Software and Cybersecurity Lab

CS445 Lab6

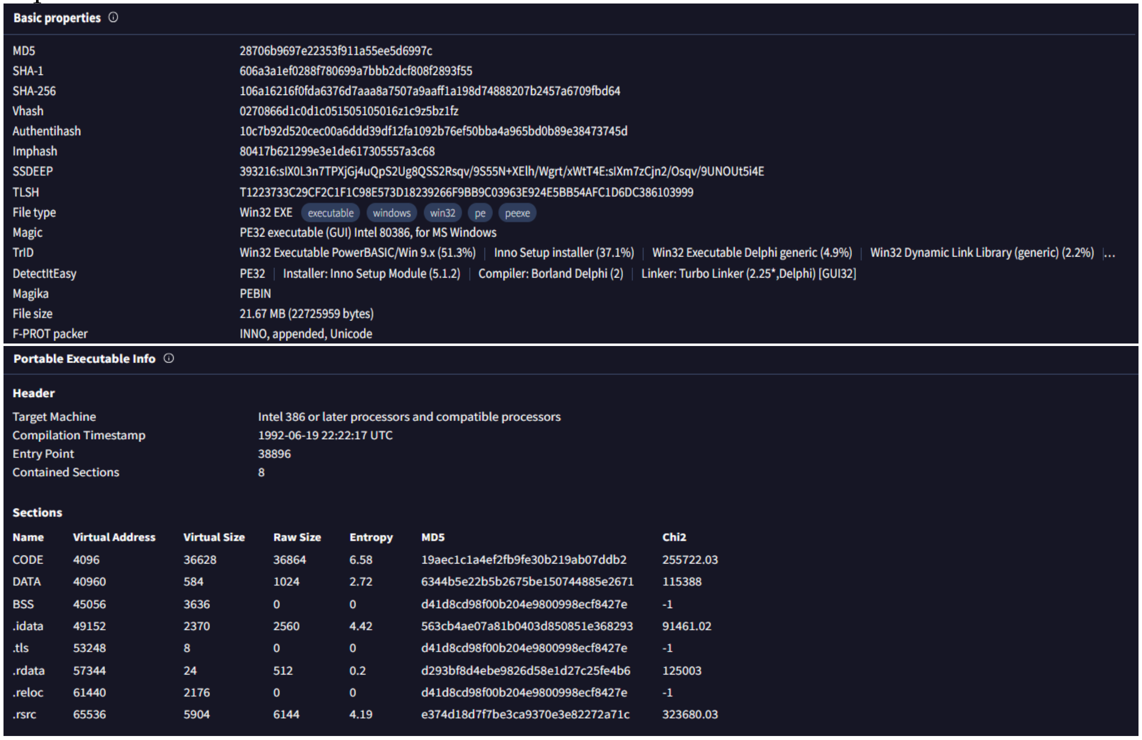
Name: Dipean Dasgupta **ID: 202151188**

Task: Analyzing and verification of security of a suspicious file using two popular tools PEStudio and VirusTotal.com and identifying potential malware and understanding the importance of multiple layers of verification.

Subtask1: Analyzing a File

File Chosen: staruml-5.O-with-cm.exe(Installer code file)

1. **Code anomalies**: Malware or tampering may be indicated by anomalies such as misaligned sections, erroneous headers, or corrupted PE structures. These problems could impair system security by causing crashes, erroneous file execution, or attacker exploitation.



Basic properties

MD5	28706b9697e22353f911a55ee5d6997c
SHA-1	606a3a1ef0288f780699a7bbb2dcf808f2893f55
SHA-256	106a16216f0fda6376d7aaa8a7507a9aaff1a198d74888207b2457a6709fbd64
Vhash	0270866d1c0d1c051505105016z1c9z5bz1fz
Authentihash	10c7b92d520cec00a6ddd39df12fa1092b76ef50bba4a965bd0b89e38473745d
Imphash	80417b621299e3e1de617305557a3c68
SSDEEP	393216:sIX0L3n7TPXjGj4uQpS2Ug8QSS2Rsqv/9S55N+XElh/Wgrt/xWtT4E:sIXm7zCjn2/Osqv/9UNOUt5i4E
TLSH	T1223733C29CF2C1F1C98E573D18239266F9BB9C03963E924E5BB54AFC1D6DC386103999
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable PowerBASIC/Win 9.x (51.3%) | Inno Setup installer (37.1%) | Win32 Executable Delphi generic (4.9%) | Win32 Dynamic Link Library (generic) (2.2%) |...
DetectItEasy	PE32 | Installer: Inno Setup Module (5.1.2) | Compiler: Borland Delphi (2) | Linker: Turbo Linker (2.25*,Delphi) [GUI32]
Magika	PEBIN
File size	21.67 MB (22725959 bytes)
F-PROT packer	INNO, appended, Unicode

Portable Executable Info

Header

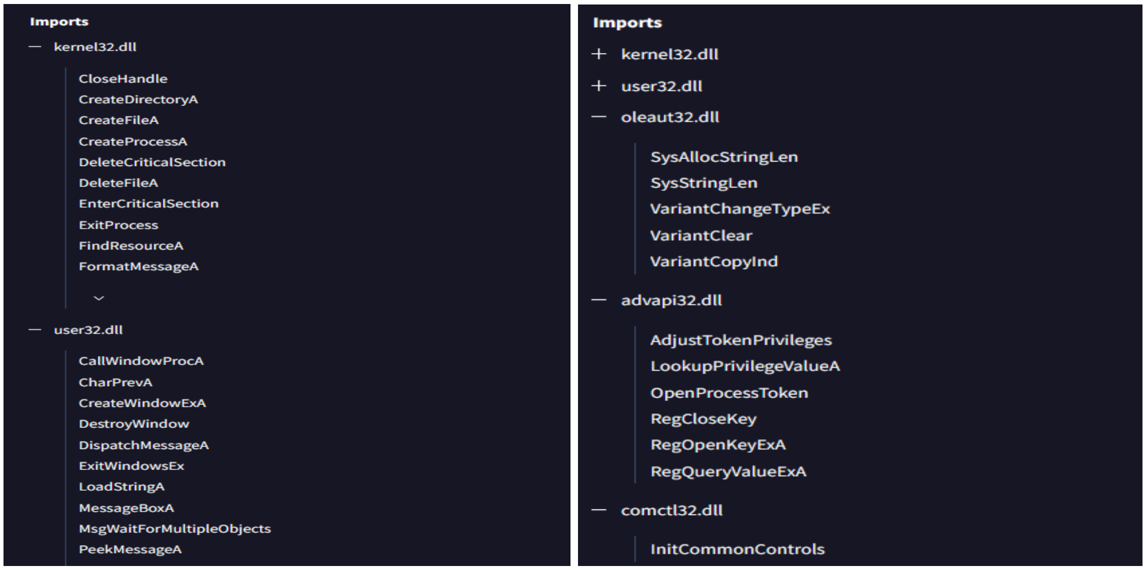
Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	1992-06-19 22:22:17 UTC
Entry Point	38896
Contained Sections	8

