb509a2c286ea87deae4cea17bbf2fa4b780595d2ead77c  
dada.exe

71.35 KB  
Size

2018 11 16 23:26:28 UTC  
3 years ago

EXE

overlay

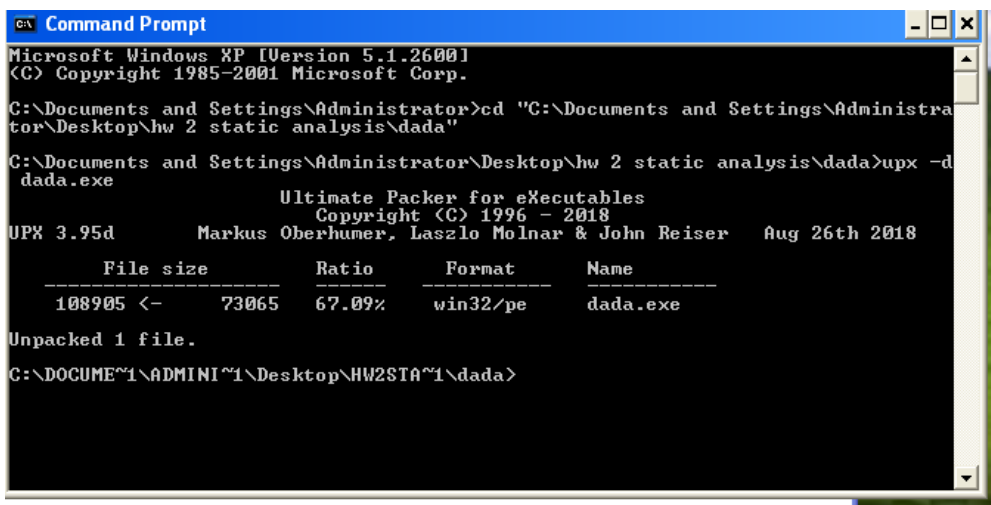
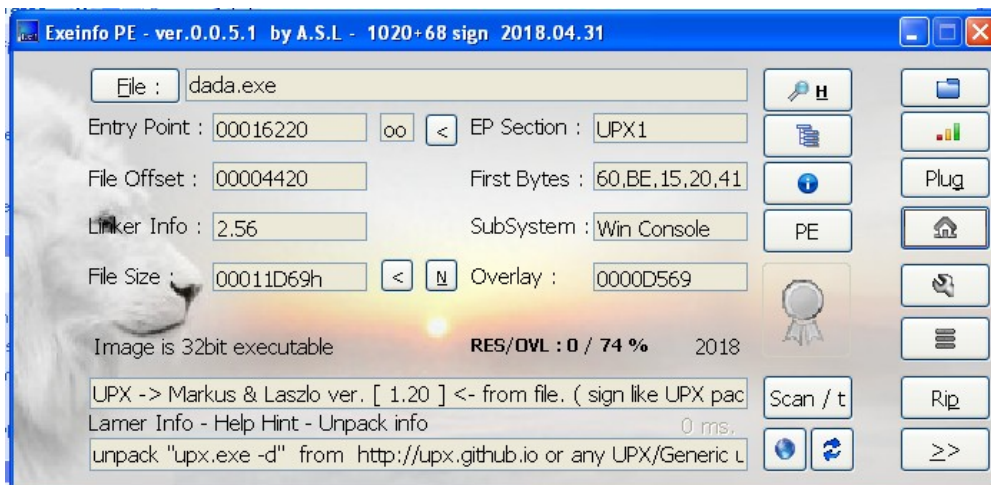
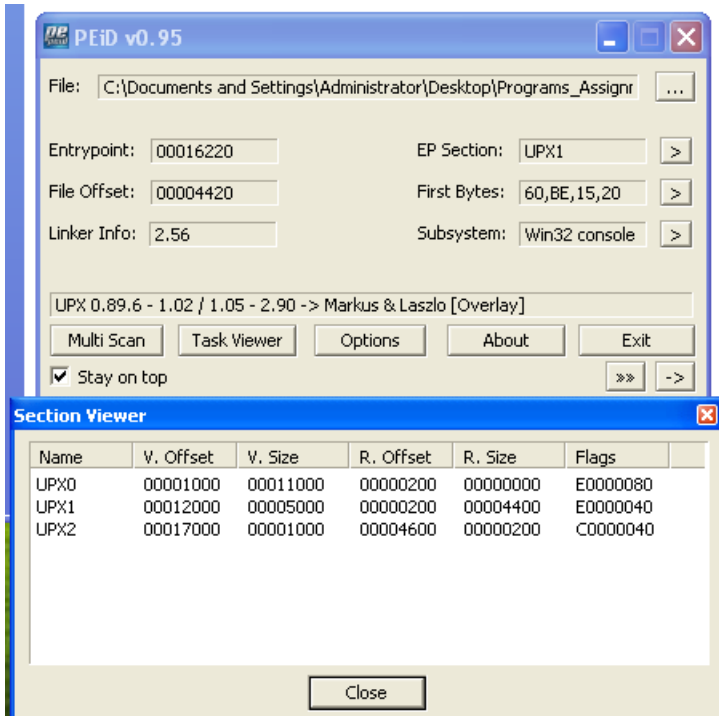
pcrc

