**Nanocore RAT**

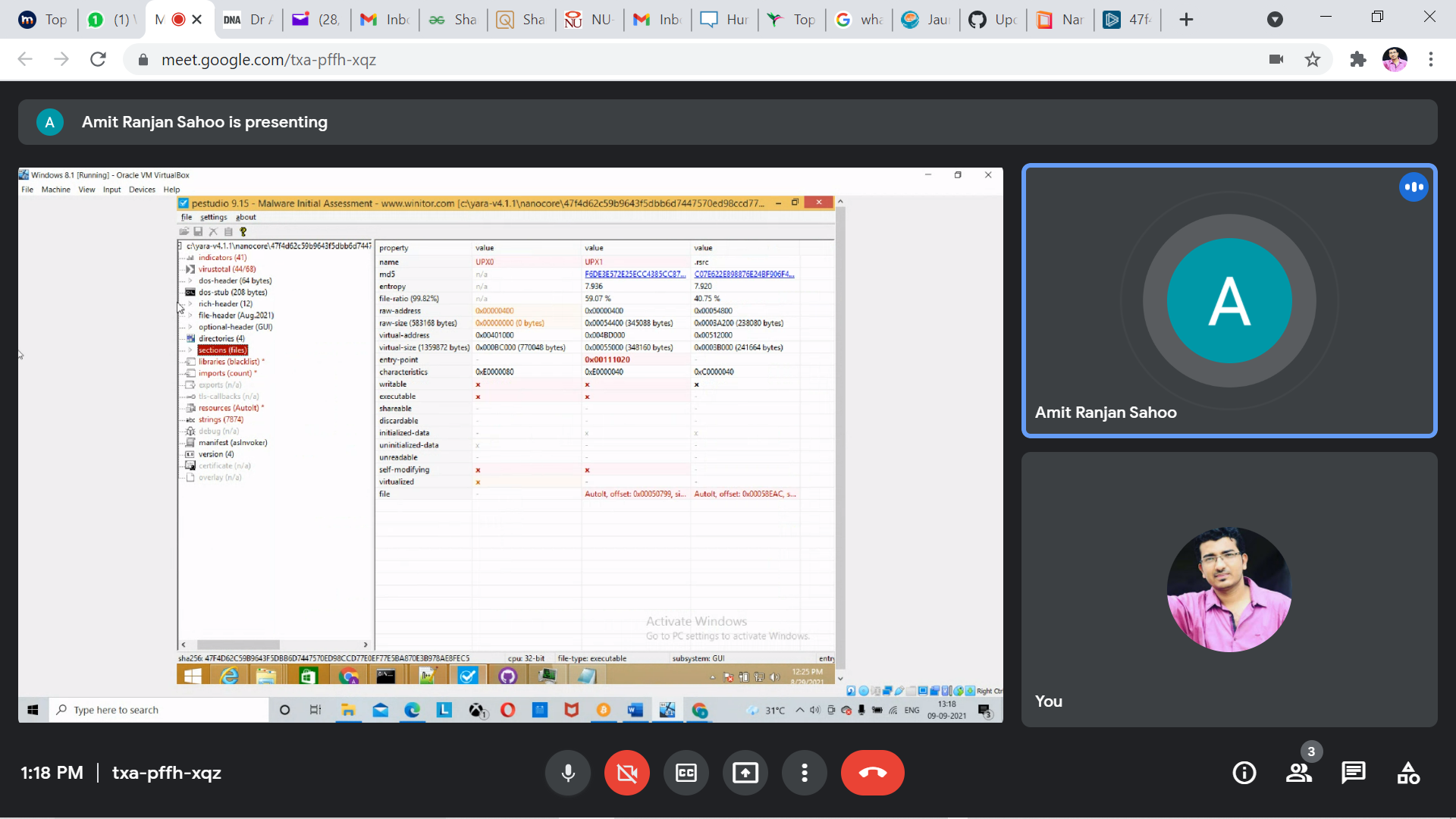
NanoCore Malware is a RAT that has become popular in recent years. Since it was discovered in 2013, multiple different versions have been leaked on underground forums. The latest leaked version was 1.2.2.0 in March 2015 and is available online to download for free. *NanoCore RAT* comes with a few base plugins and the ability to expand its functionality, so threat actors can develop additional features for other malicious actions. There is already a wide range of NanoCore plugins available online that can be used for cryptocurrency mining, ransomware attacks, and more.

