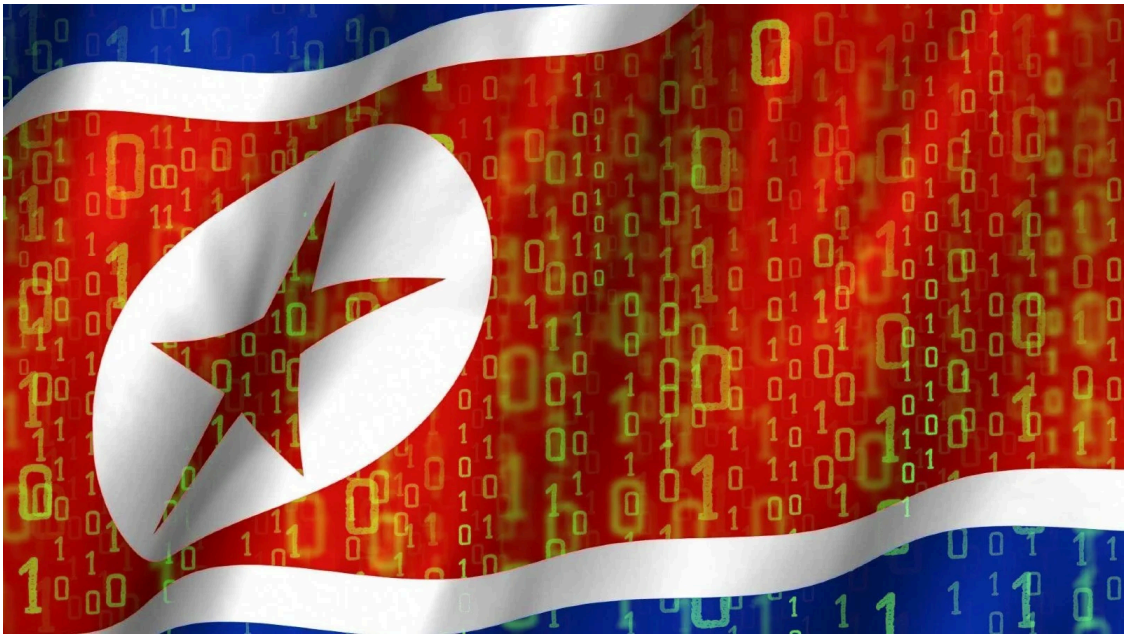
North Korean hackers attack EU targets with Konni RAT malware

