CERT-UA

cert.gov.ua/article/38374

general information

The Governmental Computer Emergency Response Team of Ukraine CERT-UA received information on the distribution of e-mails on the topic "Wage arrears" among government agencies of Ukraine. Attached to the letter is the document "Wage arrears.xls", which contains legitimate statistics and macros. At the same time, hex-coded data has been added to the mentioned document as an attachment. The macro, after activation, will decode the data, create the EXE-file "Base-Update.exe" on the computer and execute it.

This file is a downloader developed using the GoLang programming language. The program will download and run another bootloader, which, in turn, will download and run malware GraphSteel and GrimPlant on your computer.

The detected activity is associated with the activity of the group UAC-0056.

Indicators of compromise

Files:

```
da305627acf63792acb02afaf83d94d1
c1afb561cd5363ac5826ce7a72f0055b400b86bd7524da43474c94bc480d7eff Wage arrears.xls
06124da5b4d6ef31dbfd7a6094fc52a6
9e9fa8b3b0a59762b429853a36674608df1fa7d7f7140c8fccd7c1946070995a Base-Update.exe
(GoDownloader)
36ff9ec87c458d6d76b2afbd5120dfae
8ffe7f2eeb0cbfbe158b77bbff3e0055d2ef7138f481b4fac8ade6bfb9b2b0a1 java-sdk.exe
(GoDownloader)
4a5de4784a6005aa8a19fb0889f1947a
99a2b79a4231806d4979aa017ff7e8b804d32bfe9dcc0958d403dfe06bdd0532 oracle-java.exe
(GrimPlant)
6b413beb61e46241481f556bb5cdb69c
c83d8b36402639ea3f1ad5d48edc1a22005923aee1c1826afabe27cb3989baa3 microsoft-
cortana.exe (GraphSteel) (2022-03-20)
```

Network:

```
hxxp: // 194 [.] 31.98.124: 443 / i
hxxp: // 194 [.] 31.98.124: 443 / p
hxxp: // 194 [.] 31.98.124: 443 / m
ws: // 194 [.] 31.98.124: 443 / c
194 [.] 31.98.124
```

Hosts:

```
% TMP% \ Base-Update.exe
% USERPROFILE% \. Java-sdk \ java-sdk.exe
% USERPROFILE% \. Java-sdk \ oracle-java.exe
% USERPROFILE% \. Java-sdk \ microsoft-cortana.exe
```

Graphic images