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
CODE	4096	36628	36864	6.58	19aec1c1a4ef2fb9fe30b219ab07ddb2	255722.03
DATA	40960	584	1024	2.72	6344b5e22b5b2675be150744885e2671	115388
BSS	45056	3636	0	0	d41d8cd98f00b204e9800998ecf8427e	-1
.idata	49152	2370	2560	4.42	563cb4ae07a81b0403d850851e368293	91461.02
.tls	53248	8	0	0	d41d8cd98f00b204e9800998ecf8427e	-1
.rdata	57344	24	512	0.2	d293bf8d4ebe9826d58e1d27c25fe4b6	125003
.reloc	61440	2176	0	0	d41d8cd98f00b204e9800998ecf8427e	-1
.rsrc	65536	5904	6144	4.19	e374d18d7f7be3ca9370e3e82272a71c	323680.03

No such Abnormalities found.

2. **Imported Functions:** Functions like CreateRemoteThread, WriteProcessMemory, and network APIs may be imported by malicious files. These features provide serious security vulnerabilities by enabling dangerous operations including privilege escalation, process injection, and unauthorized network access.

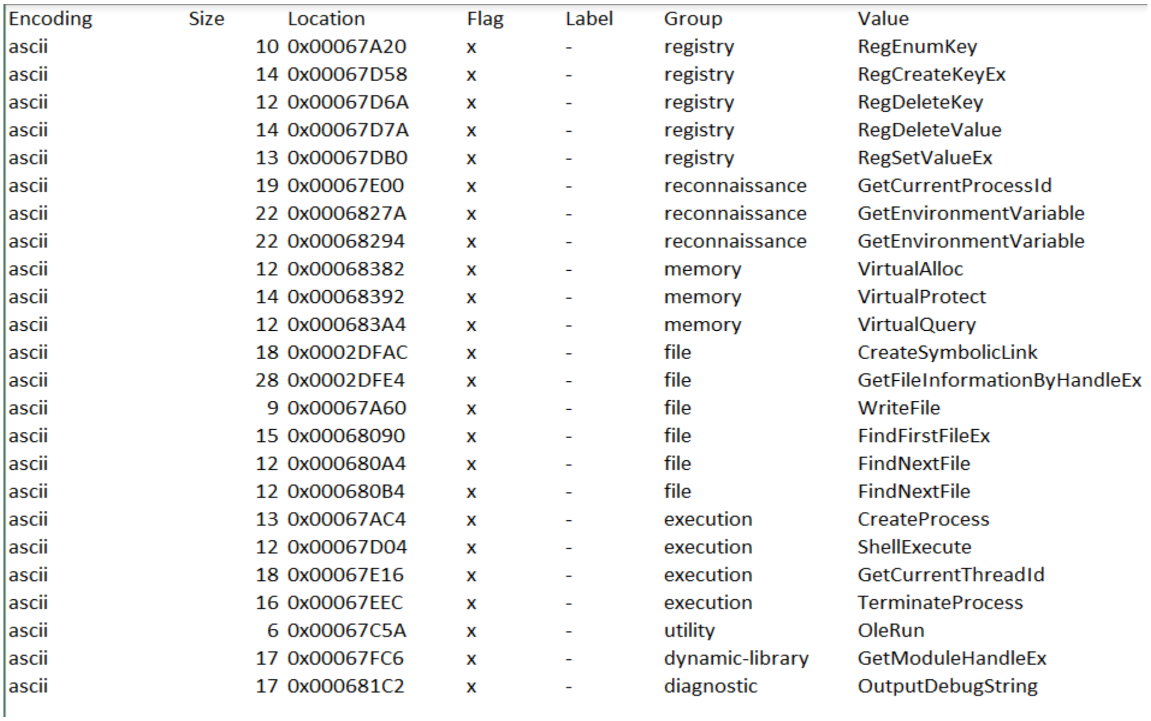


```
Imports
— kernel32.dll
    CloseHandle
    CreateDirectoryA
    CreateFileA
    CreateProcessA
    DeleteCriticalSection
    DeleteFileA
    EnterCriticalSection
    ExitProcess
    FindResourceA
    FormatMessageA
— user32.dll
    CallWindowProcA
    CharPrevA
    CreateWindowExA
    DestroyWindow
    DispatchMessageA
    ExitWindowsEx
    LoadStringA
    MessageBoxA
    MsgWaitForMultipleObjects
    PeekMessageA
```

```
Imports
+ kernel32.dll
+ user32.dll
— oleaut32.dll
    SysAllocStringLen
    SysStringLen
    VariantChangeTypeEx
    VariantClear
    VariantCopyInd
— advapi32.dll
    AdjustTokenPrivileges
    LookupPrivilegeValueA
    OpenProcessToken
    RegCloseKey
    RegOpenKeyExA
    RegQueryValueExA
— comctl32.dll
    InitCommonControls
```

These are the all imports libraries and functions used by the file.

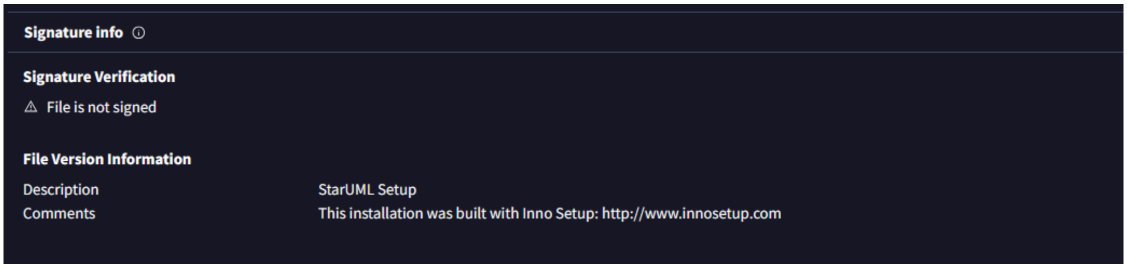
3. **Strings Analysis:** Hardcoded instructions for malicious activities can be found by examining suspicious strings, such as URLs, IP addresses, or obfuscated commands. Encrypted strings are frequently used in attacks to indicate attempts to avoid discovery or conceal sensitive actions.



