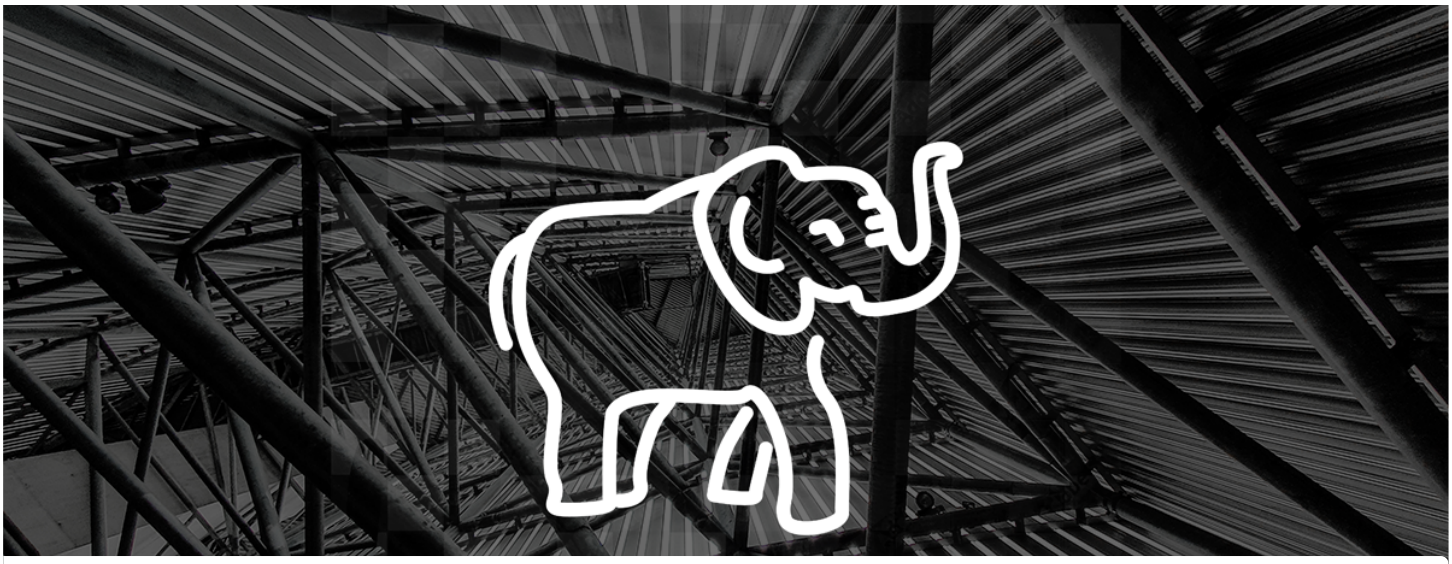


#Threat Research #Cybersecurity Awareness #Managed Detection and Response

By **Martin Zugec** / Apr 25, 2022

Deep Dive into the Elephant Framework – A New Cyber Threat in Ukraine

At the beginning of the invasion of Ukraine, we released a security advisory with recommendations based on different risk tiers. Since then, our Threat Intelligence (TI) and Managed Detection and Response (MDR) teams have been actively monitoring the situation and identifying active threats. Not surprisingly, the highest risk group contains businesses and organizations located in Ukraine, especially government entities and critical infrastructure.

One of the groups actively engaged in pro-Russian cyber-attacks is **UAC-0056.** This group has been active since at least March 2021, and its primary objective seems to be cyber espionage with a focus on key state sectors. Other names for this group are Lorec53, UNC2589, EmberBear, LorecBear, BleedingBear, SaintBear, and TA471.

This group has been associated with attacks using OutSteel and GraphSteel stealers (malicious software designed to steal data). OutSteel was written in the AutoIt language, while GraphSteel was written in the Go language (often referred to as Golang). While both languages are known for their ease of use, AutoIt is a simpler language often used by system administrators and scripters. The behavior of Go-based GraphSteel is also more sophisticated – while its primary purpose is harvesting credentials, it is also

currently. The original announcement by the Computer Emergency Response Team of Ukraine (CERT-UA) regarding GraphSteel indicates an average level of certainty for attribution to UAC-0056.

