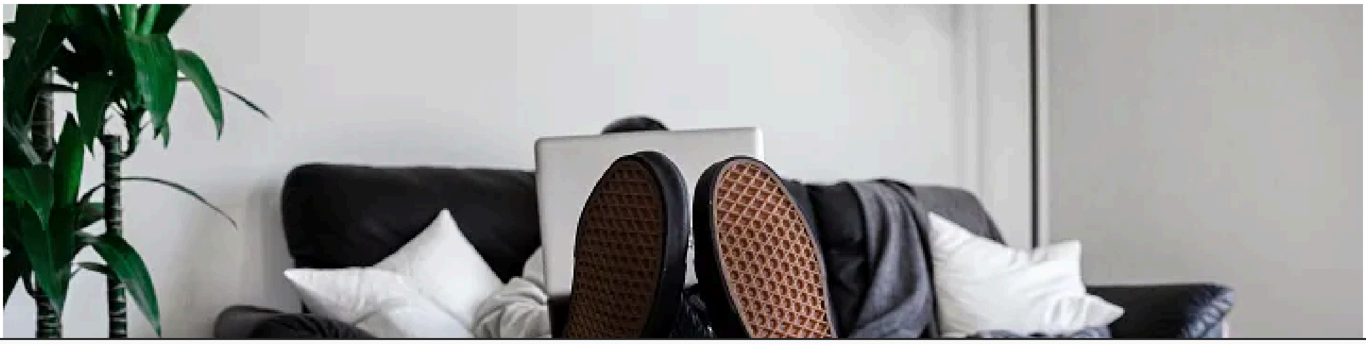
Open in app ↗ Sign up Sign in

Medium Search Write



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 $/month

In this article we'll take a close look at the techniques described by Trellix researchers Mathanraj Thangaraju and Sijo Jacob in their recent piece for the Trellix blog entitled Beyond File Search: A Novel Method for Exploiting the "search-ms" URI Protocol Handler. In this post, Thangaraju and Jacob explore a recent campaign where threat actors exploit built-in Windows search capabilities in conjunction with WebDAV to trick unwitting victims into executing malware on their systems. The team at Trellix always delivers top-notch work and I appreciate how well they explain attacks like the one covered here.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

A Valuable Focus on Initial Access Detection

As detection specialists, we have seen lots of different methods by which attackers breach our systems. The philosophy of “assume breach” is a powerful guiding force in our work, and we are rightly accustomed to working hand-in-hand with our incident responder colleagues to address the post-compromise activity that we find.

But, think about how much headache, time, and money could be saved by catching more cyberattacks early — at the Initial Access phase or shortly

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Note: According to the Trellix researchers, the WebDAV/search-ms techniques described here serve as an initial access vector for AsyncRAT and RemcosRAT. I believe them: my goal here is only to better understand the *delivery* mechanism, and not necessarily to perform a comprehensive, deep-dive analysis of the malware itself!

Understanding the Threat

As the Trellix researchers show, the attack is a classic phish, but using a compromised or malicious web server to give the victim a view of the

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

cybersecurity, and I had worked with computers since 2010! If you are new to WebDAV, you can learn all you need to know about it here.

2. The **search-ms protocol** is simply a means by which you can query the “Windows Search index” using a URI. This sounds fancy, but all it means is that search-ms provides a means to query the contents of files and folders using a component of a URL. In the case of this threat, that URL will be searching for specifically-named content on a malicious WebDAV server. There’s no need to become a search-ms protocol expert to successfully detect this attack, but if you want to read more about it, you

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

professionals bad-mouth or denigrate the end users (who spend their days creating value at their organizations).

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

If I double-click the “_pdf” link file, nothing happens. Hmm…not very satisfying. Trying another malicious URL, I am once again presented with

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

To overcome this obstacle, I decided to make use of the subdomain relations of the *.webdav.drivehq.com site on VirusTotal, shown here:

VirusTotal

VirusTotal

VirusTotalwww.virustotal.com

VirusTotal knows about 52 subdomains of this site, several of which are flagged for malicious activity. VirusTotal knows, so therefore, so do I! Using a

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Best believe I use IDLE

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Just browsing and lightly-interacting with the malicious files being served up via WebDAV created a huge volume of process creation logs in my lab. These logs, while high-volume, are also somewhat informative, telling me that:

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

file created in the AppData\Local\Temp directory and verified that they are the same:

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

reflective code loading going on each time the PowerShell above ran, and I was well on my way to having my data stolen by something like AsyncRAT and shipped off to the attacker for them to profit off of.

Remember, my goal is not to exhaustively dissect the malware that infected my test VM. I just want to better understand this interesting/novel/emerging initial access vector, so that we can review the existing detection coverage and, as Dr. Fauci used to say, possibly give it a boost!

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

search terms like “Invoice.” However, I didn’t have the opportunity to test this concept, so I can’t guarantee it will work!

```
title: Search-ms and WebDAV Indicators in URL
id: 5039f3d2-406a-4c1a-9350-7a5a85dc84c2
status: experimental
description: Detects URL pattern used by search-ms/WebDAV initial access campaign.
references:
    - https://www.trellix.com/en-us/about/newsroom/stories/research/beyond-file-sear
author: Micah Babinski
date: 2023/07/31
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Local File Creation

The local temporary WebDAV file creation mentioned earlier creates an interesting opportunity to detect WebDAV abuse, and I was unable to find any open-source rules to detect this behavior. The Sigma rule below will alert on local creation of temporary WebDAV files with any of the suspicious file extensions I saw during the research.

```
title: WebDAV Temporary Local File Creation
id: 4c55738d-72d8-490e-a2db-7969654e375f
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Process Execution

WebDAV usage is not suspicious on its own. We need some detection concepts that will help us identify the bad stuff. Double-clicking .lnk files like the malicious "Invoice_9283_pdf" shortcut shown above will result in explorer.exe spawning whatever executable the LNK file targets. Since the WebDAV-delivered .vbs script file resides in the WebDAV server directory, we know that the resulting process Command Line will contain the path to this directory, which from what I've seen always contains DavWWWRoot. This Sigma rule from Netron Systems covers this technique, but is limited to net

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

```
date: 2023/07/31
tags:
    - attack.execution
    - attack.t1059.001
    - attack.t1204
logsource:
    category: process_creation
    product: windows
detection:
    selection_img:
        ParentImage|endswith: '\explorer.exe'
        Image|endswith:
            - '\wscript.exe'
            - '\cscript.exe'
            - '\cmd.exe'
    selection_cmd:
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

I am 100% open to and appreciative of any feedback you might wish to offer on my work. I've really enjoyed sharing some of the research I conduct on my off-time with the security community, and am so grateful for those who choose to read and share it. 🙏 If you'd like to access the Sigma rules I've included on GitHub, you can do so here:

Sigma-Rules/2023_WebDAV_SearchMS at main · mbabinski/Sigma-Rules

A repository of my own Sigma detection rules. Contribute to mbabinski/Sigma-Rules development by creating an account on...

nski/Sigma-

ny own Sigma detection rules.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

256 Followers

Cybersecurity pro, featuring bagpiping and GIS chops. Lives with wife Quinn and son Malcolm. Loves mountains, Indian food, and mountains of Indian food.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app