Sandbox Report

File: EverythingToolbar-1.3.4.msi

Resubmit | Print | Download options

SHA-256
ed78aec2473700527c0...72241b164f8b798b5e77a

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

Behavioral threat indicators

Suspicious 26

Found a potential E-Mail address in binary/memory

Source File/Memory

Relevance 3/10

MITRE ATT&CK Email Collection T1114

Details Pattern match: "v@l.f" Pattern match: "2@n.kz" Pattern match: "o@g8.ir" Pattern match: "v@o.r"

Reads configuration files (.ini files)

Source API Call

Relevance 4/10

MITRE ATT&CK File and Directory Discovery T1083

Details "EverythingToolbar.Launcher.exe" reads file "C:\Users\desktop.ini" "EverythingToolbar.Launcher.exe" reads file "C:\Users\%OSUSER%\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\desktop.ini" "EverythingToolbar.Launcher.exe" reads file "C:\Users\%OSUSER%\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\desktop.ini"

"EverythingToolbar.Launcher.exe" reads file "C:\Users\%OSUSER%\Desktop\desktop.ini" "EverythingToolbar.Launcher.exe" reads file "C:\Users\%OSUSER%\Documents\desktop.ini" "EverythingToolbar.Launcher.exe" reads file "C:\Users\%OSUSER%\Music\desktop.ini" "EverythingToolbar.Launcher.exe" reads file "C:\Users\%OSUSER%\Pictures\desktop.ini" "EverythingToolbar.Launcher.exe" reads file "C:\Users\%OSUSER%\Videos\desktop.ini" "EverythingToolbar.Launcher.exe" reads file "C:\Users\%OSUSER%\Downloads\desktop.ini" "EverythingToolbar.Launcher.exe" reads file "C:\Users\%OSUSER%\OneDrive\desktop.ini" "EverythingToolbar.Launcher.exe" reads file "C:\Program Files (x86)\desktop.ini"

Opens a handle to the specified process

Source API Call

Relevance 3/10

MITRE ATT&CK Process Discovery T1057

Details "EverythingToolbar.Launcher.exe" opens a process "C:\Program Files (x86)\EverythingToolbar\EverythingToolbar.Launcher.exe" (UID: 00000000-00004976)

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

Source File/Memory

Relevance 4/10

MITRE ATT&CK Extra Window Memory Injection T1055.011

Details "Shell_TrayWnd" (Taskbar window class may be used to inject into explorer with the SetWindowLong method) in Source: 00000000-00004976-0000044C-2079036122 "Shell_TrayWnd" (Taskbar window class may be used to inject into explorer with the SetWindowLong method) in Source: 00000000-00004976.00000000.350957.50CC0000.00000002.mdmp 00000000-00004976.00000001.352878.50CC0000.00000002.mdmp 00000000-00004976.00000002.354796.50CC0000.00000002.mdmp "Progman" (Program manager) in Source: 00000000-00004976.00000000.350957.50CC0000.00000002.mdmp 00000000-00004976.00000001.352878.50CC0000.00000002.mdmp 00000000-00004976.00000002.354796.50CC0000.00000002.mdmp

Monitors specific registry key for changes

Source API Call

Relevance 4/10

MITRE ATT&CK Query Registry T1012

Details "EverythingToolbar.Launcher.exe" monitors "HKCU_Classes" (Filter: 268435461; Subtree: 1) "EverythingToolbar.Launcher.exe" monitors "HKCU\Software\Microsoft\Windows\CurrentVersion\Themes\Personalize" (Filter: 268435461; Subtree: 0) "EverythingToolbar.Launcher.exe" monitors "HKCU\Control Panel\Colors" (Filter: 268435461; Subtree: 0) "EverythingToolbar.Launcher.exe" monitors "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Accent" (Filter: 268435461; Subtree: 0)

Creates new processes

Source	API Call
Relevance	8/10
MITRE ATT&CK	Native API T1106
Details	"msiexec.exe" is creating a new process (Name: "C:\Windows\syswow64\MsiExec.exe") "MsiExec.exe" is creating a new process (Name: "C:\Program Files (x86)\EverythingToolbar\EverythingToolbar.Launcher.exe")

Scans for the windows taskbar (may be used for explorer injection)

Source	API Call
Relevance	10/10
MITRE ATT&CK	Extra Window Memory Injection T1055.011
Details	"EverythingToolbar.Launcher.exe" searching for class "Shell_TrayWnd"

