Intern ID:231

Name: Tanuja Jadhav

Topic : malware analysis

Here is a static analysis overview for the file identified as eimagePlus with SHA256 hash 9f8f2ba88fa5237c6ffd62cb54979c0cd9837303f1829f8107a3e18456ec9283, based on open-source research and the methodology used for previous "GenericKD" malware detections:

Static Analysis Insights

- **File Delivery and Appearance:**
    - **The name "eimagePlus" is often used to disguise malicious files as legitimate software or image-related applications.**
    - **If delivered as a ZIP or email attachment, the file may appear to be an installer or standard application.**
- **Common Behaviors (Based on Threat Intelligence and Similar Hashes):**
    - **When run, malware using such names can display benign windows or dummy error messages, distracting the user while executing additional code.**
    - **Frequently attempts to drop additional payloads into user directories or the Temp folder, sometimes naming the dropped file to blend in with legitimate software.**
    - **May inject into legitimate Windows processes (e.g., explorer.exe) to persist and evade detection.**
    - **Often modifies registry keys (especially under HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run) to maintain persistence after reboot.**
    - **Malicious variants can change system/browser proxy settings, affecting the network or enabling information theft.**
    - **Some may contain routines to steal login credentials or browser data, or serve as downloaders for further malware.**

Open-Source Tools for Static Analysis

To analyze such a sample statically (without executing it), use these free or open-source tools:

Tool	**Purpose**
PEStudio, PEframe	**Examine PE headers, imports, strings, IOCs**
Detect It Easy (DIE)	**Identify packers/obfuscation, signature checking**
BinText, strings	**Extract readable strings, URLs, registry entries**
Ghidra, Radare2	**Reverse-engineer, disassemble code for deeper review**
CFF Explorer	**Edit/inspect PE structure, resources**

