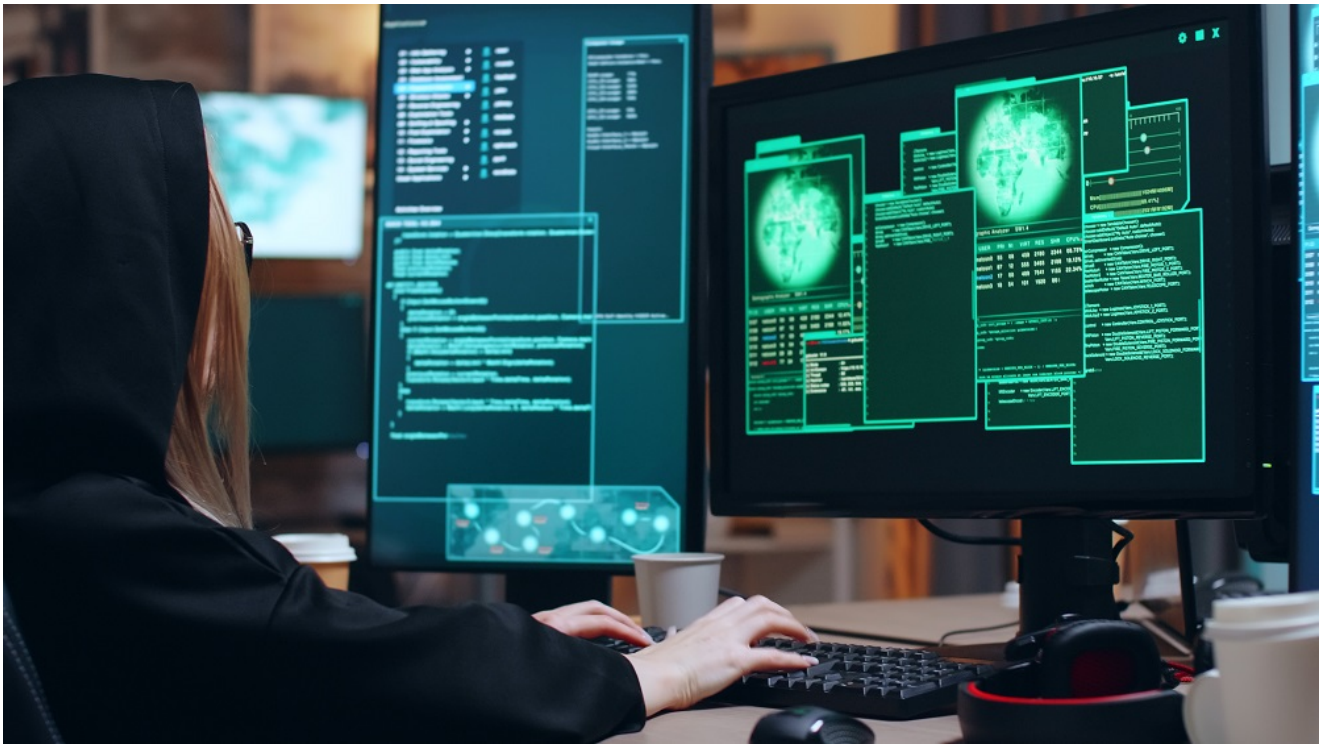
More AgentTesla Keylogger And Nanocore RAT In One Bundle

myonlinesecurity.co.uk/more-agenttesla-keylogger-and-nanocore-rat-in-one-bundle/

June 25, 2019

By: Derek | Last Updated on 07 April 2022



We are seeing a continuation of even more AgentTesla malspam campaigns again this morning. However today's is somewhat different to usual and also delivers a Nanocore RAT. Actually the Nanocore RAT is downloading the AgentTesla keylogger. And after a bit of digging around and seeing an Open Directory listing on the AgentTesla download site we found another multi-stage JavaScript downloader which delivers what looks like Dunhini /Houdini /h-worm and WSHRAT along with more Nanocore or at least using the same C2 and download structures as recent nanocore samples.

Once again the scumbags sending these are using ISO attachments, which generally speaking are very badly detected by antiviruses, mailscanners or perimeter defences. Many AV and "next gen" anti-malware services do not routinely scan an ISO file but rely on detecting the extracted file. This is one of the few file types that you are actually slightly safer using Windows 7.

You need a 3rd party extraction (unzipping) program to extract the executable content from the container. Winzip & Winrar along with several other 3rd party unzipping tools does do this, but are not set to open iso files by default, so need a few clicks from you to do it. Windows 7 will natively try to open the ISO in Windows ISO burner and copy it to a cd/dvd for you. Whereas the more modern & "safer" OS W8.1 and W10 will normally offer to mount the ISO. This means open it as a virtual cd drive so the .exe file is shown in file explorer ready for you to click on & run. While the exe file is inside the ISO container it is safe and will not harm you. It should not automatically run when mounted.

Many ISO do have an auto-run command embedded (for example Microsoft Windows 10 or Office downloads) , but I can't see one in these.