Calls an API typically used to set the date and time of the file

Source	API Call
Relevance	2/10
MITRE ATT&CK	Timestomp T1070.006
Details	"EverythingToolbar.Launcher.exe" called "SetFileTime" on file C:\Users\%OSUSER%\AppData\Local\EverythingToolbar\EverythingToolbar.Launche_Url_vaj5fmsnib0mkvub0wvxkpwbnuhugm51\1.3.4.0\x32uhste.newcfg (UID: 00000000-00004976) "EverythingToolbar.Launcher.exe" called "SetFileTime" on file C:\Users\%OSUSER%\AppData\Local\Temp\EverythingToolbar.log (UID: 00000000-00004976)

Queries process information

Source	API Call
Relevance	4/10
MITRE ATT&CK	Process Discovery T1057
Details	"EverythingToolbar.Launcher.exe" queried SystemProcessInformation at 00000000-00004976-00000C13-4484539777 [PID: 4976] "EverythingToolbar.Launcher.exe" queried SystemProcessInformation at 00000000-00004976-00000C13-4484549937 [PID: 4976] "EverythingToolbar.Launcher.exe" queried SystemProcessInformation at 00000000-00004976-00000C13-4484842016 [PID: 4976]

"EverythingToolbar.Launcher.exe" queried SystemProcessInformation at 00000000-00004976-00000C13-4484849878 [PID: 4976]
"EverythingToolbar.Launcher.exe" queried SystemProcessInformation at 00000000-00004976-00000C13-4490288619 [PID: 4976]
"EverythingToolbar.Launcher.exe" queried SystemProcessInformation at 00000000-00004976-00000C13-4490294774 [PID: 4976]
"EverythingToolbar.Launcher.exe" queried SystemProcessInformation at 00000000-00004976-00000C13-4490483747 [PID: 4976]
"EverythingToolbar.Launcher.exe" queried SystemProcessInformation at 00000000-00004976-00000C13-4490490431 [PID: 4976]

Uses a Windows Living Off The Land Binaries (LOL bins)

Source	Monitored Target
Relevance	3/10
Details	Process "%WINDIR%\system32\msiexec.exe" launched with commandline "/V" (UID: 00000000-00010180) Process "%WINDIR%\syswow64\MsiExec.exe" launched with commandline "-Embedding BEFDF77F3FFCA8278B64CC5DA8DD0210 C" (UID: 00000000-00006212)

Queries kernel debugger information

Source	API Call
Relevance	6/10
MITRE ATT&CK	Debugger Evasion T1622
Details	"EverythingToolbar.Launcher.exe" at 00000000-00004976-00000C13-4484988742

Creates guarded memory regions (anti-debugging trick to avoid memory dumping)

Source	API Call
Relevance	10/10
MITRE ATT&CK	Disable or Modify Tools T1562.001
Details	"EverythingToolbar.Launcher.exe" is allocating memory with PAGE_GUARD access rights (Handle: 4294967295); (PID: 4976)

Calls an API typically used to query local/system time as file time

Source	API Call
Relevance	3/10
MITRE ATT&CK	Timestomp T1070.006
Details	"EverythingToolbar.Launcher.exe" called "FileTimeToSystemTime" (UID: 00000000-00004976)

Calls an API typically used for keylogging

Source	API Call
Relevance	10/10
MITRE ATT&CK	Keylogging T1056.001
Details	"EverythingToolbar.Launcher.exe" called "GetKeyState" with parameters {"nVirtKey": "1"} "EverythingToolbar.Launcher.exe" called "GetKeyState" with parameters {"nVirtKey": "2"}

Spawned processes likely due to injection

Source	Monitored Target
Relevance	3/10
MITRE ATT&CK	Process Injection T1055
Details	Process "%PROGRAMFILES%\(x86)\EverythingToolbar\EverythingToolbar.Launcher.exe" spawned likely due to injection

Sends traffic on typical HTTP outbound port, but without HTTP header

Source	Network Traffic
Relevance	5/10
MITRE ATT&CK	Web Protocols T1071.001
Details	TCP traffic to 20.72.205.209 on port 443 is sent without HTTP header

Spawned process connects to a network

Source	Monitored Target
Relevance	5/10
MITRE ATT&CK	Application Layer Protocol T1071
Details	Process "%WINDIR%\System32\msiexec.exe" connects to 20.72.205.209 on port 443 (TCP)

Multiple POSTs requests with same length but different payloads to a webserver (HTTPS)

Source	Network Traffic

Relevance 5/10

MITRE ATT&CK Data Transfer Size Limits T1030

Details Found more than 2 POST requests like this POST /RST2.srf HTTP/1.0Connection: Keep-Alive Content-Type: application/soap+xml Accept: */* User-Agent: MSAWindows/45 (OS 10.0.22621.0.0 ni_release; IDK 10.0.22621.1 ni_release; Cfg 16.000.29325.00; Test 0) Content-Length: 4694 Host: login.live.com with payload ==> <?xml version="1.0" encoding="UTF-8"?><s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" .....

