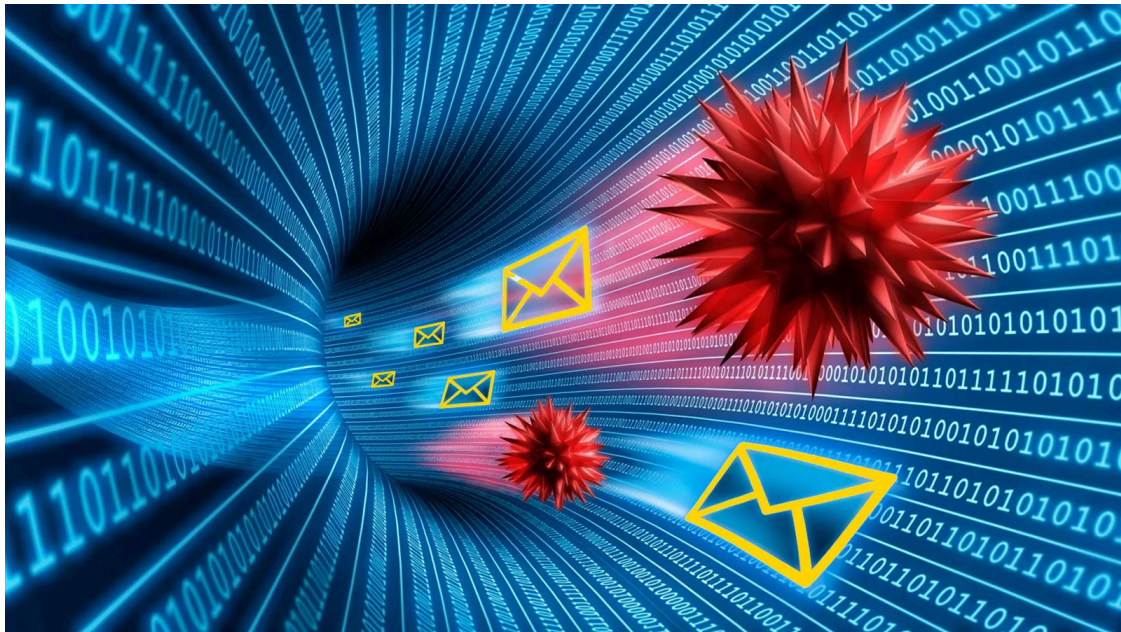


Fake antivirus updates used to deploy Cobalt Strike in Ukraine

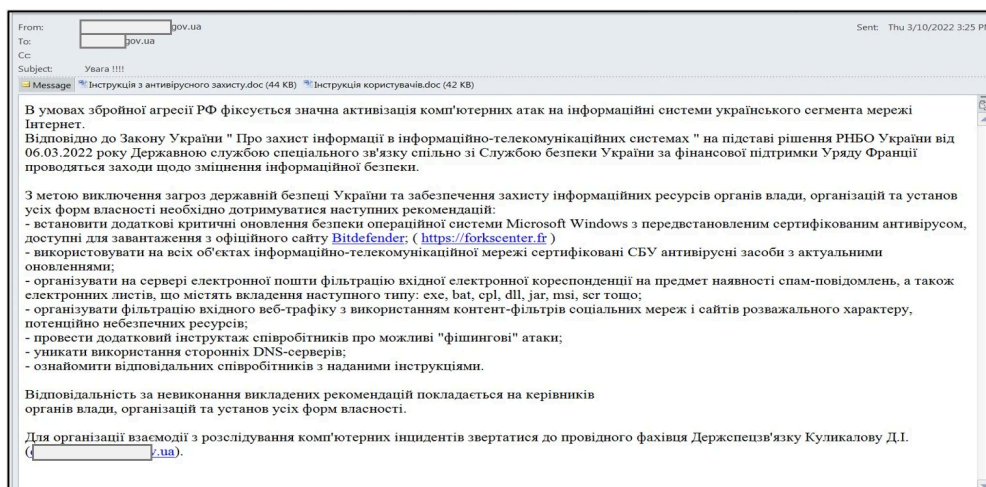
By Bill Toulas

Published: 2022-03-14 · Archived: 2026-04-05 14:40:17 UTC



Ukraine's Computer Emergency Response Team is warning that threat actors are distributing fake Windows antivirus updates that install Cobalt Strike and other malware.

The phishing emails impersonate Ukrainian government agencies offering ways to increase network security and advise recipients to download "critical security updates," which come in the form of a 60 MB file named "BitdefenderWindowsUpdatePackage.exe."

