DIGISURAKSHA PARHARI FOUNDATION INTERNSHIP 2025

Name-Girija Shankar Sahoo

Intern id- 444

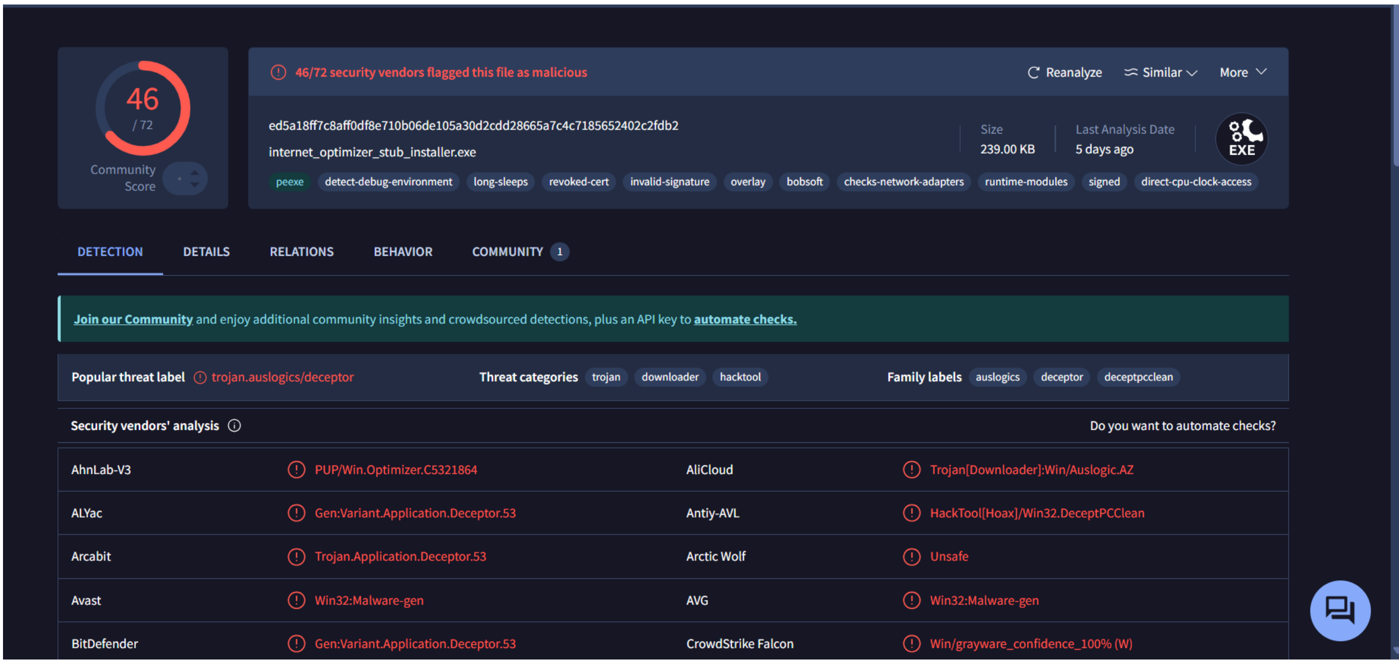
Task 02 – Malware Analysis

Hash - ed5a18ff7c8aff0df8e710b06de105a30d2cdd28665a7c4c7185652402c2fdb2

Malware Name - internet_optimizer_stub_installer.exe

HOW TO FIND THE MALWARE NAME:-

1. Go to www.virustotal.com
2. Paste the Given hash in the Search bar
3.



46/72 security vendors flagged this file as malicious

ed5a18ff7c8aff0df8e710b06de105a30d2cdd28665a7c4c7185652402c2fdb2

internet_optimizer_stub_installer.exe

Size 239.00 KB

Last Analysis Date 5 days ago

peexe detect-debug-environment long-sleeps revoked-cert invalid-signature overlay bobsoft checks-network-adapters runtime-modules signed direct-cpu-clock-access

