Pivoting through malicious infrastructure: from ZoomPortable to Windscribe

theta.co.nz/news-blogs/cyber-security-blog/pivoting-through-malicious-infrastructure-from-zoomportable-to-windscribe/

12/04/2021

Theta Cyber Security reports on an undetected malware campaign running since at least December 2020, delivering stealthy trojaned copies of a popular VPN product - and how we found it.

We'll cover off a technical analysis of some of the malicious infrastructure associated with these campaigns as well as hunting guidance to look for indicators of compromise associated with ZoomPortable and Windscribe.

This report article is released in conjunction with another [1] from Inde, who have further focused on exploring some of the artefacts associated with ZoomPortable.

Operational Cost

Adversaries can make operational mistakes in the configuration of their malicious infrastructure for a variety of reasons. Maintaining good, operationally safe hygiene when setting up this infrastructure is difficult and requires diligence on behalf of the threat actors - imposing a cost on them that they must bear in order to remain undetected for as long as possible. Failure to do so provides detection opportunities to diligent hunters.

Despite the long campaign dwell time discussed here [2] - with its setup dating to December 2020 – some 4 months before publishing this report, this article highlights 3 mistakes that we observed and exploited as defenders for hunting purposes:

- The sequential IPs hosting shared infrastructure between at least veehy[.]com & zoom-download.huvpn[.]com and links to two other domains and an additional IP address.

- Infrastructure reuse in hosting the ZoomPortable campaign that led to the discovery of a related WindScribe (aka VPN) campaign via hosting it on the same domain as was used for the ZoomPortable campaign.
- Code Signing Certificate re-use between these two campaigns that further ties the two malware families together.

“ZoomPortable”

In late March 2021, Theta observed the earliest currently documented example of `zoom.exe`[3] (via *ZoomPortable* [4]) spawning malicious behaviour [5] - namely a certain *b.ps1* [6] - in the wild. This PowerShell script was a curiously obfuscated [7] environmental reconnaissance package that sent system and environmental data back to a command and control server - plausibly to then be selected for delivery of follow-on capabilities in the form of a second stage payload from the threat actor based on their own criteria.

Whilst this behaviour was detected and blocked as it happened, the trail of where this binary came from unfortunately went cold. Our team could trace the installation of ZoomPortable.exe back some days earlier as coming from a browser download but the user’s device was unfortunately wiped before browser forensics could be conducted and network traffic for the download was not captured. We also noted in our initial analysis that there were no public references to a *zoom portable* version, and some of the configuration of the software appeared odd [8].

At the time, we put this incident down to either a phishing campaign or a backdoored lookalike zoom package that tricked the victim into downloading and installing from somewhere other than the zoom directly - with the latter likely based on conversations with the user and email analysis turning over no signs of a phish. Because ZoomPortable contains legitimate (and working) Zoom components, legitimate Zoom.us network traffic was also observed, hampering technical analysis and further confusing the situation.

Theta shared some of these findings to various trusted partners in the cyber security community at the time – and thankfully ZoomPortable.exe and its malicious nature were later also observed and corroborated by other members of the cyber security community in New Zealand in early April 2021 (approximately two weeks later) after their own version b.ps1 was detected - complete with a new hard-coded C2 address.

Excellent work has been done with further analysis [9] of this malware campaign – with more still to come. The disruption of this wider campaign is something we are proud to have been able to contribute to.

It was this later, largely community-driven and collaborative investigation that subsequently uncovered two websites masquerading as the legitimate zoom.us website. Some of this overlapping infrastructure and its components are the focus of this article. Both veehy[.]com [10] & zoom-download.huvpn[.]com [11] were detected by partners who worked backwards after they were alerted when their own copies of *ZoomPortable.exe* had spawned b.ps1. Both these domains had links to ZoomPortable.exe binary hosted in Amazon Web Services.