By Bill Toulas

Published: 2022-07-23 · Archived: 2026-04-05 13:40:13 UTC

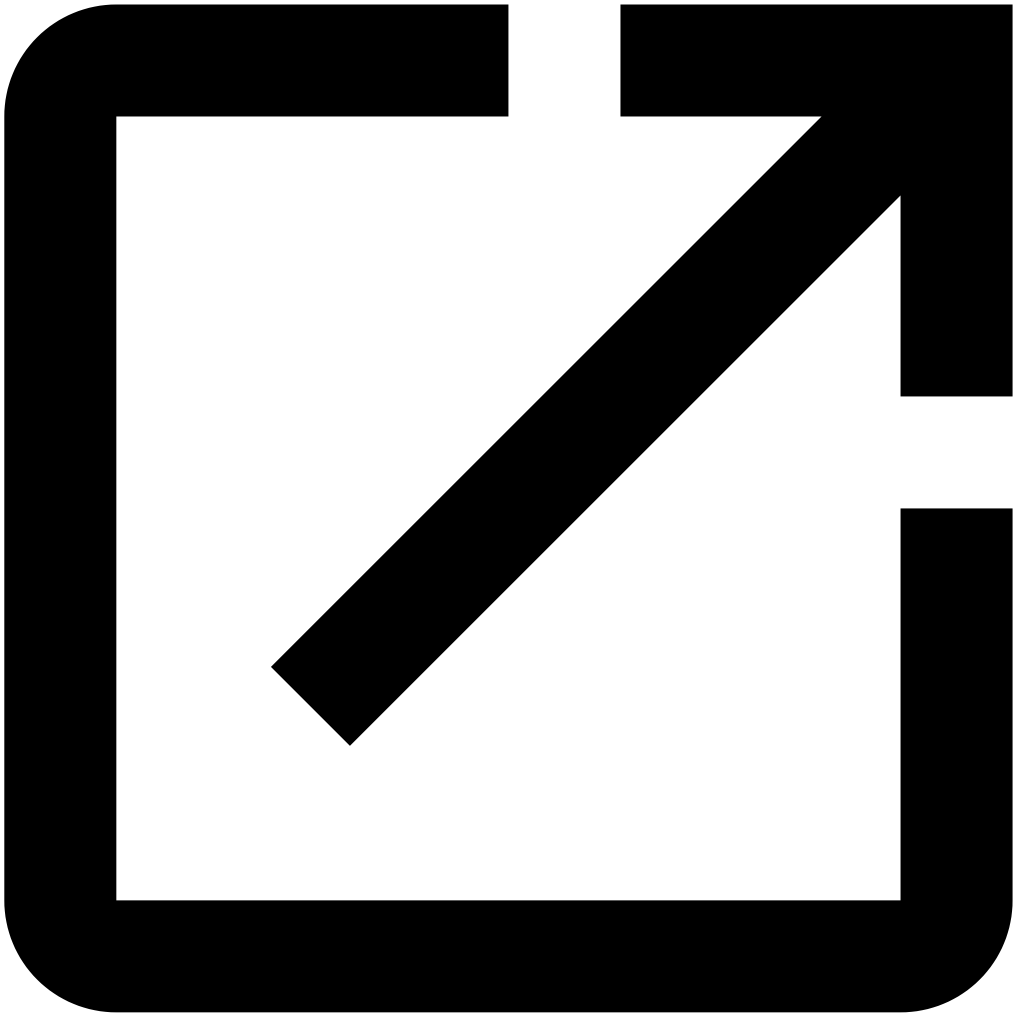


Threat analysts have uncovered a new campaign attributed to APT37, a North Korean group of hackers, targeting high-value organizations in the Czech Republic, Poland, and other European countries.

In this campaign, the hackers use malware known as Konni, a remote access trojan (RAT) capable of establishing persistence and performing privilege escalation on the host.

Konni has been associated with North Korean cyberattacks since 2014, and most recently, it was seen in a spear-phishing campaign targeting the Russian Ministry of Foreign Affairs.


DIE LINKE.
0:00

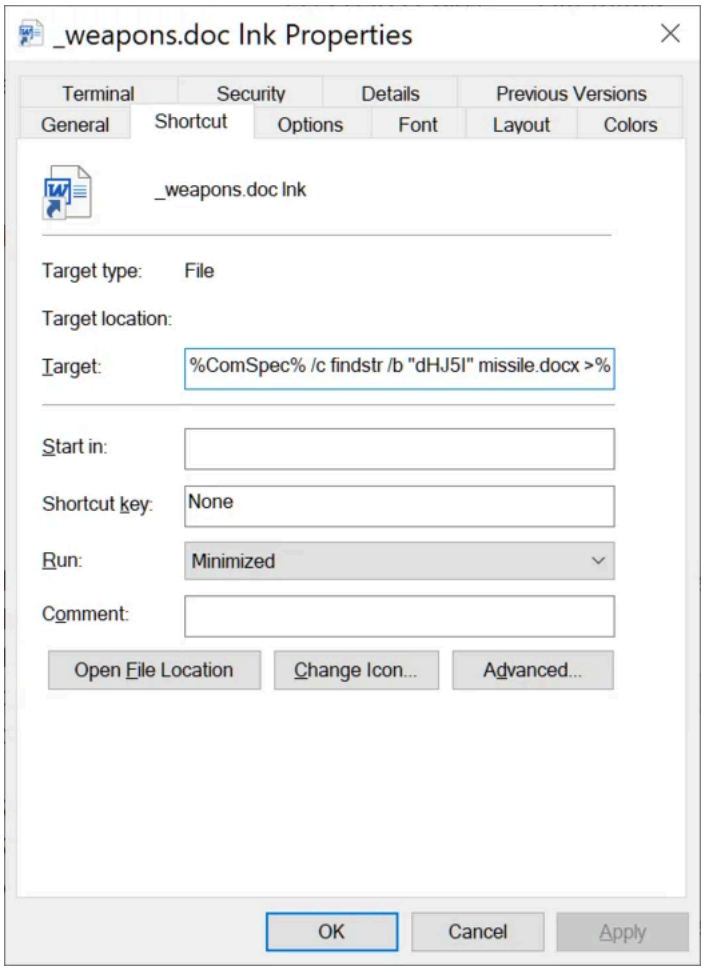


The latest and still ongoing campaign was observed and analyzed by researchers at Securonix, who call it STIFF#BIZON, and resembles tactics and methods that match the operational sophistication of an APT (advanced persistent threat).

The STIFF#BIZON campaign

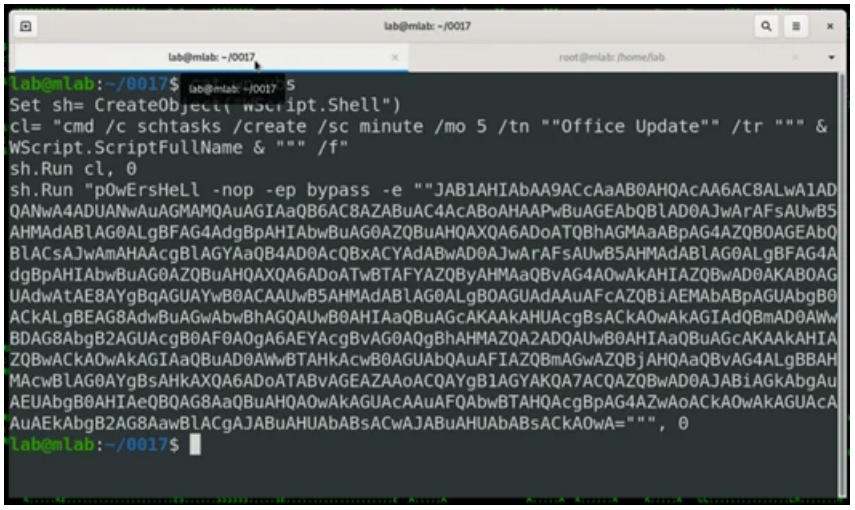
The attack begins with the arrival of a phishing email with an archive attachment containing a Word document (missile.docx) and a Windows Shortcut file (_weapons.doc.lnk.lnk).

