Home (https://www.bleepingcomputer.com/)
> News (https://www.bleepingcomputer.com/news/)
> Security (https://www.bleepingcomputer.com/news/security/)
> Malware infiltrates Pidgin messenger's official plugin repository

Malware infiltrates Pidgin messenger's official plugin repository

By
Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)

August 27, 2024 01:25 PM 0

The Pidgin messaging app removed the ScreenShareOTR plugin from its official third-party plugin list after it was discovered that it was used to install keyloggers, information stealers, and malware commonly used to gain initial access to corporate networks.

The plugin was promoted as a screen-sharing tool for secure Off-The-Record (OTR) protocol and was available for both Windows and Linux versions of Pidgin.

According to ESET, the malicious plugin was configured to infect unsuspecting users with DarkGate malware (https://www.bleepingcomputer.com/news/security/darkgate-

and-pikabot-malware-emerge-as-qakbots-successors/), a powerful malware threat actors use to breach networks since QBot's dismantling by the authorities.

Sneaky Pidgin plugin

Pidgin is an open-source, cross-platform instant messaging client that supports multiple networks and messaging protocols.

Although not as popular as in the mid-2000s when multi-protocol clients were in high demand, it remains a popular choice among those seeking to consolidate their messaging accounts into a single app and has a dedicated user base of tech-savvy individuals, open-source enthusiasts, and users who need to connect to legacy IM systems.

Pidgin operates a plugin system that allows users to extend the program's functionality, enable niche features, and unlock new customization options.

Users can download them from the project's official third-party plugins list (https://pidgin.im/plugins/?publisher=all&query=&type=), currently hosting 211 addons.

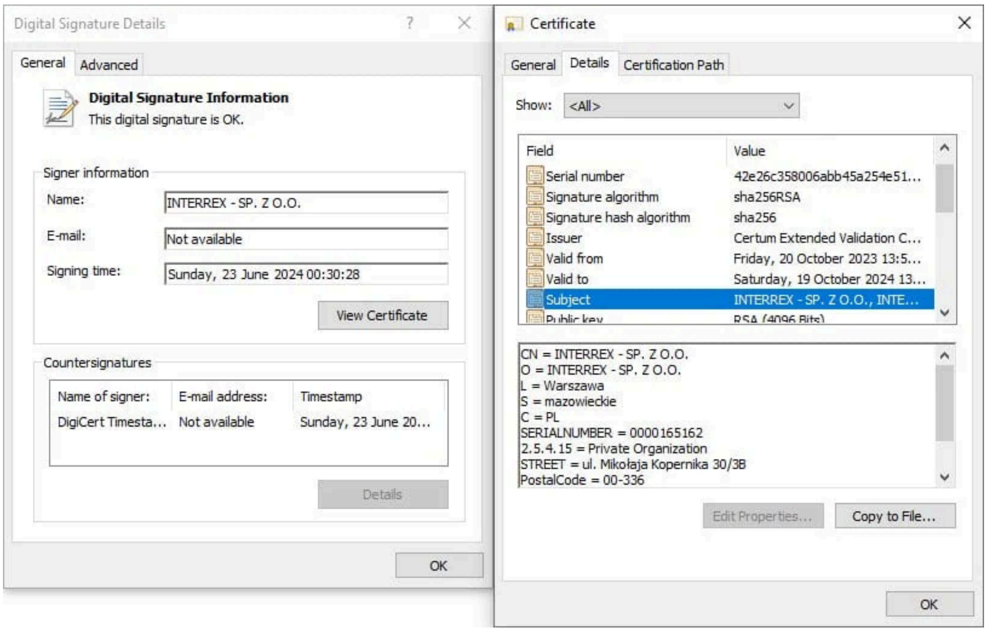
According to an announcement (http://pidgin.im/posts/2024-08-malicious-plugin/) on the project's website last week, a malicious plugin named 'ss-otr' had slipped into the list on July 6, 2024, and was only pulled on August 16 following a user report about it being a keylogger and screenshot capturing tool.

