Severity

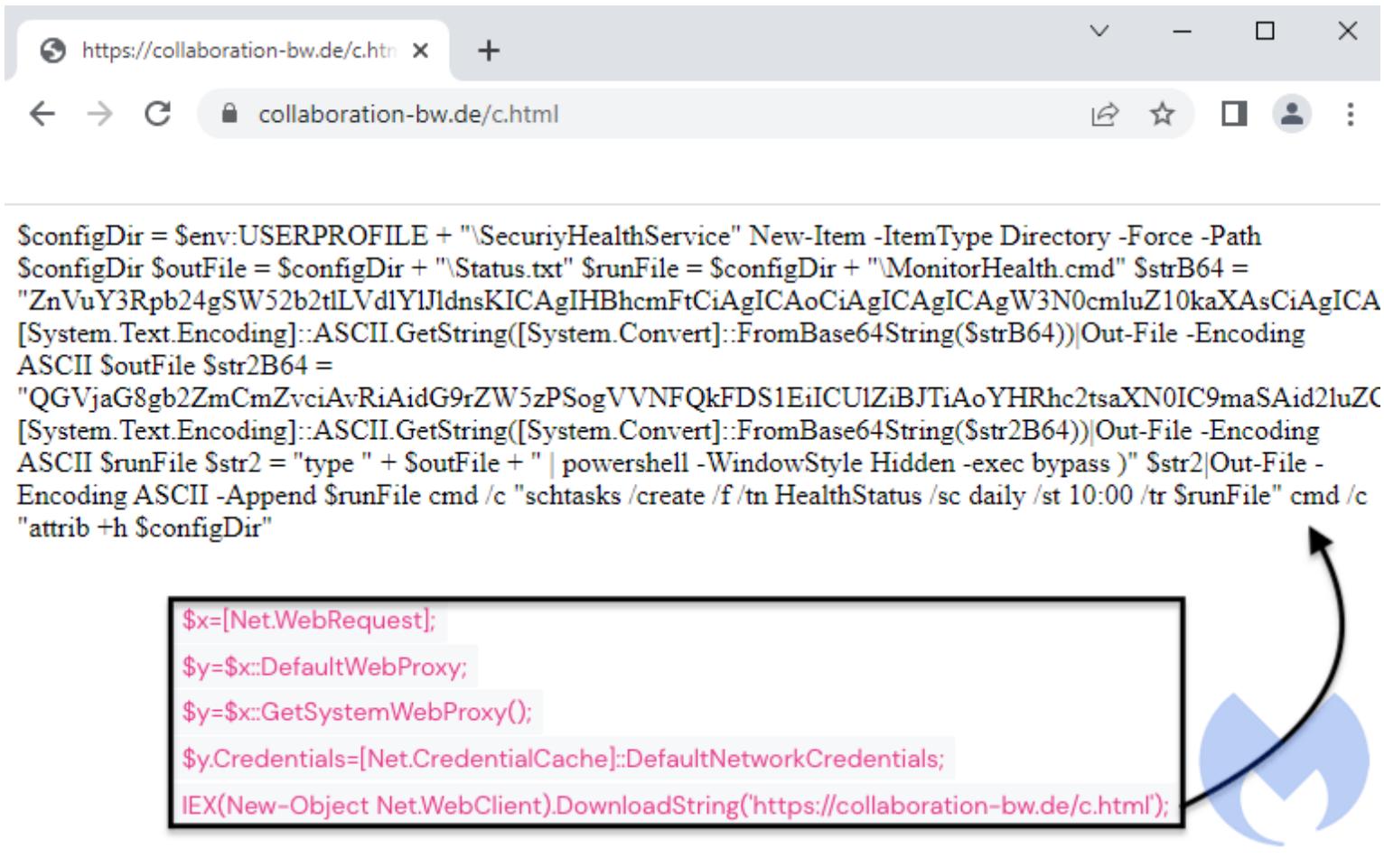
High

Analysis Summary

Researchers found an unknown threat actor targeting German users interested in the Ukraine issue and infecting them with a bespoke PowerShell RAT. The malware campaign employs a decoy site to entice users into false news bulletins regarding the Ukraine crisis. These websites provide malicious documents that install a remote administration tool (RAT) that allows remote command execution and file operations.

The threat actors involved in this campaign registered a fake site using an expired German domain name at collaboration-bw[.]de. The website had a bait document called "2022-Q2-Bedrohungslage-Ukraine" that was used to deploy the custom malware. The document purports to include information on Ukraine's current crises. The download page claims that the document offered critical information regarding the present threat posed by the Ukraine issue. When the victim clicks the link, a ZIP archive is downloaded to their machine. The compressed bundle includes a CHM file consisting of compiled HTML files. If the victim accesses the files, an error message is displayed, while the PowerShell executes a Base64 command.

After de-obfuscating the command, it executes a script obtained from the bogus Baden-Württemberg website using Invoke-Expression (IEX). It then drops two files on the computer in a folder called MonitorHealth.cmd and a script called Status.txt. The .cmd file executes Status.txt through PowerShell.



The malicious function of the custom PowerShell RAT hidden in "Status.txt" starts with collecting basic system information and the assignment of a unique client ID.

The RAT gathers basic system data before sending it to the domain "kleinm[.]de." It bypasses Windows AMSI (Anti-malware Scan Interface) using an AES-encrypted function named "bypass".

The following are the RAT's key capabilities:

- Download files (from the C2 server)
- Upload files (to the C2 server)
- Load & execute (PowerShell script)
- Execute (specific command)

It is suspected that a Russian threat actor could be targeting German users, although there are no obvious infrastructure linkages or similarities to existing TTPs. "Attributing this conduct to a single actor is difficult, and there are no solid indicators to support the attribution."

Impact

- Unauthorized Remote Access

- Information Theft
- Possible Security Bypass

Indicators of Compromise

Domain Name

- kleinm[.]de

MD5

- 62e69e18243bf653b6aca56b807536ec
- d39b09a556f98bccf2227abfab7b8e8b
- 32e0ed1d871f7ef7d730e8760be1cb73

SHA-256

- 2430f68285120686233569e51e2147914dc87f82c7dbdf07fe0c34dbb1aca77c
- 80bad7e0d5a5d2782674bb8334dcca03534aa831c37aebb5962da1cd1bec4130
- a5d8beaa832832576ca97809be4eee9441eb6907752a7e1f9a390b29bbb9fe1f

SHA-1

- e2e53f31b8d87f18abd0e0ee3783e7dd689c3101
- a1ea57d1df7ce65b14a85af580da4088c4db196f
- 4ba051a8c4b3ed29443659a6485b6d31be1e3a79

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.