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.

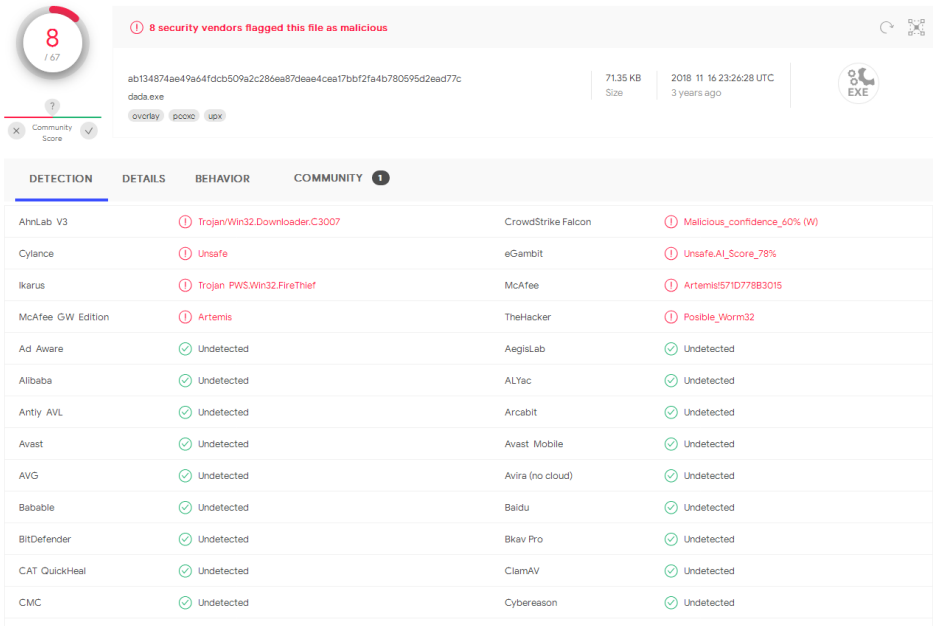
1. Perform basic static analysis on this binary. What were we able to learn?

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.)]

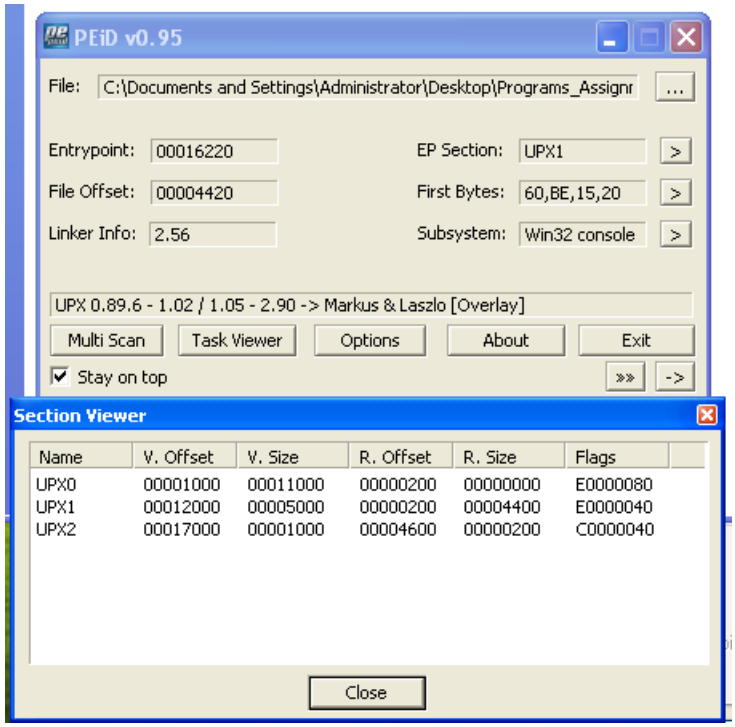
.

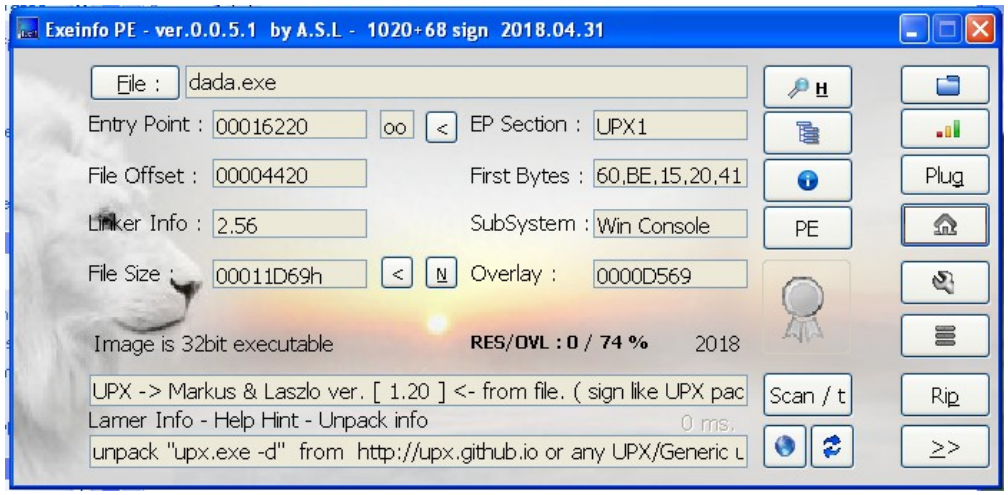
Dada-1.