> "A plugin, ss-otr, was added to the third party plugins list on July 6th. On August 16th we received a report from 0xFFFC0000 that the plugin contained a key logger and shared screen shots with unwanted parties.
>
> We quietly pulled the plugin from the list immediately and started investigating. On August 22nd Johnny Xmas was able to confirm that a keylogger was present." – Pidgin

A red flag is that ss-otr only provided binaries for download and not any source code, but due to the lack of robust reviewing mechanisms in Pidgin's third-party plugin repository, nobody questioned its security.

Plugin leads to DarkGate malware

ESET reports (https://x.com/ESETresearch/status/1828114327976415445) the plugin installer is signed with a valid digital certificate issued to *INTERREX – SP. Z O.O.*, a legitimate Polish company.



Digital Signature Information
This digital signature is OK.

Signer information

Name:	INTERREX - SP. Z O.O.
E-mail:	Not available
Signing time:	Sunday, 23 June 2024 00:30:28

Countersignatures

Name of signer:	E-mail address:	Timestamp
DigiCert Timesta...	Not available	Sunday, 23 June 20...

Show: <All>

Field	Value
Serial number	42e26c358006abb45a254e51...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Certum Extended Validation C...
Valid from	Friday, 20 October 2023 13:5...
Valid to	Saturday, 19 October 2024 13...
Subject	INTERREX - SP. Z O.O., INTE...
Public key	RSA (4096 Bits)

```
CN = INTERREX - SP. Z O.O.
O = INTERREX - SP. Z O.O.
L = Warszawa
S = mazowieckie
C = PL
SERIALNUMBER = 0000165162
2.5.4.15 = Private Organization
STREET = ul. Mikołaja Kopernika 30/3B
PostalCode = 00-336
```

Signed executable
Source: ESET

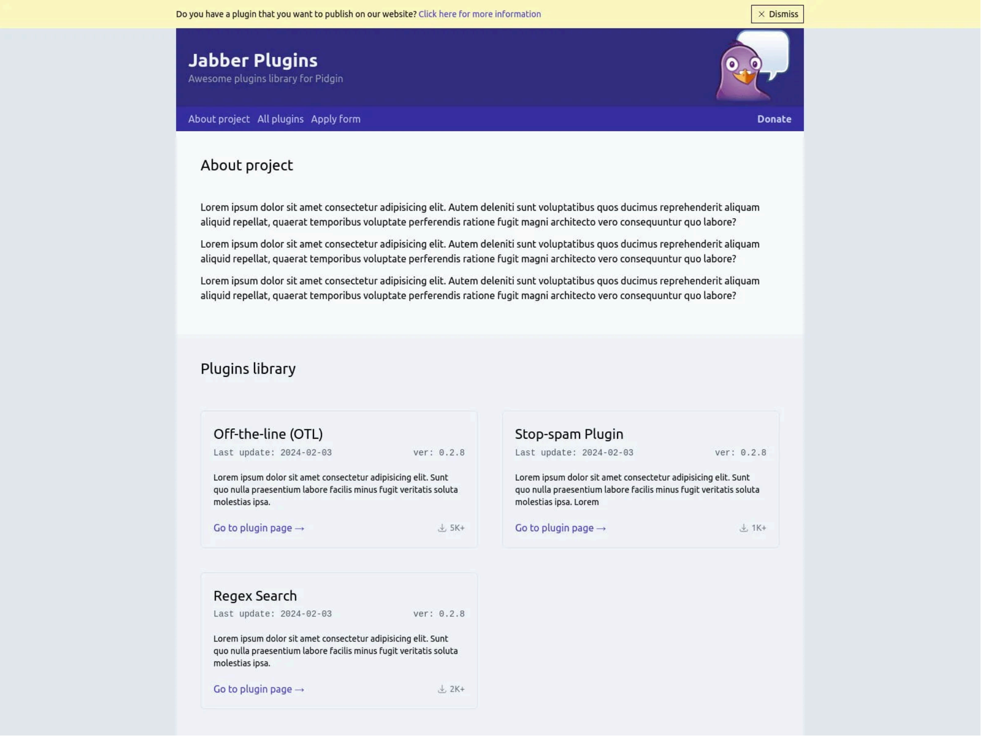
The plugin offers the advertised functionality of screen sharing but also contains malicious code, allowing it to download additional binaries from the attacker's server at jabberplugins[.]net.