For the rest of this report, we will focus on attacks involving the use of GraphSteel malware. GraphSteel is part of the Elephant Framework – a collection of tools also written in the Go language and deployed in a recent wave of phishing attacks on `.gov.ua` targets. Recently, three different attacks have been observed which relied on the Elephant Framework:

- February 11th, 2022 – SentinelOne detected an attack with fake dictionary software
- March 11th, 2022 – CERT-UA reported an attack with fake antivirus software
- March 28th, 2022 – CERT-UA reported an attack with an "Unpaid wages" email subject

Anatomy of an Attack

In all known Elephant Framework attacks, the spear-phishing tactic was used for initial compromise. The group demonstrated a good knowledge of social engineering techniques, with emails originating from spoofed Ukrainian email addresses. Email subject and body would often use trending themes (COVID) or use official-looking text.

In one of the emails, the threat actor included recommendations for effective security controls after warning about intensified computer attacks by the Russian Federation, including recommendations to use email and web traffic filtering, avoid the use of 3rd party DNS servers, and provide a briefing to employees about possible phishing attacks. This "helpful" email cleverly embedded a link to a malicious payload (masquerading as a recommended antivirus tool).

A few different techniques were used to execute the malicious launcher. In this example, the link to the malicious download is included in the body of the email. In other cases, an attached Excel spreadsheet with embedded macros was used.

Launcher Component

There are a few different variants of **launchers** for GraphSteel that we have seen to date. In the case reported by SentinelOne, the downloaded launcher was a Python script converted to an executable (using pyinstaller). In the other cases, the launcher was written in the Go language like the rest of the Elephant Framework with the launcher's name varying depending on the attack.

Why might threat actors choose the Go language, which is not a mainstream programming language, for this malicious software? Potential reasons include:

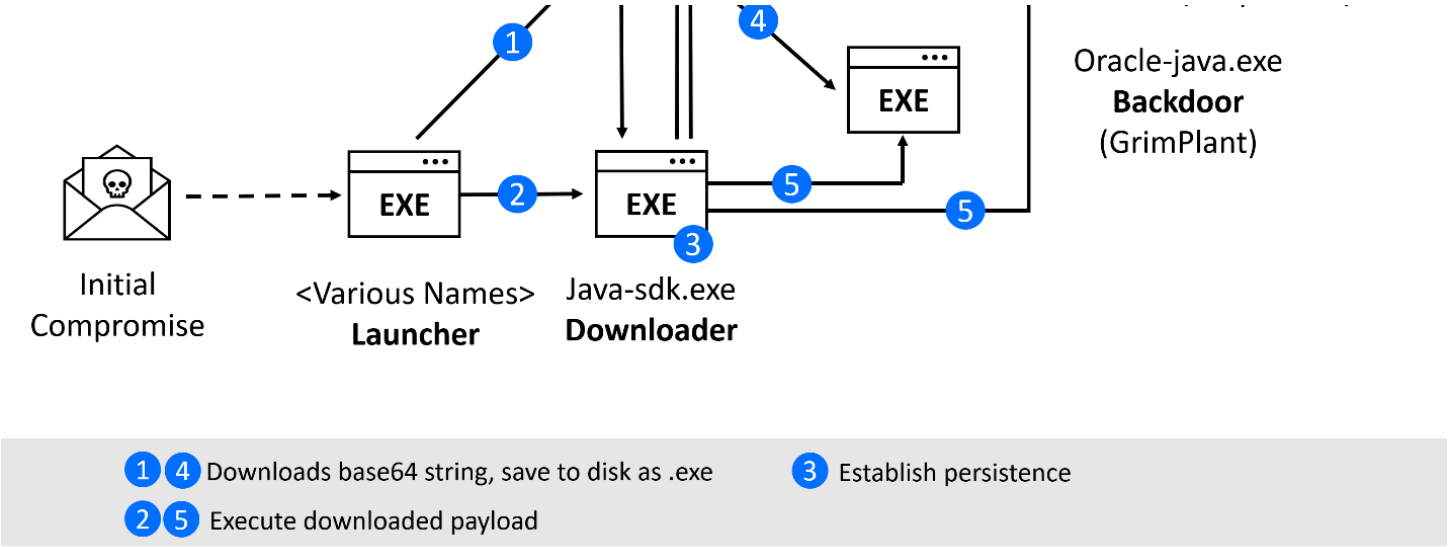
Elephant Framework; for example, for AES cipher, generating a unique client ID, or Coldfire (a malware development framework for Golang).