Encoding	Size	Location	Flag	Label	Group	Value
ascii	10	0x00067A20	x	-	registry	RegEnumKey
ascii	14	0x00067D58	x	-	registry	RegCreateKeyEx
ascii	12	0x00067D6A	x	-	registry	RegDeleteKey
ascii	14	0x00067D7A	x	-	registry	RegDeleteValue
ascii	13	0x00067DB0	x	-	registry	RegSetValueEx
ascii	19	0x00067E00	x	-	reconnaissance	GetCurrentProcessId
ascii	22	0x0006827A	x	-	reconnaissance	GetEnvironmentVariable
ascii	22	0x00068294	x	-	reconnaissance	GetEnvironmentVariable
ascii	12	0x00068382	x	-	memory	VirtualAlloc
ascii	14	0x00068392	x	-	memory	VirtualProtect
ascii	12	0x000683A4	x	-	memory	VirtualQuery
ascii	18	0x0002DFAC	x	-	file	CreateSymbolicLink
ascii	28	0x0002DFE4	x	-	file	GetFileInformationByHandleEx
ascii	9	0x00067A60	x	-	file	WriteFile
ascii	15	0x00068090	x	-	file	FindFirstFileEx
ascii	12	0x000680A4	x	-	file	FindNextFile
ascii	12	0x000680B4	x	-	file	FindNextFile
ascii	13	0x00067AC4	x	-	execution	CreateProcess
ascii	12	0x00067D04	x	-	execution	ShellExecute
ascii	18	0x00067E16	x	-	execution	GetCurrentThreadId
ascii	16	0x00067EEC	x	-	execution	TerminateProcess
ascii	6	0x00067C5A	x	-	utility	OleRun
ascii	17	0x00067FC6	x	-	dynamic-library	GetModuleHandleEx
ascii	17	0x000681C2	x	-	diagnostic	OutputDebugString

These are the suspicious strings captured in Pestudio after analyzing the file.

4. **Certificate Validation:** The validity and reliability of a file are indicated by a valid digital signature. A certificate that is incorrect or unsigned could indicate manipulation, rendering the file unsafe and possibly dangerous.



Signature info ⓘ

Signature Verification

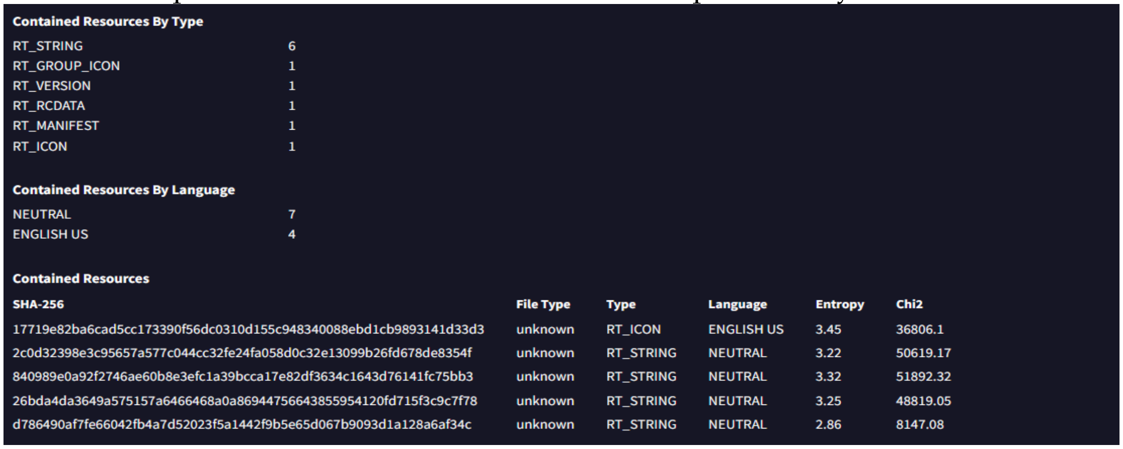
⚠ File is not signed

File Version Information

Description	StarUML Setup
Comments	This installation was built with Inno Setup: http://www.innosetup.com

The file is not signed. So, it must be not certified.

5. **Resource Sections:** Malicious payloads or configuration data may be contained in embedded resources such as executables, images, or config files. These could be used by attackers to spread further malware or take over compromised systems.



Contained Resources By Type

RT_STRING	6
RT_GROUP_ICON	1
RT_VERSION	1
RT_RCDATA	1
RT_MANIFEST	1
RT_ICON	1

Contained Resources By Language

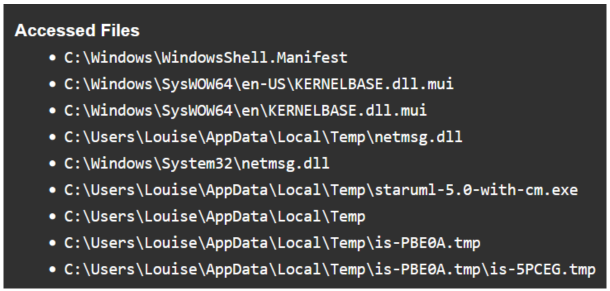
NEUTRAL	7
ENGLISH US	4

Contained Resources

SHA-256	File Type	Type	Language	Entropy	Chi2
17719e82ba6cad5cc173390f56dc0310d155c948340088ebd1cb9893141d33d3	unknown	RT_ICON	ENGLISH US	3.45	36806.1
2c0d32398e3c95657a577c044cc32fe24fa058d0c32e13099b26fd678de8354f	unknown	RT_STRING	NEUTRAL	3.22	50619.17
840989e0a92f2746ae60b8e3efc1a39bcca17e82df3634c1643d76141fc75bb3	unknown	RT_STRING	NEUTRAL	3.32	51892.32
26bda4da3649a575157a6466468a0a86944756643855954120fd715f3c9c7f78	unknown	RT_STRING	NEUTRAL	3.25	48819.05
d786490af7fe66042fb4a7d52023f5a1442f9b5e65d067b9093d1a128a6af34c	unknown	RT_STRING	NEUTRAL	2.86	8147.08