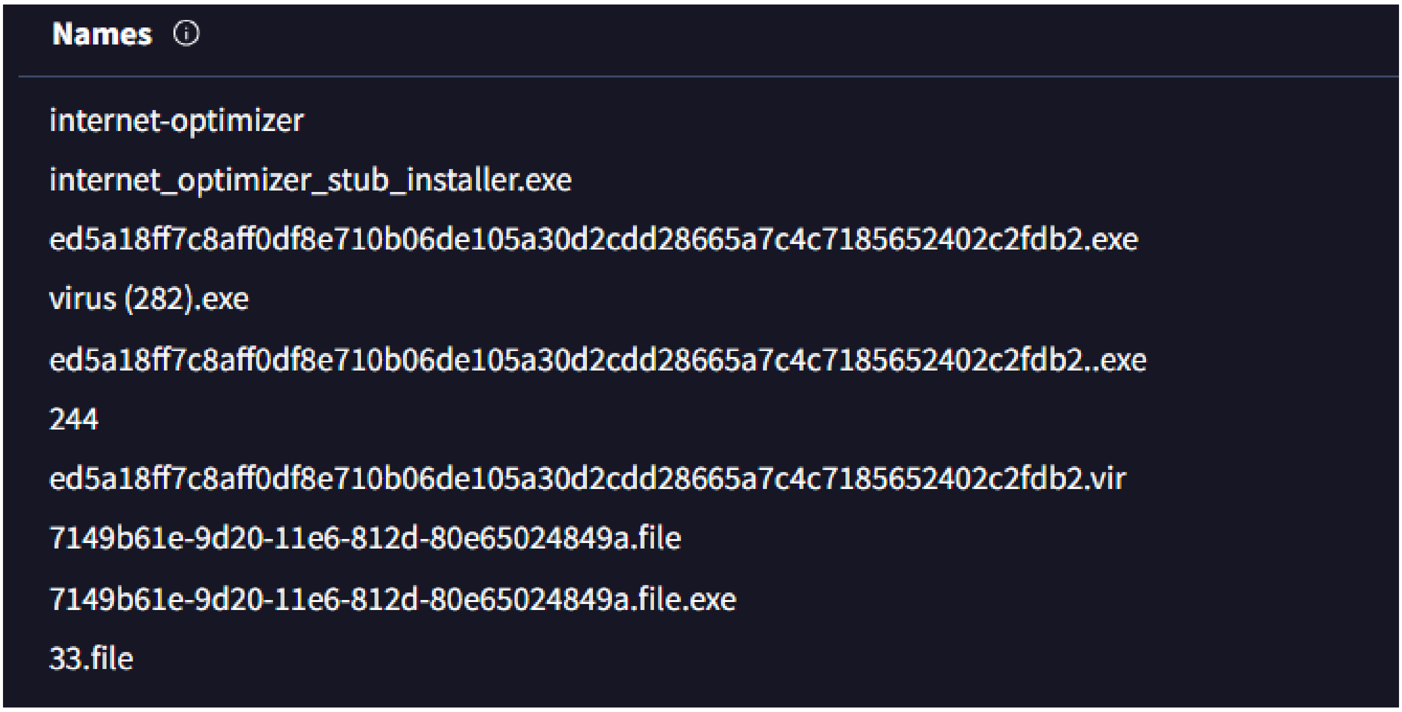
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.auslogics/deceptor Threat categories trojan downloader hacktool Family labels auslogics deceptor deceptpcclean

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	PUP/Win.Optimizer.C5321864	AliCloud	Trojan[Downloader]:Win/Auslogic.AZ
ALYac	Gen:Variant.Application.Deceptor.53	Antiy-AVL	HackTool[Hoax]/Win32.DeceptPCClean
Arcabit	Trojan.Application.Deceptor.53	Arctic Wolf	Unsafe
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
BitDefender	Gen:Variant.Application.Deceptor.53	CrowdStrike Falcon	Win/grayware_confidence_100% (W)