When the LNK file is opened, code runs to find a base64-encoded PowerShell script in the DOCX file to establish C2 communication and download two additional files, 'weapons.doc' and 'wp.vbs'.



Properties of the malicious shortcut file

The downloaded document is a decoy, supposedly a report from Olga Bozheva, a Russian war correspondent. At the same time, the VBS file runs silently in the background to create a scheduled task on the host.

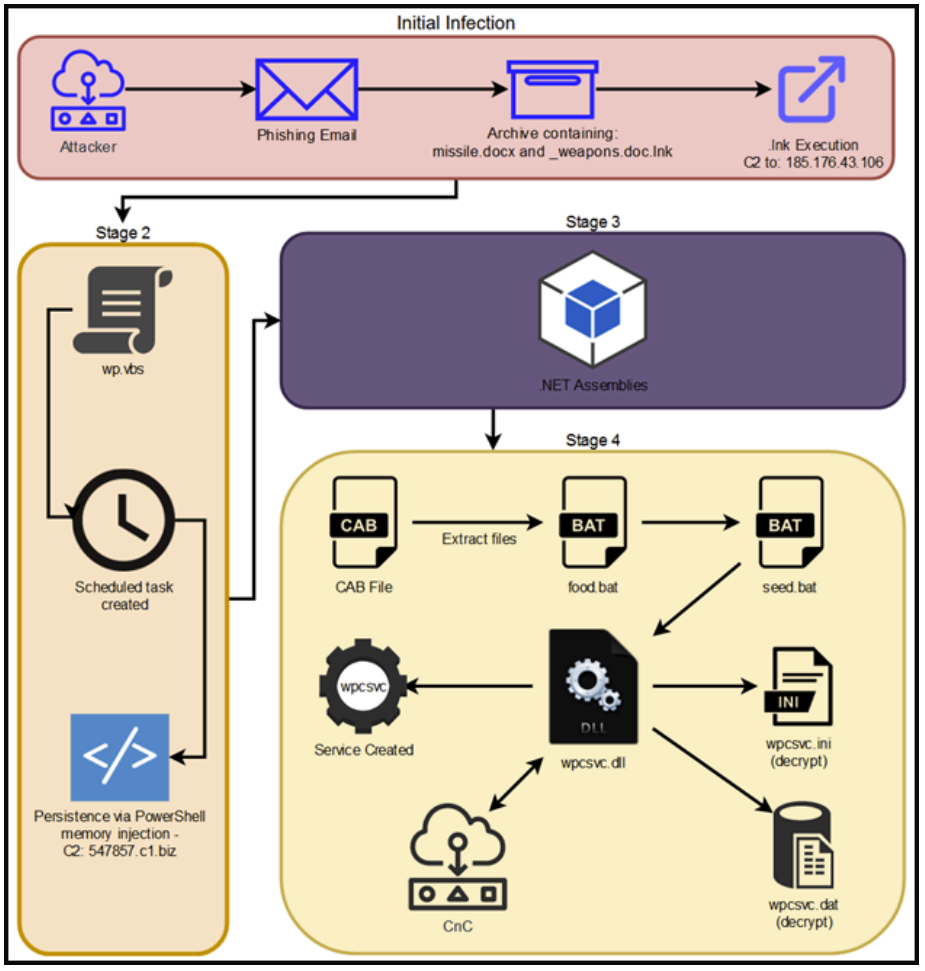


Base64-encoded PowerShell adds scheduled task *(Securonix)*

At this phase of the attack, the actor has already loaded the RAT and established a data exchange link, and is capable of performing the following actions:

- Capture screenshots using the Win32 GDI API and exfiltrate them in GZIP form.
- Extract state keys stored in the Local State file for cookie database decryption, useful in MFA bypassing.
- Extract saved credentials from the victim's web browsers.
- Launch a remote interactive shell that can execute commands every 10 seconds.

In the fourth stage of the attack, as shown in the diagram below, the hackers download additional files that support the function of the modified Konni sample, fetching them as compressed ".cab" archives.



Infection chain diagram *(Securonix)*

These include DLLs that replace legitimate Windows service libraries like the "wpcsvc" in System32, which is leveraged for executing commands in the OS with higher user privileges.

Possible links to APT28

While the tactics and toolset point to APT37, Securonix underscores the possibility of APT28 (aka FancyBear) being behind the STIFF#BIZON campaign.

"There seems to be a direct correlation between IP addresses, hosting provider, and hostnames between this attack and historical data we've previously seen from FancyBear/APT28," concludes the report.

State-sponsored threat groups often attempt to mimic the TTPs of other skillful APTs to obscure their trace and mislead threat analysts, so the chances of misattribution, in this case, are significant.