Additional Infrastructure and Sequential IPs

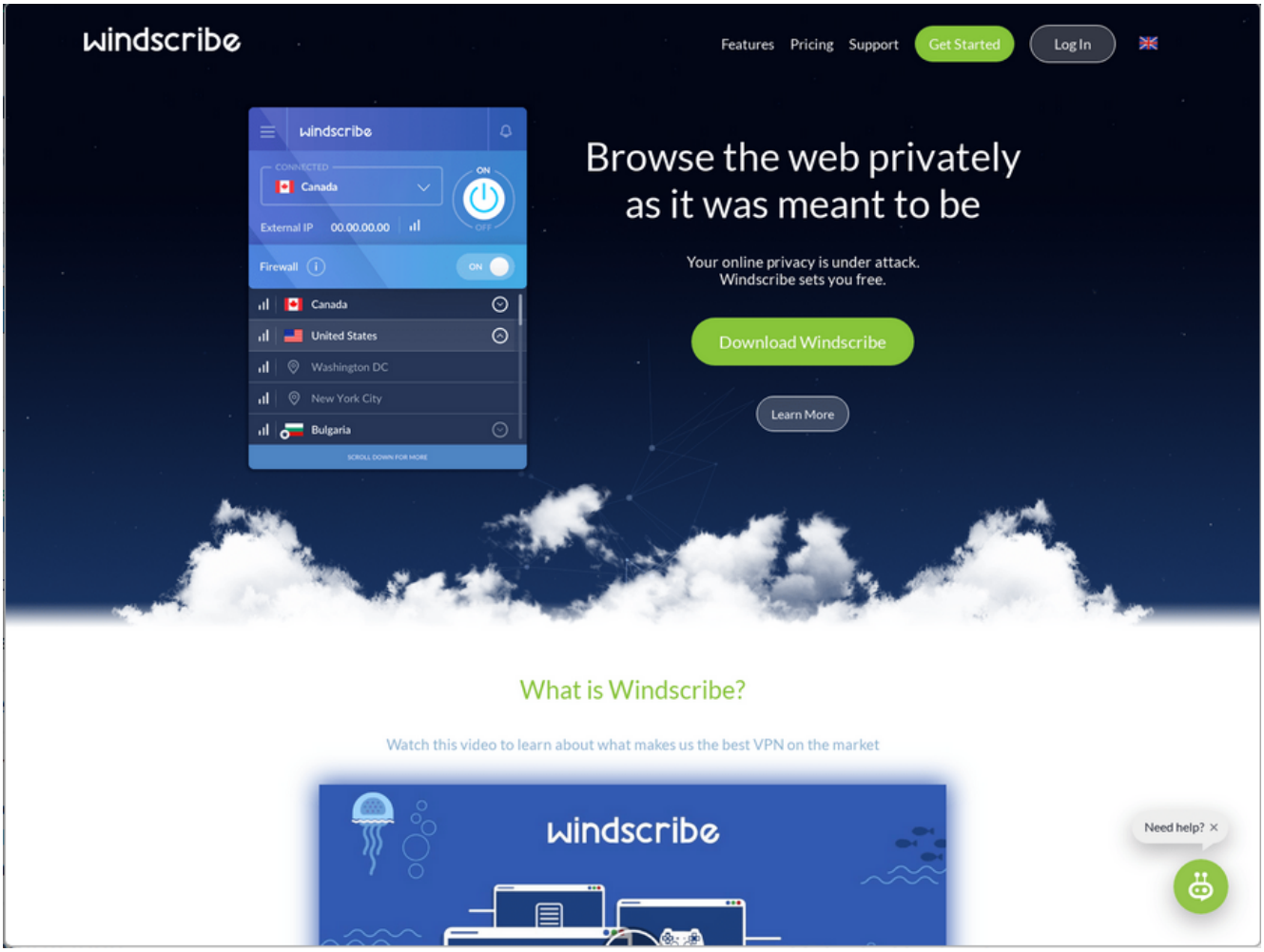
Veehy and huvpn both appeared to be identical in their configurations: clones of the legitimate Zoom.us website and occupied the sequential IPs 5.39.216[.]178 & 5.39.216[.]179 at the time of discovery.