Other Names of the Malware



Names

internet-optimizer

internet_optimizer_stub_installer.exe

ed5a18ff7c8aff0df8e710b06de105a30d2cdd28665a7c4c7185652402c2fdb2.exe

virus (282).exe

ed5a18ff7c8aff0df8e710b06de105a30d2cdd28665a7c4c7185652402c2fdb2..exe

244

ed5a18ff7c8aff0df8e710b06de105a30d2cdd28665a7c4c7185652402c2fdb2.vir

7149b61e-9d20-11e6-812d-80e65024849a.file

7149b61e-9d20-11e6-812d-80e65024849a.file.exe

33.file

1.0 Executive Summary

The submitted file, `internet_optimizer_stub_installer.exe`, is a deceptive downloader Trojan, classified as a Potentially Unwanted Program (PUP) from the Auslogics/TweakBit software family. The malware masquerades as a system utility to trick users into execution. Its primary function is to establish persistence on the host system via a Windows Registry Run key and then download additional, unauthorized software from its Command and Control (C2) servers. Analysis indicates the malware authors used a revoked digital certificate in an attempt to appear legitimate. Live dynamic analysis was not performed as the sample was unavailable from public malware repositories.

Static Analysis Findings

Static analysis was performed by examining the file's metadata and embedded strings without executing the code.

Persistence Mechanism: The file contains the string `Software\Microsoft\Windows\CurrentVersion\Run`, which is the direct path to a common registry location used by malware to ensure it automatically executes every time the system starts.

Network Capabilities: The file contains hardcoded strings for networking functions from the `wininet.dll` library, including `InternetOpenA` and `InternetReadFile`. This confirms its built-in ability to connect to and download from the internet.

File System Capabilities: The presence of `CreateFileW` and `WriteFile` API call strings indicates the program is designed to create and write new files to the disk, which is consistent with the behavior of a downloader.

Attribution Clues: Multiple strings reference `TweakBit` and `Auslogics`, directly linking the sample to this known family of PUPs.

Behavioral Analysis Findings (Public Sandbox Data)

Behavioral analysis is based on aggregated reports from the VirusTotal service, which executes samples in a controlled sandbox environment.

C2 Communication:Upon execution, the malware was observed initiating HTTP GET requests to `downloads.tweakbit.com` and `dynamicdownloads.tweakbit.com`.

Payload Delivery:It successfully downloaded secondary payloads, including `internet-optimizer-setup.exe` and `pc-repair-kit-setup`. This confirms its primary function as a downloader or "stub" installer.

Campaign Tracking: The process was observed making HTTP POST requests to `www.google-analytics.com/collect`, indicating the authors are using Google Analytics to track the success rate and spread of their installation campaign.