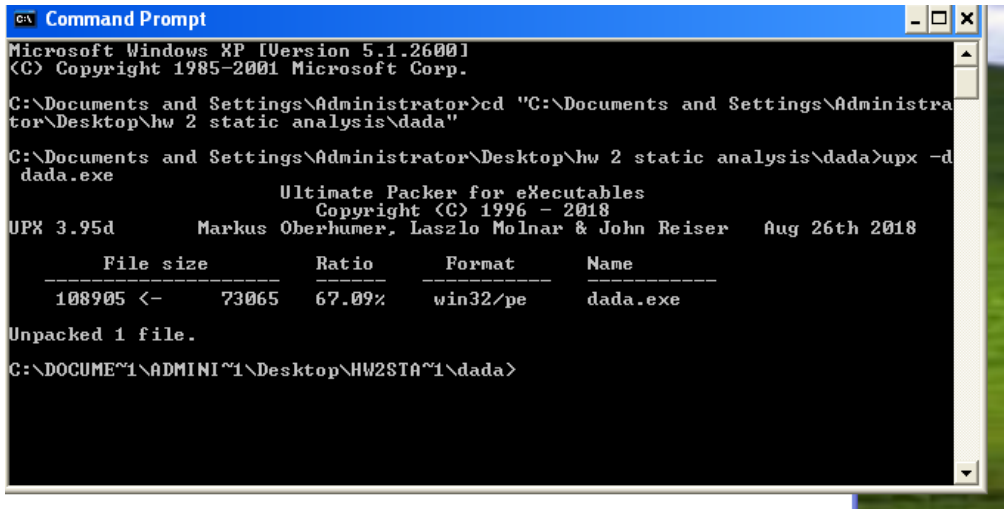


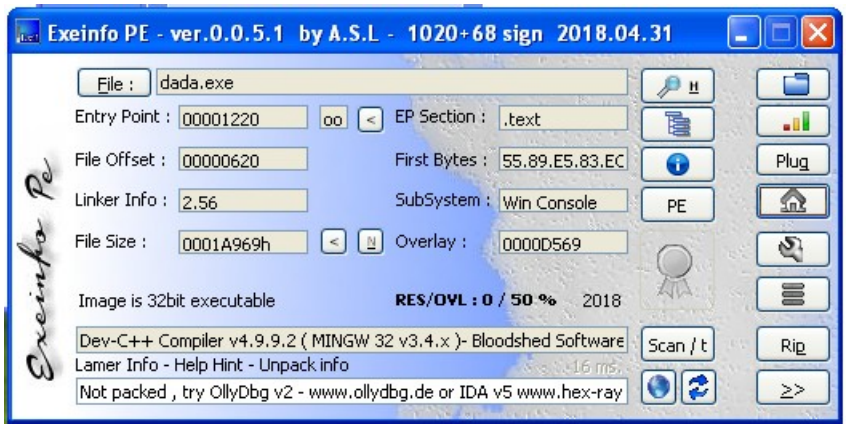
Ikarus says trojan

its packed with upx


PEiD v0.95
File: C:\Documents and Settings\Administrator\Desktop\Programs_Assignr
Entrypoint: 00016220
EP Section: UPX1
File Offset: 00004420
First Bytes: 60,BE,15,20
Linker Info: 2.56
Subsystem: Win32 console
UPX 0.89.6 - 1.02 / 1.05 - 2.90 -> Markus & Laszlo [Overlay]
Multi Scan
Task Viewer
Options
About
Exit
Stay on top
Section Viewer
Name V. Offset V. Size R. Offset R. Size Flags
UPX0 00001000 00011000 00000200 00000000 E0000080
UPX1 00012000 00005000 00000200 00004400 E0000040
UPX2 00017000 00001000 00004600 00000200 C0000040
Close


Exeinfo PE - ver.0.0.5.1 by A.S.L - 1020+68 sign 2018.04.31
File : dada.exe
Entry Point : 00016220
EP Section : UPX1
File Offset : 00004420
First Bytes : 60,BE,15,20,41
Linker Info : 2.56
SubSystem : Win Console
File Size : 00011D69h
Overlay : 0000D569
Image is 32bit executable
RES/OVL : 0 / 74 %
2018
UPX -> Markus & Laszlo ver. [1.20] <- from file. (sign like UPX pac
Lamer Info - Help Hint - Unpack info
unpack "upx.exe -d" from http://upx.github.io or any UPX/Generic
Plug
PE
Scan / t
Rip


Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>cd "C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\dada"
C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\dada>upx -d dada.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2018
UPX 3.95d Markus Oberhumer, Laszlo Molnar & John Reiser Aug 26th 2018
File size Ratio Format Name
108905 <- 73065 67.09% win32/pe dada.exe
Unpacked 1 file.
C:\DOCUME~1\ADMINI~1\Desktop\HW2STA~1\dada>

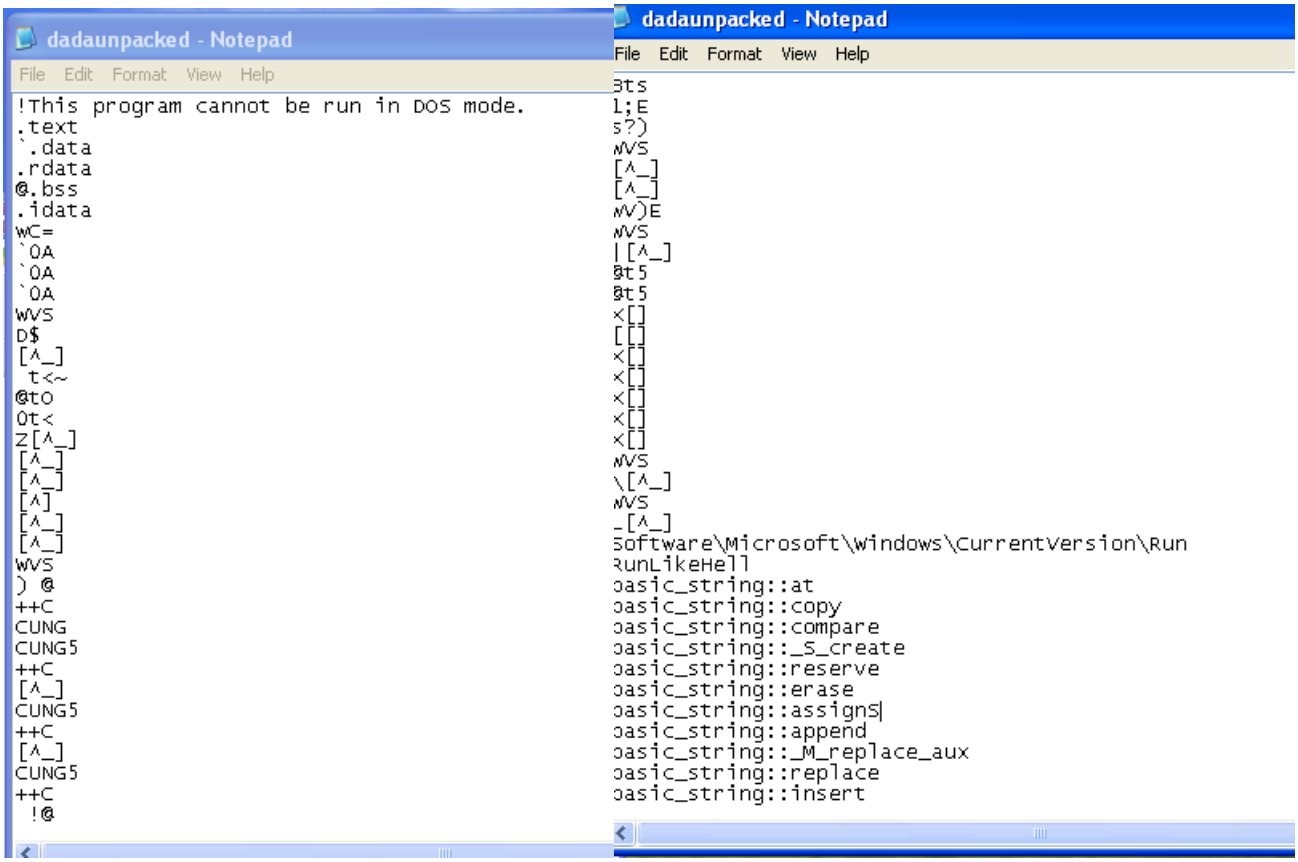


After unpacking the malware seems to have been compiled with Dev-C++ Compiler and Bloodshed Software.