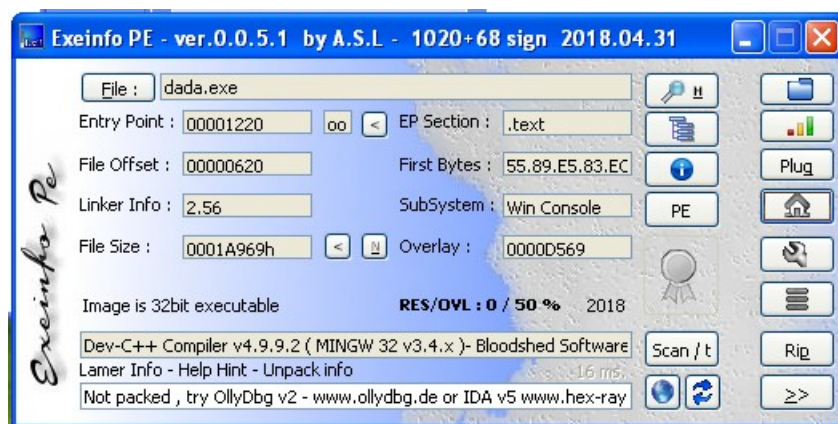
upx

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
AhnLab V3	① Trojan:Win32.Downloader.C3007	CrowdStrike Falcon	① Malicious_confidence_60% (W)
Cylance	① Unsafe	eGambit	① Unsafe_AI_Score_78%
Ikarus	① Trojan: PWS.Win32.FireThief	McAfee	① Artemis571D778B3015
McAfee GW Edition	① Artemis	TheHacker	① Possible_Worm32
Ad Aware	③ Undetected	AegisLab	③ Undetected
Alibaba	③ Undetected	ALYac	③ Undetected
Antiy AVL	③ Undetected	Arcabit	③ Undetected
Avast	③ Undetected	Avast Mobile	③ Undetected
AVG	③ Undetected	Avira (no cloud)	③ Undetected
Babable	③ Undetected	Baidu	③ Undetected
BitDefender	③ Undetected	Bkav Pro	③ Undetected
CAT QuickHeal	③ Undetected	ClamAV	③ Undetected
CMC	③ Undetected	Cybereason	③ Undetected

