Sandbox Report

File: EverythingToolbar-1.3.4.msi

Resubmit | Print | Download options

SHA-256
ed78aec2473700527c0...72241b164f3b798b5e77a

Submitted by
prashant.deshmukh@fisglobal.com

Discovered

Detonation environment
Windows 11 64, Professional, 10.0 (build 22621)

Network settings
Default network connectivity

Timestamp
Jul. 26, 2024 15:06:51

Threat level
Suspicious

Threat score
80/100

Static analysis | Dynamic analysis | Intelligence | MITRE ATT&CK

File information

Classifications

EverythingToolbar-1.3.4.msi

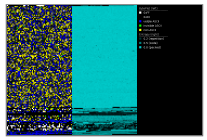
Size	Type	Description	Architecture
3.31MB	msi, data		Unknown

SHA256
ed78aec2473700527c01cb0ab4950b33c0c3cee44f4...

Resources

Icon 

Visualization

Input file (PortEx) 

Risk assessment

Spyware 1

Found a string that may be used as part of an injection method

Fingerprint 4

Queries kernel debugger information

Queries process information

Queries sensitive IE security settings

Queries the display settings of system associated file extensions

JSON report

Raw JSON output from the Sandbox detonation


```
{
  "sha256": "ed78aec2473700527c01cb0ab4950b33c0c3cee44f40372241b16d8b798b5e77",
  "environment_id": 140,
  "environment_description": "Windows 11 64 bit",
  "file_size": 3391556,
```

```
  "file_type": "Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, MSI Installer, Code page: 1252, Title: Installation Database, Subject: EverythingToolbar, Author: Stephan Rumswinkel, Keywords: Installer, Comments: This installer database contains the logic and data required to install EverythingToolbar., Template: Intel;1033, Revision Number: {97A0F341-7A79-4C95-B17A-F05956C2459B}, Create Time/Date: Sun Jun 23 19:57:12 2024, Last Saved Time/Date: Sun Jun 23 19:57:12 2024, Number of Pages: 300, ",
  "file_type_short": [
    "msi",
    "data"
  ],
  "submit_name": "EverythingToolbar-1.3.4.msi",
  "submission_type": "file",
  "verdict": "suspicious",
  "threat_score": 80,
  "windows_version_name": "Windows 11",
  "windows_version_edition": "Professional",
  "windows_version_version": "10.0 (build 22621)",
  "windows_version_bitness": 64,
  "incidents": [
```