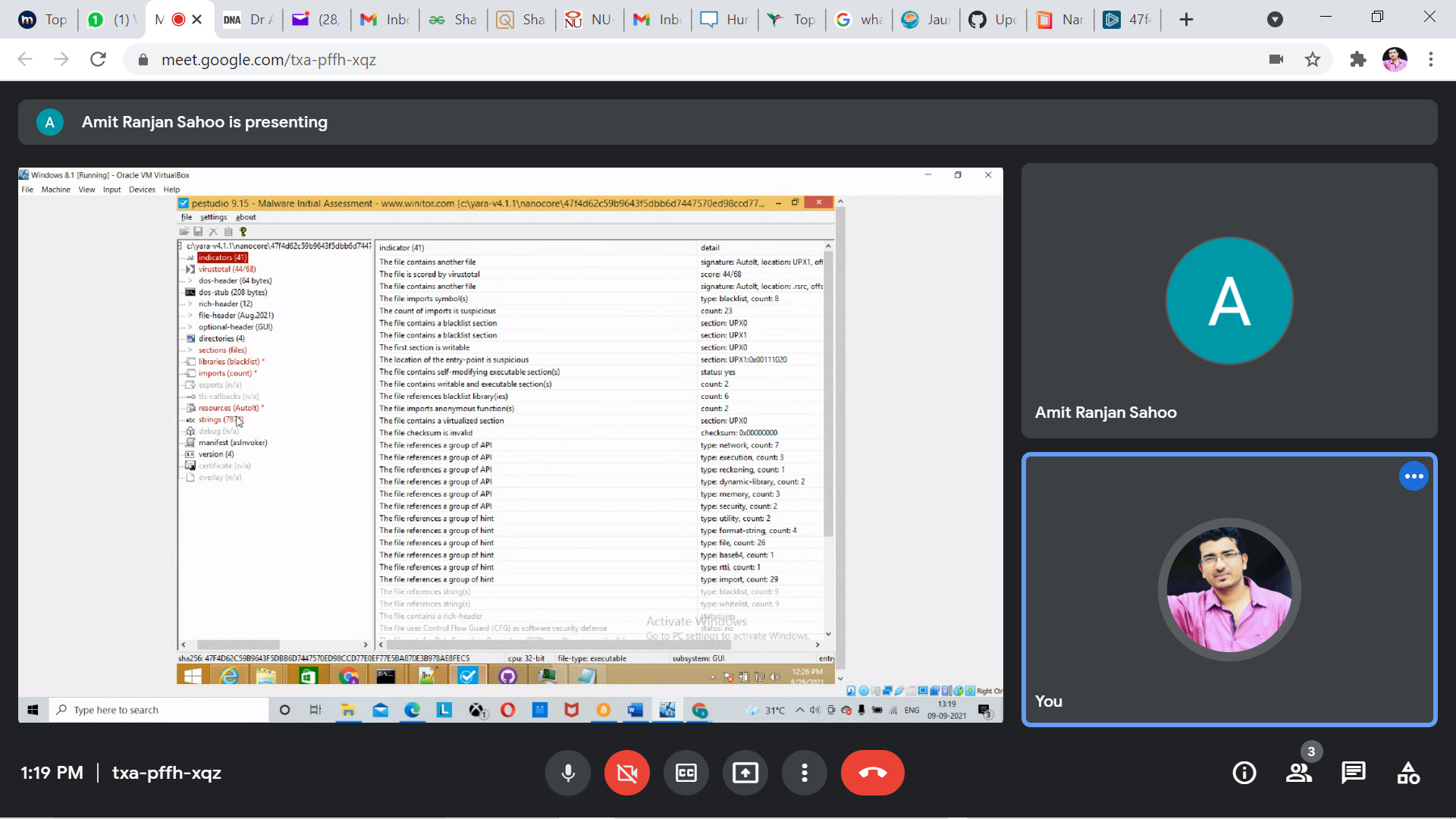
**Static Analysis**

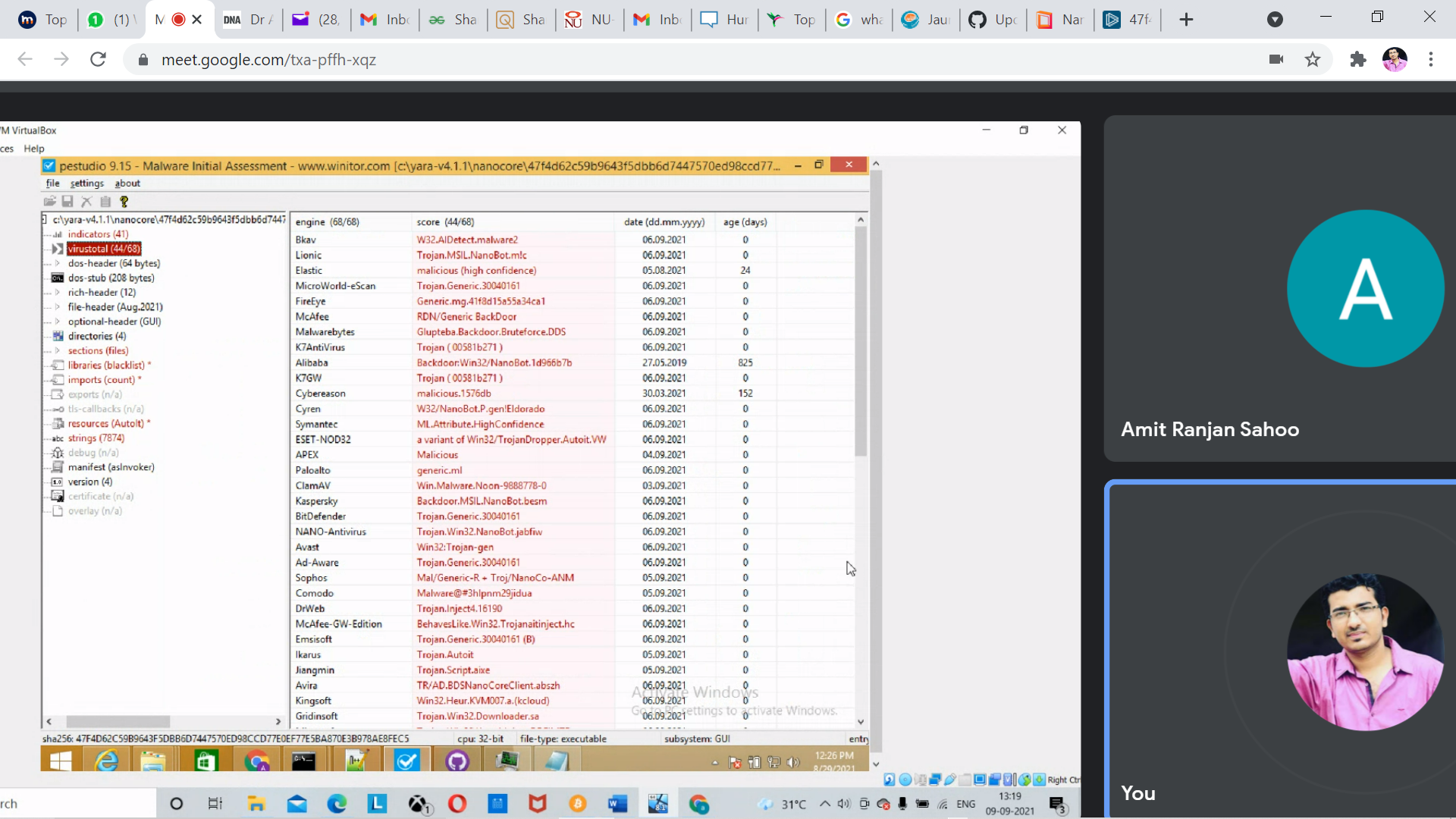
From PE studio

Indicator:

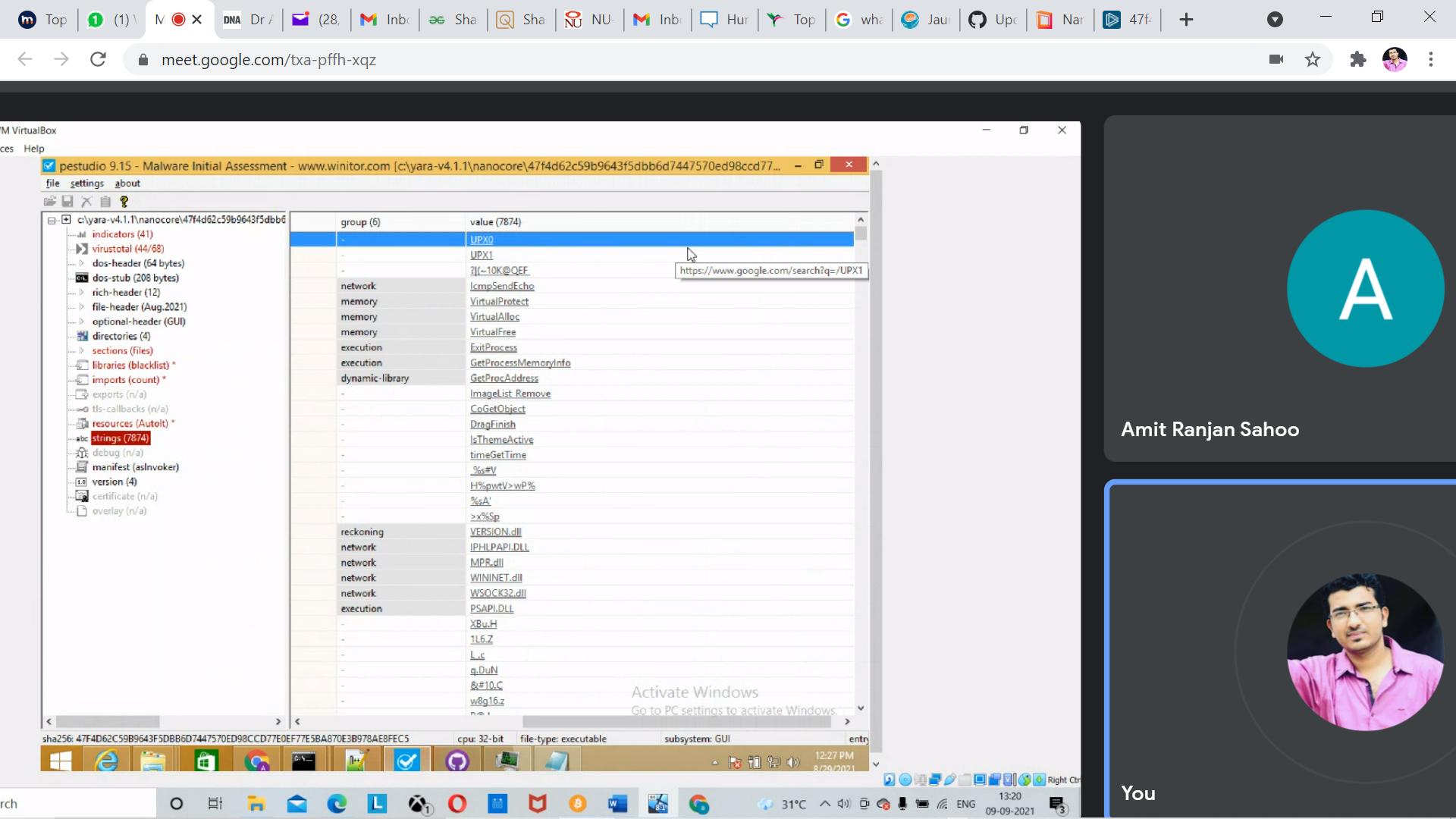
File contains another file: signature: AutoIt, location: UPX1, offset: 0x00050799, size: -1S



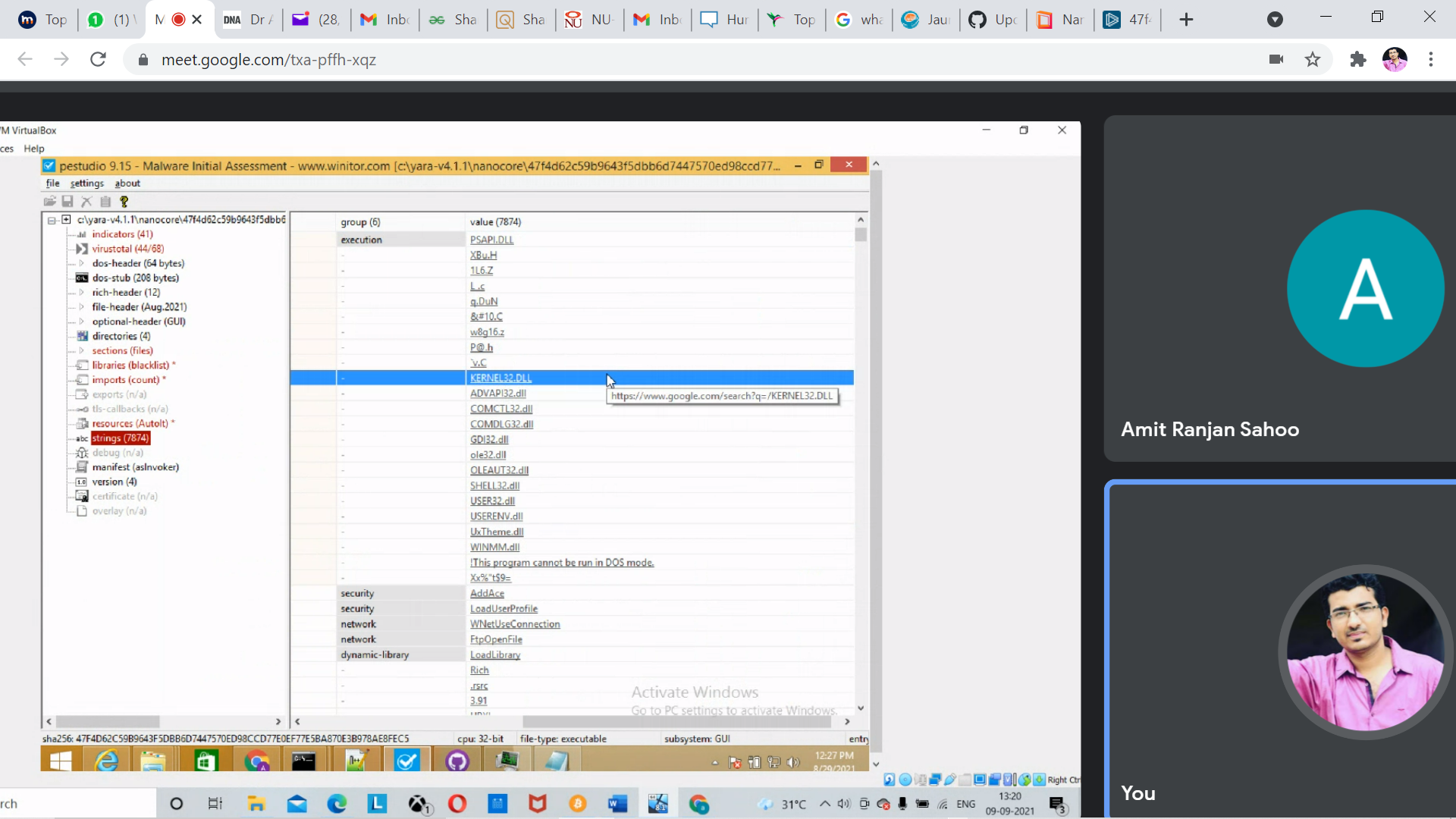




Strings



This exe is using Kernel32Dll



**Dynamic Analysis**

UPX compressed Win32 Executable (35.7%)

Imports :