The downloaded payloads are either PowerShell scripts or the DarkGate malware, which is also signed by an Interrex certificate.

A similar mechanism is implemented for the Linux version of the Pidgin client, so both platforms are covered.

ESET says that the same malicious server, which has been taken down now, hosted additional plugins named OMEMO, Pidgin Paranoia, Master Password, Window Merge, and HTTP File Upload.

These plugins were almost certainly also delivering DarkGate, indicating that ScreenShareOTR was just one small part of a broader-scale campaign.



Do you have a plugin that you want to publish on our website? Click here for more information

Jabber Plugins

Awesome plugins library for Pidgin

About project

Lorem ipsum dolor sit amet consectetur adipisicing elit. Autem deleniti sunt voluptatibus quos ducimus reprehenderit aliquam aliquid repellat, quaerat temporibus voluptate perferendis ratione fugit magni architecto vero consequuntur quo labore?

Lorem ipsum dolor sit amet consectetur adipisicing elit. Autem deleniti sunt voluptatibus quos ducimus reprehenderit aliquam aliquid repellat, quaerat temporibus voluptate perferendis ratione fugit magni architecto vero consequuntur quo labore?

Lorem ipsum dolor sit amet consectetur adipisicing elit. Autem deleniti sunt voluptatibus quos ducimus reprehenderit aliquam aliquid repellat, quaerat temporibus voluptate perferendis ratione fugit magni architecto vero consequuntur quo labore?

Plugins library

Off-the-line (OTL)
Last update: 2024-02-03 ver: 0.2.8

Lorem ipsum dolor sit amet consectetur adipisicing elit. Sunt quo nulla praesentium labore facilis minus fugit veritatis soluta molestias ipsa.

Stop-spam Plugin
Last update: 2024-02-03 ver: 0.2.8

Lorem ipsum dolor sit amet consectetur adipisicing elit. Sunt quo nulla praesentium labore facilis minus fugit veritatis soluta molestias ipsa. Lorem

Regex Search
Last update: 2024-02-03 ver: 0.2.8

Lorem ipsum dolor sit amet consectetur adipisicing elit. Sunt quo nulla praesentium labore facilis minus fugit veritatis soluta molestias ipsa.

Threat actor's website
Source: ESET

Those who installed it are recommended to remove it immediately and perform a full system scan with an antivirus tool, as DarkGate may be lurking on their system.

After publishing our story, Pidgin's maintainer and lead developer, Gary Kramlich, notified us on Mastodon (https://infosec.exchange/@grimmy@mastodon.social/113035335884182662) to say that they do not keep track of how many times a plugin is installed.

To prevent similar incidents from happening in the future, Pidgin announced that, from now on, it will only accept third-party plugins that have an OSI Approved Open Source License, allowing scrutiny into their code and internal functionality.

Update 8/27/24: Updated story to note that Pidgin does not keep track of plugin downloads.

Related Articles:

North Korean hackers exploit VPN update flaw to install malware (https://www.bleepingcomputer.com/news/security/north-korean-hackers-exploit-vpn-update-flaw-to-install-malware/)

Hackers are exploiting critical bug in LiteSpeed Cache plugin (https://www.bleepingcomputer.com/news/security/hackers-are-exploiting-critical-bug-in-litespeed-cache-plugin/)

Litespeed Cache bug exposes millions of WordPress sites to takeover attacks (https://www.bleepingcomputer.com/news/security/litespeed-cache-bug-exposes-millions-of-wordpress-sites-to-takeover-attacks/)

Russia blocks Signal for 'violating' anti-terrorism laws (https://www.bleepingcomputer.com/news/security/russia-blocks-signal-for-violating-anti-terrorism-laws/)

PKfail Secure Boot bypass lets attackers install UEFI malware (https://www.bleepingcomputer.com/news/security/pkfail-secure-boot-bypass-lets-attackers-install-uefi-malware/)