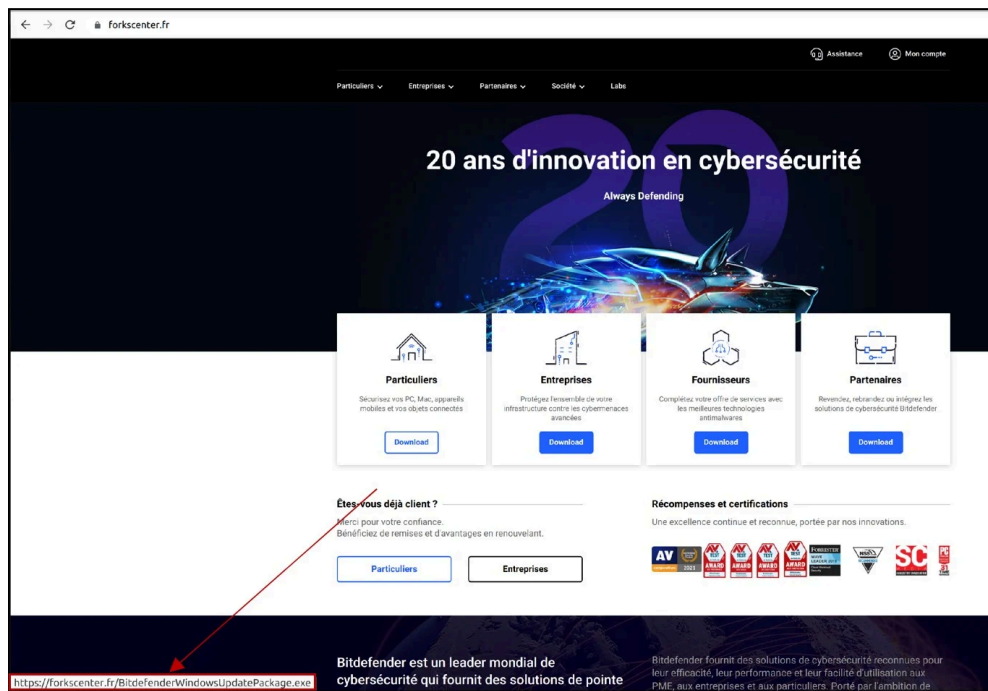


Phishing email urging the download of a fake AV updatер (CERT-UA)

These emails contain a link to a French website (now offline) that offers download buttons for the alleged AV software updates. Another website, nirsoft[.]me, was also [discovered by MalwareHunterTeam](#) to be acting as the command and control server for this campaign.



Visit Advertiser website [GO TO PAGE](#)



Malware-delivering website

Source: CERT-UA

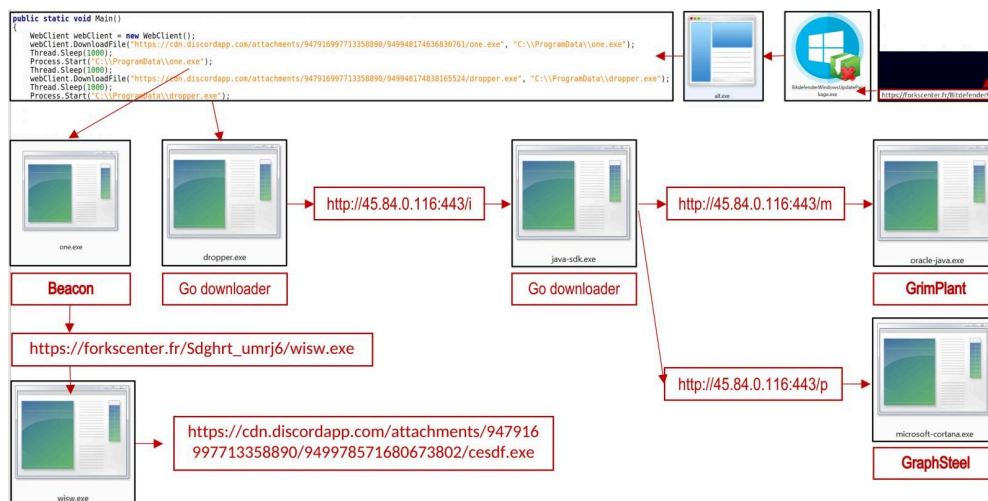
When a victim downloads and run this fake BitDefender Windows update [VirusTotal], the screen below will be shown prompting the users to install a 'Windows Update Package.'

However, this 'update' actually downloads and installs the one.exe file [VirusTotal] from the Discord CDN, which is a Cobalt Strike beacon.