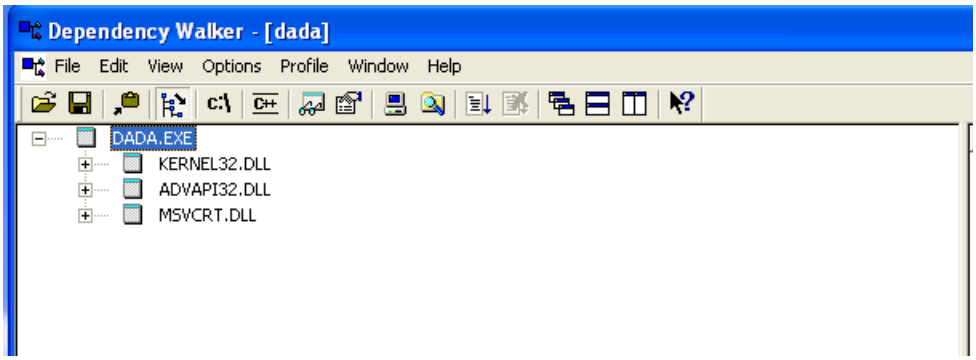
compiler-stamp	0x5BC9680D (Thu Oct 18 22:13:49 2018 - UTC)

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

https://pastebin.com/wxVdNFRE



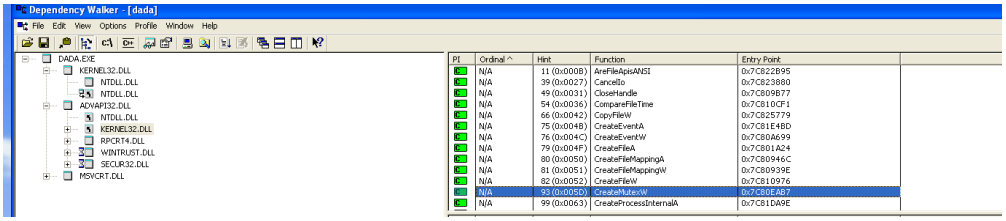
There is a suspicious entry in the strings, RunLikeHell.



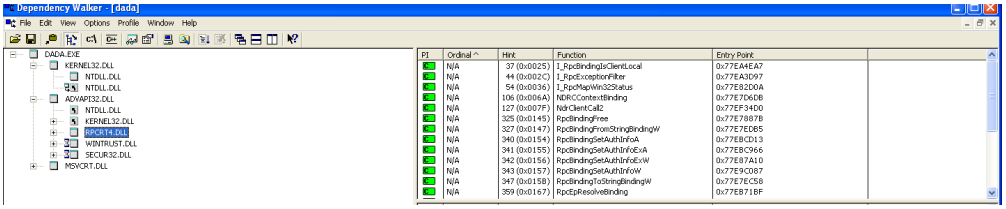
KERNEL32.dll (from lecture, might have access to memory, files, and hardware)

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)

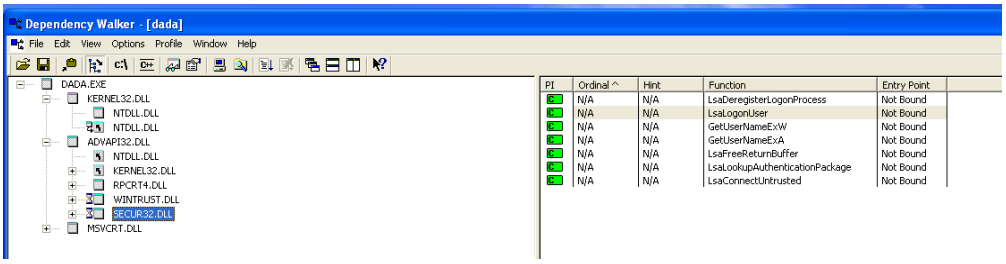
Uses threads



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

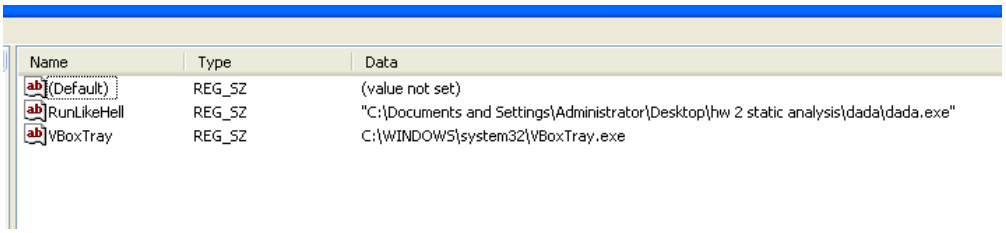
What we learned:

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.

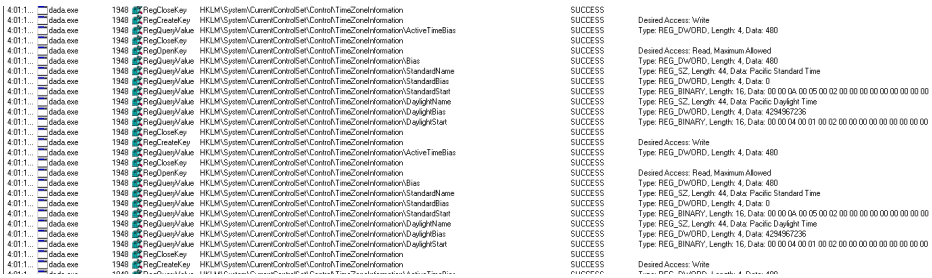
dada has created a new registry called HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\RunLikeHell