Calls an API typically to import asymmetric cryptographic keys into a CSP

Source API Call

Relevance 1/10

MITRE ATT&CK Asymmetric Cryptography T1573.002

Details "EverythingToolbar.Launcher.exe" called "BCryptImportKeyPair" with parameters {"hAlgorithm": "50770160" "pszBlobType": "RSAPUBLICBLOB" "phKey": "PYzP" "pbInput": "RSA1" "cbInput": "163" "dwFlags": "0"} "EverythingToolbar.Launcher.exe" called "BCryptImportKeyPair" with parameters {"hAlgorithm": "50770160" "pszBlobType": "RSAPUBLICBLOB" "phKey": "a003966ae3010000" "pbInput": "RSA1" "cbInput": "163" "dwFlags": "0"} "EverythingToolbar.Launcher.exe" called "BCryptImportKeyPair" with parameters {"hAlgorithm": "50770160" "pszBlobType": "RSAPUBLICBLOB" "phKey": "f004966ae3010000" "pbInput": "RSA1" "cbInput": "163" "dwFlags": "0"} "EverythingToolbar.Launcher.exe" called "BCryptImportKeyPair" with parameters {"hAlgorithm": "50770160" "pszBlobType": "RSAPUBLICBLOB" "phKey": "c004966ae3010000" "pbInput": "RSA1" "cbInput": "163" "dwFlags": "0"} "EverythingToolbar.Launcher.exe" called "BCryptImportKeyPair" with parameters {"hAlgorithm": "50770160" "pszBlobType": "RSAPUBLICBLOB" "phKey": "4006966ae3010000" "pbInput": "RSA1" "cbInput": "163" "dwFlags": "0"} "EverythingToolbar.Launcher.exe" called "BCryptImportKeyPair" with parameters {"hAlgorithm": "50770160" "pszBlobType": "RSAPUBLICBLOB" "phKey": "0004966ae3010000" "pbInput": "RSA1" "cbInput": "163" "dwFlags": "0"} "EverythingToolbar.Launcher.exe" called "BCryptImportKeyPair" with parameters {"hAlgorithm": "50770160" "pszBlobType": "RSAPUBLICBLOB" "phKey": "9004966ae3010000" "pbInput":

Calls an API typically used to acquire handle to a key container within a CSP

Source API Call

Relevance 1/10

MITRE ATT&CK Obfuscated Files or Information T1027

Details "EverythingToolbar.Launcher.exe" called "CryptAcquireContextA" with parameters {"phProv": "e02f976ae3010000" "dwProvType": "1" "dwFlags": "4026531840"} "EverythingToolbar.Launcher.exe" called "CryptAcquireContextA" with parameters {"phProv": "803e976ae3010000" "dwProvType": "1" "dwFlags": "4026531840"} "EverythingToolbar.Launcher.exe" called "CryptAcquireContextA" with parameters {"phProv": "0028976ae3010000" "dwProvType": "1" "dwFlags": "4026531840"} "EverythingToolbar.Launcher.exe" called "CryptAcquireContextA" with parameters {"phProv": "0031976ae3010000" "dwProvType": "1" "dwFlags": "4026531840"} "EverythingToolbar.Launcher.exe" called "CryptAcquireContextA" with parameters {"phProv": "c02e976ae3010000" "dwProvType": "1" "dwFlags": "4026531840"} "EverythingToolbar.Launcher.exe" called "CryptAcquireContextA" with parameters {"phProv": "e026976ae3010000" "dwProvType": "1" "dwFlags": "4026531840"} "EverythingToolbar.Launcher.exe" called "CryptAcquireContextA" with parameters {"phProv": "`4" "dwProvType": "1" "dwFlags": "4026531840"} "EverythingToolbar.Launcher.exe" called "CryptAcquireContextA" with parameters {"phProv": "D" "dwProvType": "1" "dwFlags":

"1" "dwFlags": "4026531840"} "EverythingToolbar.Launcher.exe" called "CryptAcquireContextA" with parameters {"phProv": "e038976ae3010000"