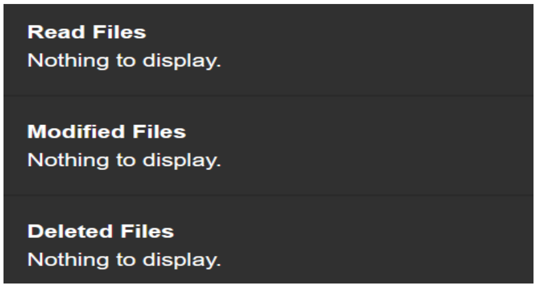
6. **Execution Flow:** In order to avoid discovery or acquire persistence, malicious files frequently alter control flows or APIs. System security can be jeopardized by unusual execution patterns, such as suspicious system calls or file change.

CAPE Sandbox report is shared below for execution flow:



Accessed Files

- C:\Windows\WindowsShell.Manifest
- C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
- C:\Windows\SysWOW64\en\KERNELBASE.dll.mui
- C:\Users\Louise\AppData\Local\Temp\netmsg.dll
- C:\Windows\System32\netmsg.dll
- C:\Users\Louise\AppData\Local\Temp\staruml-5.0-with-cm.exe
- C:\Users\Louise\AppData\Local\Temp
- C:\Users\Louise\AppData\Local\Temp\is-PBE0A.tmp
- C:\Users\Louise\AppData\Local\Temp\is-PBE0A.tmp\is-5PCEG.tmp



Read Files

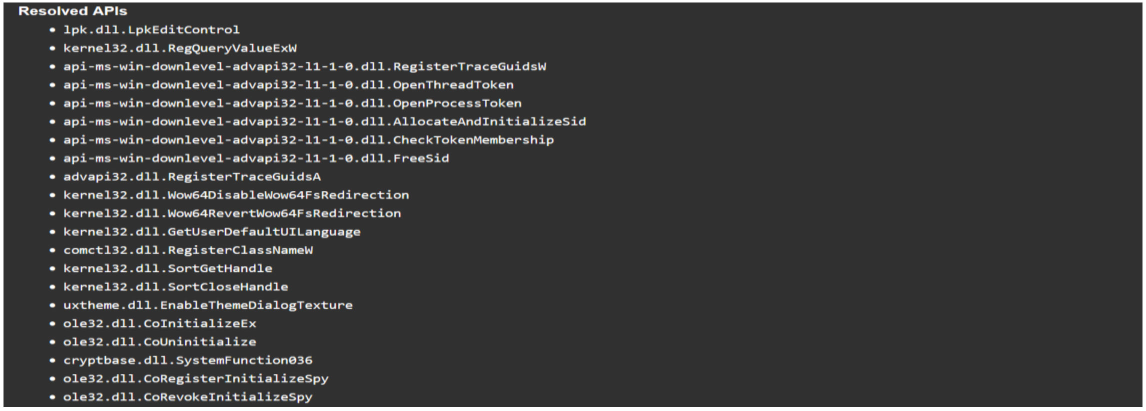
Nothing to display.

Modified Files

Nothing to display.

Deleted Files

Nothing to display.

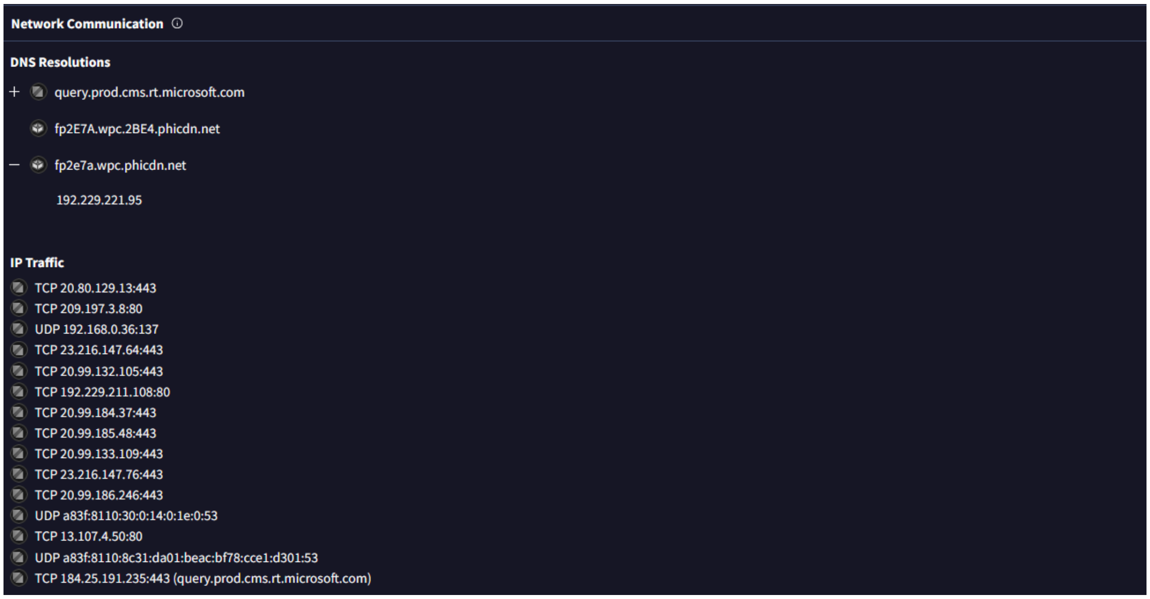


Resolved APIs

- lpk.dll.LpkEditControl
- kernel32.dll.RegQueryValueExW
- api-ms-win-downlevel-advapi32-l1-1-0.dll.RegisterTraceGuidsW
- api-ms-win-downlevel-advapi32-l1-1-0.dll.OpenThreadToken
- api-ms-win-downlevel-advapi32-l1-1-0.dll.OpenProcessToken
- api-ms-win-downlevel-advapi32-l1-1-0.dll.AllocateAndInitializeSid
- api-ms-win-downlevel-advapi32-l1-1-0.dll.CheckTokenMembership
- api-ms-win-downlevel-advapi32-l1-1-0.dll.FreeSid
- advapi32.dll.RegisterTraceGuidsA
- kernel32.dll.Wow64DisableWow64FsRedirection
- kernel32.dll.Wow64RevertWow64FsRedirection
- kernel32.dll.GetUserDefaultUILanguage
- comctl32.dll.RegisterClassNameW
- kernel32.dll.SortGetHandle
- kernel32.dll.SortCloseHandle
- uxtheme.dll.EnableThemeDialogTexture
- ole32.dll.CoInitializeEx
- ole32.dll.CoUninitialize
- cryptbase.dll.SystemFunction036
- ole32.dll.CoRegisterInitializeSpy
- ole32.dll.CoRevokeInitializeSpy

No sort of malicious or suspicious activity detected.