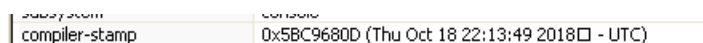
Ikarus says trojan

its packed with upx



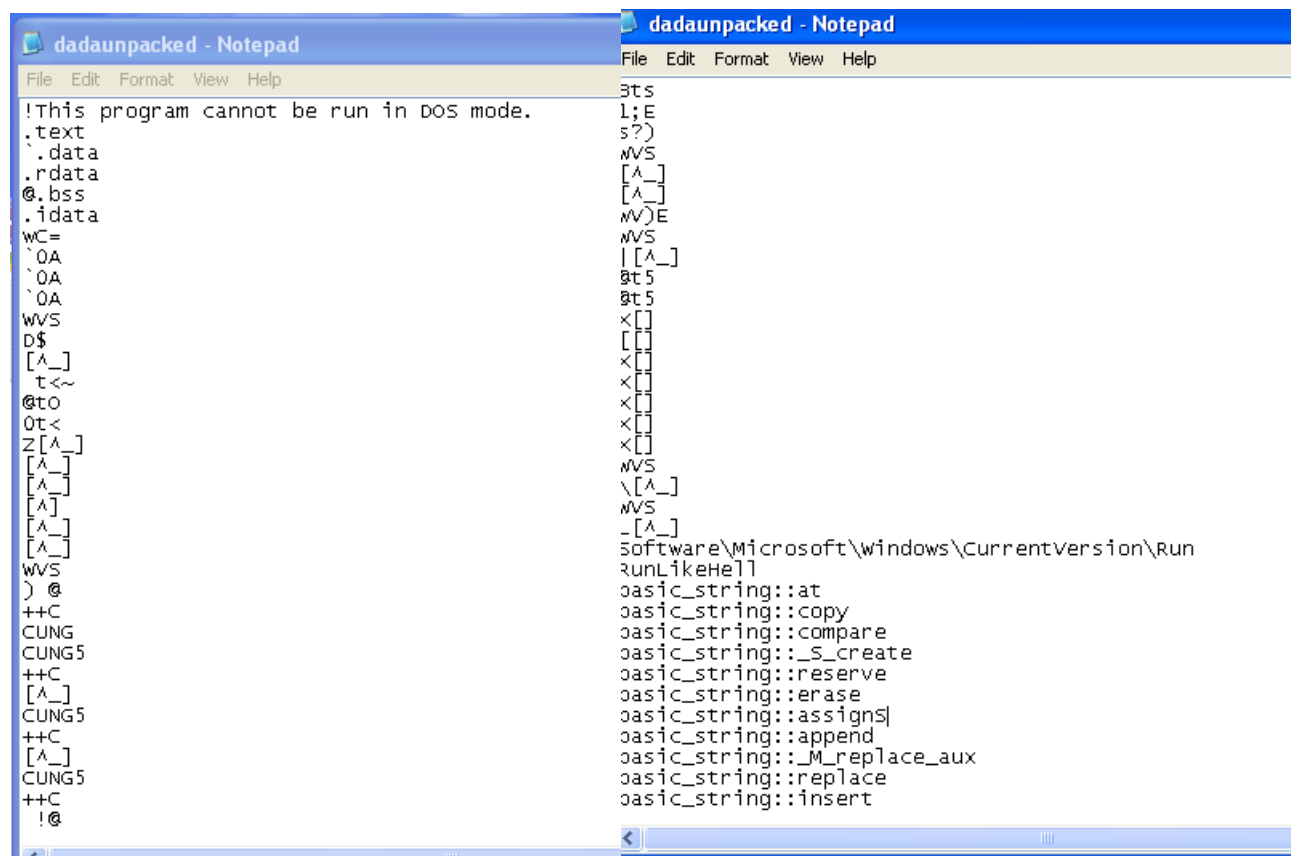


After unpacking the malware seems to have been compiled with Dev-C++ Compiler and Bloodshed Software.

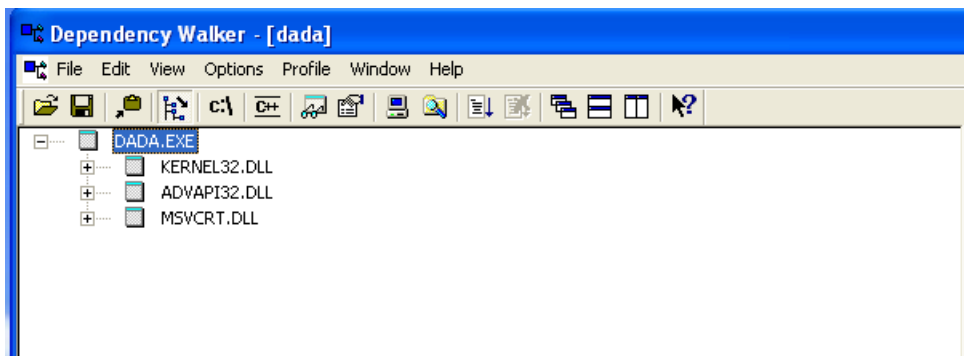


The malware appears to have a compilation timestamp of Thursday October 18 22:13:49 2018 UTC.

<https://pastebin.com/wxVdNFRE>



There is a suspicious entry in the strings, RunLikeHell.

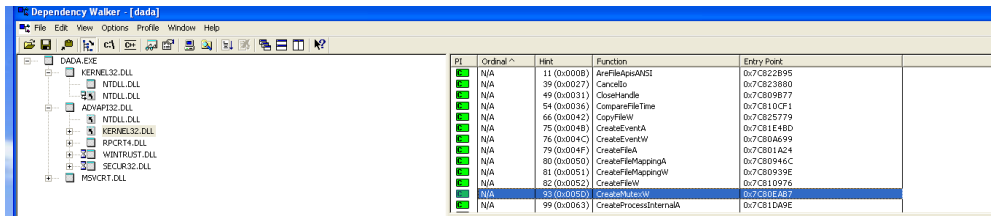


KERNEL32.dll (from lecture, might have access to memory, files, and hardware)

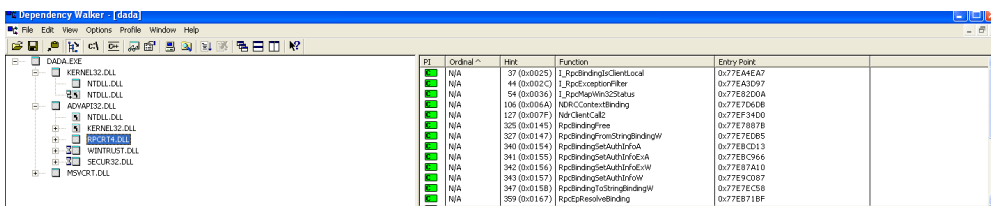
advapi32.dll: (<https://www.file.net/process/advapi32.dll.html> can shutdown or restart the machine, has access to the windows registry, has access to user accounts, can start and stop windows services)

MSVCRT (<https://docs.python.org/3/library/msvcrt.html> used in some windows services, there might be a service involved)

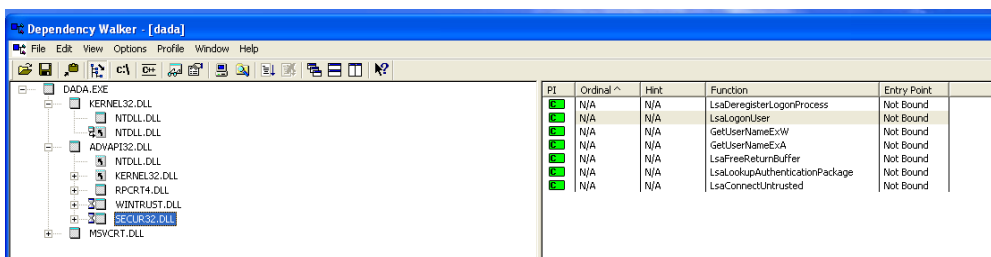
## Uses threads



## Gets your network information:



## Creates new logon sessions:



RegCreateKeyExA probably creates a registry key that will be visible in regedit  
fprintf might print to a file

## What we learned:

Dada is packed by upx. Dada contains a suspicious string called “RunLikeHell”. Dada may have been compiled by Dev-C++ Compiler and Bloodshed Software, on Thursday October 18 22:13:49 2018 UTC.