**Imports**

MPR.dll

COMDLG32.dll

IPHLPAPI.DLL

UxTheme.dll

OLEAUT32.dll

SHELL32.dll

PSAPI.DLL

USERENV.dll

VERSION.dll

WINMM.dll

WININET.dll

GDI32.dll

KERNEL32.DLL

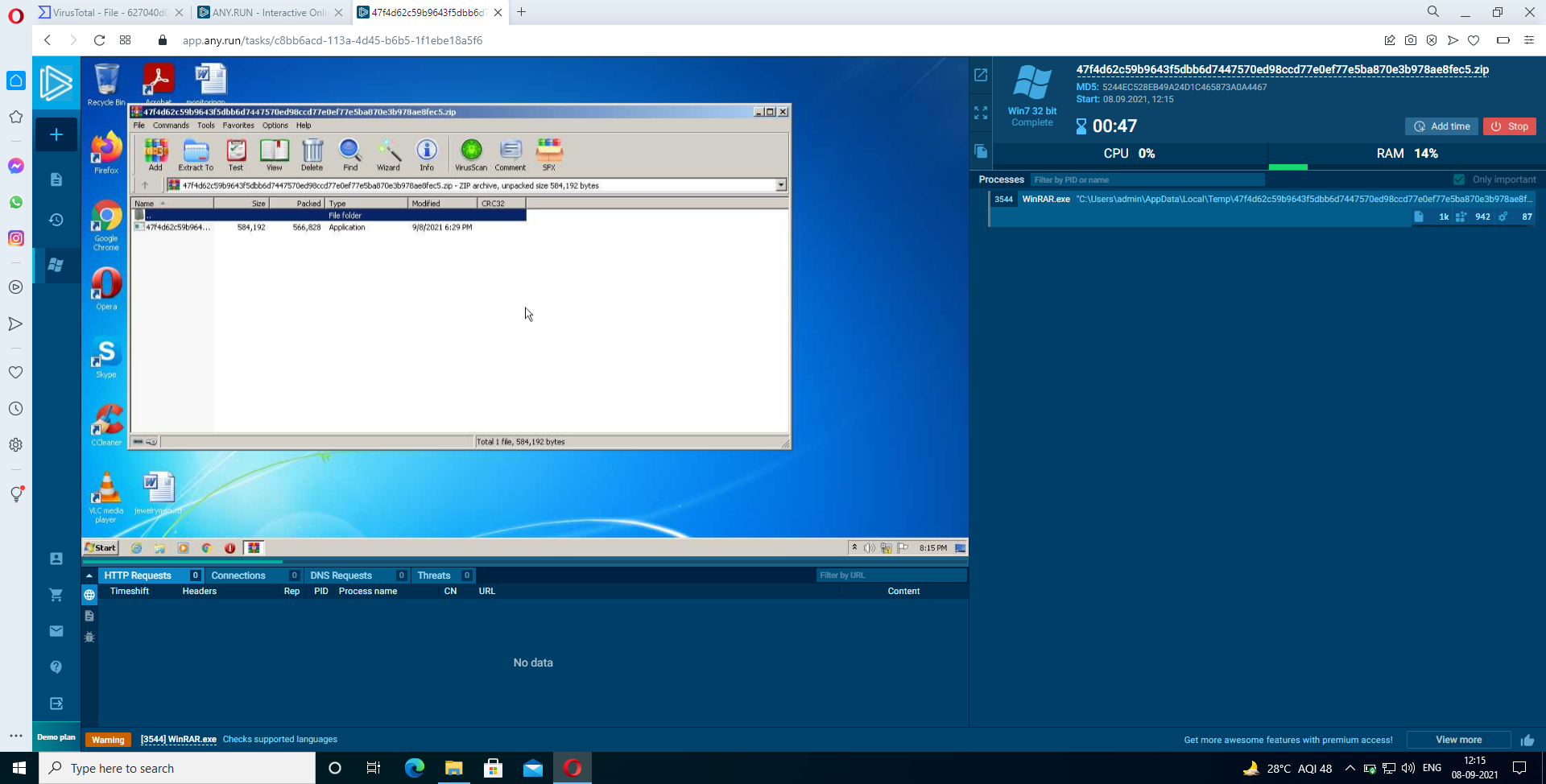
WSOCK32.dll

ADVAPI32.dll

ole32.dll

COMCTL32.dll

USER32.dll



**TRiD Information**

-----------------

Identify any file type with TrID

=================================

It’s not uncommon to encounter unknown file types, especially if you receive a lot of emails with attachments in them. Of course, before clicking on any of these unknown files, it’s best to identify what kind of file it is because they might be malicious and could harm your PC. TrID is a tool that identifies unknown file types for users. Developed by Marco Pontello, TrID can provide users with the information they need to know about a file before they open it.

.exe | UPX compressed Win32 Executable (39.3%)

.exe | Win32 EXE Yoda's Crypter (38.6%)

.dll | Win32 Dynamic Link Library (generic) (9.5%)

.exe | Win32 Executable (generic) (6.5%)

.exe | Generic Win/DOS Executable (2.9%)

**This gives an indication that it could be Malware as UPX and Crypter have the highest probability**

**Process Information**

Dropped files

1.\Users\admin\AppData\Local\Temp\aut2FDC.tmp

\Users\admin\AppData\Local\Temp\divlridlybkx

Same Process ID 3984

**Session ID gets deleted.**

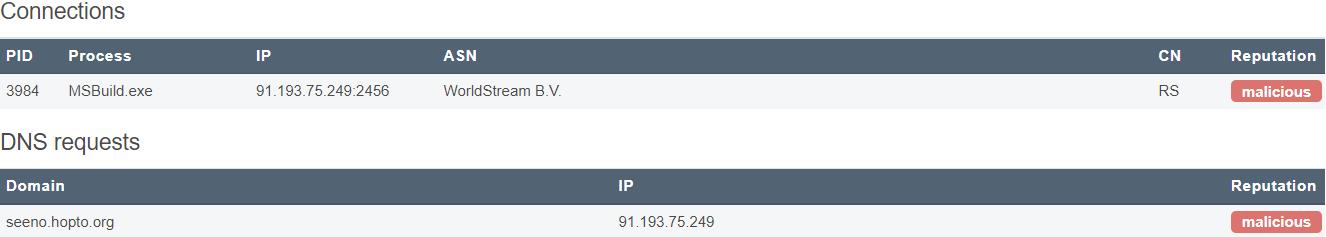
2.Users\admin\AppData\Roaming\90059C37-1320-41A4-B58D-2B75A9850D2F\catalog.dat

**This is the file released by the antivirus companies(Specifically NORTON AV) which is dropped by this malware.**

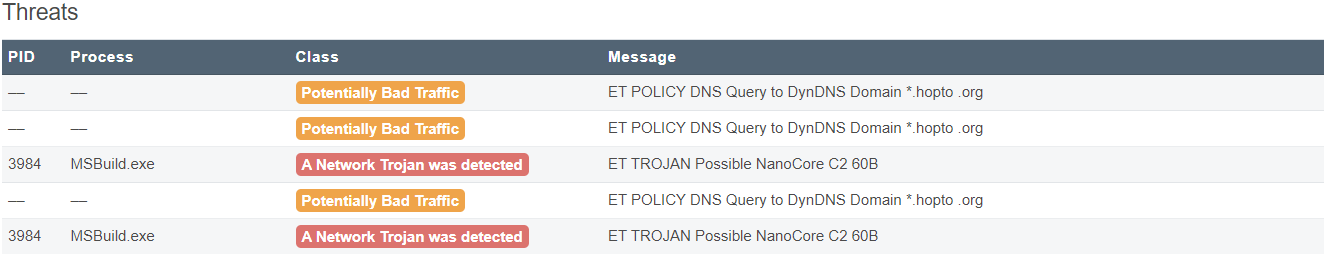
3.\Users\admin\AppData\Roaming\90059C37-1320-41A4-B58D-2B75A9850D2F\run.dat

The compromised process creates an 8-byte file called run.dat in specified folder. So to remove the footprint it drops the file

MSBuild - a tool used for building apps and gives users an XML schema “that controls how the build platform processes and builds software” - to filelessly deliver RemcosRAT, and RedLine stealer using callbacks. The malicious MSBuild files we observed in this campaign contained encoded executables and shellcode, with some, hosted on Russian image-hosting site, “joxi[.]net.” While we were unable to determine the distribution method of the .proj files, the objective of these files was to execute either Remcos or RedLine Stealer. The majority of the samples we analyzed deliver Remcos as the final payload.



