International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2020): 7.803

Novel Technique to Hide Identity of Alina Malware

Dhruv R. Gajjar

Abstract: ***Laptop infection's purpose billions of bucks of monetary each year. As to speak approximately this in current year is to make attention in humans approximately ongoing fraud approximately laptop malware and to save you them approximately it. Almost current assaults are finished the use of encrypted laptop malware form. Which maximum tough as it makes undetectable malware to be scanned through antivirus. Even it bypasses the firewalls after which does its effect on laptop or a laptop community system.***

1. Introduction

1.1 What is Encryption?

In cryptography, encryption is the way toward encoding data. This cycle changes Over the primary portrayal of the data, known as plaintext, into an elective structure known as cipher text. In a perfect world, just approved gatherings can unravel a code textual content returned to plaintext and get to the first data. Encryption doesn't itself forestall impedance however denies a future interceptor's crystalline element.

For unique reasons, an encryption contrives normally makes use of a pseudo - sporadic encryption key made with the aid of using an estimation. It is doable to unscramble the message while not having the important thing but, for an all - round deliberate encryption conspire, massive computational property and competencies are required. An accredited beneficiary can absolutely unscramble the message with the important thing given with the aid of using the originator to beneficiaries but now no longer to unapproved clients.

1.2 What is Malware?

A laptop infection is any such laptop application that, while executed, copies itself through converting different laptop packages and embeddings its very own code. If this replication succeeds, the affected regions are then predicted to be "corrupted" with a laptop disease.

1.3 What is Alina malware?

Alina is a Point of Sales Malware or POS RAM Scraper this is utilized by cybercriminals to scrape credit card and debit card statistics from the factor of sale system. It first commenced to scrape statistics in past due 2012. It resembles JackPOS Malware.

1.4 How does Alina malware works?

Once executed, it receives set up at the user's laptop and assessments for updates. If an update is found, it removes the present Alina code and installs the trendy version. Then, for brand spanking new installations, it provides the report direction to an AutoStart run key to preserve persistence. Finally, it provides java. exe to the %APPDATA% listing and executes it the usage of the parameter alina=<path_to_executable> for new installations or, update=<orig_exe>; <new_exe> for upgrades.

Alina inspects the user's techniques with the assist of Windows API calls:

Create Tool help 32 Snapshot () takes an image of all walking techniques

Process32First () /Process32Next () retrieve the track 1 and track 2 records withinside the technique reminiscence

Alina continues a blacklist of techniques, if there's no technique records withinside the blacklist it makes use of OpenProcess () to study and technique the contents withinside the reminiscence dump. Once the information is scraped Alina sends it to C&C servers the usage of an HTTP POST command this is hardcoded in binary.

1.5 What is Encrypting Malware?

A scrambled contamination is a laptop contamination that encodes its payload with the aim of creating spotting the contamination greater troublesome. In any case, due to the fact something encoded desires a decryptor or a key an antivirus can make use of the decryptor because the method for discovery.

1.6 How does encrypting malware works?

Malware writers make use of a collection of bodily and digital intends to unfold malware that contaminate devices and organizations. For instance, vindictive tasks may be conveyed to a framework with a USB power or can unfold over the net via power - through downloads, which certainly malevolent tasks to frameworks without the client's endorsement or records. Phishing assaults are some other normal types of malware conveyance wherein messages masked as right messages includes pernicious connections or connections that can deliver the malware executable to clueless customers. Modern malware attacks often spotlight the usage of an order and - manipulate employee that lets in threat entertainers to talk with the contaminated frameworks, exfiltrate sensitive records or even distantly manipulate the undermined device or employee.

Arising traces of malware contain new avoidance and obscurity strategies which can be supposed to trick customers in addition to protection administrators and adverse to malware gadgets too. An element of those avoidance strategies relies upon simple strategies, for example, making use of net intermediaries to shroud malignant site visitors or supply IP addresses. More delicate risks contain polymorphic malware, which could again and again extrude its simple code to circumvent region

instruments, adverse to sandbox strategies, which allow the malware to differentiate whilst it's miles being dissected and defer execution till after it leaves the sandbox, and report much less malware, which lives simply withinside the framework's RAM to strive now no longer to be found.

2. How to get prevented from malware?

Utilize a firewall to avoid all coming near institutions from the net to administrations that ought now no longer to be overtly accessible. As a count of course, strive now no longer to disclaim each unmarried coming near affiliation and simply allow administrations you expressly want to provide to the relaxation of the world.

Authorize a mystery key approach. Complex passwords make it difficult to interrupt mystery phrase facts on undermined LAPTOPs. This assists with forestalling or breaking factor damage whilst a LAPTOP is undermined.

Guarantee that tasks and customers of the LAPTOP make use of the maximum minimum diploma of blessings crucial to complete an errand. When incited for a root or UAC mystery phrase, assure that this system inquiring for organisation stage get admission to is a proper application.

Cripple AutoPlay to stop the programmed dispatching of executable facts on organisation and detachable drivers whilst now no longer wished. On the off hazard that compose get admission to is not wished, empower read - simply mode is the opportunity is accessible.

