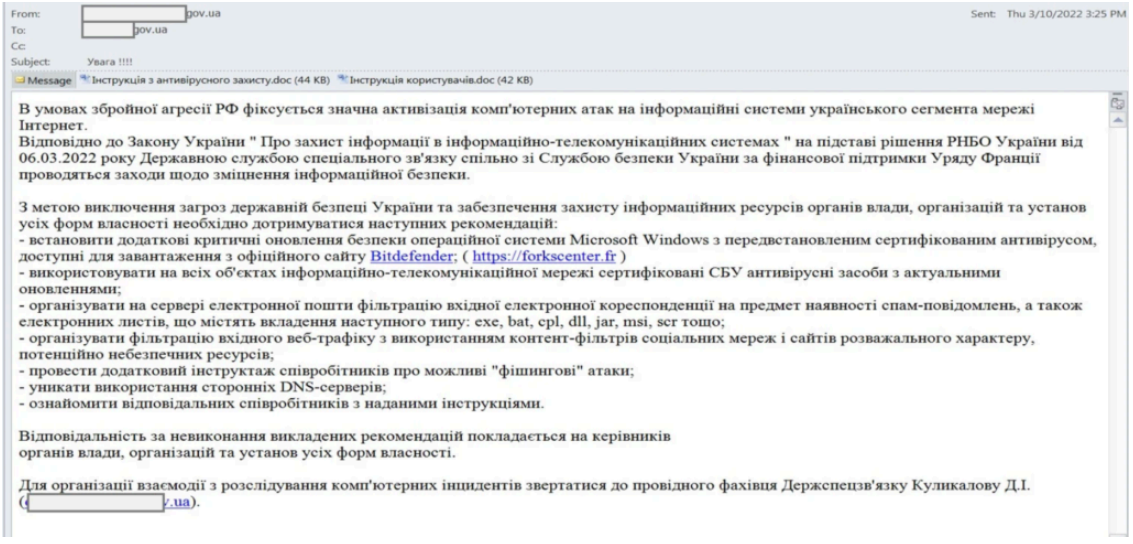
Ukraine’s CERT Warns Threat Actors For Fake AV Updates - Security Investigation

By BalaGanesh

Published: 2022-03-15 · Archived: 2026-04-05 18:46:09 UTC

Ukraine’s Computer Emergency Response Team is cautioning that threat actors are dispersing counterfeit Windows antivirus updates that introduce Cobalt Strike and other malware. The phishing messages imitate Ukrainian government offices offering ways of expanding network security and encourage beneficiaries to download “security updates,” which come as a 60 MB record named “**BitdefenderWindowsUpdatePackage.exe**.”



From: [redacted]gov.ua
To: [redacted]gov.ua
Cc:
Subject: Увага !!!!
Sent: Thu 3/10/2022 3:25 PM
Message | Інструкція з антивірусного захисту.doc (44 KB) | Інструкція користувачів.doc (42 KB)

В умовах збройної агресії РФ фіксується значна активізація комп'ютерних атак на інформаційні системи українського сегмента мережі Інтернет.
Відповідно до Закону України " Про захист інформації в інформаційно-телекомунікаційних системах " на підставі рішення РНБО України від 06.03.2022 року Державною службою спеціального зв'язку спільно зі Службою безпеки України за фінансової підтримки Уряду Франції проводяться заходи щодо зміцнення інформаційної безпеки.

