

[Home \(https://www.bleepingcomputer.com/\)](https://www.bleepingcomputer.com/) > [News \(https://www.bleepingcomputer.com/news/\)](https://www.bleepingcomputer.com/news/)  
> [Security \(https://www.bleepingcomputer.com/news/security/\)](https://www.bleepingcomputer.com/news/security/)  
> Evilnum hackers return in new operation targeting migration orgs

---

## Evilnum hackers return in new operation targeting migration orgs

---

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

June 28, 2022

05:49 PM

0

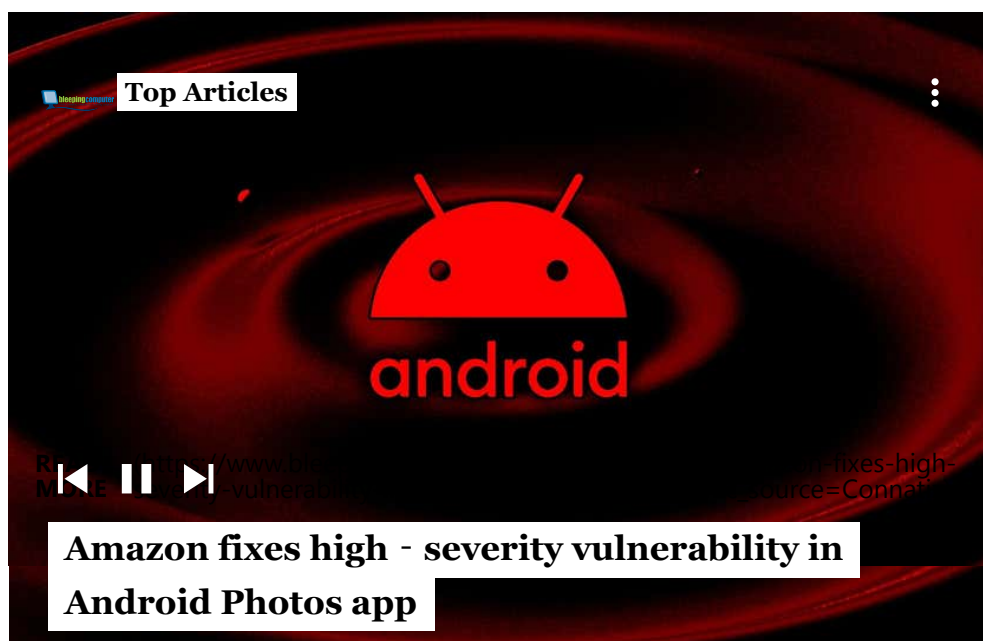


The Evilnum hacking group is showing renewed signs of malicious activity, targeting European organizations that are involved in international migration.

Evilnum is an APT (advanced persistent threat) that has been active since at least 2018 and had its campaign and tools exposed only recently, in 2020.



At that time, ESET published a technical report describing the threat group's tactics against companies in the financial technology sector, using custom, "homemade" malware.



The latest exposure is thanks to the work of Zscaler's analysts (<https://www.zscaler.com/blogs/security-research/return-evilnum-apt-updated-ttps-and-new-targets>), who tracked Evilnum's activity since the beginning of 2022, capturing various artifacts from the attacks.

## Campaign details

The targeting and the timing coincided with the Russian invasion of Ukraine, with key migration organizations receiving malicious emails containing macro-laden documents.

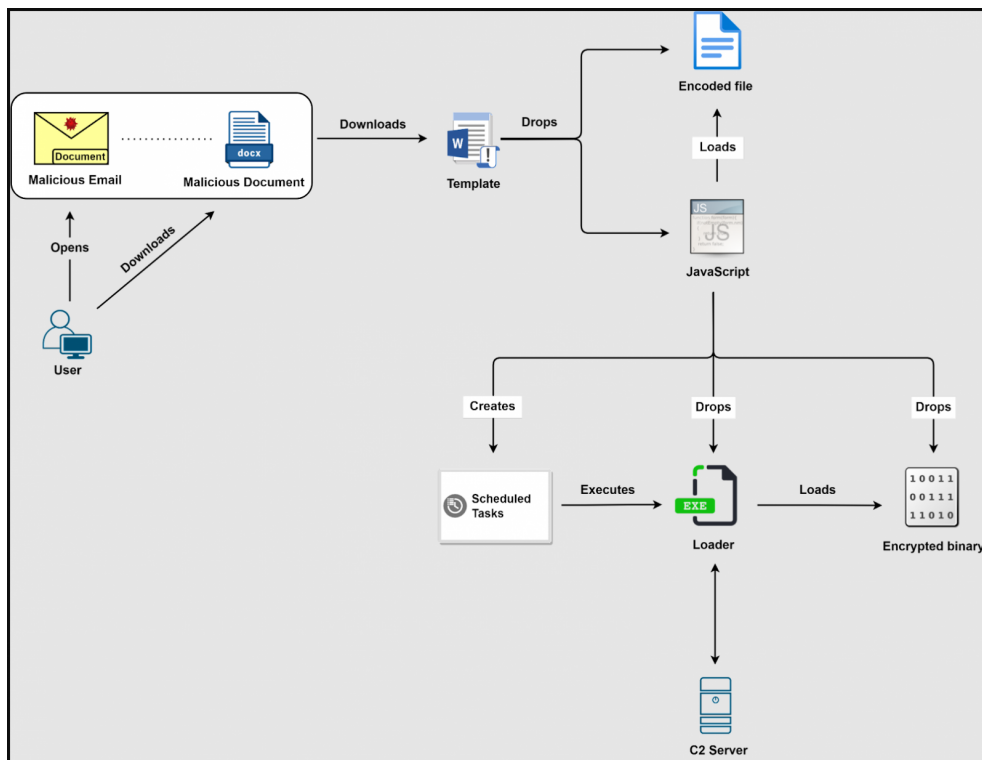




The documents used in the campaign carry varying filenames, usually containing the term "compliance." Zscaler identified at least nine different documents, all mentioned in the IoC section of the report.