7. **Network Activity:** Malicious files have the ability to create unapproved network connections in order to exfiltrate data or download other malware.
   Due to the possibility of data breaches or remote control, this presents serious concerns to network security.



Network Communication

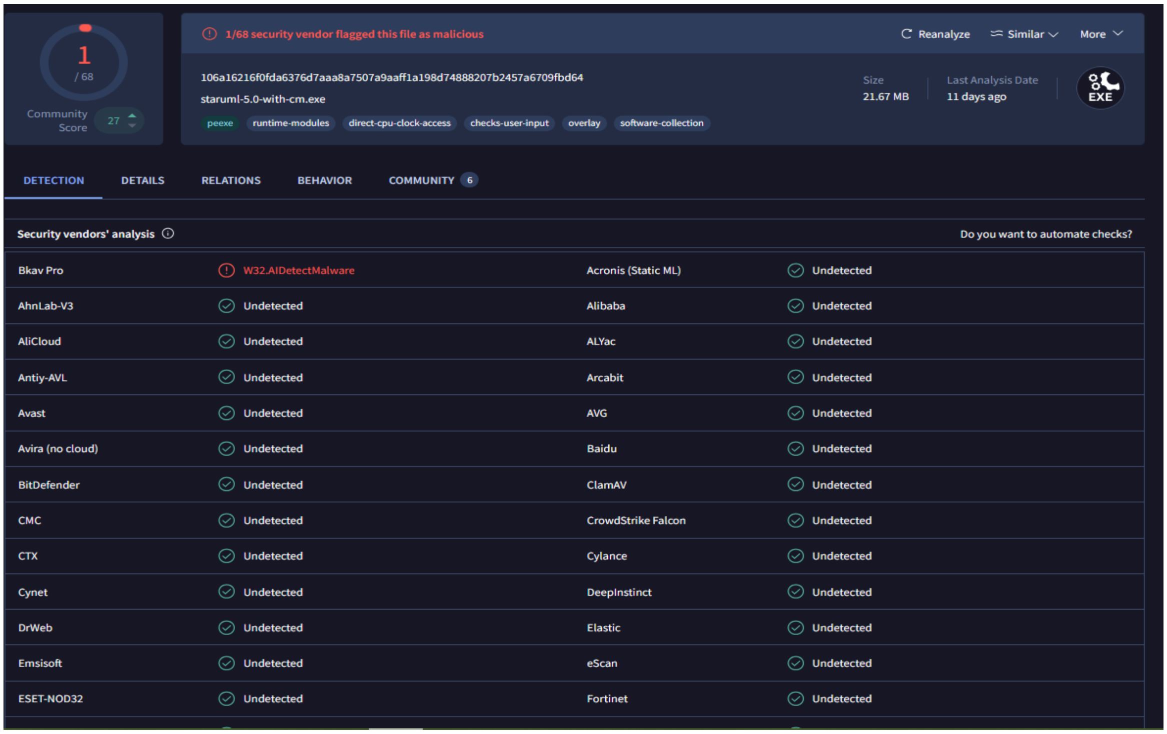
DNS Resolutions

```
+ query.prod.cms.rt.microsoft.com
  fp2E7A.wpc.2BE4.phicdn.net
- fp2e7a.wpc.phicdn.net
    192.229.221.95
```

IP Traffic

```
TCP 20.80.129.13:443
TCP 209.197.3.8:80
UDP 192.168.0.36:137
TCP 23.216.147.64:443
TCP 20.99.132.105:443
TCP 192.229.211.108:80
TCP 20.99.184.37:443
TCP 20.99.185.48:443
TCP 20.99.133.109:443
TCP 23.216.147.76:443
TCP 20.99.186.246:443
UDP a83f:8110:30:0:14:0:1e:0:53
TCP 13.107.4.50:80
UDP a83f:8110:8c31:da01:beac:bf78:cce1:d301:53
TCP 184.25.191.235:443 (query.prod.cms.rt.microsoft.com)
```

8. **File Origin and Trustworthiness:** Malware is more likely to be present in files that come from unknown or unreliable sources. When assessing whether a file is secure or a threat to system security, the credibility of the source is crucial.



1 / 68

Community Score 27

1/68 security vendor flagged this file as malicious

106a16216f0fda6376d7aaa8a7507a9aaff1a198d74888207b2457a6709fbd64

staruml-5.0-with-cm.exe

peexe · runtime-modules · direct-cpu-clock-access · checks-user-input · overlay · software-collection

Size 21.67 MB

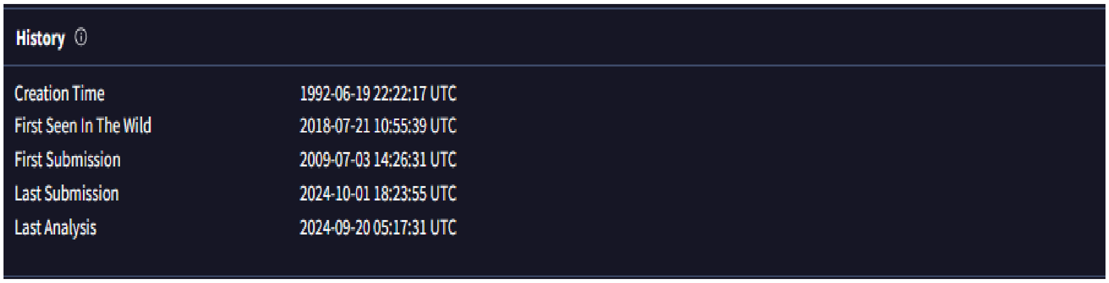
Last Analysis Date 11 days ago

Security vendors' analysis

Do you want to automate checks?