DARKGATE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/DARKGATE/)

MESSENGER (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/MESSENGER/)

PIDGIN (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PIDGIN/)

PLUGIN (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PLUGIN/)

SUPPLY CHAIN (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/SUPPLY-CHAIN/)

SUPPLY CHAIN ATTACK (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/SUPPLY-CHAIN-ATTACK/)

(https://www.bleepingcomputer.com/author/bill-toulas/)

BILL TOULAS (HTTPS://WWW.BLEEPINGCOMPUTER.COM/AUTHOR/BILL-TOULAS/)

✉ (MAILTO:BILL.TOULAS@BLEEPINGCOMPUTER.COM)
(HTTPS://TWITTER.COM/BILLTOULAS)

Bill Toulas is a tech writer and infosec news reporter with over a decade of experience working on various online publications, covering open-source, Linux, malware, data breach incidents, and hacks.

‹ PREVIOUS ARTICLE

(HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/MICROSOFT/WINDOWS-DOWNDATE-TOOL-LETS-YOU-UNPATCH-WINDOWS-SYSTEMS/)

NEXT ARTICLE ›

(HTTPS://WWW.BLEEPINGCOMPUTER.COM/OFFER/DEALS/TH 70-COURSE-DEAL-HELPS-YOU-START-A-JOURNEY-IN-CYBERSECURITY/)

Post a Comment

Community Rules (https://www.bleepingcomputer.com/posting-guidelines/)

You need to login in order to post a comment

Login

Not a member yet? Register Now (https://www.bleepingcomputer.com/forums/index.php?app=core&module=global&section=register)

POPULAR STORIES

Windows Downdate tool lets you 'unpatch' Windows systems

(https://www.bleepingcomputer.com/news/microsoft/windows-downdate-tool-lets-you-unpatch-windows-systems/)

DICK'S shuts down email, locks employee accounts after cyberattack

(https://www.bleepingcomputer.com/news/security/dicks-shuts-down-email-locks-employee-accounts-after-cyberattack/)

FOLLOW US:

[illegible]

MAIN SECTIONS

News (https://www.bleepingcomputer.com/)

VPN Buyer Guides (https://www.bleepingcomputer.com/vpn/)

SysAdmin Software Guides (https://www.bleepingcomputer.com/sysadmin/)

Downloads (https://www.bleepingcomputer.com/download/)

Virus Removal Guides (https://www.bleepingcomputer.com/virus-removal/)

Tutorials (https://www.bleepingcomputer.com/tutorials/)

Startup Database (https://www.bleepingcomputer.com/startups/)

Uninstall Database (https://www.bleepingcomputer.com/uninstall/)

Glossary (https://www.bleepingcomputer.com/glossary/)

COMMUNITY

Forums (https://www.bleepingcomputer.com/forums/)

Forum Rules (https://www.bleepingcomputer.com/forum-rules/)

Chat (https://www.bleepingcomputer.com/forums/t/730914/the-bleepingcomputer-official-discord-chat-server-come-join-the-fun/)

USEFUL RESOURCES

Welcome Guide (https://www.bleepingcomputer.com/welcome-guide/)

Sitemap (https://www.bleepingcomputer.com/sitemap/)

COMPANY

About BleepingComputer (https://www.bleepingcomputer.com/about/)

Contact Us (https://www.bleepingcomputer.com/contact/)

Send us a Tip! (https://www.bleepingcomputer.com/news-tip/)

Advertising (https://www.bleepingcomputer.com/advertise/)

Write for BleepingComputer (https://www.bleepingcomputer.com/write-for-bleepingcomputer/)

Social & Feeds (https://www.bleepingcomputer.com/rss-feeds/)

Changelog (https://www.bleepingcomputer.com/changelog/)

Terms of Use (https://www.bleepingcomputer.com/terms-of-use/) - Privacy Policy (https://www.bleepingcomputer.com/privacy/) - Ethics Statement (https://www.bleepingcomputer.com/ethics-statement/) - Affiliate Disclosure (https://www.bleepingcomputer.com/affiliate-disclosure/)