The attachment leverage the template injection and VBA code stomping technique to evade detection, leading to the execution of heavily obfuscated JavaScript.

This, in turn, decrypts and drops a malware loader ("SerenadeDACplApp.exe") and an encrypted binary ("devZUQVD.tmp"), and also creates a scheduled task ("UpdateModel Task") for persistence.



Evilnum recent attack flow (Zscaler)

The loader performs preliminary checks and loads the binary under an extracted file name. The binary injection is done using the old "Heaven's gate" technique

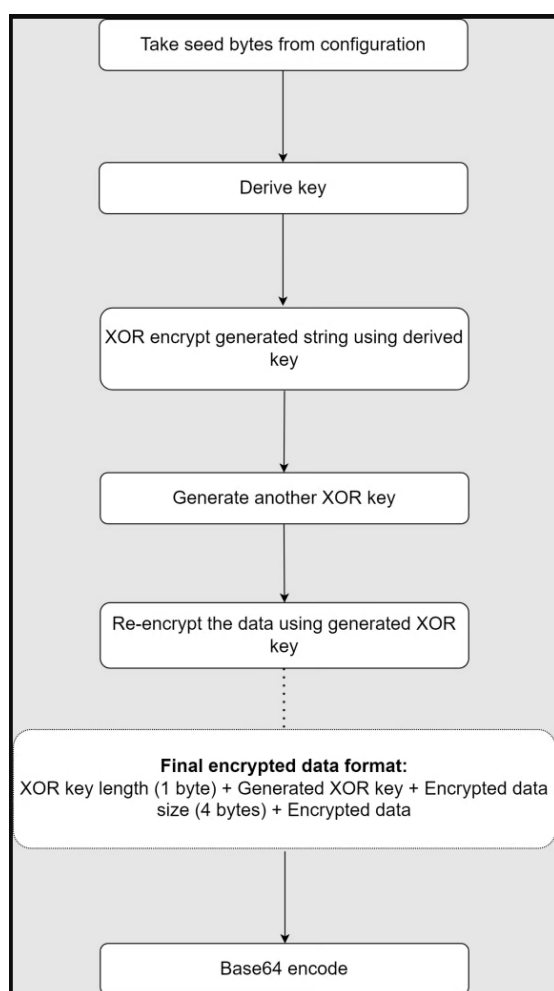
(<https://www.bleepingcomputer.com/news/security/malware-loader-goes-through-heavens-gate-to-avoid-detection/>) to evade AV detection.



This technique involves invoking 64-bit code in 32-bit processes, and while it has been mitigated in Windows 10, Evilnum still likely uses it to target machines running older OS versions.

The backdoor that is loaded on the compromised system executes to perform the following operations:

- Decrypts the backdoor configuration (C2 domains, User Agent strings, network paths, referrer strings, cookies type strings).
- Resolves API addresses from the libraries retrieved from the configuration
- Performs a mutex check
- Builds data exfiltration string to be sent as part of the beacon request
- Encrypt and encode the generated string with Base64
- Embed the encoded string inside the cookie header field by selecting one of the cookie type strings from the configuration.



**The data encryption process (Zscaler)**

Once all steps are finished, the backdoor picks a C2 domain and a path string from the configuration and sends a beacon network request. The C2 may answer with a new encrypted payload.

Additionally, the backdoor captures machine snapshots and sends them to the C2 via POST requests, exfiltrating stolen data in an encrypted form.



This report highlights that Evilnum is still an active threat, so defenders are advised to use the IoCs provided by Zscaler to protect their networks.

While the actor's origin remains unknown, its most recent victimology indicates a state-level interest in espionage campaigns, which was researchers previously linked (<https://www.bleepingcomputer.com/news/security/phishing-attacks-target-countries-aiding-ukrainian-refugees/>) to the Belarusian threat group "Ghostwriter."

## Related Articles:

Fake antivirus updates used to deploy Cobalt Strike in Ukraine  
(<https://www.bleepingcomputer.com/news/security/fake-antivirus-updates-used-to-deploy-cobalt-strike-in-ukraine/>)

Google Drive now warns you of suspicious phishing, malware docs  
(<https://www.bleepingcomputer.com/news/google/google-drive-now-warns-you-of-suspicious-phishing-malware-docs/>)

Microsoft Exchange servers hacked by new ToddyCat APT gang  
(<https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-by-new-toddycat-apt-gang/>)

Chinese hacking group Aoqin Dragon quietly spied orgs for a decade  
(<https://www.bleepingcomputer.com/news/security/chinese-hacking-group-aoqin-dragon-quietly-spied-orgs-for-a-decade/>)

Qbot malware now uses Windows MSDT zero-day in phishing attacks  
(<https://www.bleepingcomputer.com/news/security/qbot-malware-now-uses-windows-msdt-zero-day-in-phishing-attacks/>)

---

APT ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/APT/](https://www.bleepingcomputer.com/tag/apt/))

EVILNUM ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/EVILNUM/](https://www.bleepingcomputer.com/tag/evilnum/))

HACKING GROUP ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/HACKING-GROUP/](https://www.bleepingcomputer.com/tag/hacking-group/))

IMMIGRATION ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/IMMIGRATION/](https://www.bleepingcomputer.com/tag/immigration/))

MALWARE ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/MALWARE/](https://www.bleepingcomputer.com/tag/malware/))

PHISHING ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PHISHING/](https://www.bleepingcomputer.com/tag/phishing/))

---