Dada may have access to the kernel, the windows registry, user accounts, and windows services. Dada might use threads, network functions, and may create new logon sessions. Dada may add a new registry key that may be visible in regedit. It may also print to a file.

Dada-2.



dada has created a new registry called HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\RunLikeHell

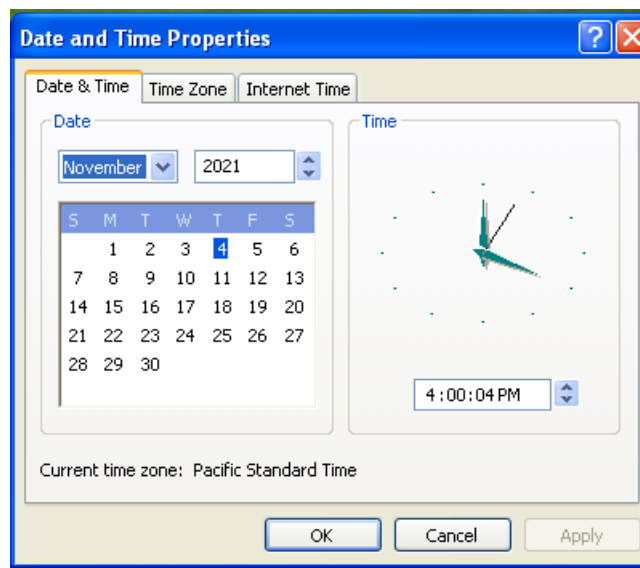
Name	Type	Data
(Default)	REG_SZ	(value not set)
RunLikeHell	REG_SZ	"C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\dada\dada.exe"
vBoxTray	REG_SZ	C:\WINDOWS\system32\VBoxTray.exe

The contents of HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run in regedit.

Because `dada.exe` is in the run directory, this means that `dada` will run at startup.



Dada appears to be interacting with time-related directories constantly. Perhaps its purpose is related to time?



Dada appears to be forcing the clock to stay at 4:00:04 PM.

What we learned:

Dada creates a new registry at HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\RunLikeHell. Dada has placed the path to its executable file as this key's value, which means that it will run at startup.

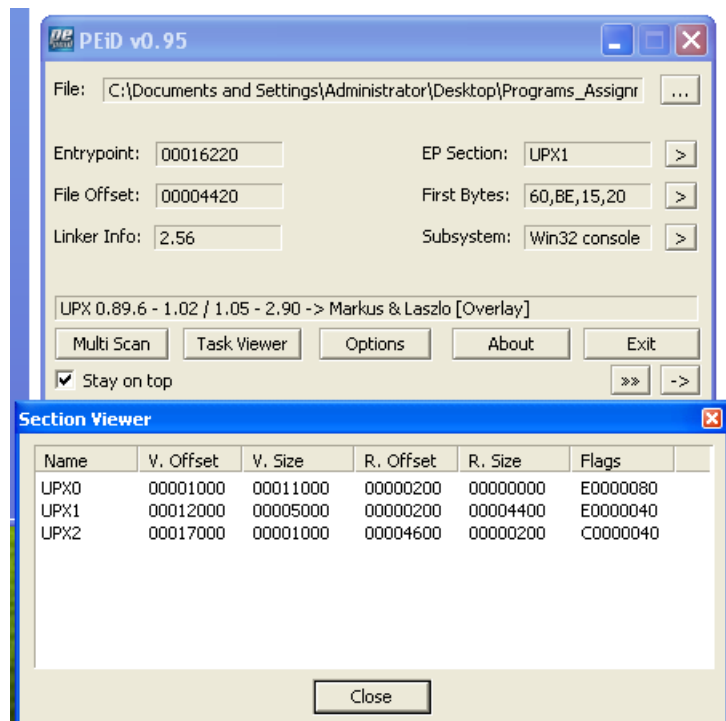
Dada appears to be constantly forcing the clock to freeze at 4:00:44 PM. Dada is constantly accessing time related registries in order to do this.

Dada-3.

Dada is a malware that runs at startup and freezes the clock to 4:00:04 PM without changing the date.

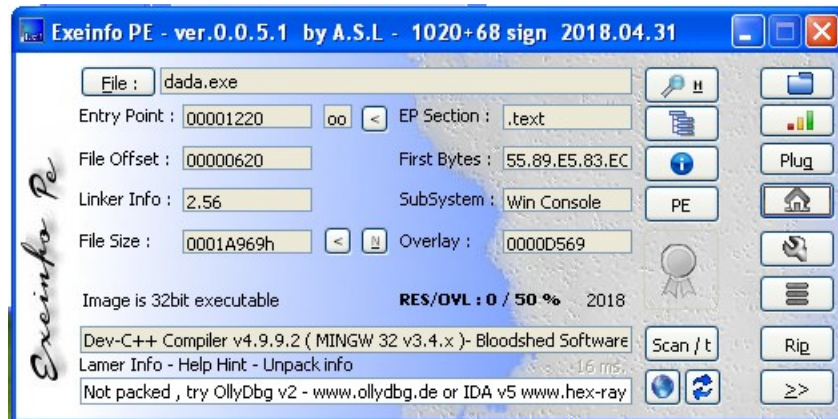


In VirusTotal, Ikarus says that the malware is a Trojan.