Mood killer document sharing if now no longer required. On the off hazard that document sharing is required, use ACLs and mystery phrase coverage to limitation get admission to. Incapacitate mysterious admittance to shared organizers. Award get admission to simply to patron debts with strong passwords to envelopes that have to be shared.

Mood killer and put off superfluous administrations. Naturally, many running frameworks introduce assistant administrations that aren't basic. These administrations are roads of assault. On the off hazard that they may be taken out, risks have much less roads of assault.

In the occasion that a chance abuses at the least one organisation benefits, impair, or block admittance to, the ones administrations till a repair is applied.

Continuously live up with the latest, specifically on LAPTOPs which have public administrations and are to be had via the firewall, for example, HTTP, FTP, mail, and DNS administrations.

Arrange your e - mail employee to hinder or put off e - mail that includes record connections which might be usually used to unfold risks, for example,. vbs,. bat,. exe,. pif and. scr facts.

Seclude bargained LAPTOPs hastily to preserve risks from spreading further. Play out a systematic research and re - set up the LAPTOPs utilising relied on media.

Train representatives now no longer to open connections besides if they may be waiting for them. Likewise, do not execute programming this is downloaded from Internet besides if it's been tested for bargained Website can reason ailment if sure software weaknesses aren't fixed.

On the off hazard that Bluetooth is not wished for mobile caller phones, it must be killed. On the off hazard which you require its utilization, assure that the machine's perceivability is about to "Covered up" so it cannot be tested with the aid of using different Bluetooth devices. In the occasion that machine mixing has to be utilized, assure that each one deviceis set to "Unapproved", requiring acclaim for each affiliation demand. Try now no longer to well - known programs which might be unsigned or despatched from difficult to understand sources.

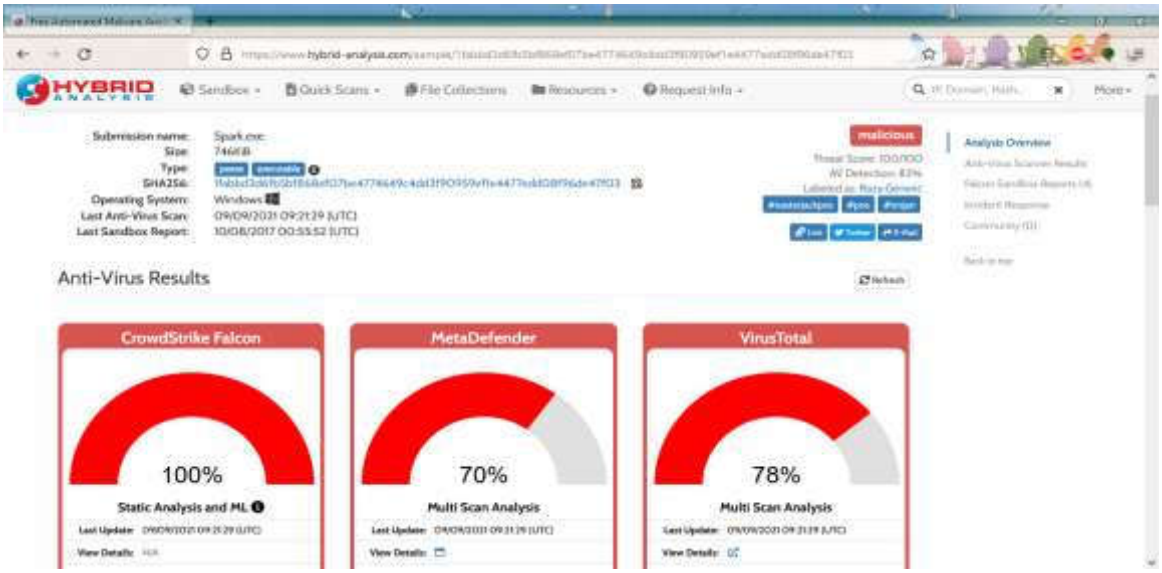
Author name (s) and affiliation (s)

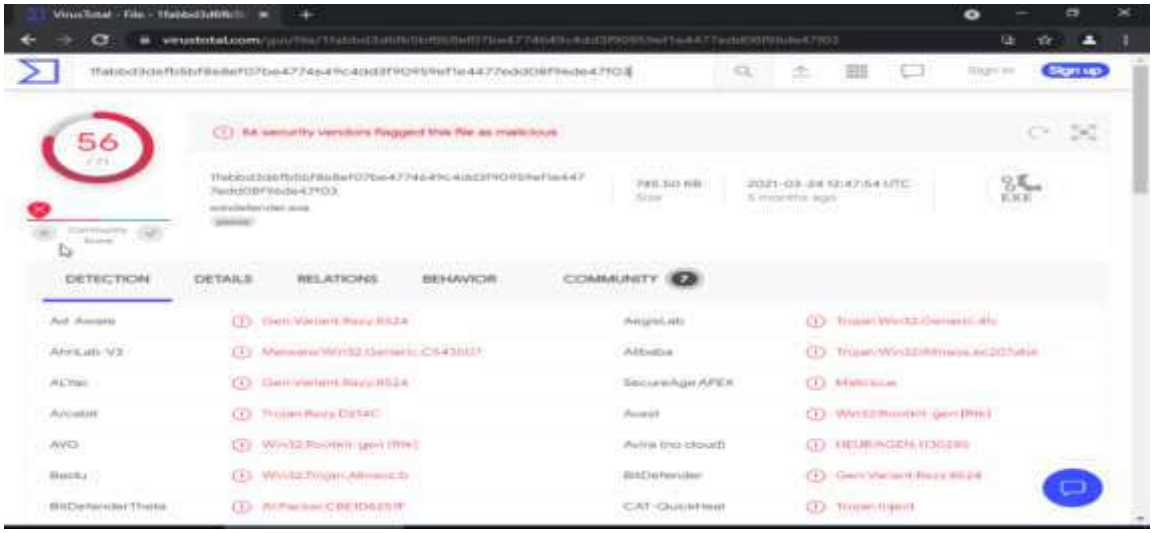
Dhruv Gajjar is a researcher in field of cyber security and cyber forensics. My google scholar link is: https: //scholar. google. com/citations?user=e - 2HlBYAAAAJ&hl=en.