Traffic passively recorded communicating with these IPs also reference a cayzor[.]com who had pointed towards 5.39.216[.]177 at the time of discovery; and cayzor’s LetsEncrypt TLS Certificate itself references an oulous[.]com in X509 alternate name metadata [12]. Oulous also resolves to 5.39.216[.]179 (thus providing the link from 5.39.216[.]179 to cayzor at 5.39.216[.]177 and oulous back at 5.39.216[.]179 [13]).

Unfortunately, we are not aware of any graphical scans or scrapes cayzor and oulous whilst under threat actor control so it is unclear exactly how or if these domains were part of the same malware campaigns, but we assess with high confidence they were under control of the same malicious actor responsible for these campaigns via the methodology described above – so they should be hunted for regardless.

Infrastructure Reuse & Similarties

Passive DNS records, certificate transparency logs and URLScan [14] all captured veehy[.]com at various points in its lifecycle. veehy[.]com was an old domain (created in 2008) [15] with the now removed subdomain vpn.veehy[.]com receiving updated TLS certificates on 22 December 2020 (along with the rest of veehy)[16]. URLScan also automatically scanned the page at this time [17]:



vpn.veehy[.]com - Image Credit: Urlscan.io

This page purports itself to be Windscribe [18] – a personal VPN product, and it had an outbound link to a similarly formatted [19] AWS hosted binary as the ZoomPortable Campaign. URLScan helpfully recorded [20] this as *https[:]//windscribe.s3.us-east-2.amazonaws[.]com/Windscribe.exe* and we assess that this binary appears to be the first stage of an earlier and overlapping but, as yet, undetected campaign by the same threat actors.

This URL was also captured [21] in VirusTotal – a popular clearing house and repository for threat researchers and cyber security Professionals on the 10th of December 2020.
VirusTotal recorded that the body (aka the file Windscribe.exe) of the subsequent transaction had SHA-256 hash of *1495500d6c8613fda22b0e0c8f2ab0ba5d244d6b166c5d854a47000a91f44ab1*
The file this hash was derived from was also ingested at this time and is available on VirusTotal [22] – where at the time of this article it continues to have 0 detections.

