Warning about “HermeticWiper Malware” by Russian APT Groups

dgc.org/en/hermeticwiper-malware/

February 25, 2022

In Light of the currently ongoing War between Russia and Ukraine, Multiple Russia-linked APT groups have used a new Data Wiping Malware dubbed HermeticWiper by the IT Security Community. References to IOCs are made with {} annotations. A corresponding list of known indicators can be found in our IOC list.

HermeticWiper – Attack Chain Number 1

The Attack chain starts with the victim receiving a malicious archive file via email (mostly .rar archives but .zip and .7zip archives have been spotted as well). The archive contains a document file that is themed after the currently ongoing war between Russia and Ukraine, however this theme can change in the future. The document contains macro code that drops and executes a VBScript when the victim is opening the document, the VBScript has been identified as a malware called GammaLoad.

This script starts by collecting information about the users and the system on which it is executed and prepares them for exfiltration to a C2-server. Then the IP address of the C2-domain {T13} is obtained, which the attacker has configured via a WMI script {T01}. Then the payload {T15.x} for the next step is downloaded and the data that has been collected is being uploaded to the configured C2-server. This connection can be identified via a specific UserAgent-string {T02} that is hardcoded in the malware.

The payload contains some sort of remote desktop application, most observed so far is UltraVNC (see {T03.x} for other possible options). This allows an attacker to execute various tasks on the affected system including wiping data and destruction of the system.

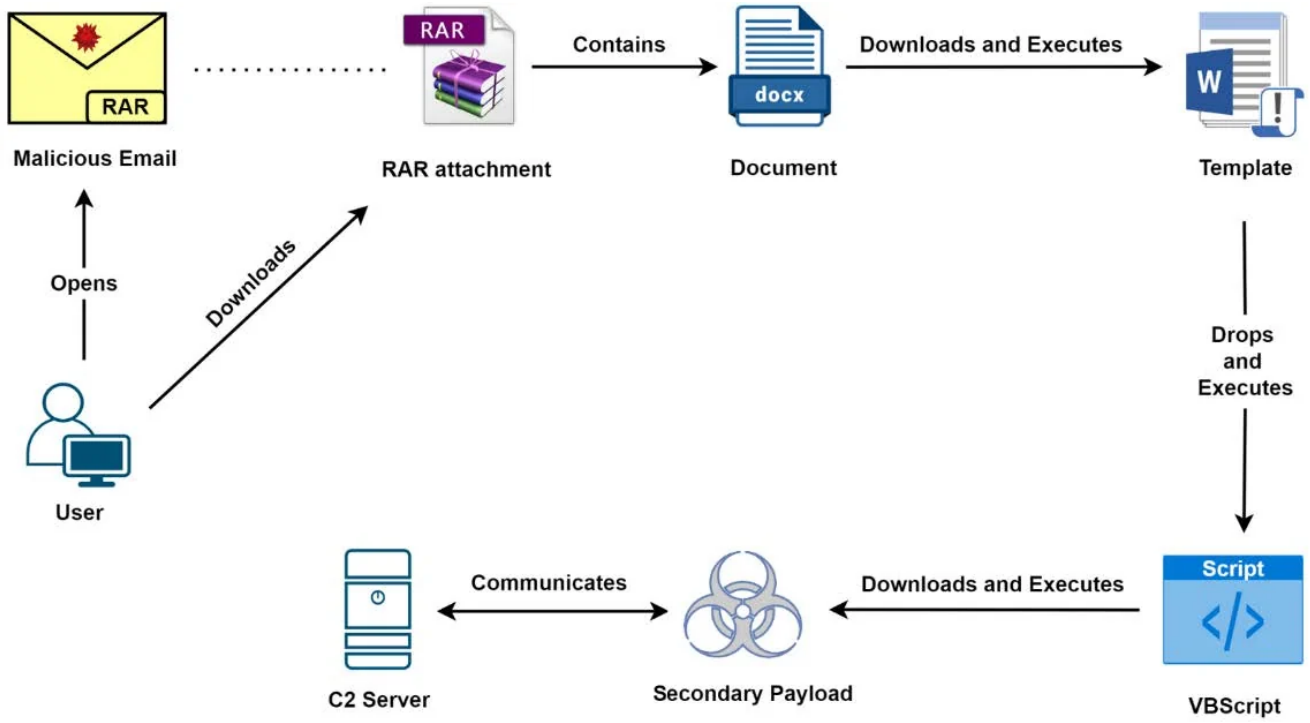

Figure 1: Visualization of the 1st attack chain (Source: [3])

HermeticWiper – Attack Chain Number 2

A second attack chain has been identified, where the victim also receives a malicious email with a malicious archive attached. This archive can be rar, zip or 7zip files, just like before. However, this time the archive contains a malicious Windows shortcut file (.lnk) that contains a malicious link to download an MSI script {T17x}. This is executed after downloading and launches an NSIS installer that, in addition to decoy files (images and documents have been observed so far), also creates a malicious DLL {T12.x} that communicates with a C2-server {T16.x} and deletes data from the victim system. This DLL disguises itself as a fake driver {T06 ->T09}.