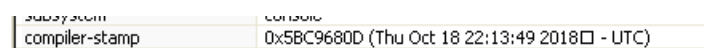


The malware appears to have been packed using upx.

It has been successfully unpacked.



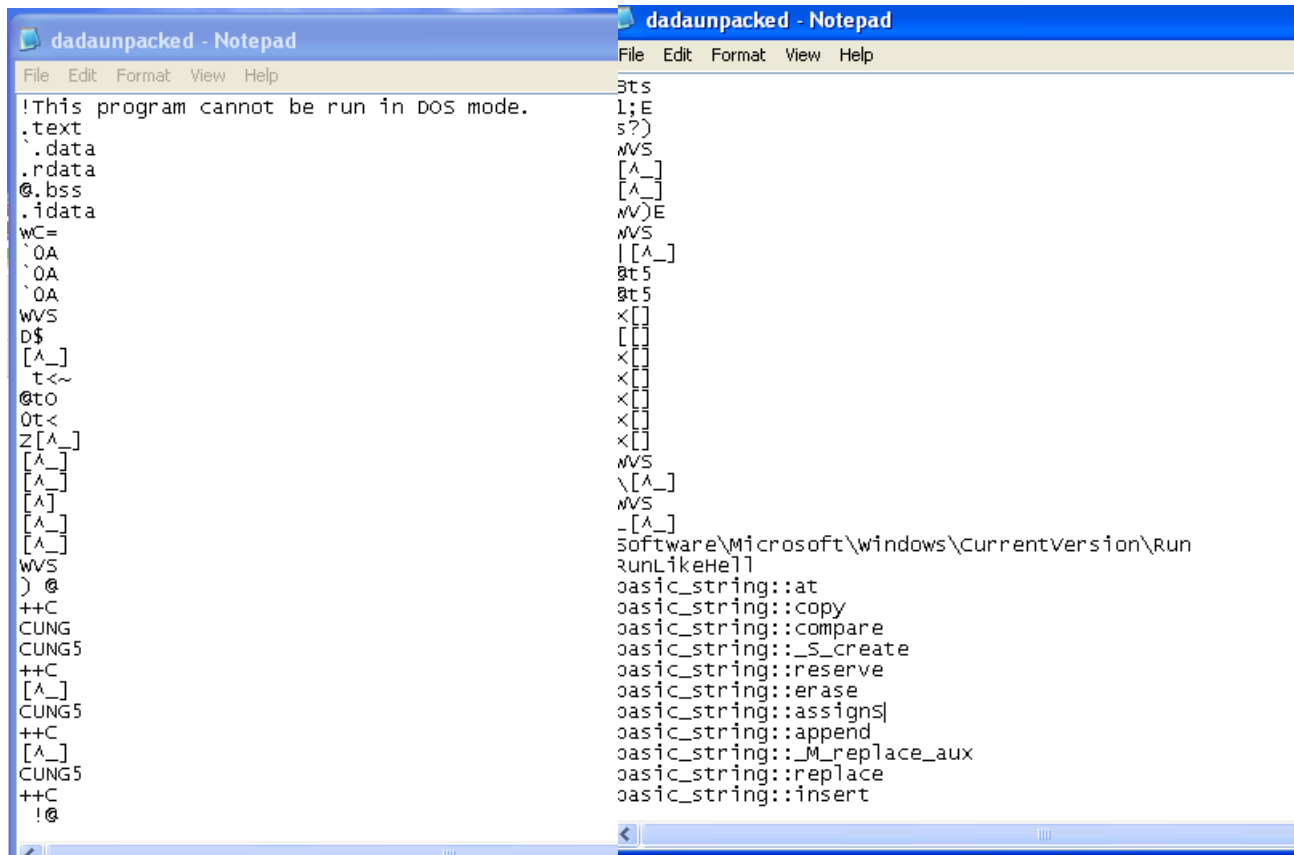
After unpacking the malware seems to have been compiled with Dev-C++ Compiler and Bloodshed Software.



The malware appears to have a compilation timestamp of Thursday October 18 22:13:49 2018 UTC.



