

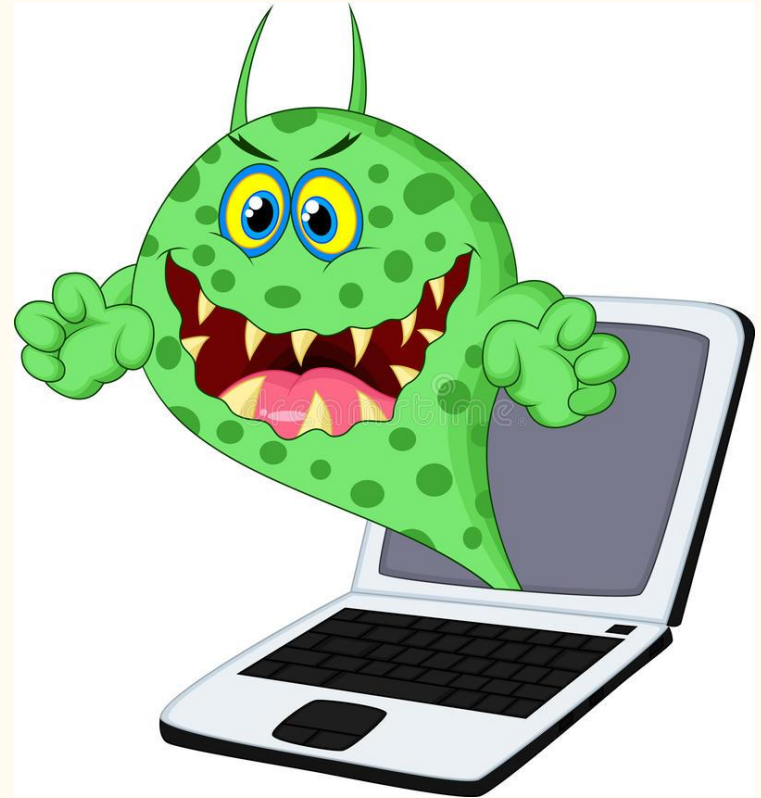
Antivirus - System Protection Suite

—

Hritik(1581192)
Kshitij(1851068)
Divya(1851185)
Sayantan(1851033)

What is a malware?

- Derived from **Malicious-Software**
- A set of instructions to cause undesirable effects on a system
- Can self replicate^[1]
- Could be of various types based on its actions



How malware affects systems

There are various possible ways of infection, some of them are ...

- File infections by attaching itself to executable files^[1]
- Boot sector infections, by overwriting the boot sector^[1]
- Macro viruses, executed with macro commands like word processors and excel

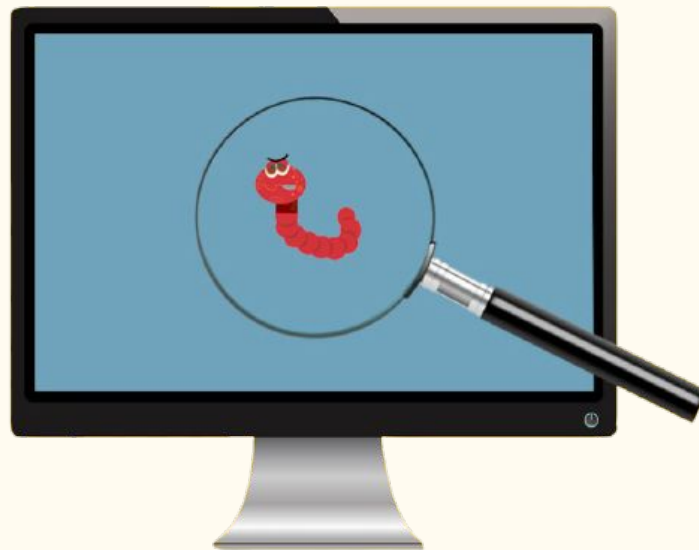
Antivirus to the rescue

- Scans files for malwares
- Can perform different types of scans^[2]
 - On demand
 - Realtime
 - Smartscan
- Monitors network activities for possible attacks



Types of detection^[2]

- Virus signatures
- Heuristic-based detection
- Behavior-based detection
- Sandbox Detection(Ex - Sigma)



