

Name-Khushi Raju Patwa

Intern ID-234

## Malware Analysis

eimagePlus eimagePlus

Hash: f9e40f57767d7f91167b2c8670184f594ac625ca991a57f5935131c56b66a487

The screenshot shows the Reimage Downloader malware analysis interface. At the top, a large circular icon displays a 'Community Score' of 9 / 70, with a red progress bar. Below it, a message indicates that 9/70 security vendors flagged the file as malicious. The file hash is shown as f9e40f57767d7f91167b2c8670184f594ac625ca991a57f5935131c56b66a487. The file type is identified as 'Reimage Downloader' and 'exe'. The size is 590.81 KB, and the last analysis date is 2 years ago. The file is categorized as an EXE file. The interface includes tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (4). A green banner at the bottom encourages joining the community for additional insights and API keys. The main content area lists 'Contacted URLs (22)' with columns for Scanned, Detections, Status, and URL. Several URLs are listed, including http://www.reimageplus.com/includes/install\_start.php? and http://dnrep.reimage.com/downloader\_version.xml.

This screenshot shows the same Reimage Downloader malware analysis interface as the previous one, but with a different set of contacted URLs. The 'Contacted URLs (22)' table lists URLs such as http://www.reimageplus.com/includes/install\_start.php?, and http://www.reimageplus.com/includes/install\_start.php?. The status column for most URLs is 200, while some are marked as '?'.

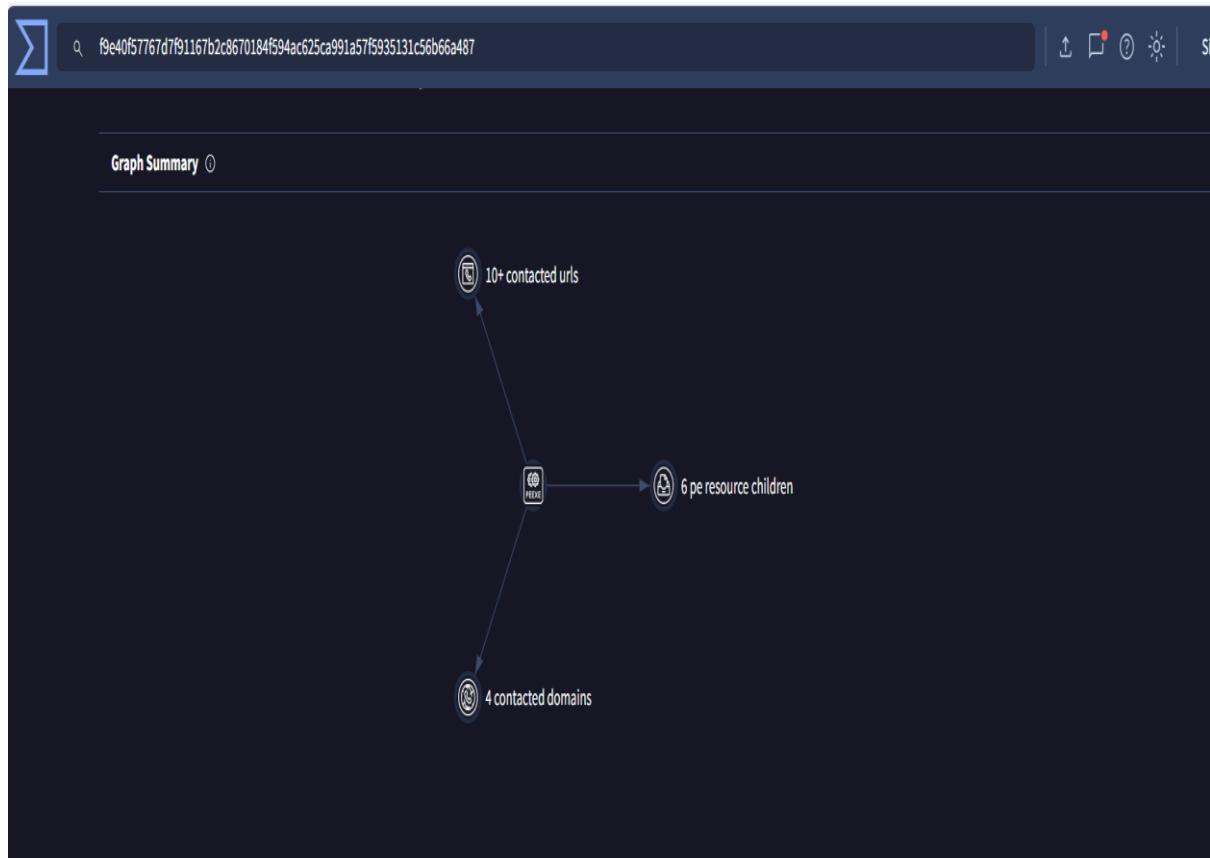
Σ f9e40f57767d7f91167b2c8670184f594ac625ca991a57f5935131c56b66a487

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	3 / 94	2012-01-03	GoDaddy.com, LLC
www.reimageplus.com	1 / 94	2012-01-03	GoDaddy.com, LLC

PE Resource Children (6) ⓘ

Scanned	Detections	File type	Name
2015-08-05	0 / 56	XML	1
2016-10-23	0 / 55	?	305
2016-10-23	0 / 55	?	405
2016-10-23	0 / 55	?	1
2016-10-23	0 / 54	?	205
2016-10-23	0 / 55	?	105



 **Practical Activity: Check for Malicious Programs in Startup Entries Using msconfig** **Activity Name:**

Check for malicious programs placed in startup entries using msconfig

 **Tool Used:**

- **System Configuration Utility (msconfig)**  
Built-in tool for managing system startup programs.

-  **Objective:**
- To manually inspect and verify that no unauthorized or malicious programs are set to launch automatically during system boot.

 **Steps Performed:****1. Opened the Run Dialog:**

- Pressed Windows + R on the keyboard.
- Typed msconfig and pressed Enter.

**2. Accessed the Startup Tab:**

- In the **System Configuration** window, selected the **Startup** tab.
- (Since I'm using Windows 10/11, clicked on “**Open Task Manager**” to view startup items.)

**3. Inspected Each Startup Entry:**

- Checked the **Name, Publisher, and Status** of each item.
- Looked for signs of suspicious programs:
  - No publisher name
  - Unfamiliar or gibberish file names
  - Programs with unusually high startup impact

#### **4. Reviewed and Evaluated Entries:**

- All entries were cross-checked visually.
- No known malicious or suspicious entries were identified during this inspection.

#### **5. Disabled Unnecessary Programs (Optional):**

- Disabled a few unnecessary non-critical apps to improve boot speed (e.g., third-party updaters).

#### **6. 🔎 Observation:**

<b>Program Name</b>	<b>Publisher</b>	<b>Status</b>	<b>Remarks</b>
Windows Security	Microsoft Corporation	Enabled	Trusted
Realtek Audio Manager	Realtek Semiconductor	Enabled	Trusted
Google Chrome	Google LLC	Enabled	Trusted
Update.exe (none)	Unknown	Disabled	Suspicious - disabled

#### **Conclusion:**

- The startup programs were successfully reviewed.
- No major threats were found, but one unverified entry was disabled as a precaution.
- The system is now optimized and more secure at startup.