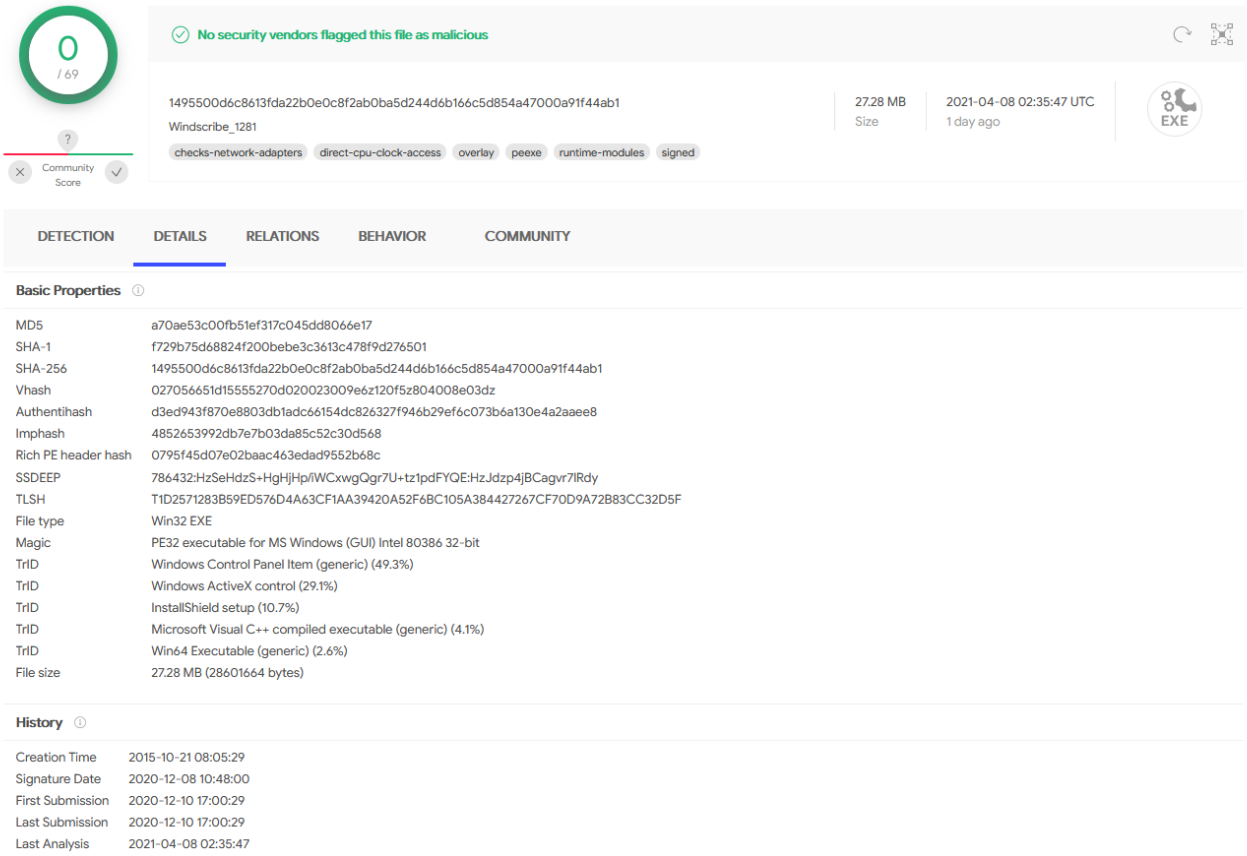


Image Credit: VirusTotal

View enlarged image

Signing Certificate Overlap

Whilst the vpn.veehy[.]com page and the windscribe.exe download link was already removed from the internet prior to detection, we can see several components of the aforementioned `Windscribe.exe`[23] overlap with the original `zoom.exe`[24] that was detected right at the start of this report - both binaries are signed with the same DigiCert EV Codesigning Certificate: Issued to TRATTORIA WYKI SP Z O O:

Image Credit: VirusTotal

Adversaries obtaining codesigning certificates to aid in camouflaging their tooling is nothing new, but this overlap provides several further detection opportunities for us:
This certificate (SN: 074A080F649B2D5B784675B302A963B7 // Thumbprint: B43C94F107B19D2B23DB41F45D5ADCBC5342CD46) points to several other suspicious files that are likely related to the Windscribe/VPN campaign – namely:

WindscribePatchExe [25] - SHA256: da88dc8fbc02a32d336fc8a20f67f01fc3fe833068d0275cb7f5610566d28824

Windscribe TAP install helper [26] - SHA256: fb55cc18b16707eeb53dd51e0e4e1e7046fd7a9e1b2ec1f5a128cef8810bcbd9

Windscribe.aiui [27] - SHA256: 77986a638410d6d312e5eef8dd142182b50623a3aae361ccf7e6d997ec1b7581

At the time of analysis these files again have no detections in VirusTotal – but should be considered likely malicious due to the multiple points of overlapping infrastructure and TTPs with the known bad ZoomPortable campaign.

Note: Legitimate WindScribe appears to be signed with it's own, different, signing certificate (SN: 0f5ee43beea50ed5f0ec765bf65b1350 // Thumbprint: 2d89451abf19019641927f6fa09be531d84981b6) – further re-enforcing the suspiciousness of the TRATTORIA WYKI issued certificate in this context.

Summary

Our analysis (as well as others) is currently ongoing, but points to the strong possibility of malicious backdoored VPN products being deployed from December 2020 that remain undetected to this time, as well as the previously undetected ZoomPortable campaign remaining in the wild. We do not yet have any indication of how widely installed or targeted either campaign was, or what the end goal of the threat actor was. So far information about these campaigns is scant.