The launcher does not have the malware payload embedded – instead, it acts as a combination of a downloader and dropper. Upon execution, the launcher connects to the command and control (C&C) server, downloads the malware payload encoded as base64 string, saves it to the local disk and then executes it. The address of the C&C server is hardcoded in this executable and, in all recorded cases, the file dropped by this executable is named `Java-sdk.exe`.

Downloader Component

`Java-sdk.exe` acts as a **downloader** of the Elephant Framework and, as you probably are expecting by now, is written in the Go language. It uses a similar technique as the launcher – first connecting to a C&C server, then streams a string encoded in base64 which contains the malicious payload, saves it as an executable to disk, and executes it. The address of the C&C server is not embedded – it is provided by the launcher as a `base64(AES(<C&C>))` argument. Two different malware files are downloaded – GraphSteel (`Microsoft-cortana.exe`) and GrimPlant (`Oracle-java.exe`) which are automatically executed. **GrimPlant** is a relatively simple backdoor that allows remote execution of PowerShell commands. **GraphSteel** is used for data exfiltration of credentials, certificates, passwords, and other sensitive information.

This downloader component is also responsible for establishing persistence by creating a registry value `Java-SDK` under the registry key `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\`.



Typical flow of an attack based on the Elephant Framework

This covers our findings for the initial phase where the Elephant Framework is deployed to the compromised machine. In the next section, we will look in more detail at the core components of the Elephant Framework, GrimPlant and GraphSteel. Both implants are written in the Go language, comprehensive research is available from Intezer.

GrimPlant (Backdoor) Component

GrimPlant's primary purpose is to allow a threat actor to execute PowerShell commands remotely. The address of the C&C server is provided by `Java-sdk.exe` using the command line parameter `-addr`. This address is not provided in plain text, instead, it uses the same `base64(AES(<C&C>))` syntax as the downloader.

Communication with the C&C server uses port 80 and is based on gRPC – an open-source Remote Procedure Call (RPC) framework, originally designed by Google. The communications are encrypted with TLS, with the certificate hardcoded in the binary.

After establishing a connection to the C&C server, GrimPlant sends a heartbeat message every 10 seconds. Included in the heartbeat message is information about the infected endpoint (`uploadSystemInfo` function):

- Operating System – Hostname, operating system, number of CPUs
- IP Address – Runs a query to `api.ipify.org` to retrieve a public IP address
- User Info – Name, username, HomeDir

is retrieved using the same method as GrimPlant. All communication is encrypted using the AES cipher on port 443. To communicate with the C&C server, it uses WebSockets and the GraphQL query language.

Below are the functions used by this malware:

- **getFileHash()** – Checks if the file has been uploaded on the server
- **getPublicKey()** – Generates a random public key and receives a secret used to derive an AES key for subsequent communication
- **uploadChunk() –** Uploads files in chunks
- **ping() –** Sends client ID to the C&C server
- **uploadSystemInfo() –** Uploads information about the infected machine. Same implementation as GrimPlant
- **uploadCredentials() –** Uploads credentials harvested from an infected machine

The malware runs two routines to communicate with the C&C server:

- Heartbeat every 20 seconds
- Exfiltration routine every 20 minutes

The exfiltration routine:

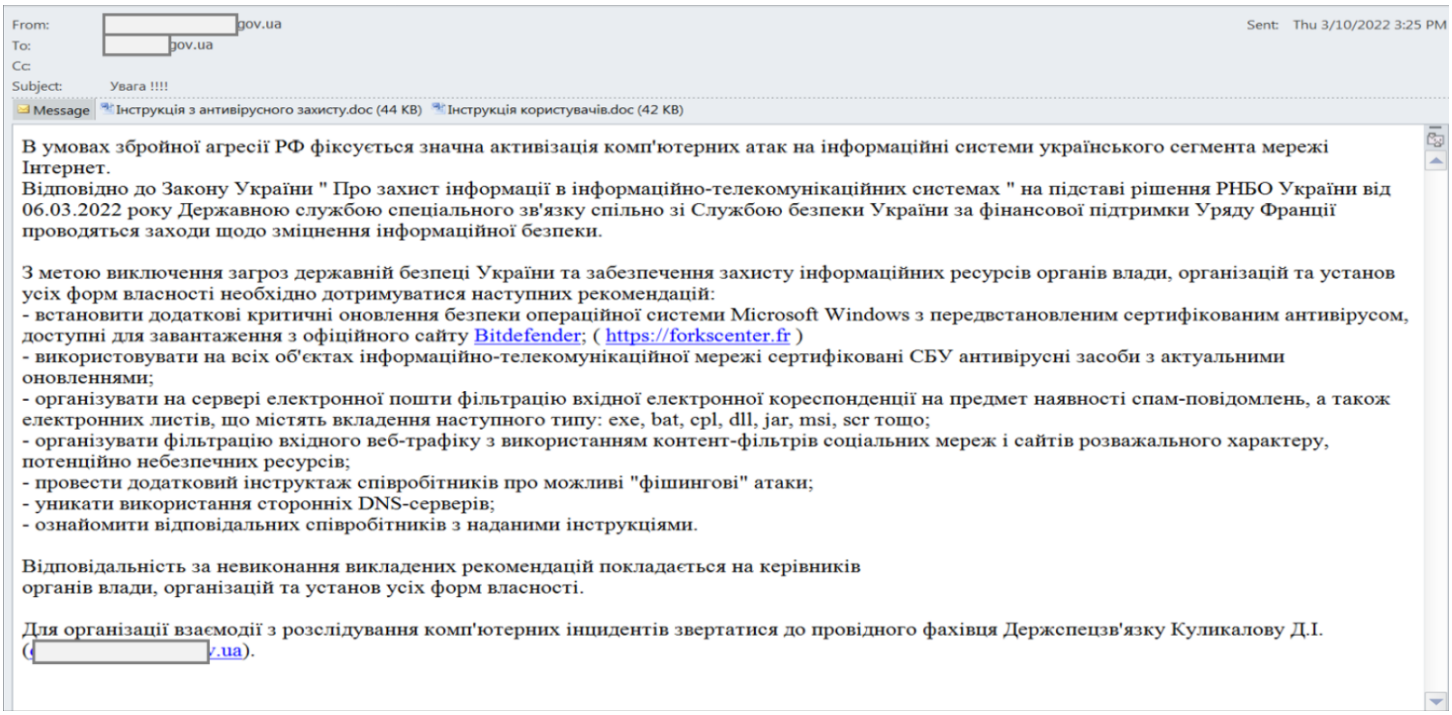
- Sends information about the infected system using the `uploadSystemInfo()` function
- Exfiltrates files using `uploadChunk()` function
  - Files are exfiltrated from folders `Documents`, `Downloads`, `Pictures`, `Desktop` and from all available drives (`D:\` to `Z:\`)
  - Limited to files that are smaller than 50 MBs and have one of the following extensions: `.txt, .doc, .xls, .ppt, .docx, .xlsx, .pptx, .ovpn, .ssh, .zip, .rar, .7z, .jpg, .png, .gif, .webp, .avi, .mkv, .mpg, .mpeg, .3gp, .csv, .json, .crt, .key`
- Harvests credentials and exfiltrates them using the `uploadCredentials()` function. Credentials and other sensitive information are extracted using different methods and from various locations:
  - Wifi passwords
  - Chrome and Firefox credentials
  - Credentials from the password vault
  - Credentials from Windows Credentials Manager
  - SSH sessions from Putty, Mobaxterm, openSSH, and Filezilla
  - Thunderbird

Exfiltration of wifi passwords is done by parsing output from `netsh wlan show profiles`, followed

```
Windows.Security.Credentials.PasswordVault;$vault.RetrieveAll() | % {
$_.RetrievePassword();$_} | Select UserName, Resource, Password | Format-
Table –HideTableHeaders
```

When one payload is not enough

The analyzed incidents mentioned in the first section of this article above are based on the Elephant Framework and use the same kill chain, except for an incident involving a faked copy of Bitdefender software. On March 11th, 2022, a phishing campaign was reported by CERT-UA that included instructions to download a fake Bitdefender antivirus product.



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]y.ua).