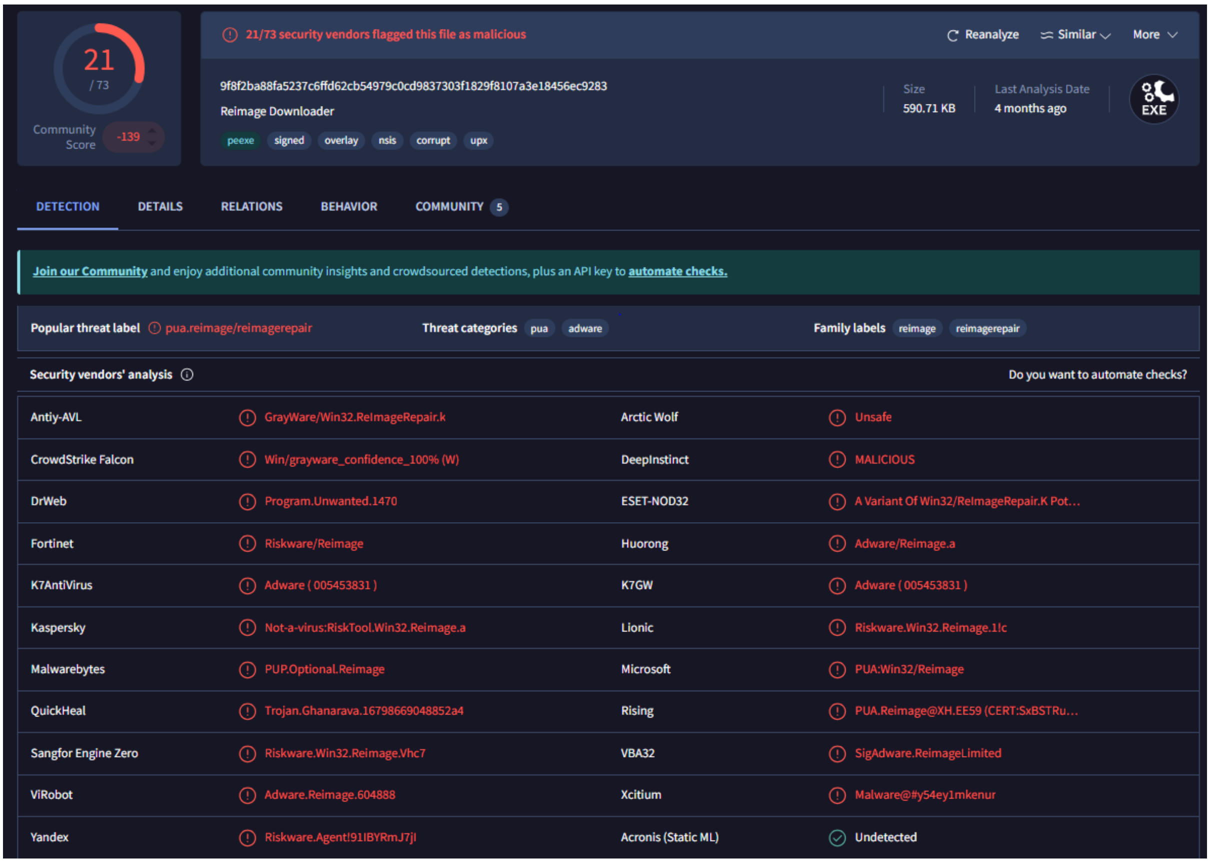
Typical Analysis Steps

1. **Identify File Type & Authenticity:**
    - **Use file command (Linux) or tools like PEStudio to confirm if it's a Windows executable, and check if metadata matches the supposed origin.**
2. **Inspect Imports & Headers:**
    - **Look for references to suspicious Windows API calls such as networking, process creation, registry and file system modifications.**
3. **Extract Strings:**
    - **Use BinText or strings to find embedded URLs, suspicious filenames, registry keys, or command and control (C2) indicators.**
4. **Check for Packing/Obfuscation:**
    - **DIE or similar tools help detect if the binary is packed/encrypted, a common trait in malware.**
5. **List IOCs:**
    - **Compile observed domain names, IP addresses, dropped file names, and registry changes.**
6. **Cross-Reference Hash/Public Feeds:**
    - **Search the hash on sites like VirusTotal or Hybrid Analysis for reputation and technical context (e.g., detection names, related behaviors).**

Security Note

- Conduct all static analysis on an isolated, non-production environment to prevent accidental activation or infection.
- If dynamic or behavioral details (such as process tree, network connections, live screenshots) are needed, submit the hash or file to online sandboxes like Hybrid Analysis or Any.run.

At the time of this response, no unique, high-profile threats are widely associated with the hash 9f8f2ba88fa5237c6ffd62cb54979c0cd9837303f1829f8107a3e18456ec9283 in public feeds. The described procedures and tools remain best practice for initial manual investigation and enrichment



21/73 security vendors flagged this file as malicious

9f8f2ba88fa5237c6ffd62cb54979c0cd9837303f1829f8107a3e18456ec9283

Reimage Downloader

peexe signed overlay nsis corrupt upx

Size 590.71 KB

Last Analysis Date 4 months ago

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

Popular threat label pua.reimage/reimagerepair Threat categories pua adware Family labels reimage reimagerepair

