NEWS | THREATS

New AgentTesla variant steals WiFi credentials

Posted: April 16, 2020 by Hossein Jazi

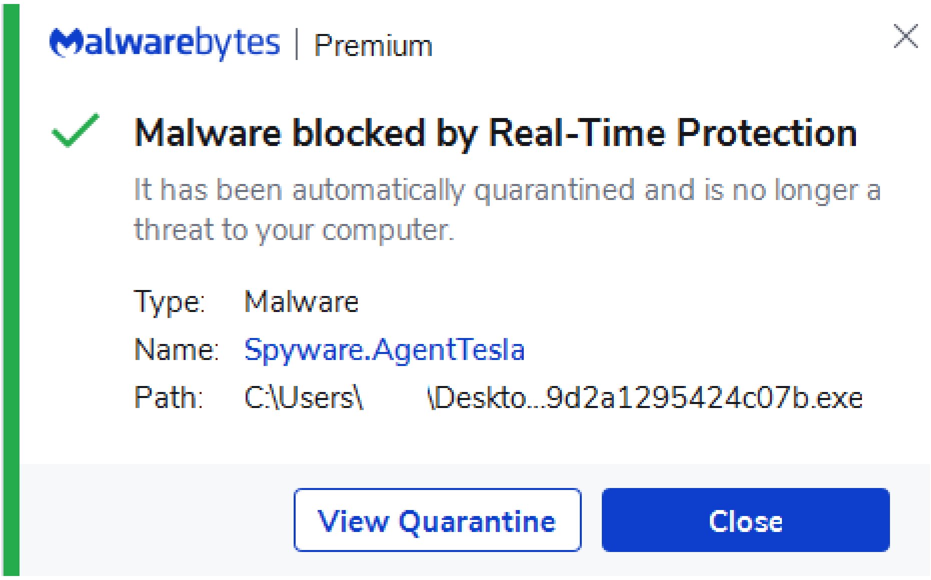
AgentTesla is a .Net-based infostealer that has the capability to steal data from different applications on victim machines, such as browsers, FTP clients, and file downloaders. The actor behind this malware is constantly maintaining it by adding new modules. One of the new modules that has been added to this malware is the capability to steal WiFi profiles.

Malwarebytes LABS

Newer variants of AgentTesla seen in the wild have the capability to collect information about a victim's WiFi profile, possibly to use it as a way to spread onto other machines. In this blog, we review how this new feature works.

Technical analysis

The variant we analyzed was written in .Net. It has an executable embedded as an image resource, which is extracted and executed at run-time (Figure 1).



Malware blocked by Real-Time Protection

It has been automatically quarantined and is no longer a threat to your computer.

Type: Malware
Name: Spyware.AgentTesla
Path: C:\Users\   \Deskto...9d2a1295424c07b.exe

Indicators of compromise

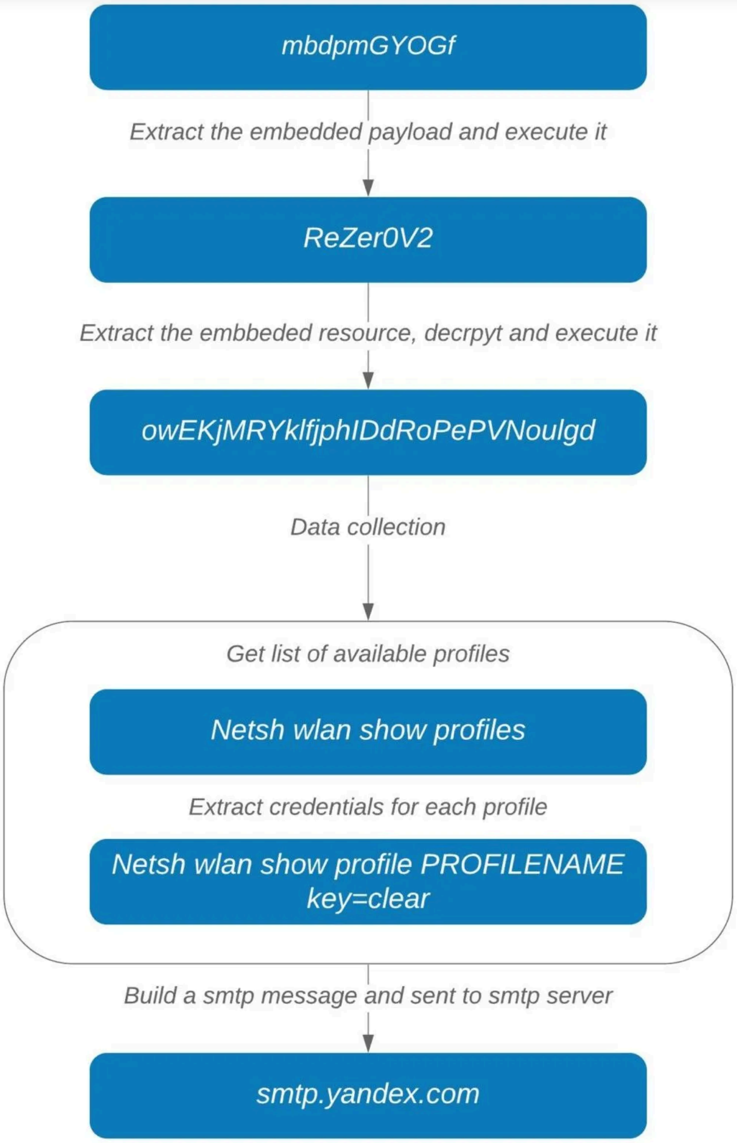
AgentTesla samples:

```
91b711812867b39537a2cd81bb1ab10315ac321a1c68e316bf4fa84badbc09b
dd4a43b0b8a68db65b00fad99519539e2a05a3892f03b869d58ee15fdf5aa044
27939b70928b285655c863fa26efded96bface9db46f35ba39d2a1295424c07b
```