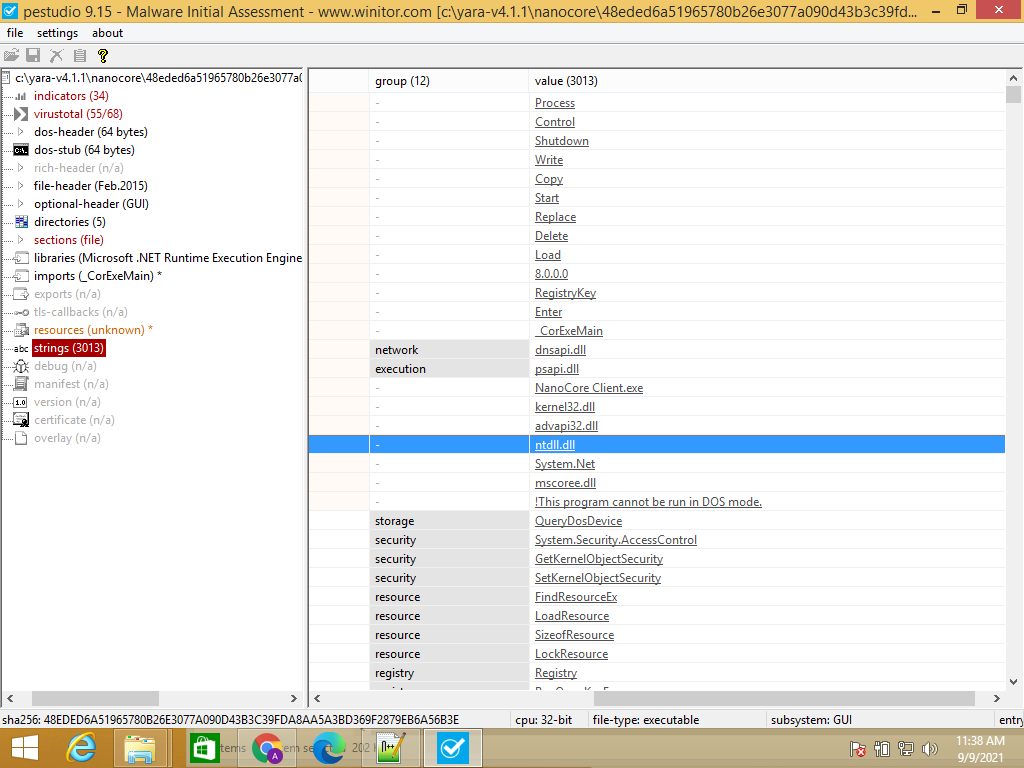
**Network Activity**

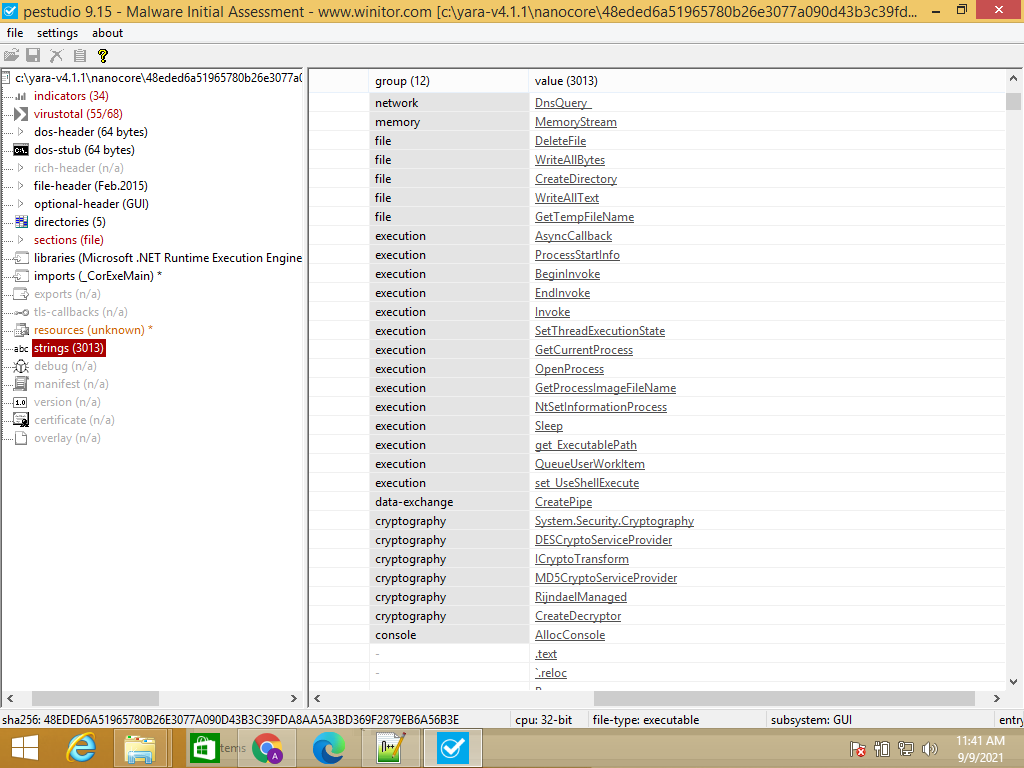


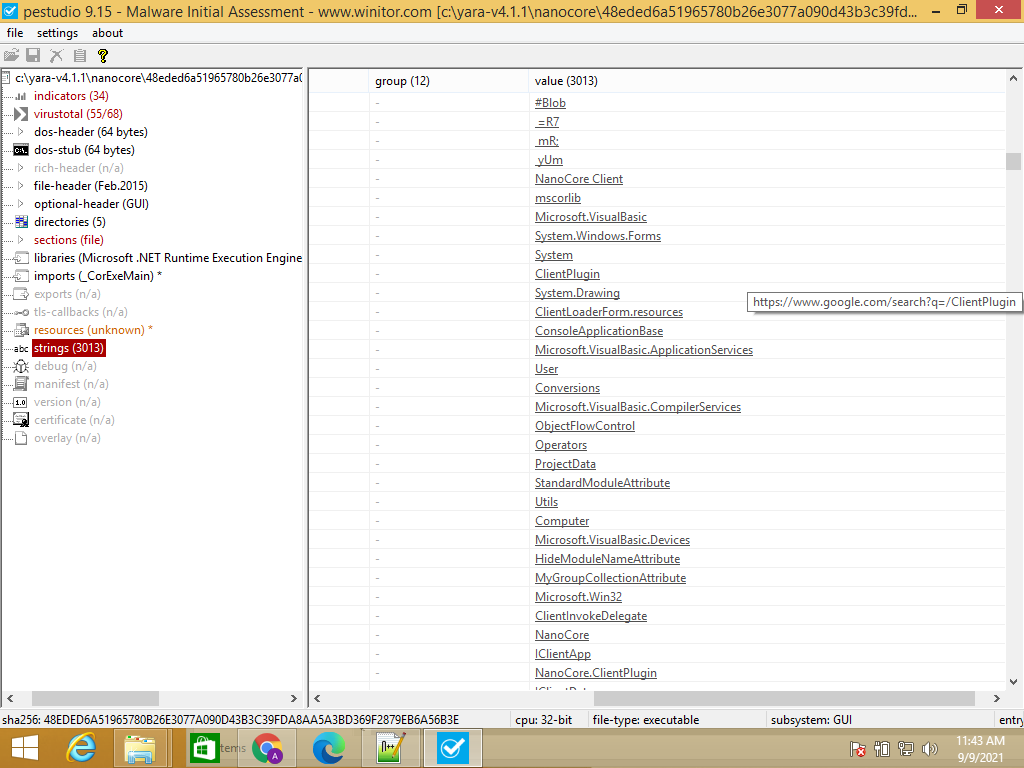
Reference

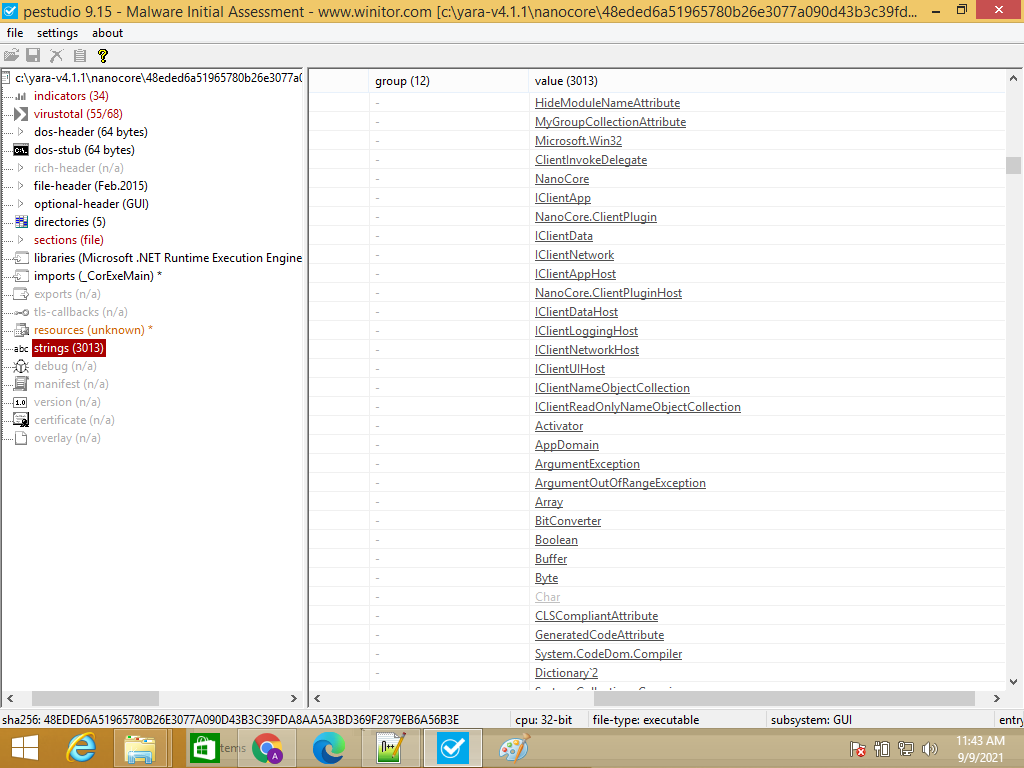
**Sample -2**

**Analysis for** **48eded6a51965780b26e3077a090d43b3c39fda8aa5a3bd369f2879eb6a56b3e**





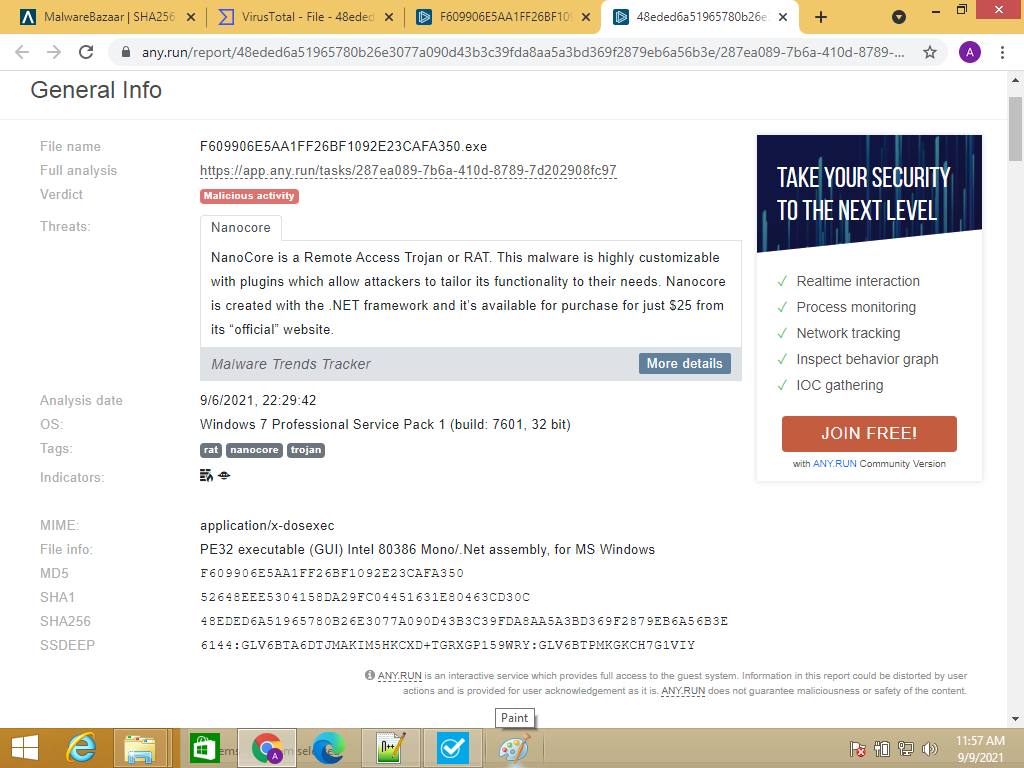