Simulation

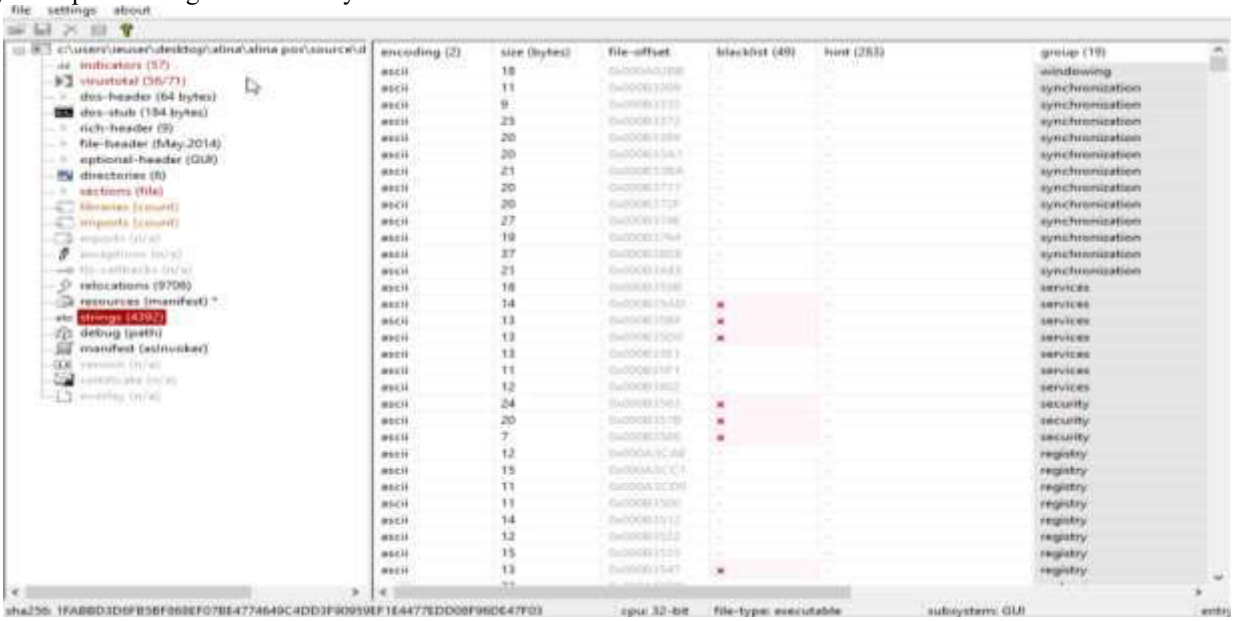
Software's: -
https: //github. com/ytisf/theZoo/tree/master/malware/Source/Original: - Alina Malware