Bkav Pro	W32.AIDetectMalware	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
AliCloud	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	ClamAV	Undetected
CMC	Undetected	CrowdStrike Falcon	Undetected
CTX	Undetected	Cylance	Undetected
Cynet	Undetected	DeepInstinct	Undetected
DrWeb	Undetected	Elastic	Undetected
Emsisoft	Undetected	eScan	Undetected
ESET-NOD32	Undetected	Fortinet	Undetected

One out of 68 security vendor flagged it as malicious.

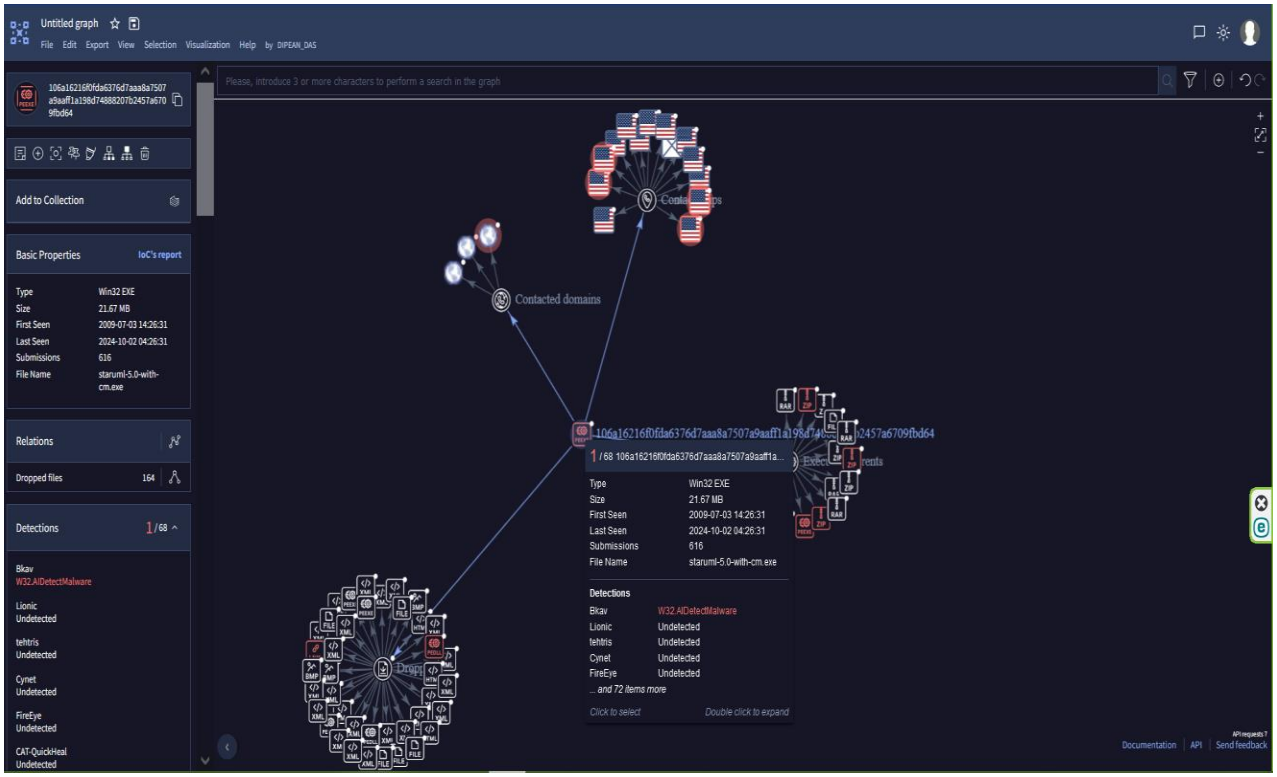


History

Creation Time	1992-06-19 22:22:17 UTC
First Seen In The Wild	2018-07-21 10:55:39 UTC
First Submission	2009-07-03 14:26:31 UTC
Last Submission	2024-10-01 18:23:55 UTC
Last Analysis	2024-09-20 05:17:31 UTC

The file was first created a long ago. So, it not circulating in recent times. Since only one has flagged it, there are not any major issue in the file.

Threat Graph



106a16216f0fda6376d7aaa8a7507a9aaff1a198d74888207b2457a6709fbd64

Basic Properties IoC's report

Type	Win32 EXE
Size	21.67 MB
First Seen	2009-07-03 14:26:31
Last Seen	2024-10-02 04:26:31
Submissions	616
File Name	staruml-5.0-with-cm.exe

Relations

Dropped files 164

Detections 1 / 68

Bkav	W32.AIDetectMalware
Lionic	Undetected
tehtris	Undetected
Cynet	Undetected
FireEye	Undetected
CAT-QuickHeal	Undetected

1 / 68 106a16216f0fda6376d7aaa8a7507a9aaff1a...

Type	Win32 EXE
Size	21.67 MB
First Seen	2009-07-03 14:26:31
Last Seen	2024-10-02 04:26:31
Submissions	616
File Name	staruml-5.0-with-cm.exe

Detections

Bkav	W32.AIDetectMalware
Lionic	Undetected
tehtris	Undetected
Cynet	Undetected
FireEye	Undetected

... and 72 items more

Click to select   Double click to expand

This is the threat graph of the file. Details of the malicious file detected is also displayed.