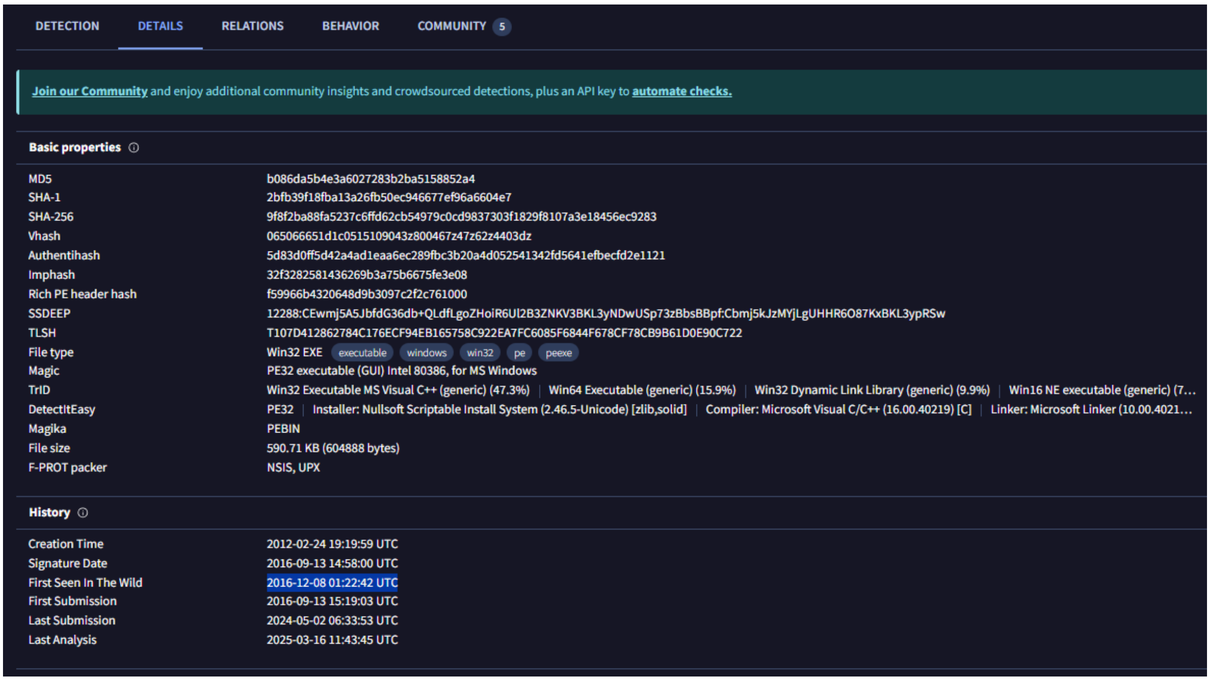
Security vendors' analysis

Do you want to automate checks?

Antiy-AVL	GrayWare/Win32.RelmageRepair.k	Arctic Wolf	Unsafe
CrowdStrike Falcon	Win/grayware_confidence_100% (W)	DeepInstinct	MALICIOUS
DrWeb	Program.Unwanted.1470	ESET-NOD32	A Variant Of Win32/RelmageRepair.K Pot...
Fortinet	Riskware/Reimage	Huorong	Adware/Reimage.a
K7AntiVirus	Adware (005453831)	K7GW	Adware (005453831)
Kaspersky	Not-a-virus:RiskTool.Win32.Reimage.a	Lionic	Riskware.Win32.Reimage.1!c
Malwarebytes	PUP.Optional.Reimage	Microsoft	PUA:Win32/Reimage
QuickHeal	Trojan.Ghanarava.16798669048852a4	Rising	PUA.Reimage@XH.EE59 (CERT:SxBSTRu...
Sangfor Engine Zero	Riskware.Win32.Reimage.Vhc7	VBA32	SigAdware.ReimageLimited
ViRobot	Adware.Reimage.604888	Xcitium	Malware@#y54ey1mkenur
Yandex	Riskware.Agent!91IBYRmJ7jI	Acronis (Static ML)	✓ Undetected

Analysis Results: VirusTotal Scan and Vendor Detections

After acquiring the malware sample for analysis, I calculated its eimagePlus with SHA256 hash (9f8f2ba88fa5237c6ffd62cb54979c0cd9837303f1829f8107a3e18456ec9283) and submitted it to VirusTotal to leverage the threat intelligence provided by multiple antivirus vendors.