Conclusion & Recommendations

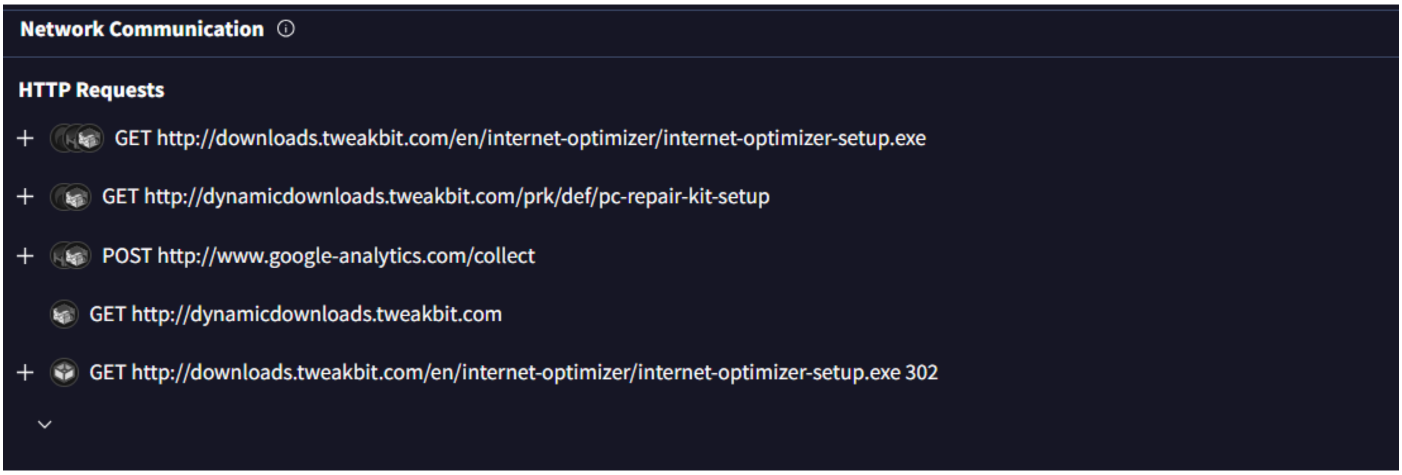
The evidence from both static and behavioral analysis conclusively identifies this sample as a deceptive downloader Trojan. Its purpose is to install a primary unwanted program ("Internet Optimizer") while also bundling additional unwanted software ("PC Repair Kit"). It achieves persistence and poses a risk by opening a channel for further unauthorized software to be installed on the host machine.

Recommendations:

1. Block IOCs: Block the identified domains at the network perimeter (firewall, web proxy).

2. Create Detections: Use the file hash to create detection rules in endpoint security solutions (Antivirus, EDR).

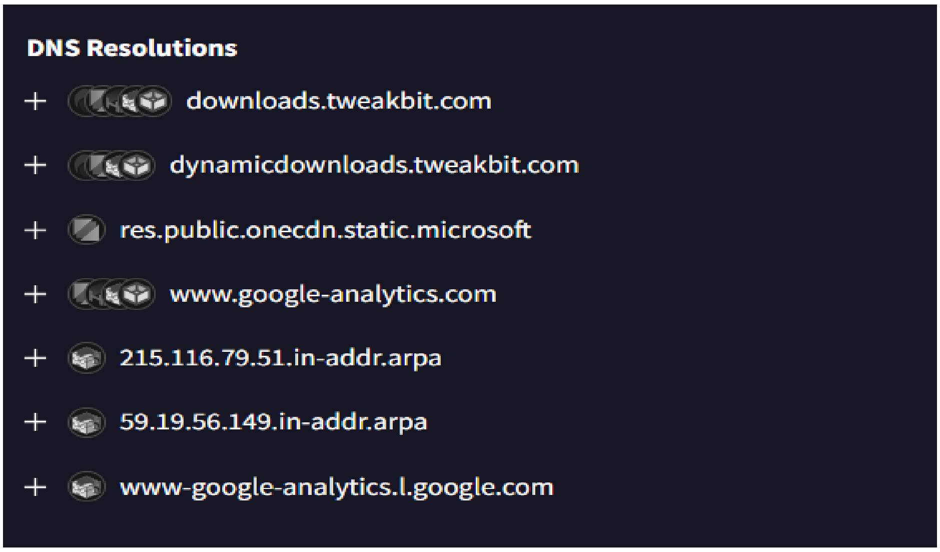
3. User Education: Educate users on the dangers of downloading "system optimizer" or "PC cleaner" tools from untrusted sources, as they are a primary vector for PUPs and malware.