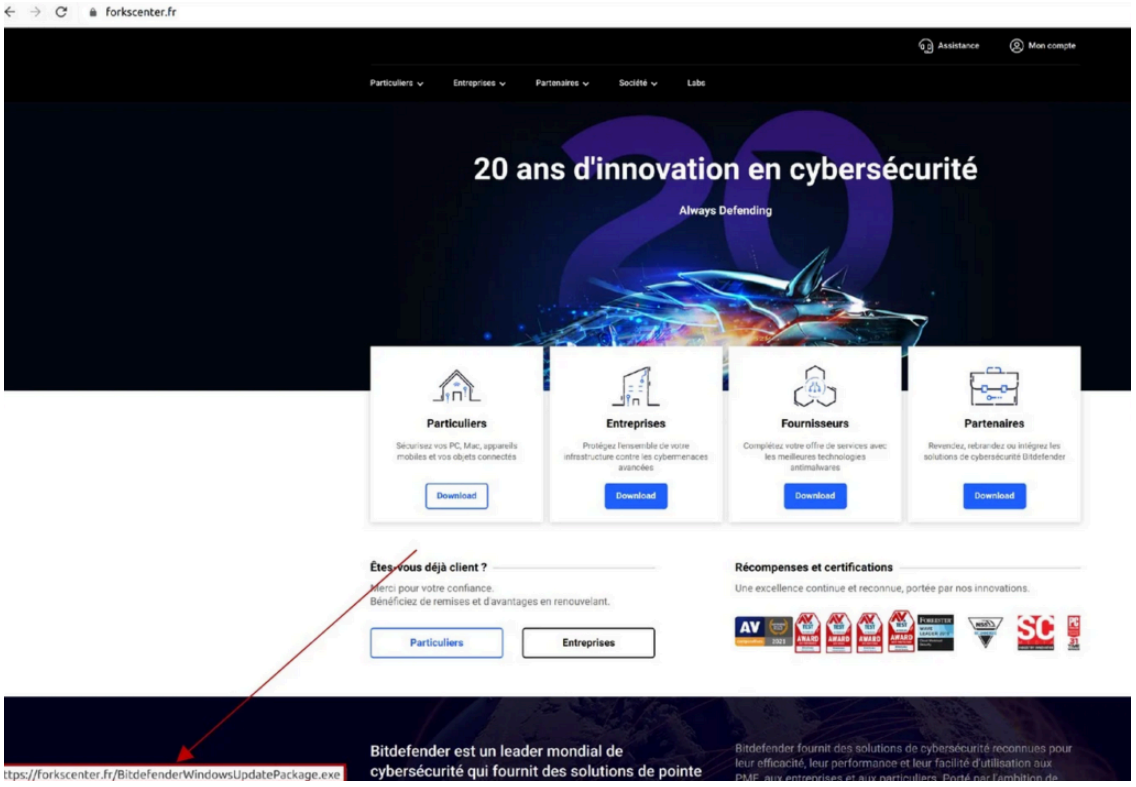
З метою виключення загроз державній безпеці України та забезпечення захисту інформаційних ресурсів органів влади, організацій та установ усіх форм власності необхідно дотримуватися наступних рекомендацій:
- встановити додаткові критичні оновлення безпеки операційної системи Microsoft Windows з передвстановленим сертифікованим антивірусом, доступні для завантаження з офіційного сайту Bitdefender; (https://forkscenter.fr)
- використовувати на всіх об'єктах інформаційно-телекомунікаційної мережі сертифіковані СБУ антивірусні засоби з актуальними оновленнями;
- організувати на сервері електронної пошти фільтрацію вхідної електронної кореспонденції на предмет наявності спам-повідомлень, а також електронних листів, що містять вкладення наступного типу: exe, bat, cpl, dll, jar, msi, scr тощо;
- організувати фільтрацію вхідного веб-трафіку з використанням контент-фільтрів соціальних мереж і сайтів розважального характеру, потенційно небезпечних ресурсів;
- провести додатковий інструктаж співробітників про можливі "фішингові" атаки;
- уникати використання сторонніх DNS-серверів;
- ознайомити відповідальних співробітників з наданими інструкціями.

Відповідальність за невиконання викладених рекомендацій покладається на керівників органів влади, організацій та установ усіх форм власності.

Для організації взаємодії з розслідування комп'ютерних інцидентів звертатися до провідного фахівця Держспецзв'язку Куликалову Д.І. ([redacted]v.ua).

CERT-UA

These messages contain a connection to a French site (presently disconnected) that offers download buttons for the supposed Antivirus updates. Another site, **nirsoft[.]me**, was likewise found by **MalwareHunterTeam** to be going about as the command and control server for this mission.



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.' In any case, this 'update' really downloads and introduces the one.exe document [VirusTotal] from the Discord CDN, which is a Cobalt Strike reference point.