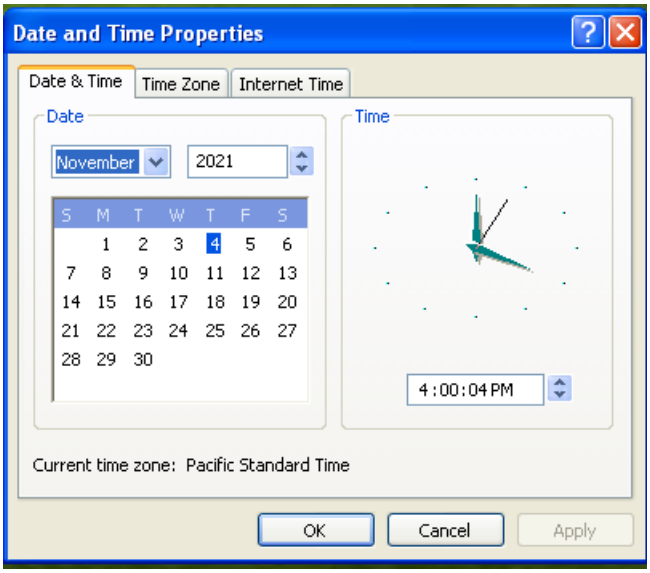
Name	Type	Data
(Default)	REG_SZ	(value not set)
RunLikeHell	REG_SZ	"C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\dada\dada.exe"
VBoxTray	REG_SZ	C:\WINDOWS\system32\VBoxTray.exe

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.

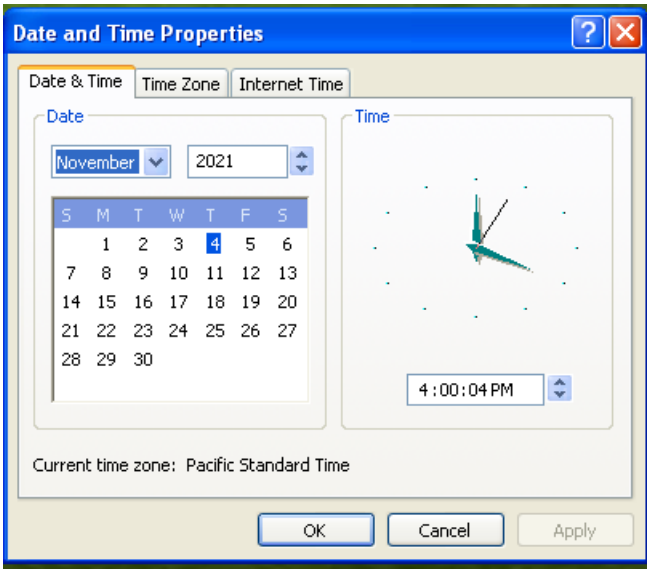
What we learned:

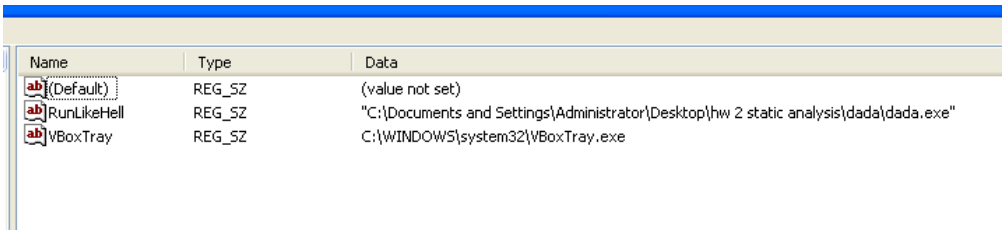
Dada creates a new registry at HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\RunLikeHell. Dada has placed the path to its executable file as this key's value, which means that it will run at startup.

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.