Websites: -
https: //www.virustotal. com: - Virus Total

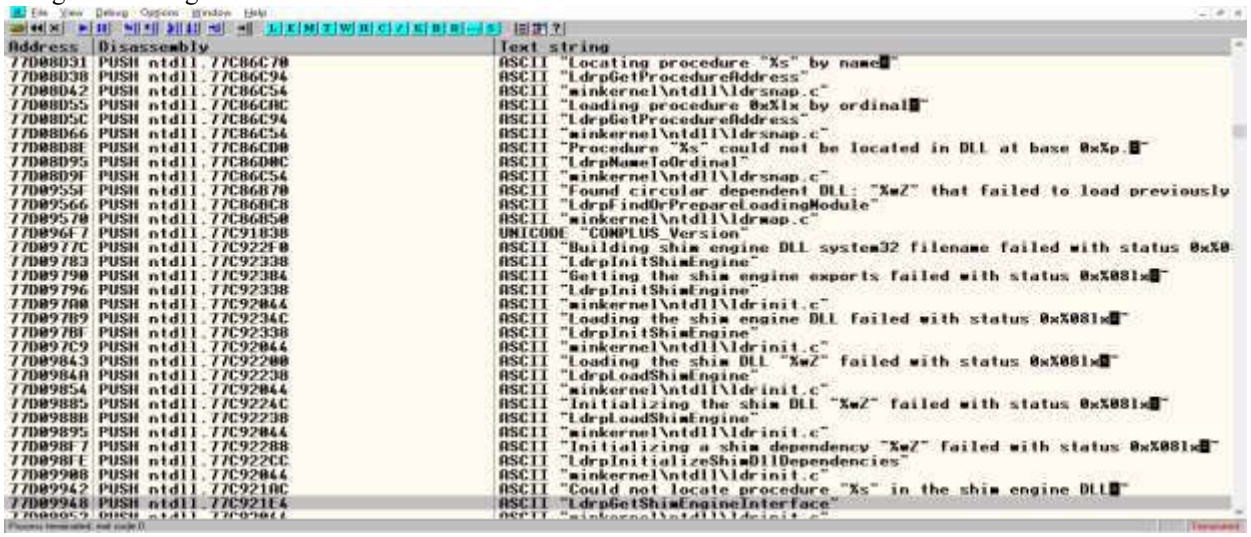




Analysis Report of Original File of Hybrid Sandbox

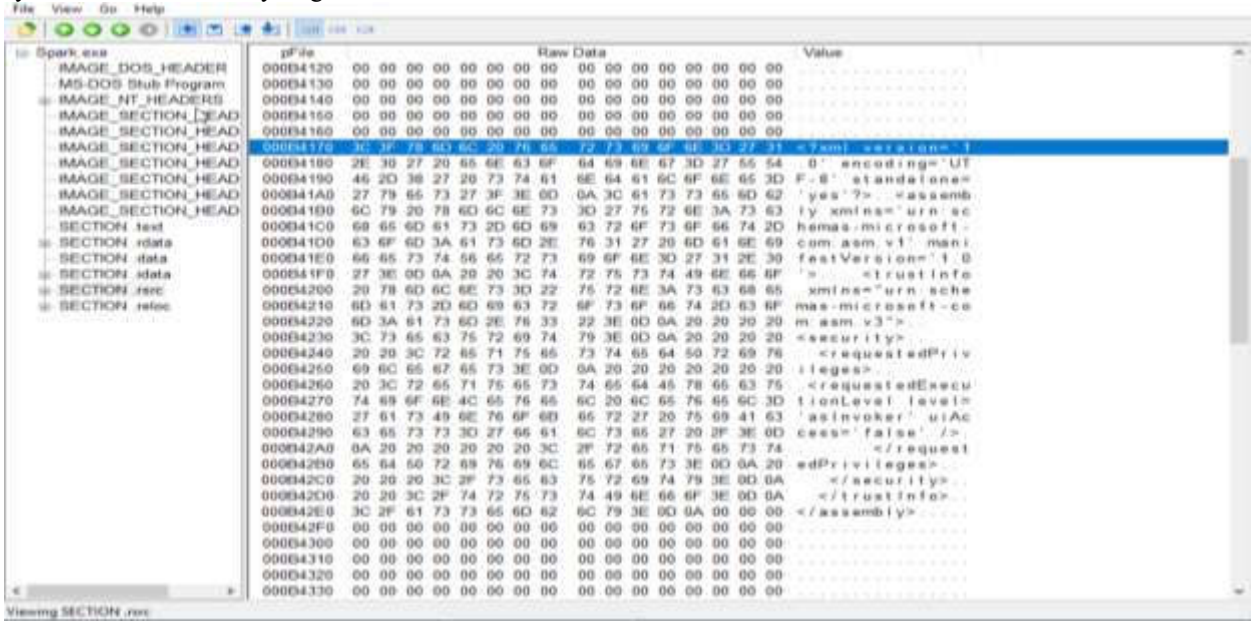


String used in original file to call functions

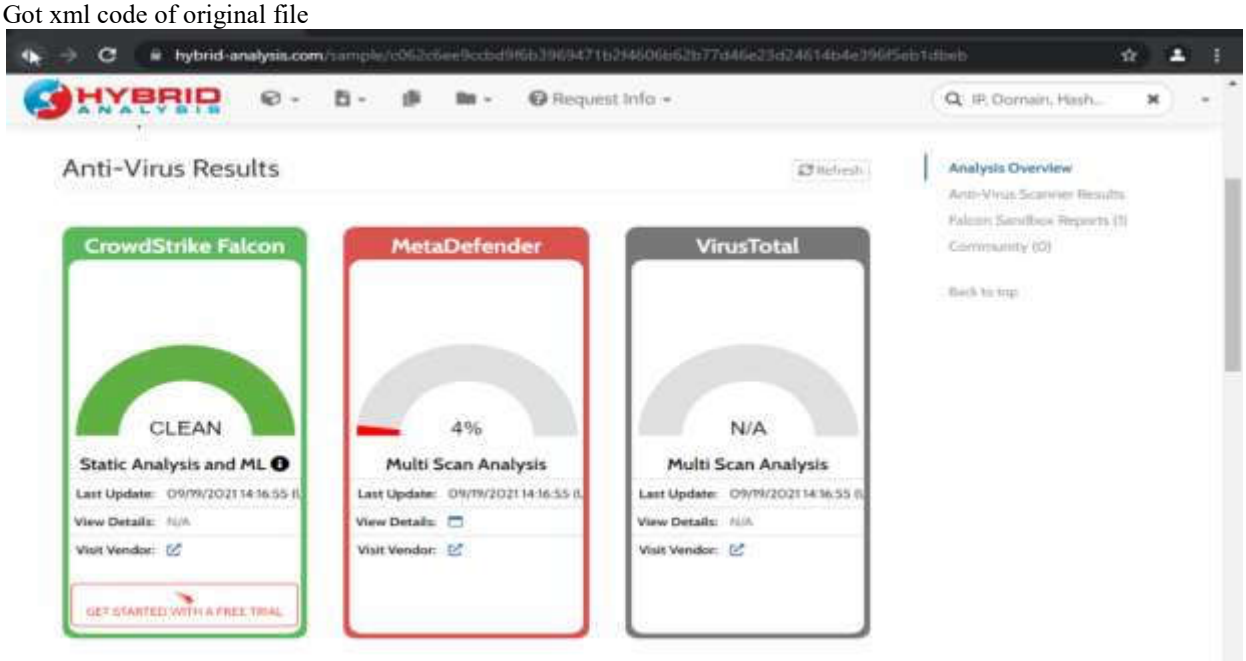


Address	Disassembly	Text string
77D88D31	PUSH ntdll.77C86C70	ASCII "Locating procedure "%s" by name"
77D88D38	PUSH ntdll.77C86C94	ASCII "LdrpGetProcedureAddress"
77D88D42	PUSH ntdll.77C86C54	ASCII "minkernel\ntdll\ldrsnap.c"
77D88D55	PUSH ntdll.77C86CBC	ASCII "Loading procedure 0x%lx by ordinal"
77D88D5C	PUSH ntdll.77C86C94	ASCII "LdrpGetProcedureAddress"
77D88D66	PUSH ntdll.77C86C54	ASCII "minkernel\ntdll\ldrsnap.c"
77D88D8E	PUSH ntdll.77C86CD8	ASCII "Procedure "%s" could not be located in DLL at base 0x%p."
77D88D95	PUSH ntdll.77C86D0C	ASCII "LdrpNameToOrdinal"
77D88D9F	PUSH ntdll.77C86C54	ASCII "minkernel\ntdll\ldrsnap.c"
77D8955F	PUSH ntdll.77C86B70	ASCII "Found circular dependent DLL: "%wZ" that failed to load previously
77D89566	PUSH ntdll.77C86BCB	ASCII "LdrpFindOrPrepareLoadingModule"
77D89570	PUSH ntdll.77C86B50	ASCII "minkernel\ntdll\ldrmap.c"
77D896F7	PUSH ntdll.77C91830	UNICODE "COMPLUS_Version"
77D8977C	PUSH ntdll.77C922F0	ASCII "Building shim engine DLL system32 filename failed with status 0x%0