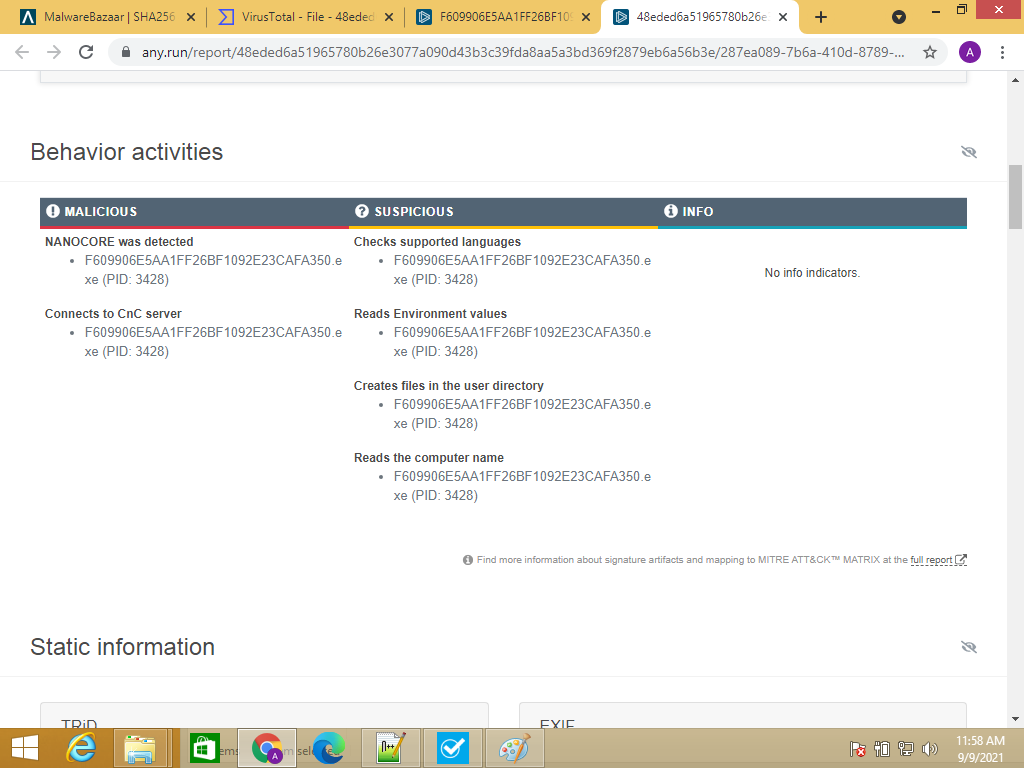


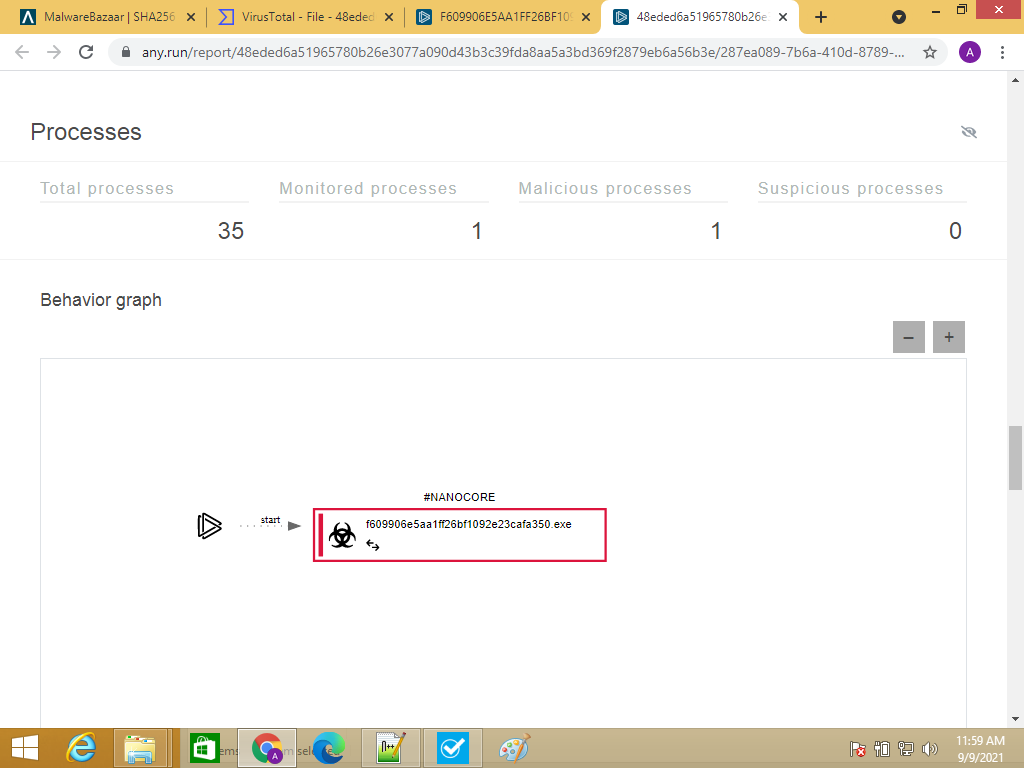


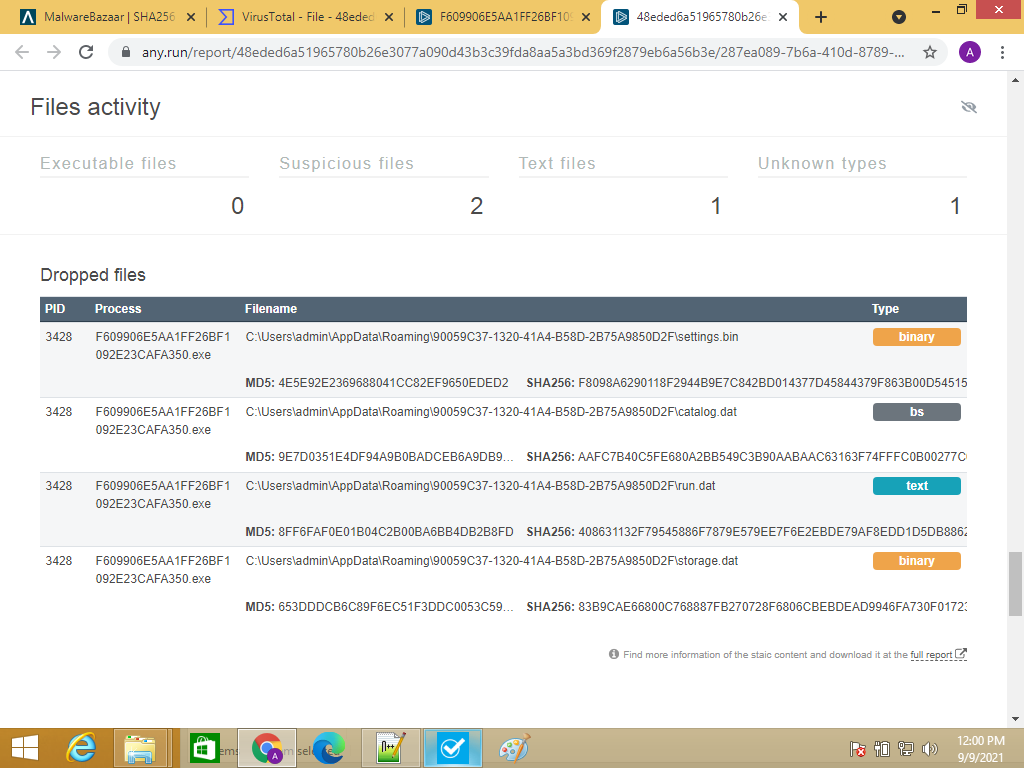


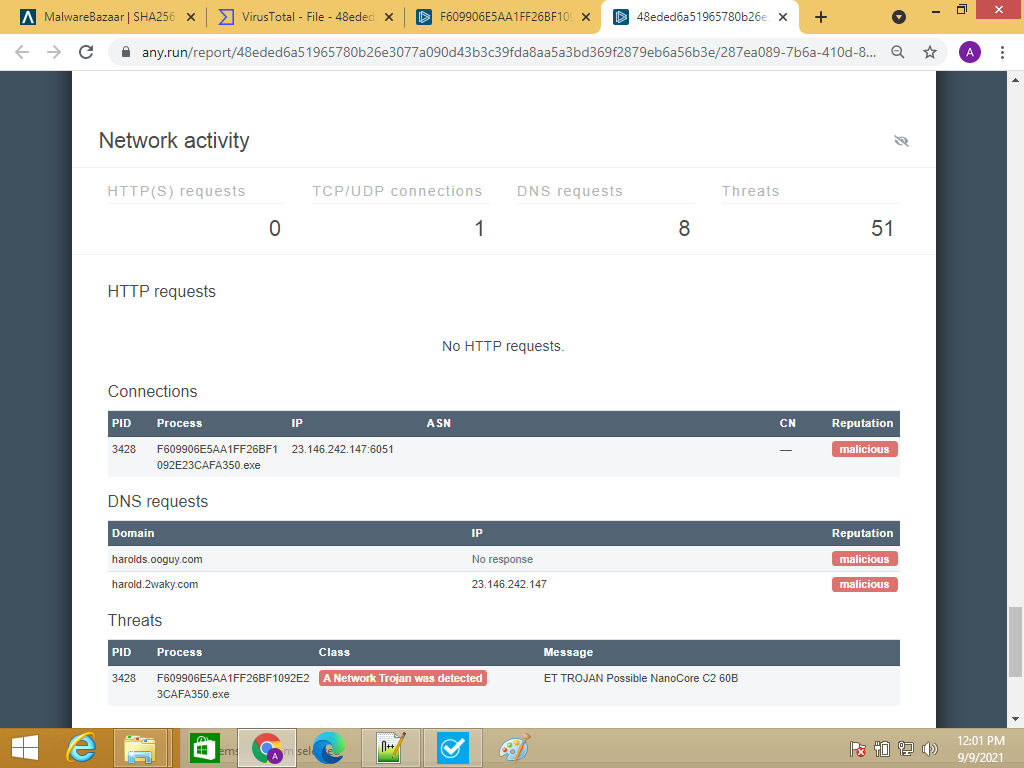
Dynamic Analysis on Any.run











Yara Rule(Custom)

rule probable\_malware{

meta:

description="This is first yara rule to find out possible malware family"