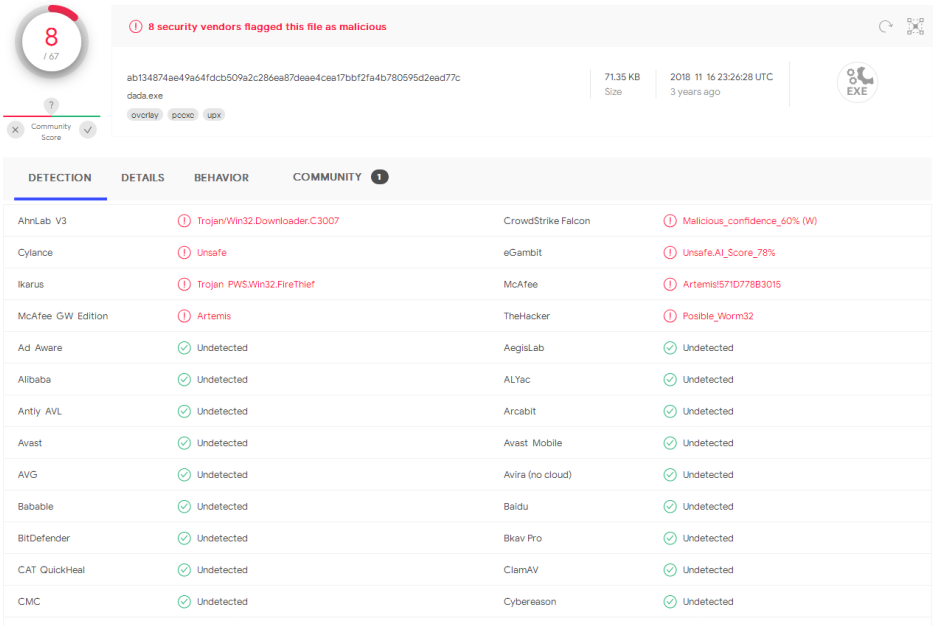


Name	Type	Data
(Default)	REG_SZ	(value not set)
RunLikeHell	REG_SZ	"C:\Documents and Settings\Administrator\Desktop\hw 2 static analysis\dada\dada.exe"
VBoxTray	REG_SZ	C:\WINDOWS\system32\VBoxTray.exe

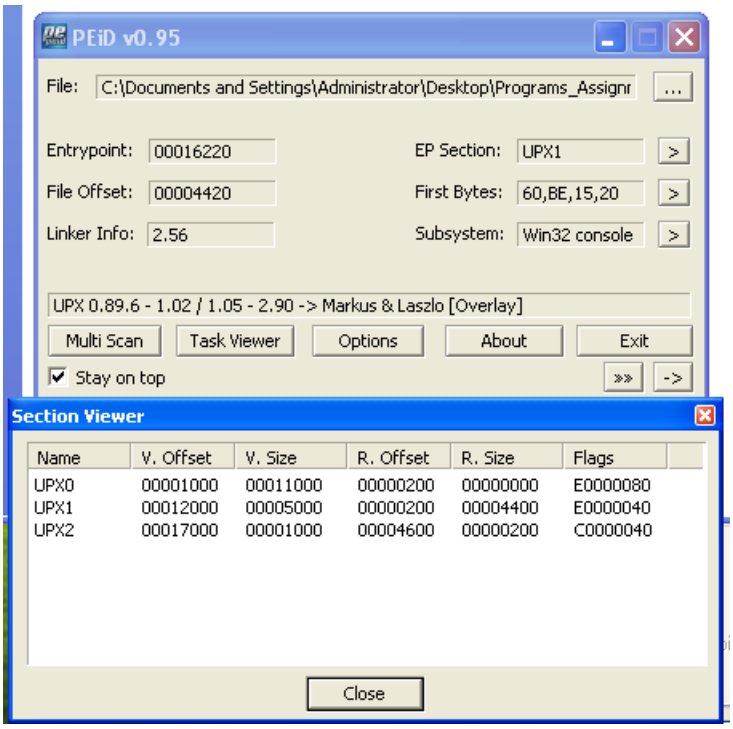
How to remove the malware:

Open regedit and go to HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run and delete the value of RunLikeHell, then reboot the machine.

Analysis:

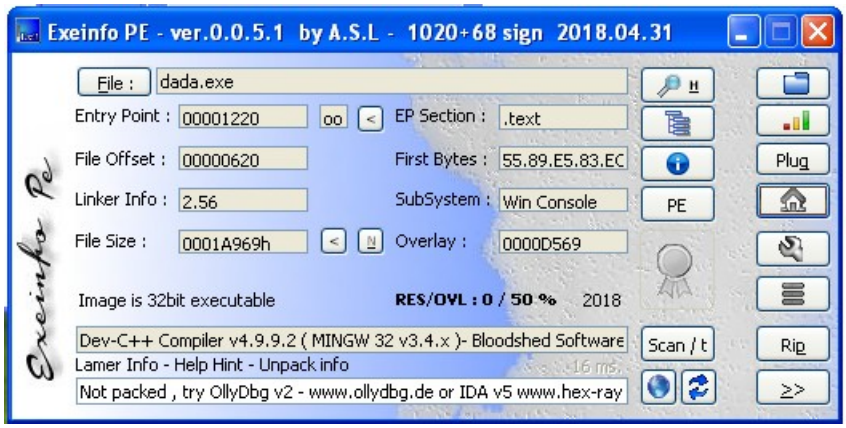


In VirusTotal, Ikarus says that the malware is a Trojan.

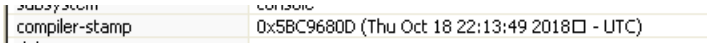


The malware appears to have been packed using upx.

It has been successfully unpacked.