Signature analysis^[3]_[4]

- Usually the first and most common approach
- Antivirus maintains a database of signatures of known viruses
- Signatures could be simply static hash or more complex analysis of the virus
- Files are scanned for matching signatures
- Requires updates constantly
- Not very effective against new viruses

Heuristic Based^[5]

- Can detect new viruses or polymorphic viruses
- Decompiles and examines the source code for matches with existing virus code
- Marks positive if matches above a certain threshold
- Can sometimes generate false positives

Behaviour Based^[6]

- Malware tries to perform suspicious activity in background like ...
 - Installing rootkit to lock out the computer
 - Settings of other programs are changed
 - Registering for starting up automatically
- Observes the behaviour of a running process
- If finds suspicious activities, then flags it as virus
- Can detect completely new viruses, with different signatures from anything in databases

Sandbox analysis^[7]

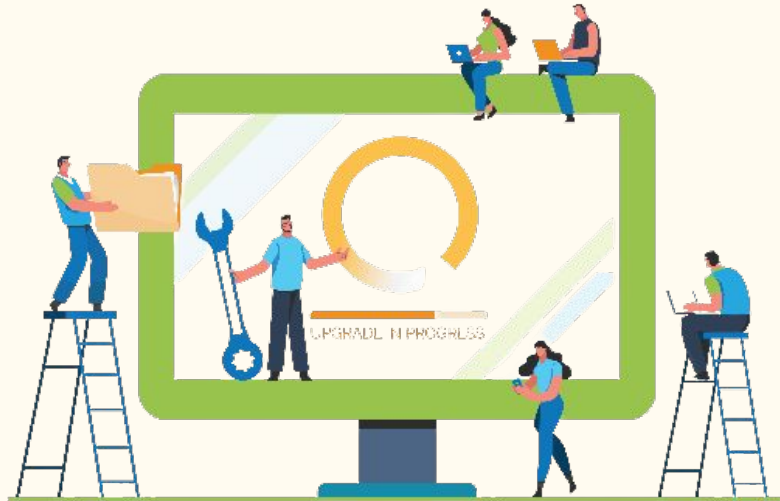
- Programs are executed in virtual environment first
- They are monitored for suspicious behaviour
- If found safe, it is executed in real environment
- Quite heavy process, so generally not used in personal systems

Beacon-based Network Activity Analysis^[8]

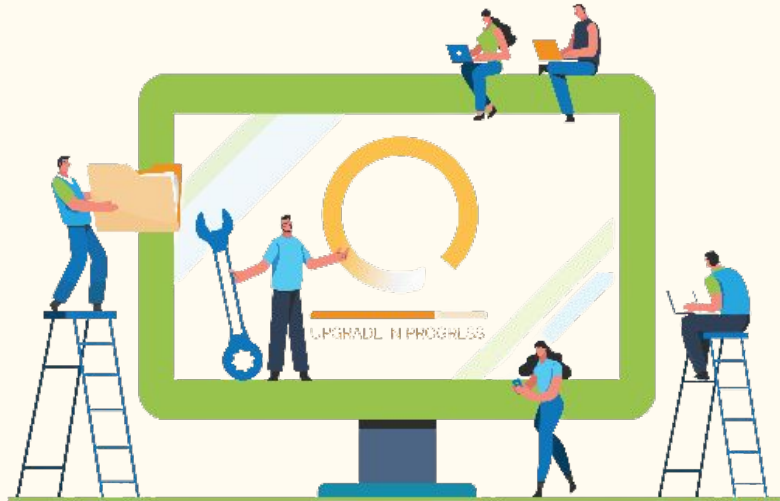
- Malwares usually needs to communicate with the attacker
- Command & Control(C&C) servers allows communication with attacker and victim machine
- A compromised machine would periodically check with the C&C servers
- This activity can be revealed over time
- NTP servers could be a common false positives

Our Progress

- Scanning files for viruses on local system
- Live website security analysis through browser extension



Demo - Scanning files for viruses on local system



Windows Defender vs Our Antivirus

- Windows defender failed to detect virus in a sample file

Scan options

Run a quick, full, custom, or Microsoft Defender Offline scan.