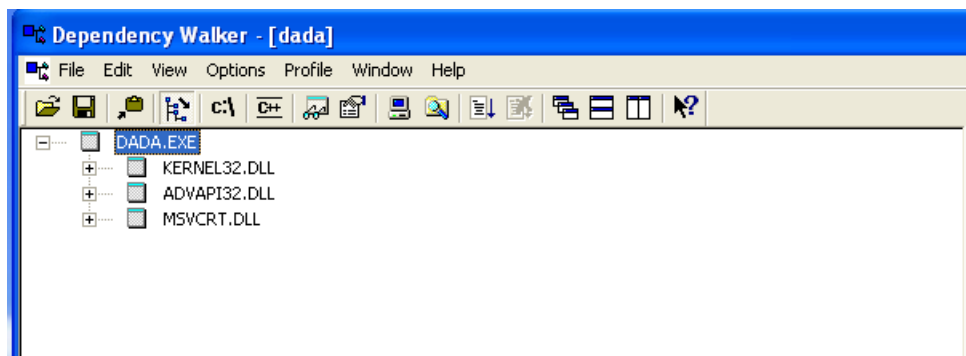
<https://pastebin.com/wxVdNFRE>



```
dadaunpacked - Notepad
File Edit Format View Help
!This program cannot be run in DOS mode.
.text
.data
.rdata
@.bss
.idata
wC=
`0A
`0A
`0A
wVS
D$
[ ^_ ]
t<~
@to
0t<
Z[ ^_ ]
[ ^_ ]
[ ^_ ]
[ ^_ ]
[ ^_ ]
wVS
) @
++C
CUNG
CUNG5
++C
[ ^_ ]
CUNG5
++C
[ ^_ ]
CUNG5
++C
!@

dadaunpacked - Notepad
File Edit Format View Help
3ts
l;E
s?)
mVS
[ ^_ ]
[ ^_ ]
mV)E
mVS
| [ ^_ ]
0t 5
0t 5
x[ ]
[ ]
[ ]
x[ ]
x[ ]
x[ ]
x[ ]
x[ ]
x[ ]
mVS
\ [ ^_ ]
mVS
- [ ^_ ]
Software\Microsoft\windows\CurrentVersion\Run
RunLikeHell
basic_string::at
basic_string::copy
basic_string::compare
basic_string::_S_create
basic_string::reserve
basic_string::erase
basic_string::assign
basic_string::append
basic_string::_M_replace_aux
basic_string::replace
basic_string::insert
```

There is a suspicious entry in the strings, RunLikeHell.

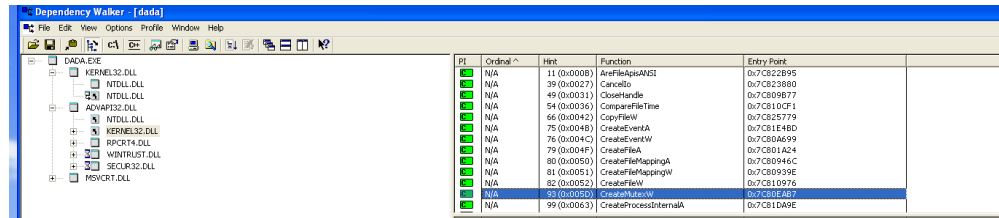


KERNEL32.dll (from lecture, might have access to memory, files, and hardware)

advapi32.dll: (<https://www.file.net/process/advapi32.dll.html> can shutdown or restart the machine, has access to the windows registry, has access to user accounts, can start and stop windows services)

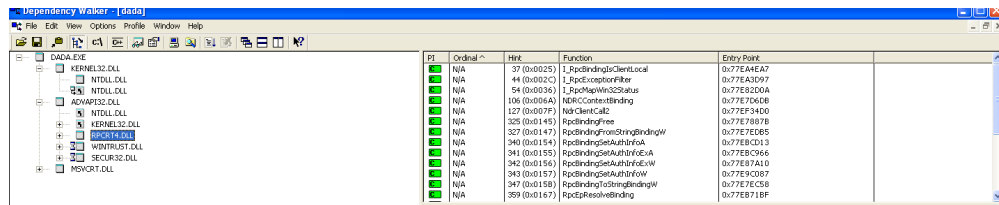
MSVCRT (<https://docs.python.org/3/library/msvcrt.html> used in some windows services, there might be a service involved)

## Uses threads



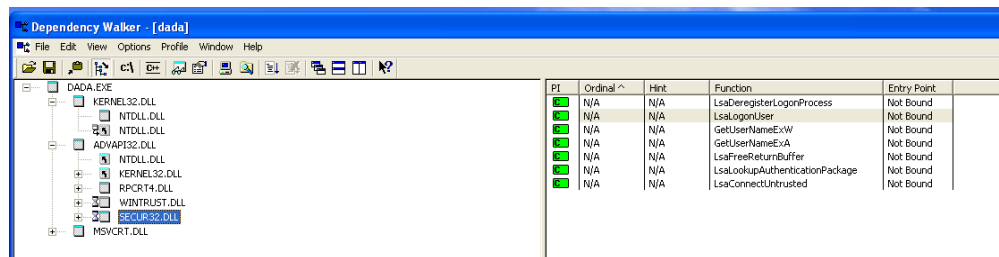
PI	Ordinal ^	Hint	Function	Entry Point
N/A	11 (0x000B)		AreFileApisANSI	0x7C82B995
N/A	39 (0x0027)		CancelIo	0x7C823880
N/A	49 (0x0031)		CloseHandle	0x7C809877
N/A	54 (0x0036)		CompareFileTime	0x7C810CF1
N/A	66 (0x0042)		CopyFileW	0x7C825779
N/A	75 (0x004B)		CreateEventA	0x7C81E48D
N/A	76 (0x004C)		CreateEventW	0x7C80A699
N/A	79 (0x004F)		CreateFileA	0x7C801A24
N/A	80 (0x0050)		CreateFileMappingA	0x7C80946C
N/A	81 (0x0051)		CreateFileMappingW	0x7C80939E
N/A	82 (0x0052)		CreateFileW	0x7C810976
N/A	83 (0x0053)		CreateProcess	0x7C80E7C7
N/A	99 (0x0063)		CreateProcessInternalA	0x7C811DAE