77D89783	PUSH ntdll.77C92338	ASCII "LdrpInitShimEngine"
77D89790	PUSH ntdll.77C923B4	ASCII "Getting the shim engine exports failed with status 0x%08lx"
77D89796	PUSH ntdll.77C92338	ASCII "LdrpInitShimEngine"
77D897A8	PUSH ntdll.77C92044	ASCII "minkernel\ntdll\ldrinit.c"
77D897B9	PUSH ntdll.77C9234C	ASCII "Loading the shim engine DLL failed with status 0x%08lx"
77D897BF	PUSH ntdll.77C92338	ASCII "LdrpInitShimEngine"
77D897C9	PUSH ntdll.77C92044	ASCII "minkernel\ntdll\ldrinit.c"
77D89843	PUSH ntdll.77C92200	ASCII "Loading the shim DLL "%wZ" failed with status 0x%08lx"
77D8984A	PUSH ntdll.77C92238	ASCII "LdrpLoadShimEngine"
77D89854	PUSH ntdll.77C92044	ASCII "minkernel\ntdll\ldrinit.c"
77D89885	PUSH ntdll.77C9224C	ASCII "Initializing the shim DLL "%wZ" failed with status 0x%08lx"
77D8988B	PUSH ntdll.77C92238	ASCII "LdrpLoadShimEngine"
77D89895	PUSH ntdll.77C92044	ASCII "minkernel\ntdll\ldrinit.c"
77D898F7	PUSH ntdll.77C92288	ASCII "Initializing a shim dependency "%wZ" failed with status 0x%08lx"
77D898FE	PUSH ntdll.77C922CC	ASCII "LdrpInitializeShimDllDependencies"
77D89908	PUSH ntdll.77C92044	ASCII "minkernel\ntdll\ldrinit.c"
77D89942	PUSH ntdll.77C921BC	ASCII "Could not locate procedure "%s" in the shim engine DLL"
77D89948	PUSH ntdll.77C921E4	ASCII "LdrpGetShimEngineInterface"