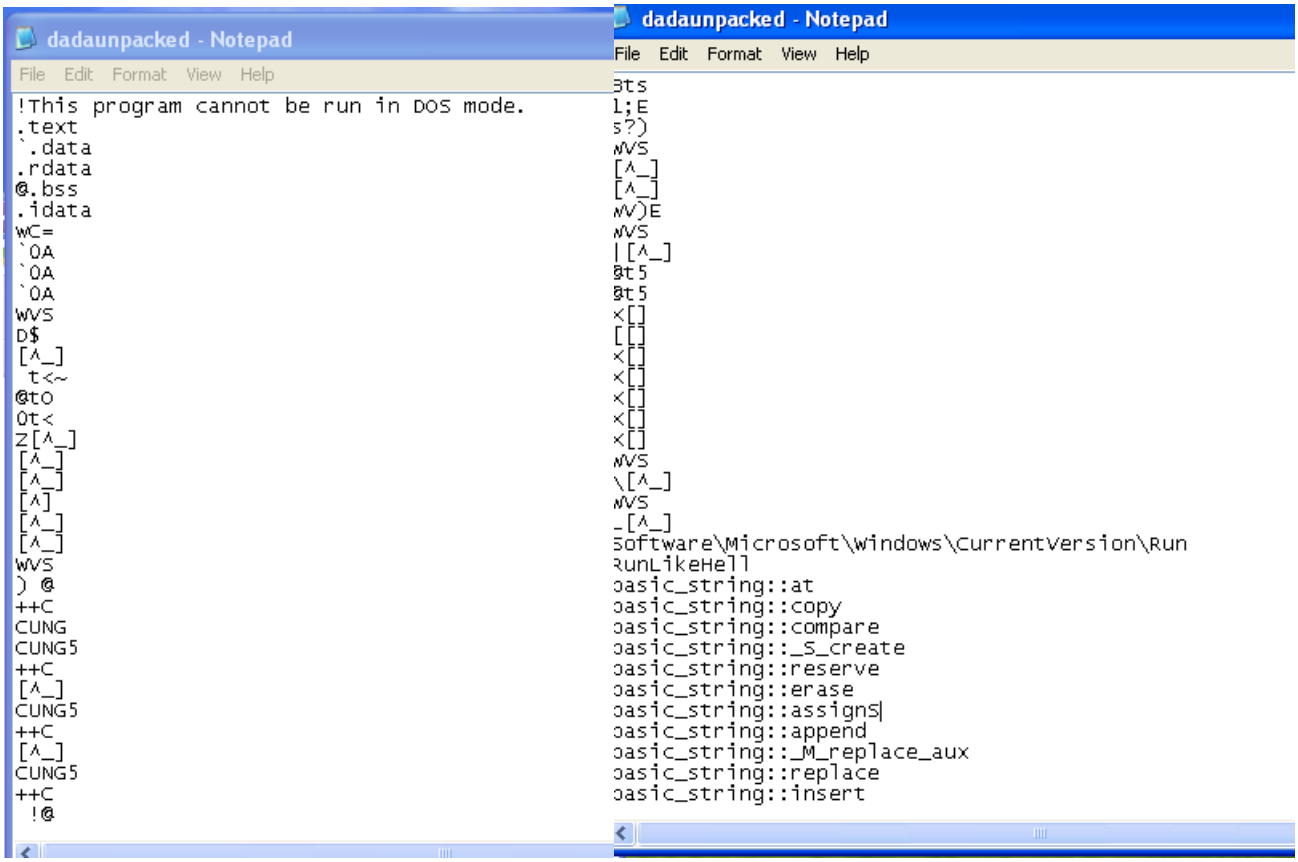


After unpacking the malware seems to have been compiled with Dev-C++ Compiler and Bloodshed Software.

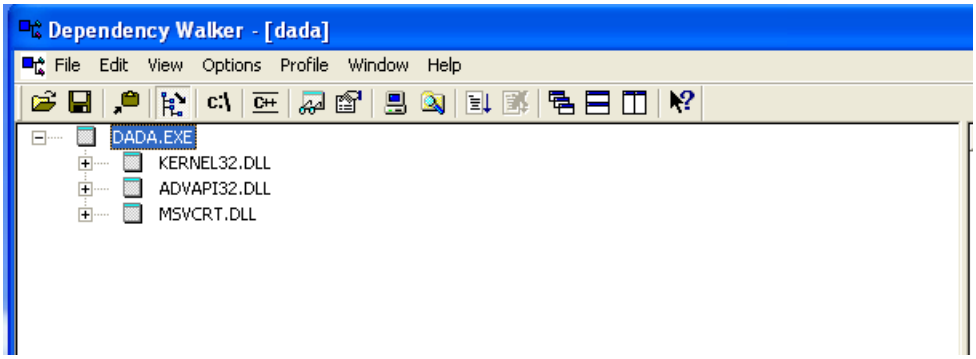


The malware appears to have a compilation timestamp of Thursday October 18 22:13:49 2018 UTC.