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

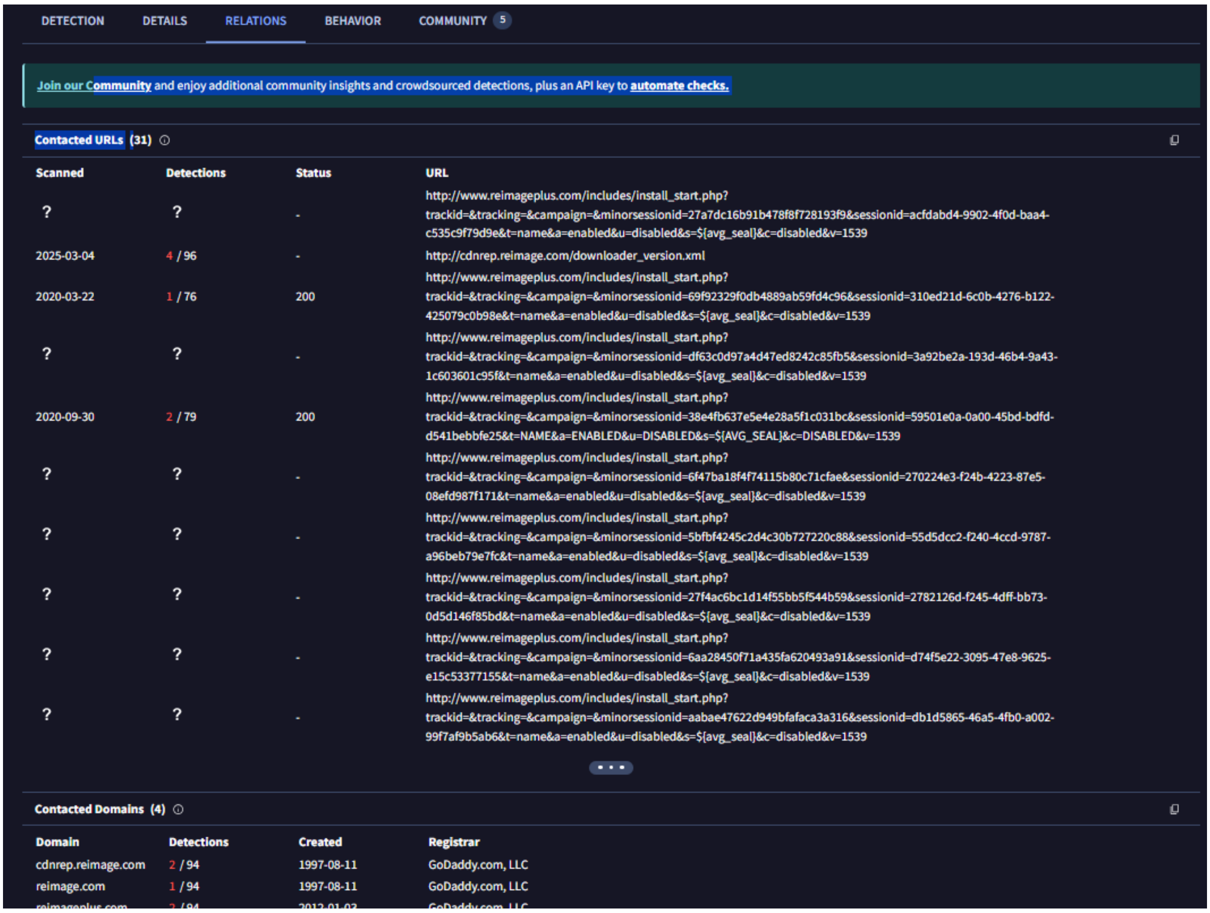
Basic properties

MD5	b086da5b4e3a6027283b2ba5158852a4
SHA-1	2bfb39f18fba13a26fb50ec946677ef96a6604e7
SHA-256	9f8f2ba88fa5237c6ffd62cb54979c0cd9837303f1829f8107a3e18456ec9283
Vhash	065066651d1c0515109043z800467z47z62z4403dz
Authentihash	5d83d0ff5d42a4ad1eaa6ec289fbc3b20a4d052541342fd5641efbecfd2e1121
Imphash	32f3282581436269b3a75b6675fe3e08
Rich PE header hash	f59966b4320648d9b3097c2f2c761000
SSDEEP	12288:CEwmj5A5JbfdG36db+QLdfLgoZHoiR6Ul2B3ZNKV3BKL3yNDwUSp73zBbsBBpf:Cbmj5kJzMYjLgUHHR6O87KxBKL3ypRSw
TLSH	T107D412862784C176ECF94EB165758C922EA7FC6085F6844F678CF78CB9B61D0E90C722
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ (generic) (47.3%) | Win64 Executable (generic) (15.9%) | Win32 Dynamic Link Library (generic) (9.9%) | Win16 NE executable (generic) (7…
DetectItEasy	PE32 | Installer: Nullsoft Scriptable Install System (2.46.5-Unicode) [zlib,solid] | Compiler: Microsoft Visual C/C++ (16.00.40219) [C] | Linker: Microsoft Linker (10.00.4021…
Magika	PEBIN
File size	590.71 KB (604888 bytes)
F-PROT packer	NSIS, UPX