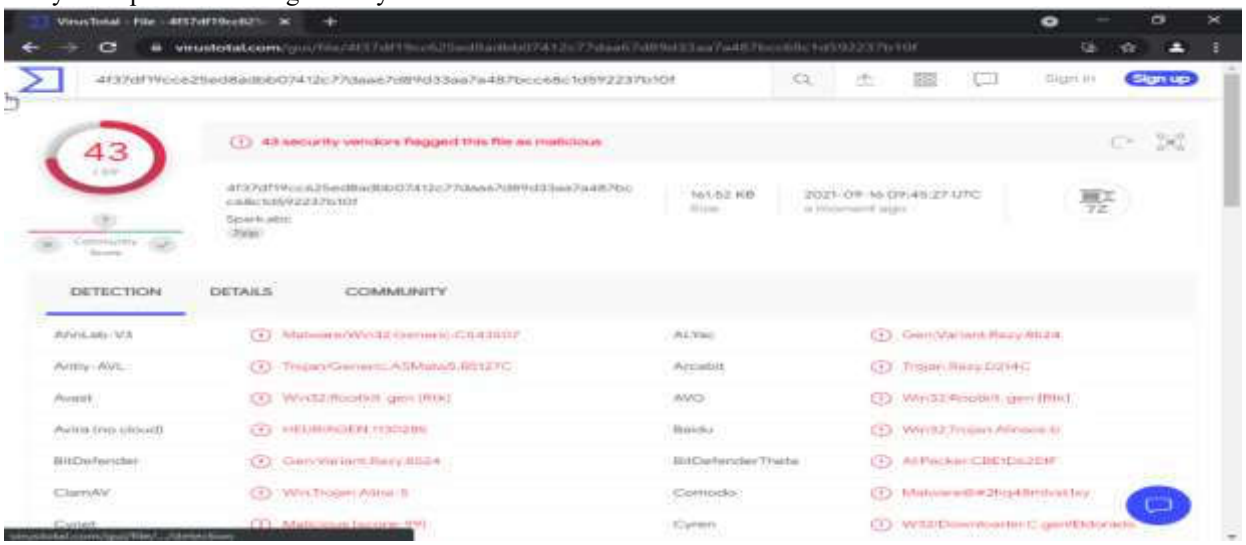
System calls functions by original file



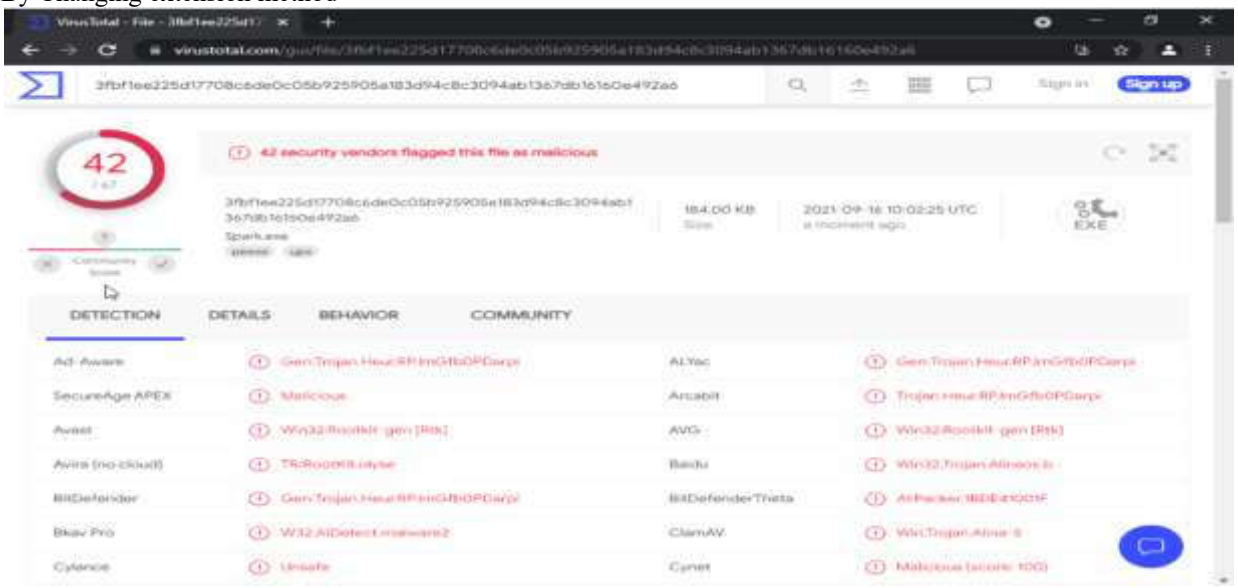
Got xml code of original file



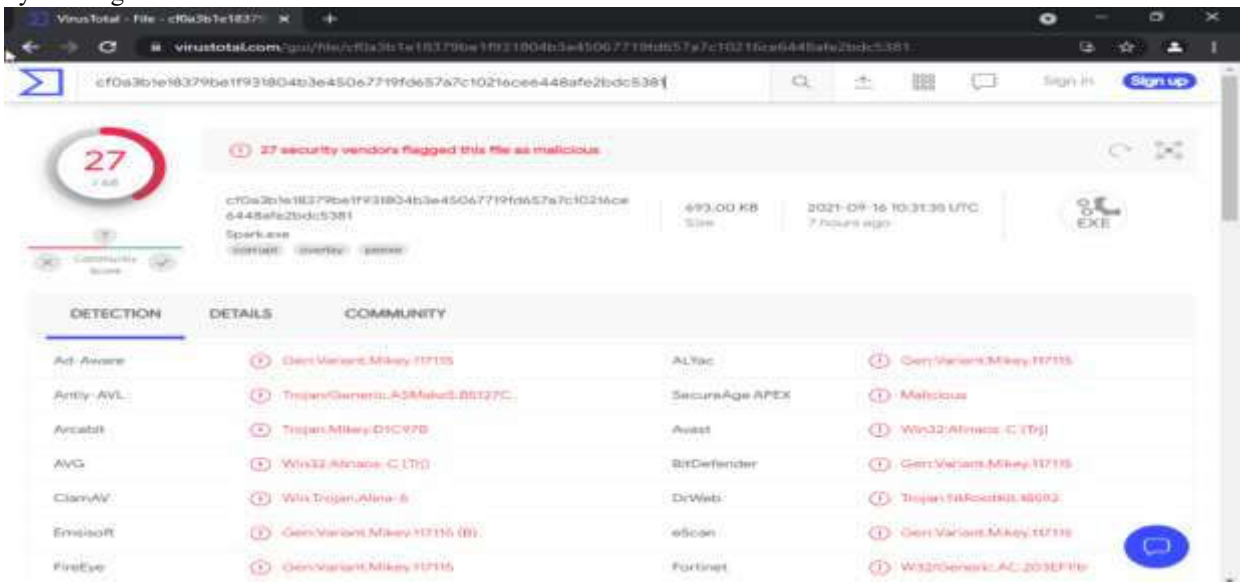
Analysis Report after changes of Hybrid Sandbox