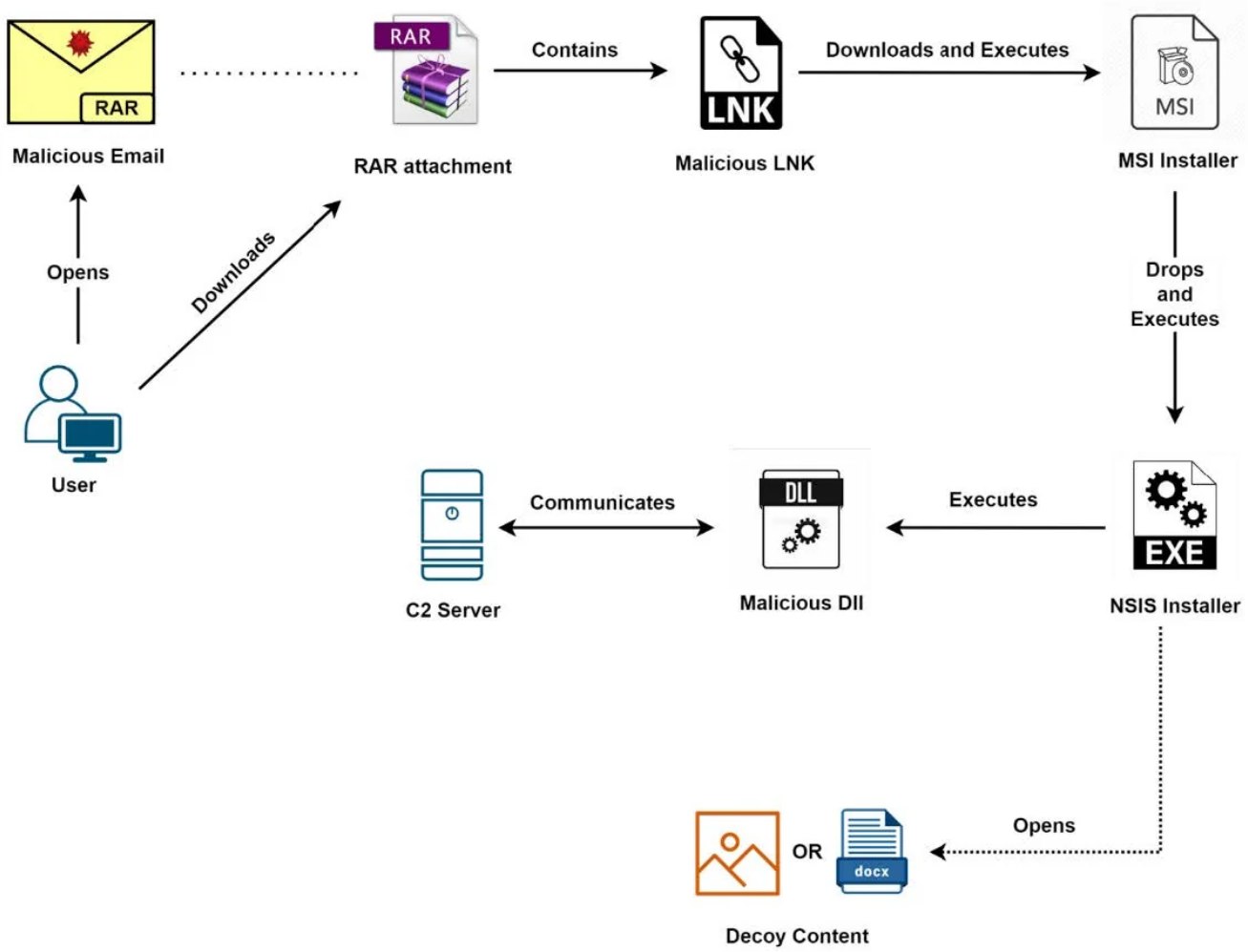

Figure 2: Visualization of the 2nd attack chain (Source: [3])

References and links

[1] https://twitter.com/ESETresearch/status/1496581903205511181
[2] https://twitter.com/threatintel/status/1496578746014437376
[3] https://www.zscaler.com/blogs/security-research/hermetic-wiper-resurgence-targeted-attacks-ukraine

Button