Sandbox Report

File: EverythingToolbar-1.3.4.msi

Resubmit | Print | Download options

SHA-256
ed78aec2473700527c01cb0ab49[redacted]

Submitted by
[redacted]@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

Tactics and Techniques observed

Click on a technique to see additional details.

- **Execution** 1
  - Native API
- **Privilege Escalation** 1
  - Process Injection 1
    - Extra Window Memory Injection
- **Defense Evasion** 6
  - Debugger Evasion
  - Impair Defenses 1
    - Disable or Modify Tools
  - Indicator Removal on Host 2
    - File Deletion
    - Timestomp
  - Modify Registry
  - Obfuscated Files or Information
- **Credential Access** 1
  - Input Capture 1
    - Keylogging
- **Discovery** 4
  - Debugger Evasion
  - File and Directory Discovery
  - Process Discovery
  - Query Registry
- **Collection** 3
  - Data from Local System
  - Email Collection
  - Input Capture 1
    - Keylogging

Process Injection 1

Extra Window Memory Injection