The original phishing email. Source: CERT-UA

Below is the full text of this phishing email (loosely translated from Ukrainian):

An increased number of computer attacks on information systems of Ukraine was detected since the beginning of the armed aggression of the Russian Federation.

Under the Law of Ukraine "On Protection of Information in Information and Telecommunication Systems" based on the decision of The National Security and Defense Council of Ukraine dated 06.03.2022, the State Service of Special Communications together with the Security Service of Ukraine, with the

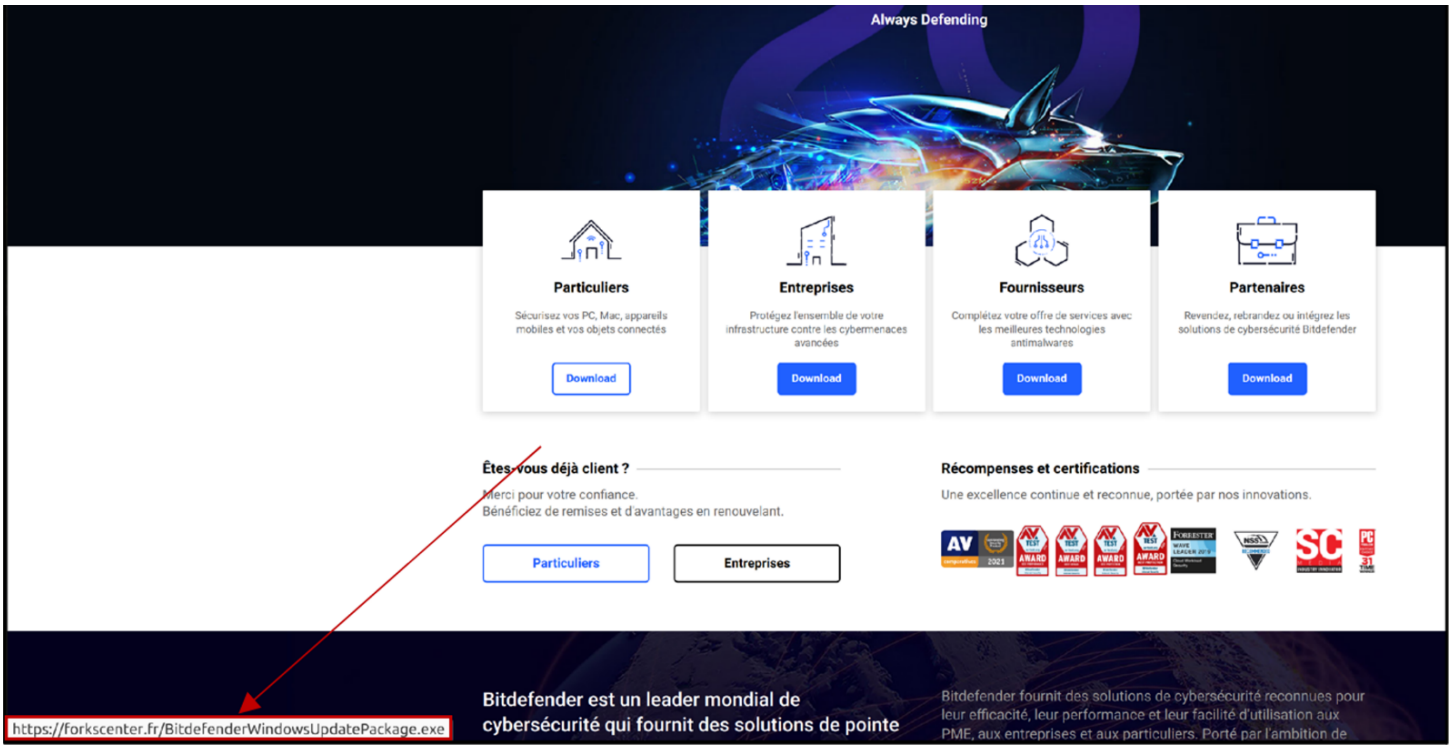
followed:

- *Install additional critical security updates for the Microsoft Windows operating system with a pre-installed certified antivirus available for download from the official Bitdefender website;*
- *Use SBU-certified up-to-date antivirus on all computers;*
- *Filter incoming e-mails on the e-mail server for the presence of spam messages, as well as e-mails containing attachments of the following types: exe, bat, cpl, dll, jar, msi, scr, etc .;*
- *Filter incoming web traffic using content filters for social networks, entertainment sites, and other potentially dangerous resources;*
- *Brief employees on the possible "phishing" attacks;*
- *Avoid the use of third-party DNS servers;*
- *Familiarize the responsible employees with the provided instructions.*

Responsibility for failure to comply with the above recommendations rests with the authorities, organizations, and institutions of all forms of ownership.