## Gets your network information:



PI	Ordinal ^	Hint	Function	Entry Point
N/A	37 (0x0025)		1_PspBindingClientLocal	0x77E4A2A7
N/A	44 (0x002C)		1_PspExceptionFilter	0x77E43D97
N/A	54 (0x0036)		1_PspQueryWin32Status	0x77E92D0A
N/A	106 (0x006A)		NdrContextBinding	0x77E70408
N/A	127 (0x007F)		NdrClientCall2	0x77EF340D
N/A	325 (0x0145)		RpddBindingFree	0x77E78878
N/A	327 (0x0147)		RpddBindingNewStringBindingW	0x77E78265
N/A	340 (0x0154)		RpddBindingSetAuthInfoA	0x77E8CD13
N/A	341 (0x0155)		RpddBindingSetAuthInfoExA	0x77E8C966
N/A	342 (0x0156)		RpddBindingSetAuthInfoW	0x77E8D410
N/A	343 (0x0157)		RpddBindingSetAuthInfoW	0x77E9C087
N/A	347 (0x015B)		RpddBindingToStringBindingW	0x77E7EC58
N/A	399 (0x0187)		RpddResolveBinding	0x77E8718F

## Creates new logon sessions:



PI	Ordinal ^	Hint	Function	Entry Point
N/A	N/A	N/A	LsaDeregisterLogonProcess	Not Bound
N/A	N/A	N/A	LsaLogonUser	Not Bound
N/A	N/A	N/A	GetUserNameExW	Not Bound
N/A	N/A	N/A	GetUserNameExA	Not Bound
N/A	N/A	N/A	LsaFreeReturnBuffer	Not Bound
N/A	N/A	N/A	LsaLookupAuthenticationPackage	Not Bound
N/A	N/A	N/A	LsaConnectUntrusted	Not Bound

RegCreateKeyExA probably creates a registry key that will be visible in regedit  
printf might print to a file

## What we learned:

Dada is packed by upx. Dada contains a suspicious string called “RunLikeHell”. Dada may have been compiled by Dev-C++ Compiler and Bloodshed Software, on Thursday October 18 22:13:49 2018 UTC.

Dada may have access to the kernel, the windows registry, user accounts, and windows services. Dada might use threads, network functions, and may create new logon sessions. Dada may add a new registry key that may be visible in regedit. It may also print to a file.



```
439.2 C:\> dada.exe 1512 regcreatekey HKLM\Software\Microsoft\Windows\CurrentVersion\Run... SUCCESS
439.3 C:\> dada.exe 1502 printfvalue HKLM\Software\Microsoft\Windows\CurrentVersion\Run\RunLikeHell... SUCCESS
439.4 C:\> dada.exe 1502 printfvalue HKLM\Software\Microsoft\Windows\CurrentVersion\Run\RunLikeHell... SUCCESS
439.5 C:\> dada.exe 1512 SetEndOfFile C:\Windows\system32\config\software.LOG SUCCESS
439.6 C:\> dada.exe 1512 SetEndOfFile C:\Windows\system32\config\software.LOG SUCCESS
```

dada has created a new registry called HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\RunLikeHell

Name	Type	Data
(Default)	REG_SZ	(value not set)
RunLikeHell	REG_SZ	"C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\dada\dada.exe"
VBoxTray	REG_SZ	C:\WINDOWS\system32\VBoxTray.exe

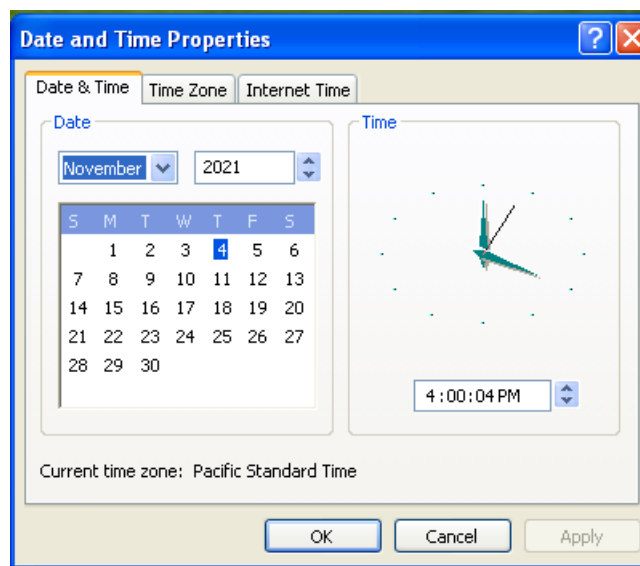
The contents of HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run in regedit.

Because dada.exe is in the run directory, this means that dada will run at startup.