https://pastebin.com/wxVdNFRE



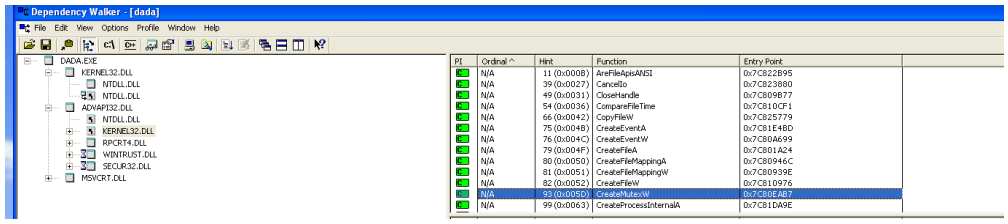
There is a suspicious entry in the strings, RunLikeHell.



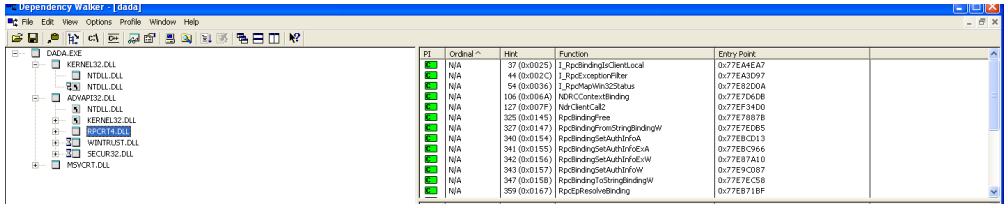
KERNEL32.dll (from lecture, might have access to memory, files, and hardware)

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)

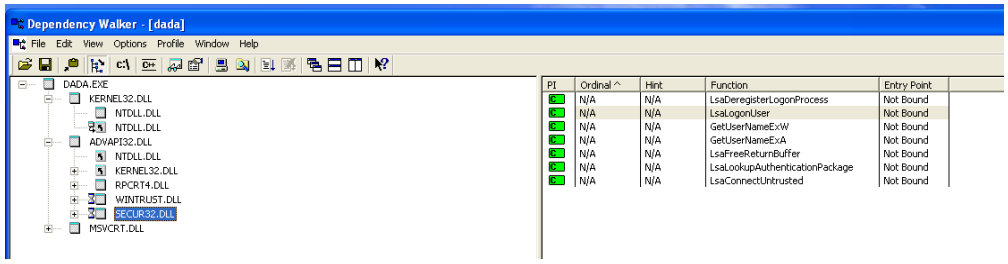
Uses threads



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.

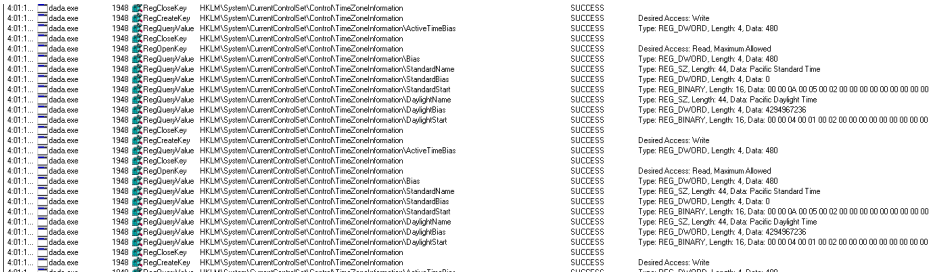
Dada may have access to the kernel, the windows registry, user accounts, and windows services. Dada might use threads, network functions, and may create new logon sessions. Dada may add a new registry key that may be visible in regedit. It may also print to a file.

dada 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

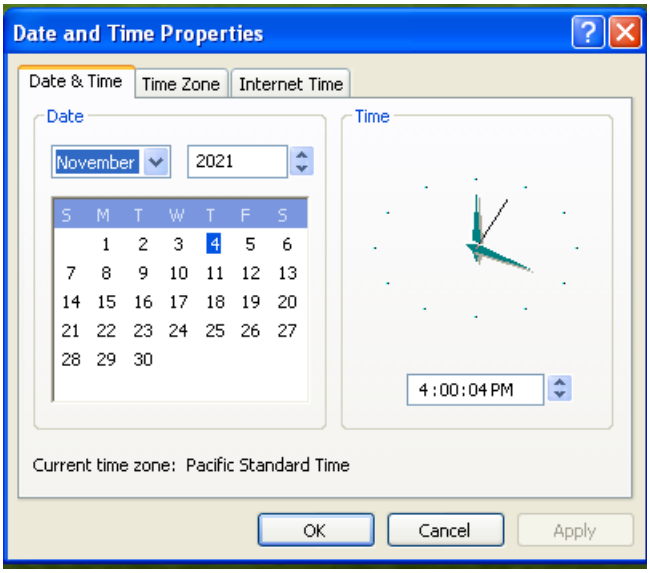
The contents of HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run in regedit.

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?

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.