The presence of these classes of software for both campaigns (a backdoored Zoom and a backdoored VPN) on endpoints coupled with the follow-on activity that has been described in the ZoomPortable campaign should be concerning to organisations of all sizes as well as home users. This is only exacerbated given the long time delta observed (circa 7 days in one example) between installation of zoomportable.exe and a malicious payload executing, as well as the use of a valid signing certificate for the backdoored but otherwise working software components - which makes for difficult detection and easy classification of a false positive alert.

Generally, a reasonably high level of instrumentation was required for detection of the ZoomPortable campaign. It required enough telemetry to catch the spawning of b.ps1 out of a signed and legitimate looking version of Zoom.exe. Without any of the network infrastructure along the way being classified as malicious and no antivirus engines flagging the files as bad - organisations without EDR or similar tooling as well as the competent hunters or responders able to make sense of the alerts generated would struggle to detect this behaviour. This plausibly explains the long campaign runtime. It would also effectively rule out the prospect of home users (who may well be interested in either a personal VPN or Zoom) or non-corporate managed devices being able to block or detect backdoored copies of ZoomPortable or Windscribe (if backdoored in a similar manner).

Although we do not have enough visibility into the victimology of these campaigns to suggest home users are impacted, Windscribe in particular would not generally be described as enterprise software. Given this, we provide the following guidance for detection.

Theta recommends hunting for these components at a minimum

- Traffic since December 2020 to the sequential IP addresses 5.39.216[.]177, 5.39.216[.]178 & 5.39.216[.]179 (ASN: 57043 // HostKey – geolocated in the Netherlands).
- Traffic since December 2020 to veehy[.]com, huvpn[.]com, cayzor[.]com or oulous[.]com.
- Any of the indicators for the ZoomPortable campaign (as referenced at https://pastebin.com/FGHXxRdu).
- Any evidence of software in your environment code signed with the DigiCert EV Codesigning Certificate Issued to TRATTORIA WYKI SP Z O O (SN: 074A080F649B2D5B784675B302A963B7 // Thumbprint: B43C94F107B19D2B23DB41F45D5ADCBC5342CD46).

- The specific components of `Windscribe.exe` - signed with this same certificate:
  - exe - SHA256: 1495500d6c8613fda22b0e0c8f2ab0ba5d244d6b166c5d854a47000a91f44ab1
  - WindscribePatchExe - SHA256: da88dc8fbc02a32d336fc8a20f67f01fc3fe833068d0275cb7f5610566d28824
  - Windscribe TAP install helper - SHA256: fb55cc18b16707eeb53dd51e0e4e1e7046fd7a9e1b2ec1f5a128cef8810bcbd9
  - aiui - SHA256: 77986a638410d6d312e5eef8dd142182b50623a3aae361ccf7e6d997ec1b7581

Theta Cyber Security would be grateful for any reports of hits for these IOCs for further co-ordination and tracking. Victimology, information regarding how victims were directed to the domains mentioned in this article and observations around follow-on activity would be most appreciated.

References

[1] https://www.inde.nz/blog/different-kind-of-zoombomb

[2] With a caveat that tight target selection on behalf of the threat actors may have significantly downsized detection opportunities – we do not have this visibility into target selection or victimology at the current time however.

[3] First discovered as SHA256: df8659f990176e4845615486055305a5dc7024c732850bc3043c64e8393dc38b – at C:\Users\<user.name>\AppData\Local\Temp\zoom\Zoom.exe

[4] First discovered as SHA256: fd03b531ad1d8d7358b7b50912841f81b6ea6e4e364ca6af8f0dc61aa7d3d152

[5] Execution flow of %temp%\`zoom.exe` -> cmd.exe -> powershell.exe -> b.ps1

[6] First discovered and reported as SHA256: f547410bd2f0b667b640e350d7c8c55cd4c2f7249e534c02c63d824c87ee2454 – b.ps1 – nb: a hard coded C2 IP in this script results in different SHA256 hashes.