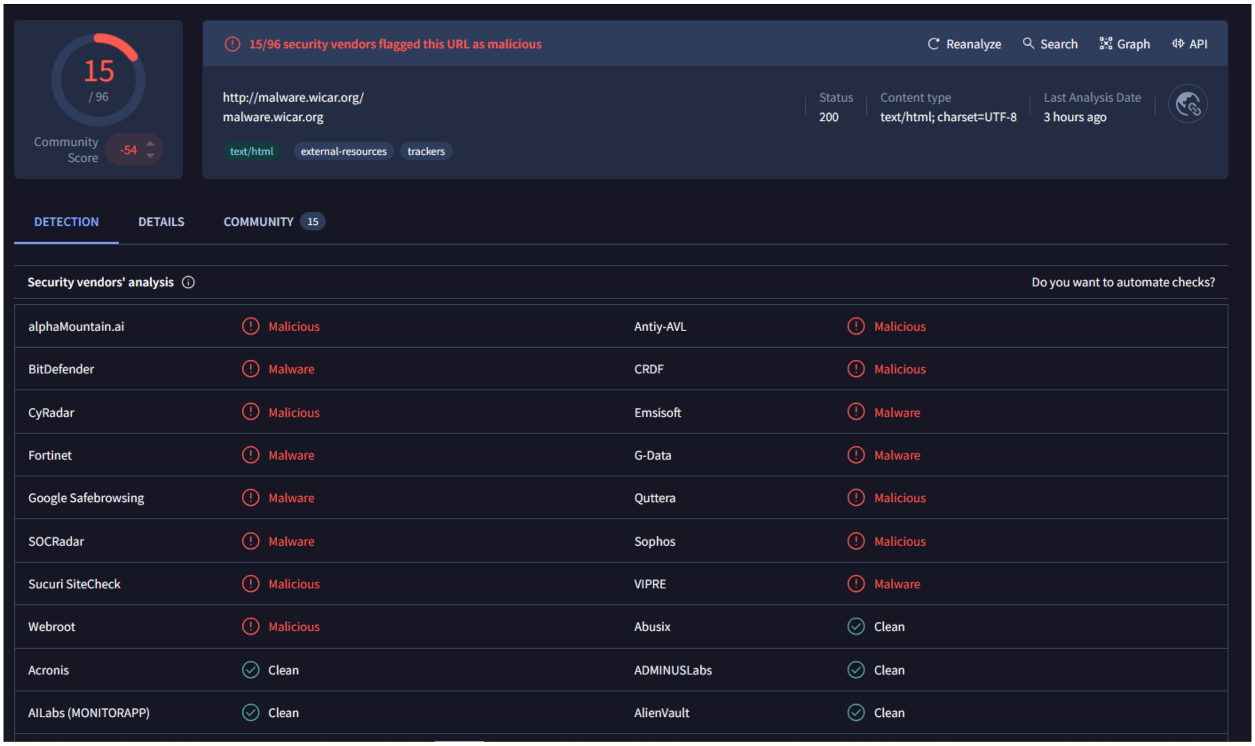
Link to the threat Graph:

https://www.virustotal.com/graph/embed/g5da9a136c62a418fa02d0d21039808cbcf07cb95da8c42bfada0b4299486d84a?theme=dark

Subtask 2: Analyzing an URL

In this section a popular malicious site for testing is chosen. Let's see How many security vendors flag the URL.

Chosen URL: http://malware.wicar.org



15/96 security vendors flagged this URL as malicious

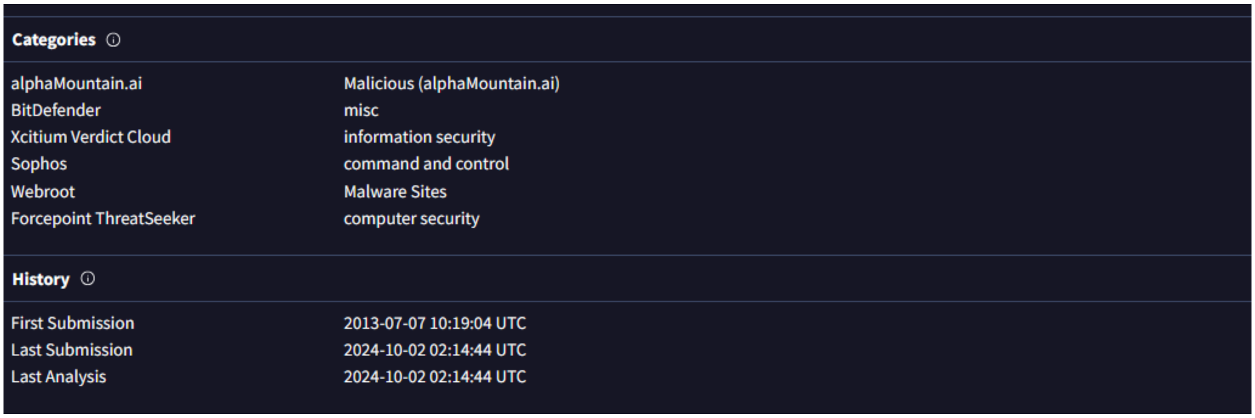
http://malware.wicar.org/
malware.wicar.org

Status	Content type	Last Analysis Date
200	text/html; charset=UTF-8	3 hours ago

Security vendors' analysis

alphaMountain.ai	Malicious	Antiy-AVL	Malicious
BitDefender	Malware	CRDF	Malicious
CyRadar	Malicious	Emsisoft	Malware
Fortinet	Malware	G-Data	Malware
Google Safebrowsing	Malware	Quttera	Malicious
SOCRadar	Malware	Sophos	Malicious
Sucuri SiteCheck	Malicious	VIPRE	Malware
Webroot	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean

As it can be seen, 15 out of 96 security vendors have detected malware in the website. So its definitely unsafe and malicious site.