First payload:

```
249a503263717051d62a6d65a5040cf408517dd22f9021e5f8978a819b18063b
```

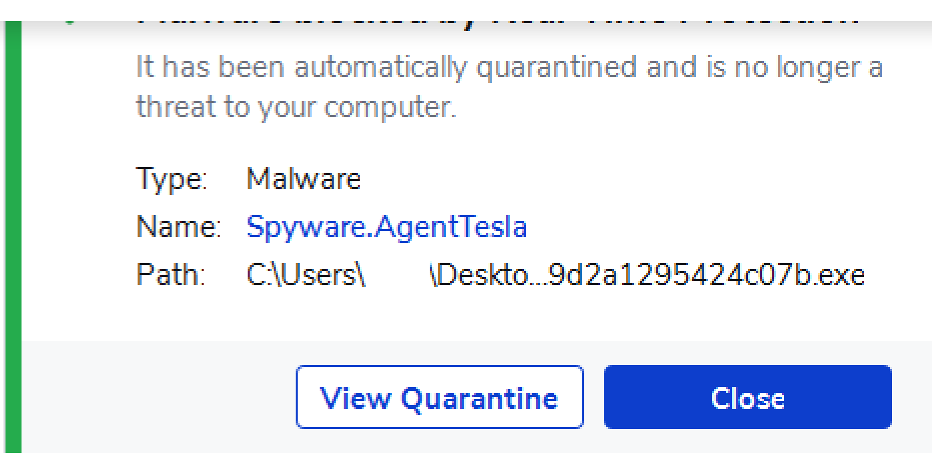
Second payload:


mbdpmGYOGf
Extract the embedded payload and execute it
ReZer0V2
Extract the embbeded resource, decrpyt and execute it
owEKjMRYklfjphIDdRoPePVNoulgd
Data collection
Get list of available profiles
Netsh wlan show profiles
Extract credentials for each profile
Netsh wlan show profile PROFILENAME key=clear
Build a smtp message and sent to smtp server
smtp.yandex.com

Popular stealer looking to expand

Since AgentTesla added the WiFi-stealing feature, we believe the threat actors may be considering using WiFi as a mechanism for spread, similar to what was observed with Emotet. Another possibility is using the WiFi profile to set the stage for future attacks.

Either way, Malwarebytes users were already protected from this new variant of AgentTesla through our real-time protection technology.



It has been automatically quarantined and is no longer a threat to your computer.

Type: Malware
Name: Spyware.AgentTesla
Path: C:\Users\ \Deskto...9d2a1295424c07b.exe

Indicators of compromise

AgentTesla samples:

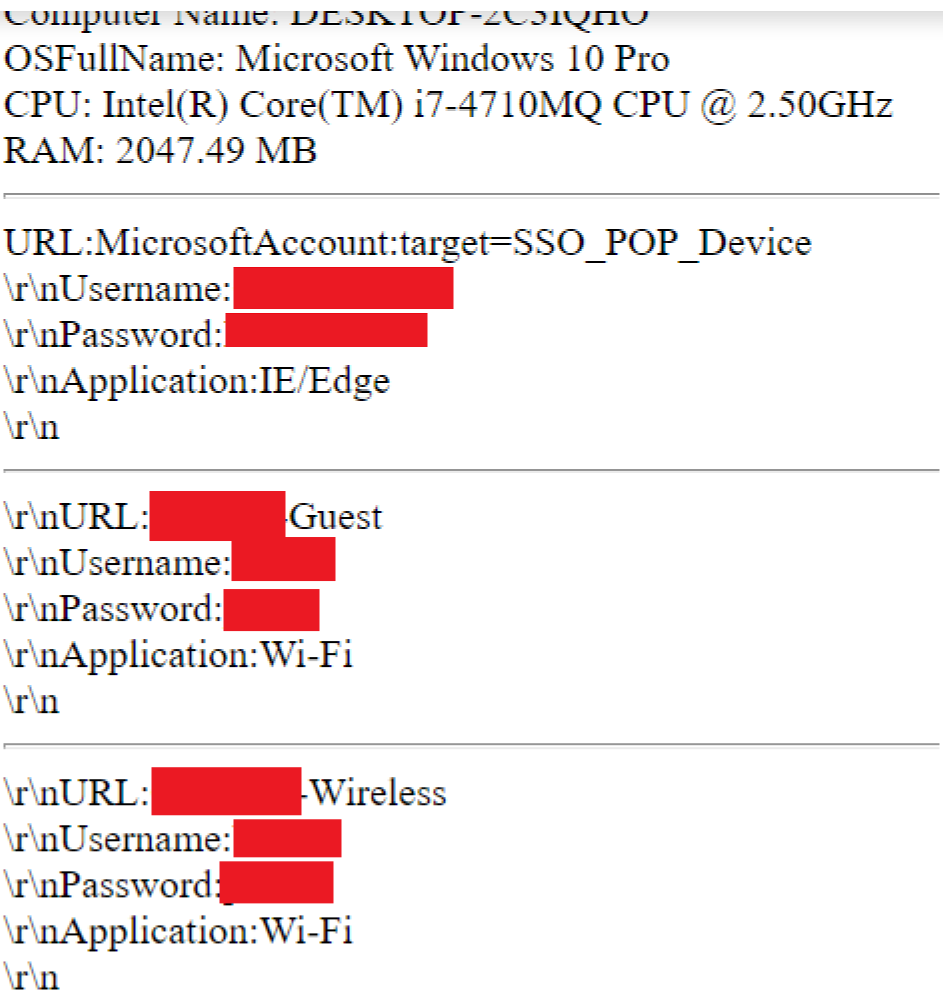
```
91b711812867b39537a2cd81bb1ab10315ac321a1c68e316bf4fa84badbc09b
dd4a43b0b8a68db65b00fad99519539e2a05a3892f03b869d58ee15fdf5aa044
27939b70928b285655c863fa26efded96bface9db46f35ba39d2a1295424c07b
```

First payload:

```
249a503263717051d62a6d65a5040cf408517dd22f9021e5f8978a819b18063b
```

Second payload:

```
63393b114ebe2e18d888d982c5ee11563a193d9da3083d84a611384bc748b1b0
```