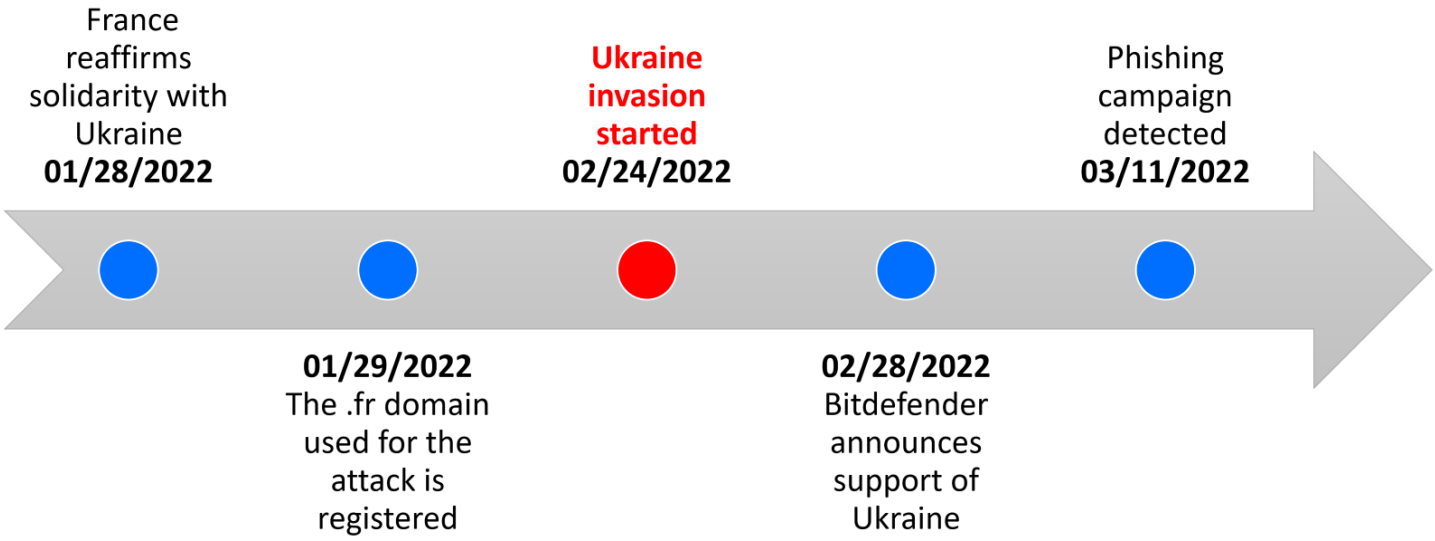
To organize cooperation in the investigation of computer incidents, contact the leading specialist of the State Special Service <REDACTED>.

The link to the “official Bitdefender website” points to the domain `forkscenter[.]fr`. This phishing site spoofs the website `bitdefender.fr`, a version of the Bitdefender website localized in the French language.