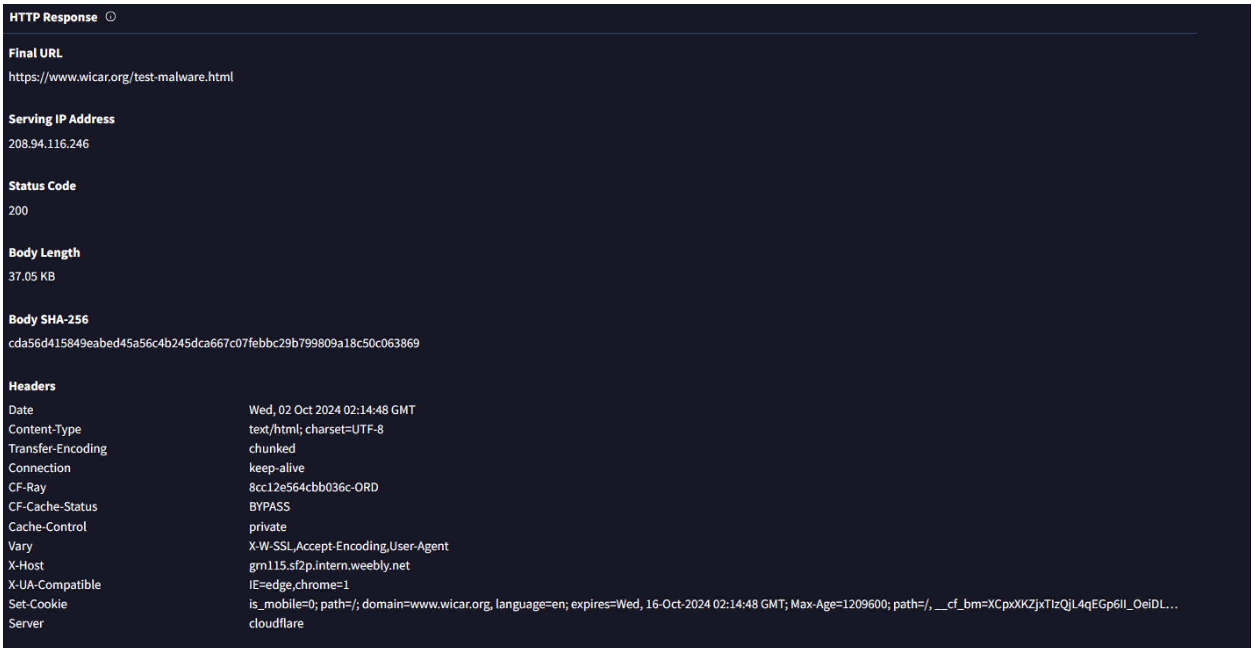
Categories

alphaMountain.ai	Malicious (alphaMountain.ai)
BitDefender	misc
Xcitium Verdict Cloud	information security
Sophos	command and control
Webroot	Malware Sites
Forcepoint ThreatSeeker	computer security

History

First Submission	2013-07-07 10:19:04 UTC
Last Submission	2024-10-02 02:14:44 UTC
Last Analysis	2024-10-02 02:14:44 UTC

History of the site and categories are displayed above.



HTTP Response

Final URL

https://www.wicar.org/test-malware.html

Serving IP Address

208.94.116.246

Status Code

200

Body Length

37.05 KB

Body SHA-256

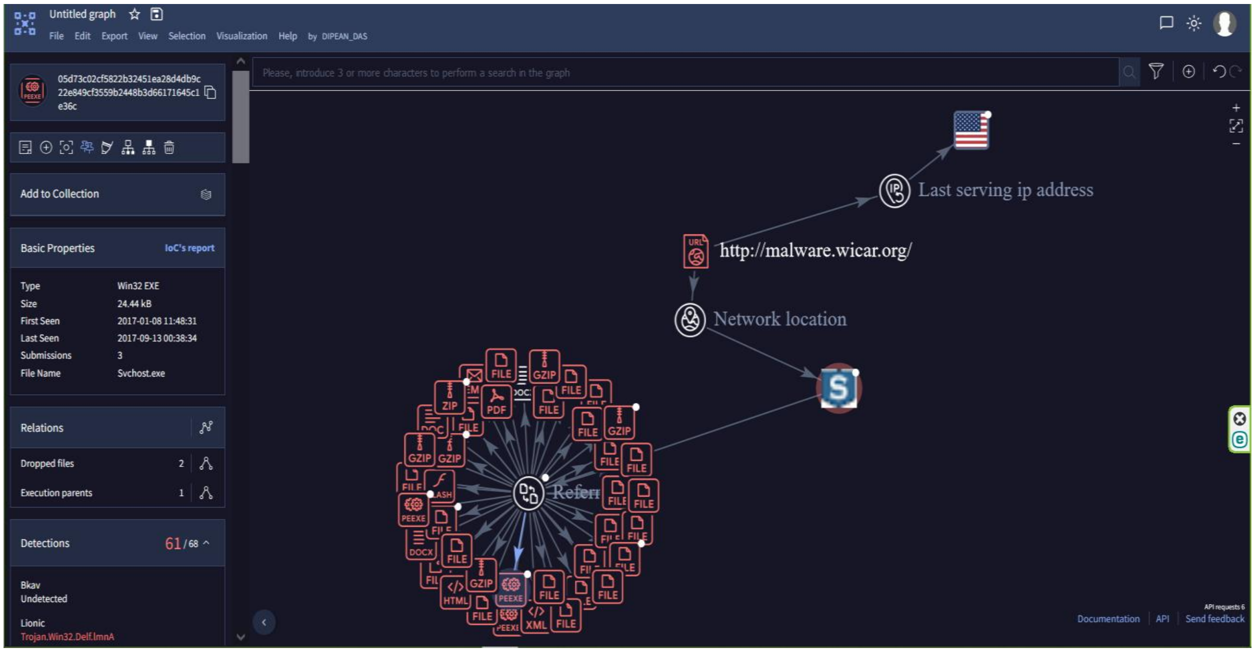
cda56d415849eabed45a56c4b245dca667c07febbc29b799809a18c50c063869

Headers

Date	Wed, 02 Oct 2024 02:14:48 GMT
Content-Type	text/html; charset=UTF-8
Transfer-Encoding	chunked
Connection	keep-alive
CF-Ray	8cc12e564cbb036c-ORD
CF-Cache-Status	BYPASS
Cache-Control	private
Vary	X-W-SSL,Accept-Encoding,User-Agent
X-Host	grn115.sf2p.intern.weebly.net
X-UA-Compatible	IE=edge,chrome=1
Set-Cookie	is_mobile=0; path=/; domain=www.wicar.org, language=en; expires=Wed, 16-Oct-2024 02:14:48 GMT; Max-Age=1209600; path=/, __cf_bm=XCpxXKZjxTIzQjL4qEGp6Il_OeiDL…
Server	cloudflare

Here the HTTP response and hash code and other details are displayed.

Threat Graph



05d73c02cf5822b32451ea28d4db9c22e849cf3559b2448b3d66171645c1e36c

Add to Collection

Basic Properties IoC's report

Type	Win32 EXE
Size	24.44 kB
First Seen	2017-01-08 11:48:31
Last Seen	2017-09-13 00:38:34
Submissions	3
File Name	Svchost.exe

Relations

Dropped files	2
Execution parents	1

Detections 61 / 68

Bkav
Undetected

Lionic
Trojan.Win32.Delf.lmnA

Threat graph of the website is shared. All the malicious file is visible in the graph. One of it has trojan horse malware which is very dangerous.

Link to the threat Graph:

https://www.virustotal.com/graph/embed/gc14840bc8c484e7789be55136dd6914bf9834950fbd643779be274be055ad1af?theme=dark