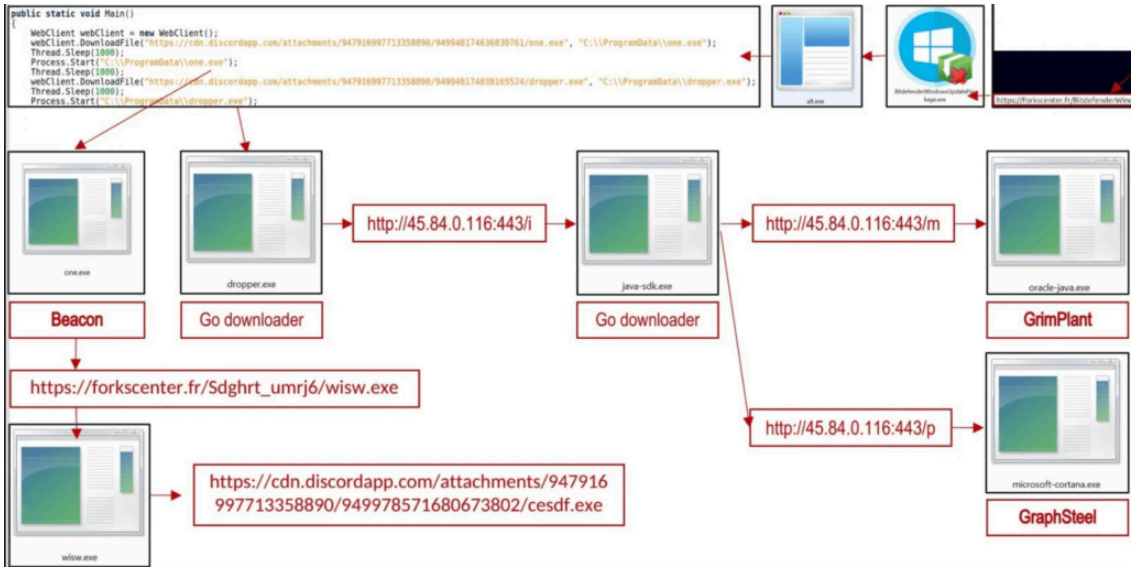
In any case, this 'update' really downloads and introduces the one.exe document [VirusTotal] from the Discord CDN, which is a Cobalt Strike reference point.

Cobalt Strike is a penetration testing suite that offers hostile security capacities, works with sidelong organization development, and guarantees perseverance.

A similar interaction gets a Go downloader (dropper.exe) which disentangles and executes a base-64-encoded record (java-sdk.exe).

This document adds another Windows registry key for persistence and furthermore downloads two additional payloads, the GraphSteel backdoor (microsoft-cortana.exe) and GrimPlant indirect access (oracle-java.exe).

All executables in the mission are pressed on the Themida tool, which shields them from reverse engineering, detection, and analysis.



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

GraphSteel and GrimPlant Malware payloads are written in GO. This program has minimal impression and low AV identification 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

Indicator of Compromise:

https://forkscenter[.]fr/Sdghrt_umrj6/wisw[.]exe
https://forkscenter[.]fr/
https://cdn[.]discordapp[.]com/attachments/947916 997713358890/949978571680673802/cesdf[.]exe
http://45[.]84[.]0[.]116:443/i
http://45[.]84[.]0[.]116:443/m
http://45[.]84[.]0[.]116:443/p
https://cdn[.]discordapp[.]com/attachments/947916997713358890/949948174838165524/dropper[.]exe
https://cdn[.]discordapp[.]com/attachments/947916997713358898/949948174636830761/one[.]exe

C:\ProgramData\dropper[.]exe
C:\ProgramData\one[.]exe

The Ukrainian Computer Emergency Response Team connects the recognized movement with the UAC-0056 gathering with medium certainty.UAC-0056, otherwise called “Lorec53”, is a modern Russian-speaking APT that utilizes a blend of phishing messages and custom backdoors to gather data from Ukrainian associations.

(Source: Bleeping computer & CERT-UA)