You can now submit suspicious sites, emails and files via our Submissions system

Jabil.com has not been hacked or had their email or other servers compromised. They are not sending the emails to you. They are just innocent victims in exactly the same way as every recipient of these emails. I first saw the sending IP / Server being used yesterday in a fake DHL campaign delivering a very similar JS downloader contacting many of the same sites.

From: "Amanda Guimarães" <AMANDA_GUIMARAES@Jabil.com>
Date: Mon 24/06/2021 22:05
Subject: FYI New Order #PO1205356266, Brazil
Attachment: NEW_PO_1205356266,pdf.iso

Body Content:

> Dear security,
>
> We are really interested in your products could you please kindly check attached?
> our new trial order please quote and confirm to us estimated delivery time to brazil.
>
> Thank you,
> **Amanda Guimarães**
> Buyer
> Belo Horizonte Site
> Desk: +55(31) 2103 – 9312
> Rod. Fernão Dias, Km 490, br381, Jardim das Alteroras
> 32670-790, Betim, MG, Brasil

Malware Details:

NEW_PO_1205356266,pdf.iso (VirusTotal) extracts to NEW_PO_1205356266,pdf.exe VirusTotal | Anyrun | Which is the nanocore binary. The C2 for this nanocore is microsoft.btc-crypto-rewards.cash 160.202.163.246

This downloads and autoruns the AgentTesla binary
http://mechanicaltools.club/download/2oxEJ50zPS4Wsdb.exe virusTotal | Anyrun |

The C2 / SMTP exfiltration for this AgentTesla is **smtp.vivaldi.net** 82.221.130.149 but I can't easily determine the email address of the miscreant.

Now when we looked at the download site for AgentTesla mechanicaltools.club we found an Open Directory listing with lots of files.

This domain was only registered yesterday 24 June 2021 using privacy protection via Namecheap as registrar and hosted by Namecheap. The home page has a default hosted by Namecheap holding page. This was obviously registered by these criminals to be used in malware campaigns.

This set of files tries to download the same nanocore that was inside the ISO container. I assume there must have been an email with links, that would trigger the download chain. The bad actors have made a bit of an error by starting the chain with a MHT file **http://mechanicaltools.club/download/mhtexp.mht** (VirusTotal) which only work in Internet Explorer and display as plain text in other browsers and will not offer the downloaded next step in the chain.

http://mechanicaltools.club/download/mhtexp.php which simply downloads
http://mechanicaltools.club/download/mhtexp.hta (VirusTotal) which in turn downloads & runs
http://mechanicaltools.club/download/mhtexp.js VirusTotal | Anyrun | which is a heavily encoded scripting file that downloads and runs these 3 files which are actually renamed .exe files not zip files at all. But all are very well detected on VirusTotal
http://doughnut-snack.live/klplu.tar.gz VirusTotal | Anyrun |
http://doughnut-snack.live/bpvpl.tar.gz VirusTotal | Anyrun |
http://doughnut-snack.live/mapv.tar.gz VirusTotal | Anyrun |

All the alleged senders, companies, names of employees, phone numbers, amounts, reference numbers etc. mentioned in the emails are all innocent and are just picked at random. Some of these companies will exist and some won't. Don't try to respond by phone or email, all you will do is end up with an innocent person or company who have had their details spoofed and picked at random from a long list that the bad guys have previously found .

The bad guys choose companies, Government departments and other organisations with subjects that are designed to entice you or alarm you into blindly opening the attachment or clicking the link in the email to see what is happening.

Email Headers:

IP	Hostname	City	Region	Country	Organisation

IP	Hostname	City	Region	Country	Organisation
45.14.112.110		Fallings Park	Wolverhampton	GB	AS60945 VeloxServ Communications Ltd

```
Received: from [45.14.112.110] (port=61347)
        by my email server with esmtp (Exim 4.92)
        (envelope-from <AMANDA_GUIMARAES@Jabil.com>)
        id 1hfW8k-00065U-9j
        for security@myonlinesecurity.co.uk; Mon, 24 Jun 2021 22:04:38 +0100
From: =?UTF-8?B?IkFtYW5kYSBHdWltYXLDo2VzIg==?= <AMANDA_GUIMARAES@Jabil.com>
To: security@myonlinesecurity.co.uk
Subject: FYI New Order #PO1205356266, Brazil
Date: 24 Jun 2021 14:04:34 -0700
Message-ID: <20190624140433.033401D494FDCED4@Jabil.com>
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="----=_NextPart_000_0012_62826778.96920426"
```

IOC:

Main object- “NEW_PO_1205356266,pdf.iso”
sha256 1b80e4d13b53c9fff4caced8bc44c2d61248d55d2cf66fd68a93fa29ccbd17c0
sha1 a13c5c54fc89be75623738257ae15bdd34f9fbdb
md5 60e8f75ba8588b97cd31992b2335f750
Dropped executable file
sha256 C:\Users\admin\Desktop\NEW_PO_1205356266,pdf.exe
a96a80d3565e9b2f55c4a9770a4a911fbbdfccf470809c59eda9b1c3b3fbc072
MD5 8d46822356da392beb731ceaaf919489
SHA-1 39f832abe4137c97c79eeb174e96b4460b93564a
sha256 C:\Users\admin\AppData\Local\Temp\windowsdefender.exe
9a53593239f4f04ca6f28e3eab6c4b51cc869c2b366e322df2d900e75b6c3da0
MD5 557b476ea0c8b987f970b9eb3cb52e5f
SHA-1 2e2ba396b8ac8b1044c8058e004fb174e788d6a4
DNS requests
domain mechanicaltools.club
domain microsoft.btc-crypto-rewards.cash
domain checkip.amazonaws.com
Connections
ip 198.54.114.213
ip 185.244.29.22
ip 160.202.163.246
ip 52.200.125.74
HTTP/HTTPS requests
url http://checkip.amazonaws.com/
url http://mechanicaltools.club/download/2oxEJ50zPS4Wsdb.exe

Main object- “bpvpl.tar.gz”
sha256 27bd6db946dd85de546f6fb9b80658e46ecd327136773c949cd212ddfd52aa4e
sha1 8b1c131f6b9dc1f020a18ab8f4fa3095224adcc9
md5 5a2b62b657782f37eb0f7c27064cffa9
Dropped executable file
sha256 C:\Users\admin\Desktop\bpvpl.tar.exe
27bd6db946dd85de546f6fb9b80658e46ecd327136773c949cd212ddfd52aa4e
Main object- “klplu.tar.gz”
sha256 272e64291748fa8be01109faa46c0ea919bf4baf4924177ea6ac2ee0574f1c1a
sha1 37b644ef5722709cd9024a372db4590916381976
md5 7099a939fa30d939ccceb2f0597b19ed
Main object- “mapv.tar.gz”
sha256 bfcde7f66c042845af095b5600d1e7a383926e2836624f7eb1690b078e9cfe28
sha1 a988b152469a8b22052377d4127f0a3ee0a92927
md5 c4c6fe64765bc68c0d6fcaf2765b5319
Main object- “2oxEJ50zPS4Wsdb.exe”
sha256 9a53593239f4f04ca6f28e3eab6c4b51cc869c2b366e322df2d900e75b6c3da0
sha1 2e2ba396b8ac8b1044c8058e004fb174e788d6a4
md5 557b476ea0c8b987f970b9eb3cb52e5f
DNS requests
domain smtp.vivaldi.net
domain checkip.amazonaws.com
Connections
ip 192.35.177.64
ip 82.221.130.149
ip 18.211.215.84
HTTP/HTTPS requests
url http://checkip.amazonaws.com/
Main object- “mhtexp.js”
sha256 27302c2238440ebf93b3e3e6639e9df3586895cc1e236952e300d07353158bc5
sha1 290431f521e45f5f2345e314ad89403a6220ff32
md5 86c75fb3cd45155afbed0a537b7b215e
Dropped executable file
sha256 C:\Users\admin\AppData\Roaming\kl-plugin.exe
272e64291748fa8be01109faa46c0ea919bf4baf4924177ea6ac2ee0574f1c1a
sha256
C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\ZSVOB39W\bpvpl.tar[1].gz
27bd6db946dd85de546f6fb9b80658e46ecd327136773c949cd212ddfd52aa4e
sha256
C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\WLQBH2R9\mapv.tar[1].gz
bfcde7f66c042845af095b5600d1e7a383926e2836624f7eb1690b078e9cfe28
DNS requests

domain microsoft.btc-crypto-rewards.cash
domain unknownsoft.duckdns.org
domain doughnut-snack.live
Connections
ip 185.247.228.14
ip 160.202.163.246
ip 172.245.14.10
HTTP/HTTPS requests
url http://microsoft.btc-crypto-rewards.cash:9966/is-ready
url http://doughnut-snack.live/klplu.tar.gz
url http://doughnut-snack.live/bpvpl.tar.gz
url http://doughnut-snack.live/mapv.tar.gz
http://mechanicaltools.club/download/2oxEJ50zPS4Wsdb.exe
http://mechanicaltools.club/download/NEW_PO_1205356266,pdf.exe
http://mechanicaltools.club/download/mhtexp.hta
http://mechanicaltools.club/download/mhtexp.js
http://mechanicaltools.club/download/mhtexp.mht
http://mechanicaltools.club/download/mhtexp.php
mhtexp.mht
MD5 381b3624498e29b48464b3251e8c5203
SHA-1 11dfc573ec4c38475c9c58a61ecba24e26358c29
SHA-256 1e4b0aa62e6cebd7991c3c68759032e767c32ad2e07d6ffb11ad7b99c9155a6c
mhtexp.hta
MD5 5a7727673fbb359f54ce36fcc1faa6df
SHA-1 976a65329869c60c763e58b8986507bf09bd568c
SHA-256 9ecc1efb8b8bf7674dcb579e76b0f7b334068e6ea2ff77fedc8d9a16867da170

Derek