Network Communication

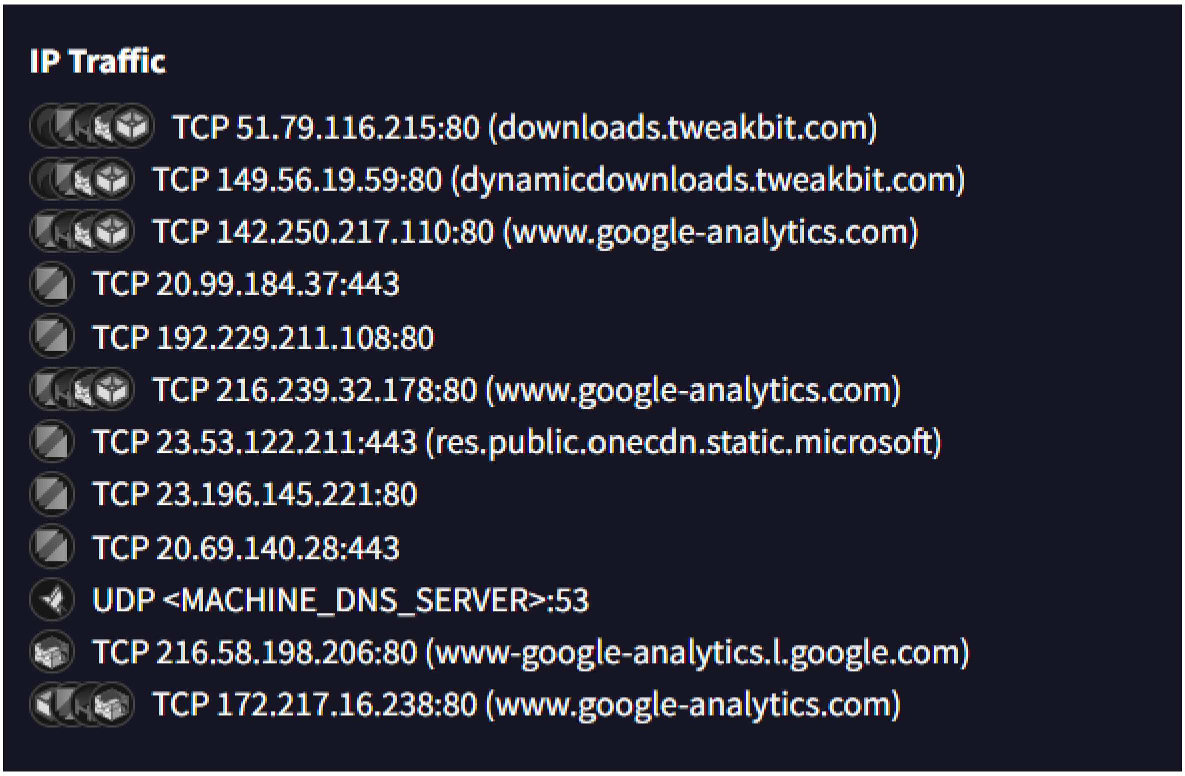
HTTP Requests

```
+ GET http://downloads.tweakbit.com/en/internet-optimizer/internet-optimizer-setup.exe
+ GET http://dynamicdownloads.tweakbit.com/prk/def/pc-repair-kit-setup
+ POST http://www.google-analytics.com/collect
  GET http://dynamicdownloads.tweakbit.com
+ GET http://downloads.tweakbit.com/en/internet-optimizer/internet-optimizer-setup.exe 302
```



DNS Resolutions

```
+ downloads.tweakbit.com
+ dynamicdownloads.tweakbit.com
+ res.public.onecdn.static.microsoft
+ www.google-analytics.com
+ 215.116.79.51.in-addr.arpa
+ 59.19.56.149.in-addr.arpa
+ www-google-analytics.l.google.com
```



IP Traffic

```
TCP 51.79.116.215:80 (downloads.tweakbit.com)
TCP 149.56.19.59:80 (dynamicdownloads.tweakbit.com)
TCP 142.250.217.110:80 (www.google-analytics.com)
TCP 20.99.184.37:443
TCP 192.229.211.108:80
TCP 216.239.32.178:80 (www.google-analytics.com)
TCP 23.53.122.211:443 (res.public.onecdn.static.microsoft)
TCP 23.196.145.221:80
TCP 20.69.140.28:443
UDP <MACHINE_DNS_SERVER>:53
TCP 216.58.198.206:80 (www-google-analytics.l.google.com)
TCP 172.217.16.238:80 (www.google-analytics.com)
```