Cobalt Strike is a widely abused penetration testing suite that offers offensive security capabilities, facilitates lateral network movement, and ensures persistence.

The same process fetches a Go downloader (dropper.exe) which decodes and executes a base-64-encoded file (java-sdk.exe).

This file adds a new Windows registry key for persistence and also downloads two more payloads, the GraphSteel backdoor (microsoft-cortana.exe) and GrimPlant backdoor (oracle-java.exe).



The infection chain of the uncovered campaign (CERT-UA)

All executables in the campaign are packed on the Themida tool, which protects them from reverse engineering, detection, and analysis.

Go payloads

Both GraphSteel and GrimPlant are malware written in Go, a versatile and [cross-platform](#) programming language with minimal footprint and low AV detection rates.

The capabilities of the two tools cover network reconnaissance, command execution, and file operations, so the fact that both are deployed in the same system is likely done for redundancy.

GraphSteel features:

- Gather hostname, username, and IP address information
- Execute commands
- Steal account credentials
- Use WebSocket and GraphQL to communicate with C2 using AES and base64 encryption

GrimPlant capabilities:

- Gather IP address, hostname, OS, username, home dir
- Execute commands received remotely and return results to C2
- Use gRPC (HTTP/2+SSL) for C2 communication

Not many technical details have been provided on these two payloads, and we can't exclude the possibility of them being known backdoors given new names in this report.

Attribution

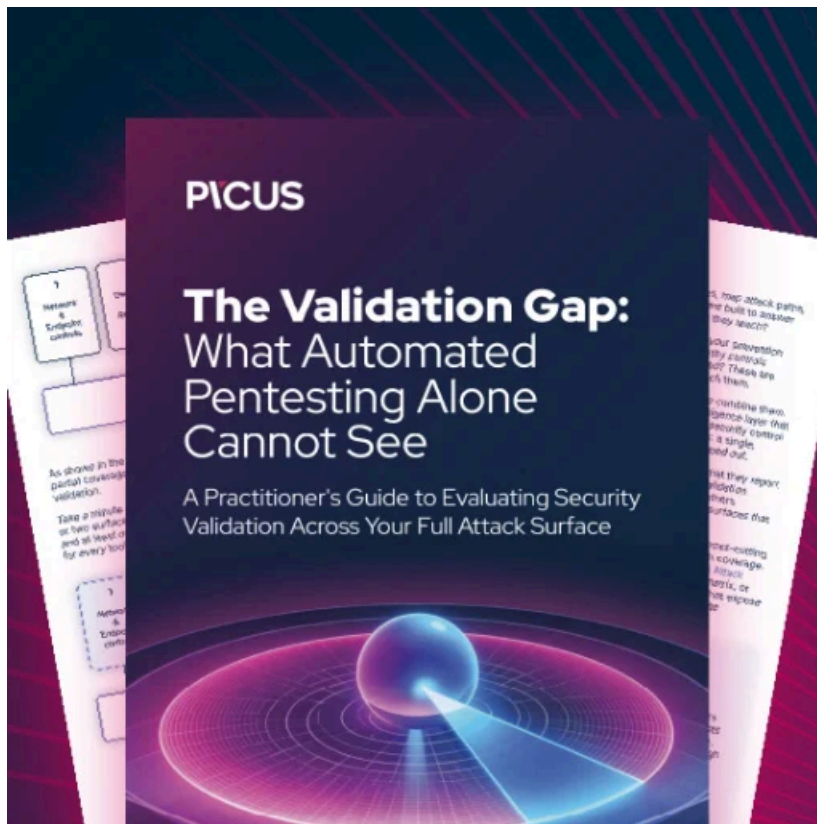
Given the current situation in Ukraine, it's easy to attribute all hostile activity to Russian and pro-Russian threat actors, and this seems to be the case here too.

The Ukrainian Computer Emergency Response Team [associates](#) the detected activity with the UAC-0056 group with medium confidence.

UAC-0056, also known as "Lorec53", is a sophisticated Russian-speaking APT that uses a combination of phishing emails and custom backdoors to collect information from Ukrainian organizations.

UAC-0056 was spotted ramping up its phishing distribution and network compromise efforts in Ukraine [since December 2021](#).

The same actor was spotted targeting [Georgian government](#) agencies with phishing lures in the recent past, so there's a high level of coordination and alignment with the [interests](#) of the Russian state.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/fake-antivirus-updates-used-to-deploy-cobalt-strike-in-ukraine/>