4:01:11	dada.exe	1348	RegOpenKey	HKLM\System\CurrentControlSet\Control\TimeZoneInformation	SUCCESS	Desired Access: Write
4:01:11	dada.exe	1348	RegCreateKey	HKLM\System\CurrentControlSet\Control\TimeZoneInformation	SUCCESS	Type: REG_DWORD, Length: 4, Data: 480
4:01:11	dada.exe	1348	RegQueryValue	HKLM\System\CurrentControlSet\Control\TimeZoneInformation\ActiveTimeBias	SUCCESS	Type: REG_DWORD, Length: 4, Data: 480
4:01:11	dada.exe	1348	RegOpenKey	HKLM\System\CurrentControlSet\Control\TimeZoneInformation	SUCCESS	Desired Access: Read, Maximum Allowed
4:01:11	dada.exe	1348	RegQueryValue	HKLM\System\CurrentControlSet\Control\TimeZoneInformation\Bias	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
4:01:11	dada.exe	1348	RegQueryValue	HKLM\System\CurrentControlSet\Control\TimeZoneInformation\StandardName	SUCCESS	Type: REG_SZ, Length: 44, Data: Pacific Standard Time
4:01:11	dada.exe	1348	RegQueryValue	HKLM\System\CurrentControlSet\Control\TimeZoneInformation\StandardBias	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
4:01:11	dada.exe	1348	RegQueryValue	HKLM\System\CurrentControlSet\Control\TimeZoneInformation\StandardStart	SUCCESS	Type: REG_BINARY, Length: 16, Data: 00 00 04 00 05 00 02 00 00 00 00 00 00 00 00 00
4:01:11	dada.exe	1348	RegQueryValue	HKLM\System\CurrentControlSet\Control\TimeZoneInformation\DaylightName	SUCCESS	Type: REG_SZ, Length: 44, Data: Pacific Daylight Time
4:01:11	dada.exe	1348	RegQueryValue	HKLM\System\CurrentControlSet\Control\TimeZoneInformation\DaylightBias	SUCCESS	Type: REG_DWORD, Length: 4, Data: 4294967296
4:01:11	dada.exe	1348	RegQueryValue	HKLM\System\CurrentControlSet\Control\TimeZoneInformation\DaylightStart	SUCCESS	Type: REG_BINARY, Length: 16, Data: 00 00 04 00 01 00 02 00 00 00 00 00 00 00 00 00
4:01:11	dada.exe	1348	RegOpenKey	HKLM\System\CurrentControlSet\Control\TimeZoneInformation	SUCCESS	Desired Access: Write
4:01:11	dada.exe	1348	RegCreateKey	HKLM\System\CurrentControlSet\Control\TimeZoneInformation	SUCCESS	Type: REG_DWORD, Length: 4, Data: 480
4:01:11	dada.exe	1348	RegQueryValue	HKLM\System\CurrentControlSet\Control\TimeZoneInformation\ActiveTimeBias	SUCCESS	Type: REG_DWORD, Length: 4, Data: 480
4:01:11	dada.exe	1348	RegOpenKey	HKLM\System\CurrentControlSet\Control\TimeZoneInformation	SUCCESS	Desired Access: Read, Maximum Allowed
4:01:11	dada.exe	1348	RegQueryValue	HKLM\System\CurrentControlSet\Control\TimeZoneInformation\Bias	SUCCESS	Type: REG_DWORD, Length: 4, Data: 480
4:01:11	dada.exe	1348	RegQueryValue	HKLM\System\CurrentControlSet\Control\TimeZoneInformation\StandardName	SUCCESS	Type: REG_SZ, Length: 44, Data: Pacific Standard Time
4:01:11	dada.exe	1348	RegQueryValue	HKLM\System\CurrentControlSet\Control\TimeZoneInformation\StandardBias	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
4:01:11	dada.exe	1348	RegQueryValue	HKLM\System\CurrentControlSet\Control\TimeZoneInformation\StandardStart	SUCCESS	Type: REG_BINARY, Length: 16, Data: 00 00 04 00 05 00 02 00 00 00 00 00 00 00 00 00
4:01:11	dada.exe	1348	RegQueryValue	HKLM\System\CurrentControlSet\Control\TimeZoneInformation\DaylightName	SUCCESS	Type: REG_SZ, Length: 44, Data: Pacific Daylight Time
4:01:11	dada.exe	1348	RegQueryValue	HKLM\System\CurrentControlSet\Control\TimeZoneInformation\DaylightBias	SUCCESS	Type: REG_DWORD, Length: 4, Data: 4294967296
4:01:11	dada.exe	1348	RegQueryValue	HKLM\System\CurrentControlSet\Control\TimeZoneInformation\DaylightStart	SUCCESS	Type: REG_BINARY, Length: 16, Data: 00 00 04 00 01 00 02 00 00 00 00 00 00 00 00 00
4:01:11	dada.exe	1348	RegOpenKey	HKLM\System\CurrentControlSet\Control\TimeZoneInformation	SUCCESS	Desired Access: Write
4:01:11	dada.exe	1348	RegCreateKey	HKLM\System\CurrentControlSet\Control\TimeZoneInformation	SUCCESS	Type: REG_DWORD, Length: 4, Data: 480

Dada appears to be interacting with time-related directories constantly. Perhaps its purpose is related to time?

The directories being accessed are HKLM\System\CurrentControlSet\Control\TimeZoneInformation and its subdirectories Bias, StandardName, StandardBias, StandardStart, DaylightName, DaylightBias, DaylightStart, and ActiveTimeBias.



Dada appears to be forcing the clock to stay at 4:00:04 PM.

What we learned:

Dada creates a new registry at HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\RunLikeHell. Dada has placed the path to its executable file as this key's value, which means that it will run at startup.

Dada appears to be constantly forcing the clock to freeze at 4:00:04 PM. Dada is constantly accessing time related registries in order to do this. The registries accessed are HKLM\System\CurrentControlSet\Control\TimeZoneInformation and its subdirectories Bias, StandardName, StandardBias, StandardStart, DaylightName, DaylightBias, DaylightStart, and ActiveTimeBias.