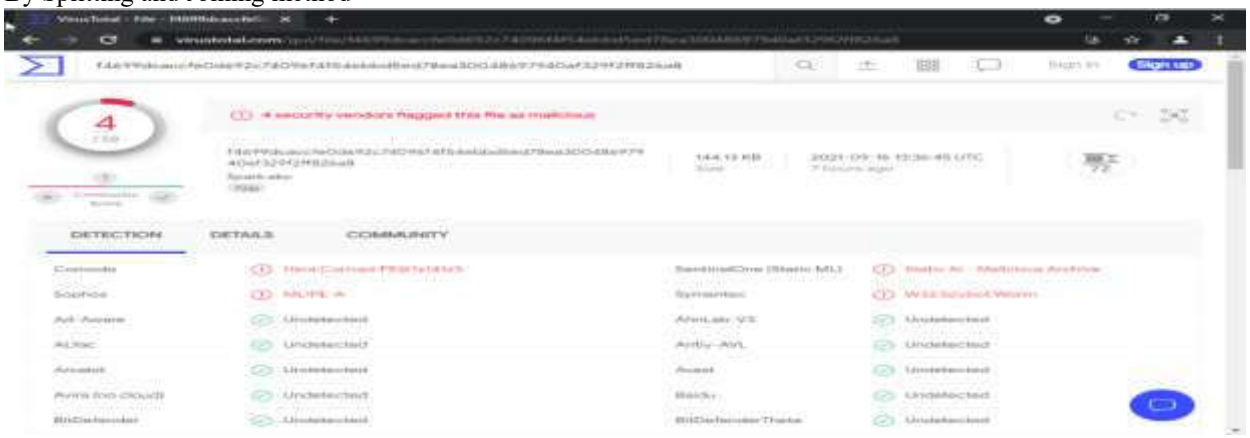
By Changing extension method



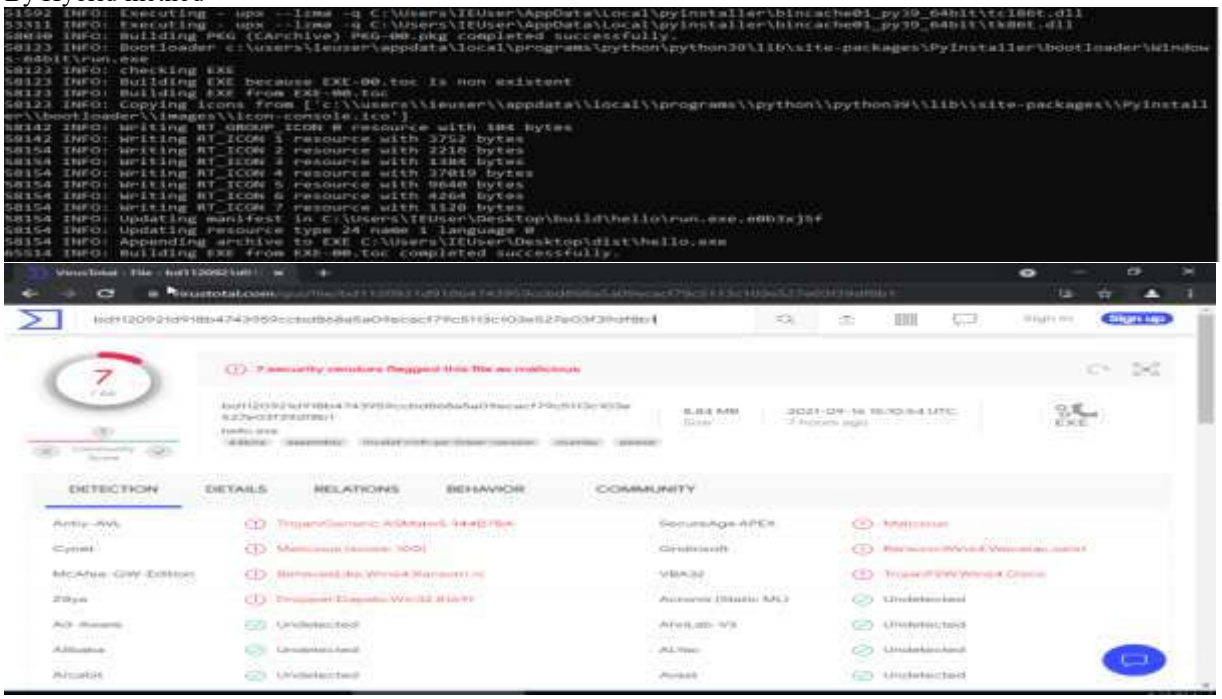
By Packing method



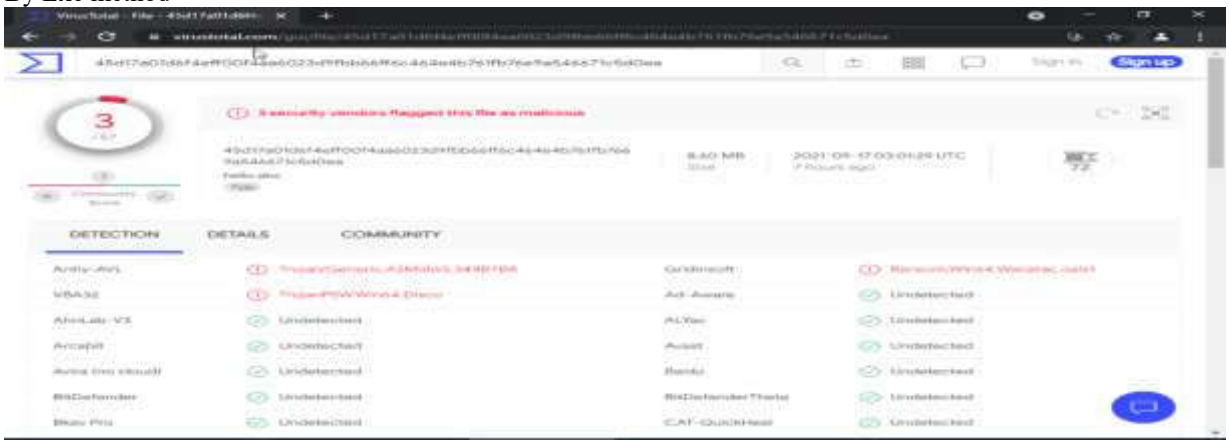
By Splitting and Joining method



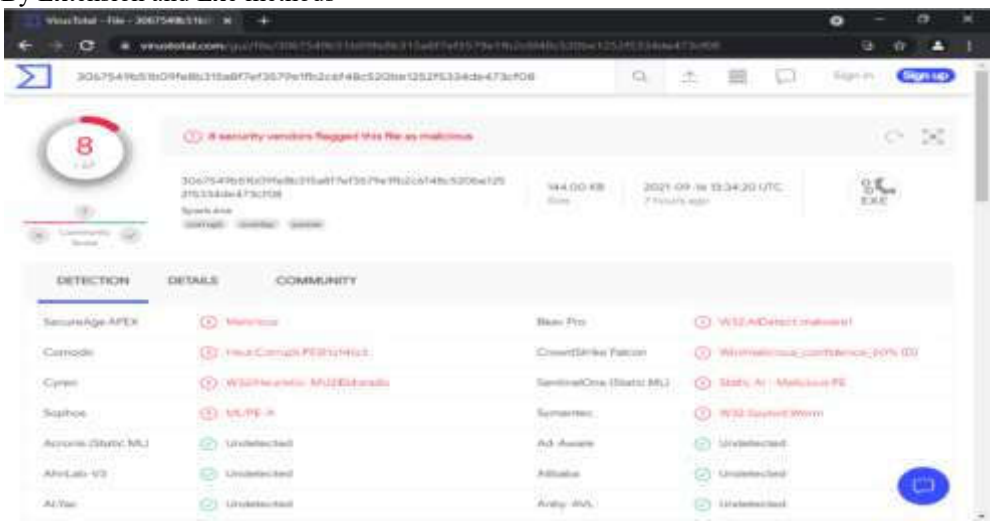
By Hybrid method



By Exe method



By Extension and Exe methods



Packing and splitting and Joining methods

All above methods uses different tools for different things. Tools which are related to malware analysis.

3. Conclusion

The experimental process concludes that in order to encrypt laptop malware and to get prevented from its impact.

First process starts with Malware analysis to know more about malware working.

Second process started with using of different methods (Changing extension, Packing, Spitting and Joining, Hybrid, Exeand Extension and Exe) which can hide identity of Alina malware.

Third stage to protect laptop from this kind of malware which works related to update and other services usage of malware are solved by possible solution shown.

References

[1] Encrypting Computer Virus: - https: //scholar.google. com/citations?user=e - 2HlBYAAAAJ&hl=en
[2] Linux Basics for Hackers: Getting Started with Networking, Scripting, and Security in Kali By: - OccupyThe Web
[3] Cyber Forensics By: - Dejey, Murugan
[4] Laptop Forensics and Cyber Crime: An Introduction, 2e By: - Britz
[5] https: //www.wikipedia. org: - Wikipedia
[6] https: //www.virustotal. com: - Virus Total
[7] Malware Analysing Tools