[7] Despite reasonably heavy obfuscation of the capabilities of the script, the IP address it pointed to was available conspicuously in unencoded form right at the start of the file – we assess this was to facilitate the actors rotating it with new hard coded IPs if they suspected or suffered from detection of their early stage C2 infrastructure or perhaps proactively as part good operational security practices. At least 2 known b.ps1's exist at the current time. This further points to the operational cost and overhead for an actor in maintaining covert and operationally safe infrastructure – although we understand there is a multistage model of C2 infrastructure with the ZoomPortable Campaign and the loss of early stage C2 does not represent detection of the later C2 stages or the capabilities associated with it. We understand b.ps1 was downloaded from a first stage of C2 infrastructure prior to being executed on the host.

[8] ie: running out of %temp% and unpacking from 7zip archives.

[9] https://pastebin.com/FGHXxRdu

[10] https://urlscan.io/result/6cc2b423-6d01-4151-93c3-b8ab36824b69/

[11] https://urlscan.io/result/cc3bd261-7edb-4253-8284-009cfe04760a/

[12] See: https://crt.sh/?id=4331658350

[13] See: https://community.riskiq.com/search/5.39.216.179/resolutions

[14] https://urlscan.io/ - a powerful utility for threat hunting and defenders in general.

[15] All the malicious domains mentioned in this article appear to have been old and likely abandoned but benign domains before being acquired by the threat actor and updated to host malicious infrastructure – which is a useful technique in avoiding the suspicion that comes with using newly registered domains.

[16] https://crt.sh/?id=3815840137

[17] https://urlscan.io/result/6250dcdf-dde4-4ce9-841f-6e762550b201/

[18] https://windscribe.com/

[19] Compare with the two known ZoomPortable binaries hosted @

https[:]//zoom-download[.]s3[.]us-east-2[.]amazonaws[.]com/ZoomPortable.exe

https[:]//zoom-portable[.]s3[.]us-east-2[.]amazonaws[.]com/ZoomPortable.exe

[20] see: https://urlscan.io/result/6250dcdf-dde4-4ce9-841f-6e762550b201/#links

[21] See:
https://www.virustotal.com/gui/url/b4b5a269db3cbaf333e754f7a58a0b723e6529fe61b5438b664795f4545f74c5/detection

[22]
https://www.virustotal.com/gui/file/1495500d6c8613fda22b0e0c8f2ab0ba5d244d6b166c5d854a47000a91f44ab1/details

[23] SHA256: 1495500d6c8613fda22b0e0c8f2ab0ba5d244d6b166c5d854a47000a91f44ab1

[24] Aka SHA256: df8659f990176e4845615486055305a5dc7024c732850bc3043c64e8393dc38b

[25]
https://www.virustotal.com/gui/file/da88dc8fbc02a32d336fc8a20f67f01fc3fe833068d0275cb7f5610566d28824/details

[26]
https://www.virustotal.com/gui/file/fb55cc18b16707eeb53dd51e0e4e1e7046fd7a9e1b2ec1f5a128cef8810bcbd9/details

[27]
https://www.virustotal.com/gui/file/77986a638410d6d312e5eef8dd142182b50623a3aae361ccf7e6d997ec1b7581/details

24/7 protection with Theta Managed Detection and Response

Concerned about keeping up with cyber threats? Our Managed Detection and Response (MDR) service is designed to be cost-effective, faster and offers quality results compared with legacy MSSPs or running technology in-house. It keeps costs down because of scale, focuses on real threats, and you'll benefit from having automation and intelligence experts involved.

Find out more about Theta Managed Detection and Response

Report by Hamish Krebs, Lead Consultant at Theta

Hamish has spent time across Australia and New Zealand responding to advanced threat actors; running large DFIR engagements in complex environments. He's also designed and deployed a variety of security solutions such as SIEMs and EDR suites across APAC.