hash1="34319d13f02fbb49f4c442196e7334c5cfffeea44777246fc75acbc373d84c2d"

strings:

$a="NanoCore Client.exe" nocase

$b="kernel32.dll" nocase

$c="QueryDosDevice"

$d="This program cannot be run in DOS mode."

$e="Sleep"

$f="DESCryptoServiceProvider"

$g="CreateDecryptor"

$h="NanoCore Client" nocase

$i="ImageList\_Remove"

$j="NanoCore.ClientPlugin" nocase

$k="RebuildHostCache"

$l="DisableProtection"

$m="Uninstall"

$n="HostDetails"

$o="FtpOpenFile"

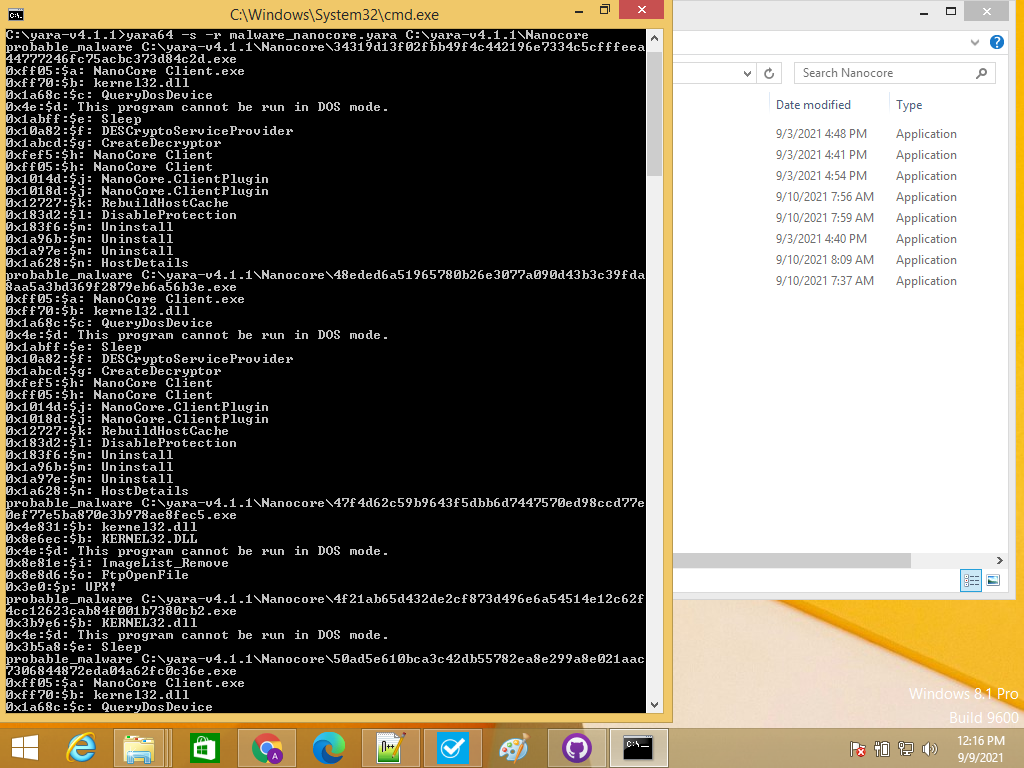
$p="UPX!"

condition:

($a or $j) or (3 of them)

}

Yara Rule on the collected samples



Reference

https://6point6.co.uk/insights/analysis-of-nanocore-rat/