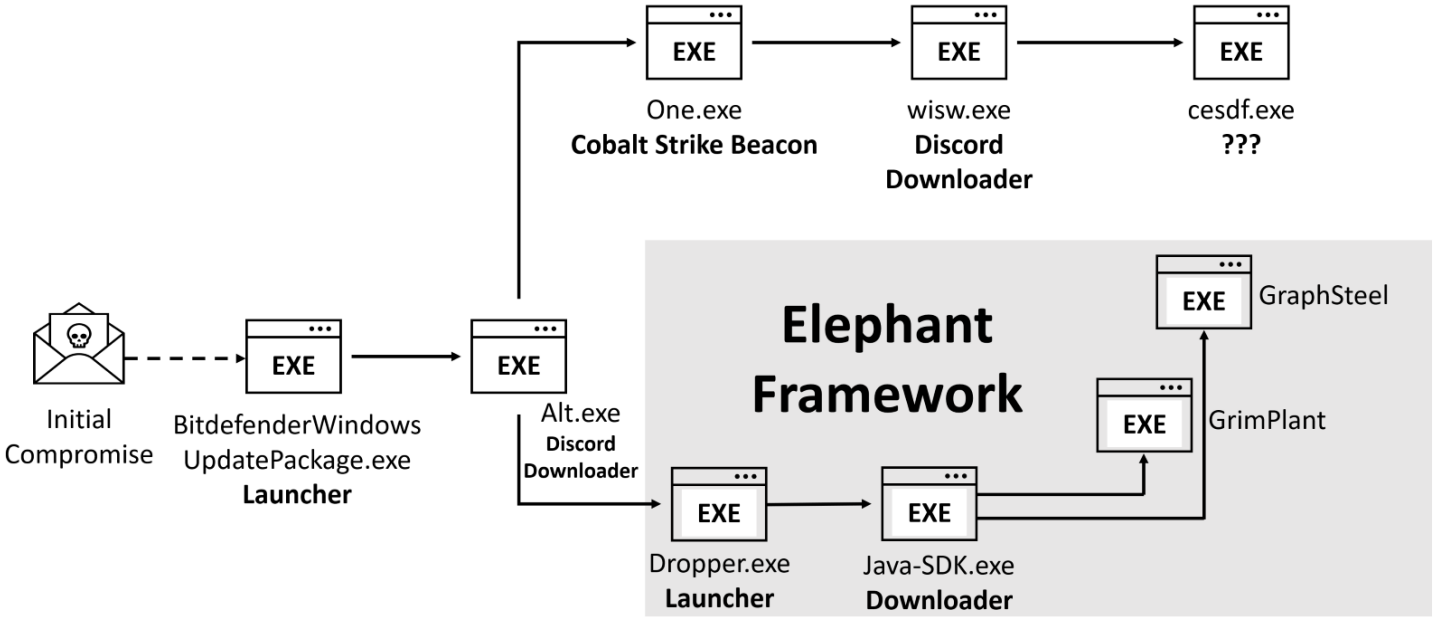


The fake Bitdefender.fr website. Source: CERT-UA

All links on this fake website are downloads for the malicious file named `BitdefenderWindowsUpdatePackage.exe`. Both France and Bitdefender have publicly declared support for Ukraine, and this may be a reason why UAC-0056 chose this context for their phishing site since this aligns with the focus of the spear-phishing email (i.e., to protect systems further due to the heightened geopolitical environment after the invasion of Ukraine).



deployed two executables. The first is a familiar Go launcher that deployed the rest of the Elephant Framework as described earlier. The second executable, `One.exe`, is a Cobalt Strike Beacon, which deployed another Discord downloader, `wisw.exe`. Persistence was established by creating a startup link called `BitdefenderControl.lnk`, which executes `wisw.exe`. Finally, the malware downloads another executable, `cesdf.exe`, from Discord. Unfortunately, this file is not available for analysis, as the download server was shut down. While the Elephant Framework deployment used `hxxp://45[.]84.0.116:443` as the C&C server, the Cobalt Strike deployment used the C&C server located at `nirsoft[.]me`.



Overview of two parallel deployments associated with the spoofed AV attack

Conclusion and Recommendations

The best protection against modern cyber-attacks is a defense-in-depth architecture. Start with reducing your attack surface and employing automated controls to prevent most security incidents. For the few incidents that get through your defenses, you want to lean on security operations, either in-house or through a managed service, and leverage strong detection and response tools.

Integrated reputation services can stop an attack during multiple stages – from an initial phishing email, through the execution of a previously unknown payload, through to the successful compromise and subsequent call home to a C&C server.

Bitdefender Threat Intelligence (TI) is such a reputation service and can be integrated with your existing security infrastructure using the REST API. The services are platform-independent and compatible with

center (SOC).

Indicators of Compromise

An up-to-date and complete list of indicators of compromise is available to Bitdefender Advanced Threat Intelligence users. The currently known indicators of compromise can be found in the table below.