Calls an API typically to import cryptographic keys into a CSP

Source API Call

Relevance 1/10

MITRE ATT&CK Data Encrypted for Impact T1486

Details "EverythingToolbar.Launcher.exe" called "CryptImportKey" with parameters {"hProv": "5076efe0" "pbData": "0602000000240000525341310004000001000100155 63bbd97670337cd939760bd18772ac58527a53de4ac41cee4c61b8856a502c9b56ed07947220bc05a132669814d4ee4943f83541fcd38b9b96949c4bae3f5f060d8bdf5aca2d26f2da67d6e1a95373cf1d061aed5e2ea8c8d3eaac248d36537e84582c3777ae08a8817ff50411ae1f0be9a2d0c7c5eb37e89b3a55997e9b8" "dwDataLen": "148" "dwFlags": "0" "phKey": "p#wP"}
"EverythingToolbar.Launcher.exe" called "CryptImportKey" with parameters {"hProv": "5076efe0" "pbData": "0602000000240000525341310004000001000100772391e63c104728adcf18e2390474262559fa7f34a4215848f43288cde875dcc92a06222e9be0592b211ff74adbb5d21a7aab5522b540b1735f2f03279221056fedbe7e534073dabee9db48f8ecebcf1dc98a95576e45cbeff5fe7c4842859451ab2dae7a8370f1b2f7a529d2ca210e3e844d973523d73d193df6c17f1314a6" "dwDataLen": "148" "dwFlags": "0" "phKey": "p$wP"}
"EverythingToolbar.Launcher.exe" called "CryptImportKey" with parameters {"hProv": "5076efe0" "pbData": "0602000000240000525341310004000001000100772391e63c104728adcf18e2390474262559fa7f34a4215848f43288cde875dcc92a06222e9be0592b211ff74adbb5d21a7aab5522b540b1735f2f03279221056fedbe7e534073dabee9db48f8ecebcf1dc98a95576e45cbeff5fe7c4842859451ab2dae

Queries sensitive IE security settings

Source Registry Access

Relevance 8/10

MITRE ATT&CK Query Registry T1012

Details "EverythingToolbar.Launcher.exe" (Path: "HKCU\SOFTWARE\MICROSOFT\INTERNET EXPLORER\SECURITY"; Key: "DISABLESECURITYSETTINGSCHECK")

Modifies proxy settings

Source Registry Access

Relevance 10/10

MITRE ATT&CK Modify Registry T1112

Details "EverythingToolbar.Launcher.exe" (Access type: "SETVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP"; Key: "PROXYBYPASS"; Value: "01000000")

Queries the display settings of system associated file extensions

Source Registry Access

Relevance 7/10

MITRE ATT&CK Data from Local System T1005

Details "EverythingToolbar.Launcher.exe" (Access type: "QUERYVAL"; Path: "HKLM\SOFTWARE\CLASSES\SYSTEMFILEASSOCIATIONS\.LNK"; Key: "ALWAYSSHOWEXT") "EverythingToolbar.Launcher.exe" (Access type: "QUERYVAL"; Path: "HKLM\SOFTWARE\CLASSES\SYSTEMFILEASSOCIATIONS\.EXE"; Key: "ALWAYSSHOWEXT") "EverythingToolbar.Launcher.exe" (Access type: "QUERYVAL"; Path: "HKLM\SOFTWARE\CLASSES\SYSTEMFILEASSOCIATIONS\.EXE"; Key: "NEVERSHOWEXT")

Writes registry keys

Source Registry Access

Relevance 3/10

MITRE ATT&CK Modify Registry T1112

Details "EverythingToolbar.Launcher.exe" (Access type: "SETVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP"; Key: "PROXYBYPASS"; Value: "01000000") "EverythingToolbar.Launcher.exe" (Access type: "SETVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP"; Key: "INTRANETNAME"; Value: "01000000") "EverythingToolbar.Launcher.exe" (Access type: "SETVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP"; Key: "UNCASINTRANET"; Value: "01000000") "EverythingToolbar.Launcher.exe" (Access type: "SETVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP"; Key: "AUTODETECT"; Value: "00000000") "EverythingToolbar.Launcher.exe" (Access type: "SETVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\SEARCH"; Key: "SEARCHBOXTASKBARMODE"; Value: "00000000")