No current threats.

Last scan: 19-01-2022 12:17 (custom scan)

0 threats found.

Scan lasted 1 seconds

19 files scanned.

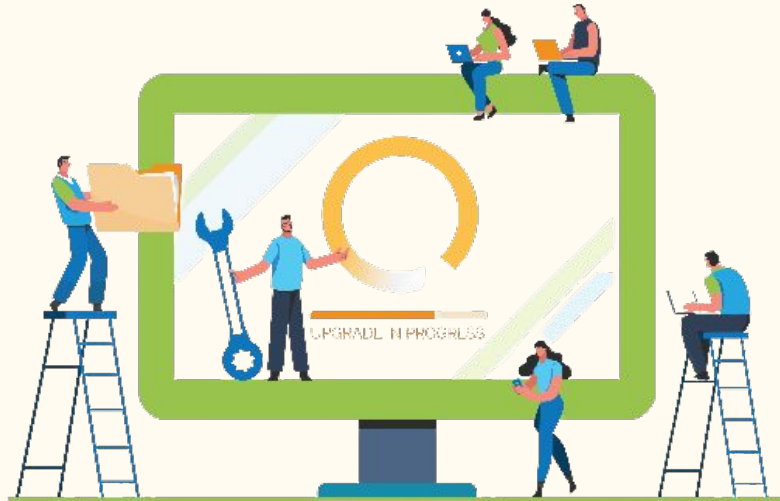
[Allowed threats](#)

[Protection history](#)

- Our antivirus was successful in detecting it

```
version: 0.0.1
description: Analyzes file with several antivirus softwares.
syntax: analyze_file -q <file id>
[✓] Analyzing file id NGUmZTQzYzYzNTZhMDdmOGZkZjYwZGNiOTRlNjJjMTI6MTY0MjAwNDAwMw==...
File Info:
sha256: a8b5c21389cc04a31c5ddaba3ea6221110e30456affc312b33a40567916fff4f
md5: 8af6854ef37b4038312afe593ec455ee
sha1: fbbecaed6fff0bb1d467949fe5afc3fb104622afb
Stats:
harmless: 0
type-unsupported: 11
suspicious: 0
confirmed-timeout: 0
timeout: 0
failure: 1
malicious: 2
undetected: 58
Threat Labelled as: trojan
AV Scan Results:
Lionic: malicious
ClamAV: malicious
McAfee: malicious
Zillya: malicious
Cyren: malicious
SymantecMobileInsight: failure
ESET-NOD32: malicious
TrendMicro-HouseCall: malicious
Avast: malicious
Cynet: malicious
Kaspersky: malicious
BitDefender: malicious
MicroWorld-eScan: malicious
Tencent: malicious
Ad-Aware: malicious
Sophos: malicious
Comodo: malicious
F-Secure: malicious
DrWeb: malicious
TrendMicro: malicious
McAfee-GW-Edition: malicious
FireEye: malicious
Emsisoft: malicious
GData: malicious
Avira: malicious
```

Demo - Website security analysis through browser extension



Future Scopes

- GUI Support
- Vulnerability detection using version info
- Web Application Firewall^[9]
- Store and detect malware byte info in database
- YARA for static analysis offline
- Sandbox implementation for dynamic analysis of low severity malwares using logs generated by malware activity
- Self managed API

Reference

- [1]<https://www.bleepingcomputer.com/forums/t/661440/how-do-viruses-replicate/>
- [2]<https://www.geeksforgeeks.org/how-an-antivirus-works/>
- [3]<https://www.kaspersky.com/blog/signature-virus-disinfection/13233/>
- [4]<https://www.lifewire.com/what-is-a-virus-signature-153629>
- [5]<https://usa.kaspersky.com/resource-center/definitions/heuristic-analysis>
- [6]<https://analyticsindiamag.com/how-antivirus-softwares-are-evolving-with-behavior-based-malware-detection-algorithms/>
- [7]<https://www.esecurityplanet.com/endpoint/sandboxing-advanced-malware-analyses-in-2021/>
- [8]<https://resources.infosecinstitute.com/topic/analyzing-malware-network-behavior/>
- [9]<https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/>

Thank You