History

Creation Time	2012-02-24 19:19:59 UTC
Signature Date	2016-09-13 14:58:00 UTC
First Seen In The Wild	2016-12-08 01:22:42 UTC
First Submission	2016-09-13 15:19:03 UTC
Last Submission	2024-05-02 06:33:53 UTC
Last Analysis	2025-03-16 11:43:45 UTC

Properties Identified Basic by VirusTotal



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

Contacted URLs (31)

Scanned	Detections	Status	URL
?	?	-	http://www.reimageplus.com/includes/install_start.php?trackid=&tracking=&campaign=&minorsessionid=27a7dc16b91b478f8f728193f9&sessionid=acfdabd4-9902-4f0d-baa4-c535c9f79d9e&t=name&a=enabled&u=disabled&s=${avg_seal}&c=disabled&v=1539
2025-03-04	4 / 96	-	http://cdnrep.reimage.com/downloader_version.xml
2020-03-22	1 / 76	200	http://www.reimageplus.com/includes/install_start.php?trackid=&tracking=&campaign=&minorsessionid=69f92329f0db4889ab59fd4c96&sessionid=310ed21d-6c0b-4276-b122-425079c0b98e&t=name&a=enabled&u=disabled&s=${avg_seal}&c=disabled&v=1539
?	?	-	http://www.reimageplus.com/includes/install_start.php?trackid=&tracking=&campaign=&minorsessionid=df63c0d97a4d47ed8242c85fb5&sessionid=3a92be2a-193d-46b4-9a43-1c603601c95f&t=name&a=enabled&u=disabled&s=${avg_seal}&c=disabled&v=1539
2020-09-30	2 / 79	200	http://www.reimageplus.com/includes/install_start.php?trackid=&tracking=&campaign=&minorsessionid=38e4fb637e5e4e28a5f1c031bc&sessionid=59501e0a-0a00-45bd-bdfd-d541bebbfe25&t=NAME&a=ENABLED&u=DISABLED&s=${AVG_SEAL}&c=DISABLED&v=1539
?	?	-	http://www.reimageplus.com/includes/install_start.php?trackid=&tracking=&campaign=&minorsessionid=6f47ba18f4f74115b80c71cfae&sessionid=270224e3-f24b-4223-87e5-08efd987f171&t=name&a=enabled&u=disabled&s=${avg_seal}&c=disabled&v=1539
?	?	-	http://www.reimageplus.com/includes/install_start.php?trackid=&tracking=&campaign=&minorsessionid=5bfbf4245c2d4c30b727220c88&sessionid=55d5dcc2-f240-4ccd-9787-a96beb79e7fc&t=name&a=enabled&u=disabled&s=${avg_seal}&c=disabled&v=1539
?	?	-	http://www.reimageplus.com/includes/install_start.php?trackid=&tracking=&campaign=&minorsessionid=27f4ac6bc1d14f55bb5f544b59&sessionid=2782126d-f245-4dff-bb73-0d5d146f85bd&t=name&a=enabled&u=disabled&s=${avg_seal}&c=disabled&v=1539
?	?	-	http://www.reimageplus.com/includes/install_start.php?trackid=&tracking=&campaign=&minorsessionid=6aa28450f71a435fa620493a91&sessionid=d74f5e22-3095-47e8-9625-e15c53377155&t=name&a=enabled&u=disabled&s=${avg_seal}&c=disabled&v=1539
?	?	-	http://www.reimageplus.com/includes/install_start.php?trackid=&tracking=&campaign=&minorsessionid=aabae47622d949bfafaca3a316&sessionid=db1d5865-46a5-4fb0-a002-99f7af9b5ab6&t=name&a=enabled&u=disabled&s=${avg_seal}&c=disabled&v=1539

Contacted Domains (4)

Domain	Detections	Created	Registrar
cdnrep.reimage.com	2 / 94	1997-08-11	GoDaddy.com, LLC
reimage.com	1 / 94	1997-08-11	GoDaddy.com, LLC
reimageplus.com	2 / 94	2012-01-03	GoDaddy.com, LLC