Opens file with deletion access rights

Source API Call

Relevance 7/10

MITRE ATT&CK File Deletion T1070.004

Details "EverythingToolbar.Launcher.exe" opened "C:\Users\%OSUSER%\AppData\Local\EverythingToolbar\EverythingToolbar.Launche_Url_vaj5fmsnib0mkvub0wvxkpwbnuhugm51\1.3.4.0\uejwpk3x.newcfg" with delete access "EverythingToolbar.Launcher.exe" opened "C:\Users\%OSUSER%\AppData\Local\EverythingToolbar\EverythingToolbar.Launche_Url_vaj5fmsnib0mkvub0wvxkpwbnuhugm51\1.3.4.0\uejwpk3tmp" with delete access "EverythingToolbar.Launcher.exe" opened "C:\Users\%OSUSER%\AppData\Local\EverythingToolbar\EverythingToolbar.Launche_Url_vaj5fmsnib0mkvub0wvxkpwbnuhugm51\1.3.4.0\x32uhstenewcfg" with delete access "EverythingToolbar.Launcher.exe" opened

"C:\Users\%OSUSER%\AppData\Local\EverythingToolbar\EverythingToolbar.Launche_Url_vaj5fmsnib0mkvub0wvxkpwbnuhugm51\1.3.4.0\x32uhste

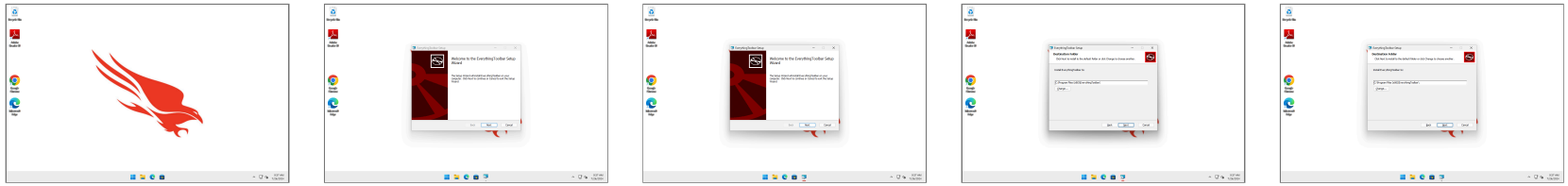
Informative 122

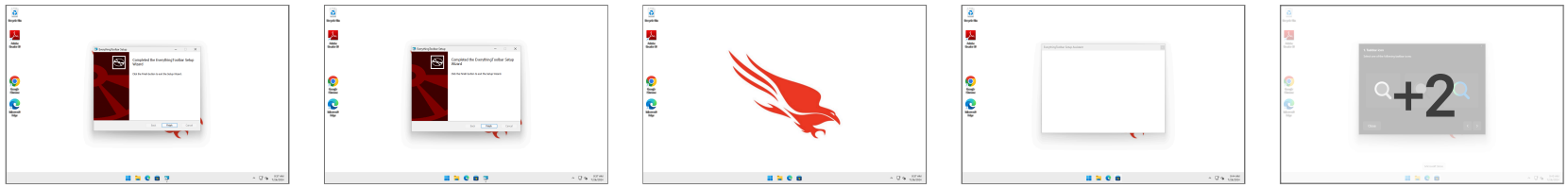
Process details

- msiexec.exe PID 3024
- msiexec.exe PID 10180
  - MsiExec.exe PID 6212
    - EverythingToolbar.Launcher.exe PID 4976

Screenshots

Show all Off





Network activity

Contacted hosts

IP address	Port	Protocol	Associated process	PID
20.72.205.209	443	TCP	taskhostw.exe	3024

1 result (1-1 shown) Items per page 5 Page 1 of 1

Suricata alerts

Events	Category	Description
224.0.0.22	Generic Protocol Command Decode	SURICATA IPv4 invalid checksum
224.0.0.22	Generic Protocol Command Decode	SURICATA IPv4 invalid checksum
192.168.0.255	Generic Protocol Command Decode	SURICATA IPv4 invalid checksum
224.0.0.22	Generic Protocol Command Decode	SURICATA IPv4 invalid checksum
192.168.0.255	Generic Protocol Command Decode	SURICATA UDPv4 invalid checksum

Extracted strings

Download extracted strings

EverythingToolbar-1.3.4.msi	109
EverythingToolbar.Launcher.exe	280
msiexec.exe	1
EverythingToolbar.log	1
x32uhste.newcfg	1
uejwpk3x.newcfg	1
screen_6.png	1

Extracted files

No verdict	3