Files hashes

MD5	SHA256	Type/Family	Source
2e0f1315c52e8b017fb6110398b28e60	ba1066f7a47b3662b1589579c9b7100a6f275a1cd82de75b166f31e9ee913562	Go downloader	Telemetry + Bitdefender research

33816414b221be4b0888ef0fbeaacb0b	6dd346a7b04f5ca6b34cb5cbbb545cbeffd50e736f3cdf71073e805eae60c136	GrimPlant	Telemetry + Bitdefender research
9ad4a2dfd4cb49ef55f2acd320659b83	-	Discord downloader (wisw.exe)	CERT-UA
b8b7a10dcc0dad157191620b5d4e5312	b5b989f8eab271b63d8ab96d00d5fb5c41ab622e6cfde46ea62189765326af5a	BitdefenderWindowsUpdatePackage.exe	CERT-UA
9ea3aaaeb15a074cd617ee1dfdda2c26	85c9bd53e9567ac4dc1e5caac2916f99c9e5bd5eec499b59668dfe997a574b48	GraphSteel	CERT-UA
4f11abdb96be36e3806bada5b8b2b8f8	476e95b4f194e4d3b0d580dc49bf5b552c9a34d5dcf7803dd97912719faa9d02	GrimPlant	CERT-UA
c8bf2386416212129015175 70e96fae7	-	Go downloader	CERT-UA
15c525b74b7251cfa1f7c471975f3f95	39b3c82b1e7e5626e380a53df4ccb52f3002749447cfab3	Go downloader	CERT-UA

a41e743e19550d4040	63ae1c27107c757 6c5046493321006bac	downloader	CERT-UA
aa5e8268e741346c76ebfd1f27941a14	2f92d416f73472db1ebe880b3bec677bcb1d96d6ad62974da00b4be5f6d61f5b	Contains cobaltstrike beacon	CERT-UA
628f41776ae3b2e8343eeb9cdcd019f2	8e77118d819681fdc49ce3362d8bfd8f51f8469353396be7113c5a8978a171f6	GraphSteel	Bitdefender research
fe63861920a3c02936b3deb0198a950f	04f76ef71d0d6f1c3da55bed846579bca8eb537643315f1196bd75c0c40cb927	GraphSteel	Bitdefender research
71bc63c9635bbbdfcb6b046d68b9236e	b48232c1343515a224eeea11f267464fb500168ab19d7d3e0b217401243d3620	GrimPlant	Bitdefender research
cbc0e802b7134e1d02df1f2eb1b1d1e2	4f4bbe75fb644cd83a64dbb256b5a82355b74b29cb7aa55e2a49f331a4ca02f7	GrimPlant	Bitdefender research
8e0eb1742b47745ff733896739	00c3bfa040aa0092f86950510885c125	Go downloader	Bitdefender research

1bfab3535b5fa97274b	71aa220bea4913c67d2eb64fb614d5722	Go downloader	research
cde5aa217c0c1a7d2f1b9dcf9904e0ad	b79636a07b9c487878217024ab8579c17026fe334228795c34c70d5c7a302bbe	Go downloader	Bitdefender research
69be9b58af0f7ff6f6f5ac72d8f7a403	7215d831898d7b8e3e195f8b8ae23b9d7859e8f51a89a5a52cde3c793a3bfe19	GraphSteel	Bitdefender research
dd076c2be578d6d9419af8f39541e2cd	a7e89781b2e42488614340521dfa520bf43939a55c02a65aae0f667190cda840	GrimPlant	Bitdefender research

File names

```
BitdefenderWindowsUpdatePackage.exe
wisw.exe
microsoft-cortana.exe
oracle-java.exe
java-sdk.exe
```

Network

IP/DNS	Source

80.66.76[.]187	Intezer blog post, also Bitdefender research
194.31.98[.]124	CERT-UA
91.242.229[.]35	SentinelOne
45.84.0[.]116	CERT-UA
45.140.146[.]17	Bitdefender research
forkscenter [.] fr	CERT-UA; Fake BD installer download site
nirsoft [.] me	CERT-UA; Cobalt Strike beacon C&C
156.146.50[.]5	CERT-UA; Source IP for phishing emails

We would like to thank Bitdefender Labs team for their help with putting this report together.

CONTACT AN EXPERT

See all topics

Read more about this topic