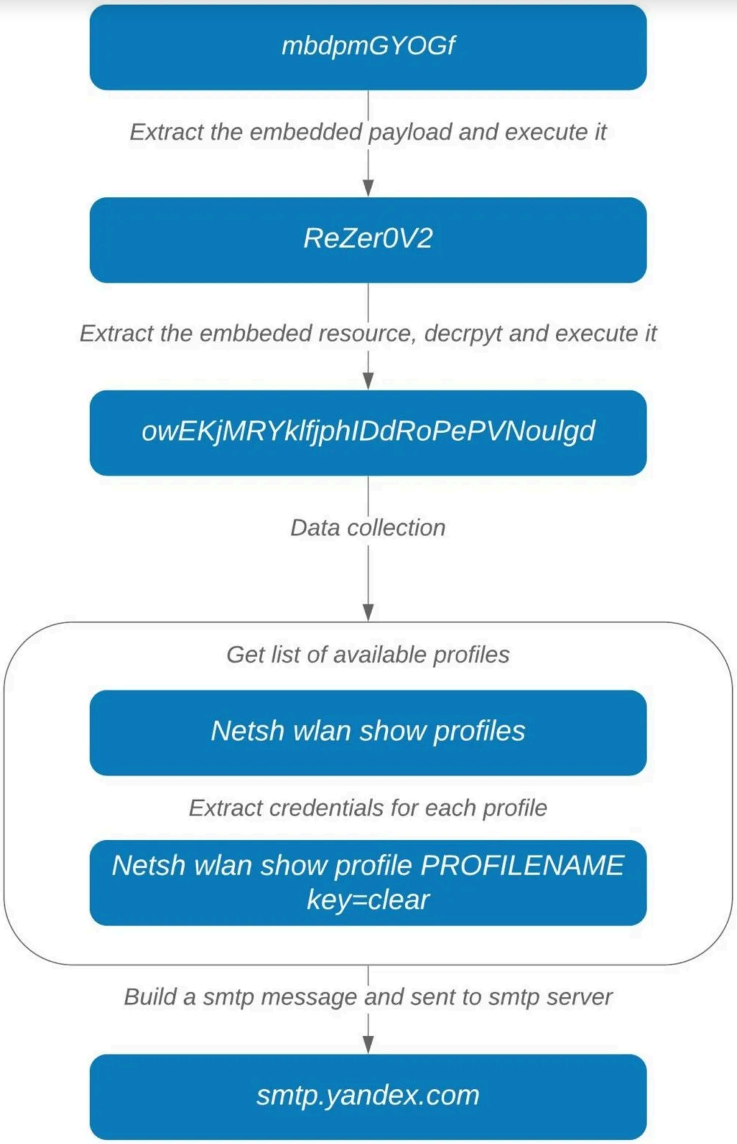
```
Computer Name: DESKTOP-2C3IQHO
OSFullName: Microsoft Windows 10 Pro
CPU: Intel(R) Core(TM) i7-4710MQ CPU @ 2.50GHz
RAM: 2047.49 MB
```

```
URL:MicrosoftAccount:target=SSO_POP_Device
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:IE/Edge
\r\n
```

```
\r\nURL:[redacted]-Guest
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:Wi-Fi
\r\n
```

```
\r\nURL:[redacted]-Wireless
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:Wi-Fi
\r\n
```

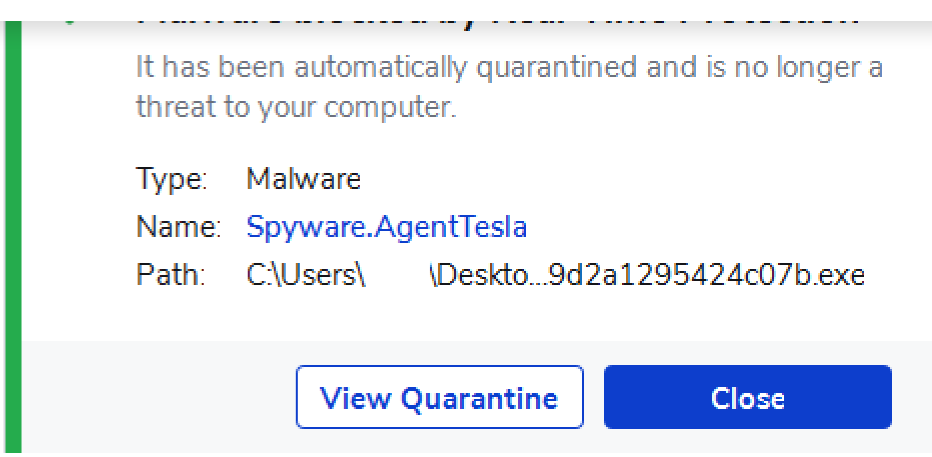
Note: If the final list has less than three elements, it won’t generate a SMTP message. If everything checks out, a message is finally sent via smtp.yandex.com, with SSL enabled (Figure 9):


mbdpmGYOGf
Extract the embedded payload and execute it
ReZer0V2
Extract the embbeded resource, decrpyt and execute it
owEKjMRYklfjphIDdRoPePVNoulgd
Data collection
Get list of available profiles
Netsh wlan show profiles
Extract credentials for each profile
Netsh wlan show profile PROFILENAME key=clear
Build a smtp message and sent to smtp server
smtp.yandex.com

Popular stealer looking to expand

Since AgentTesla added the WiFi-stealing feature, we believe the threat actors may be considering using WiFi as a mechanism for spread, similar to what was observed with Emotet. Another possibility is using the WiFi profile to set the stage for future attacks.

Either way, Malwarebytes users were already protected from this new variant of AgentTesla through our real-time protection technology.



It has been automatically quarantined and is no longer a threat to your computer.

Type: Malware
Name: Spyware.AgentTesla
Path: C:\Users\ \Deskto...9d2a1295424c07b.exe

Indicators of compromise

AgentTesla samples:

```
91b711812867b39537a2cd81bb1ab10315ac321a1c68e316bf4fa84badbc09b
dd4a43b0b8a68db65b00fad99519539e2a05a3892f03b869d58ee15fdf5aa044
27939b70928b285655c863fa26efded96bface9db46f35ba39d2a1295424c07b
```

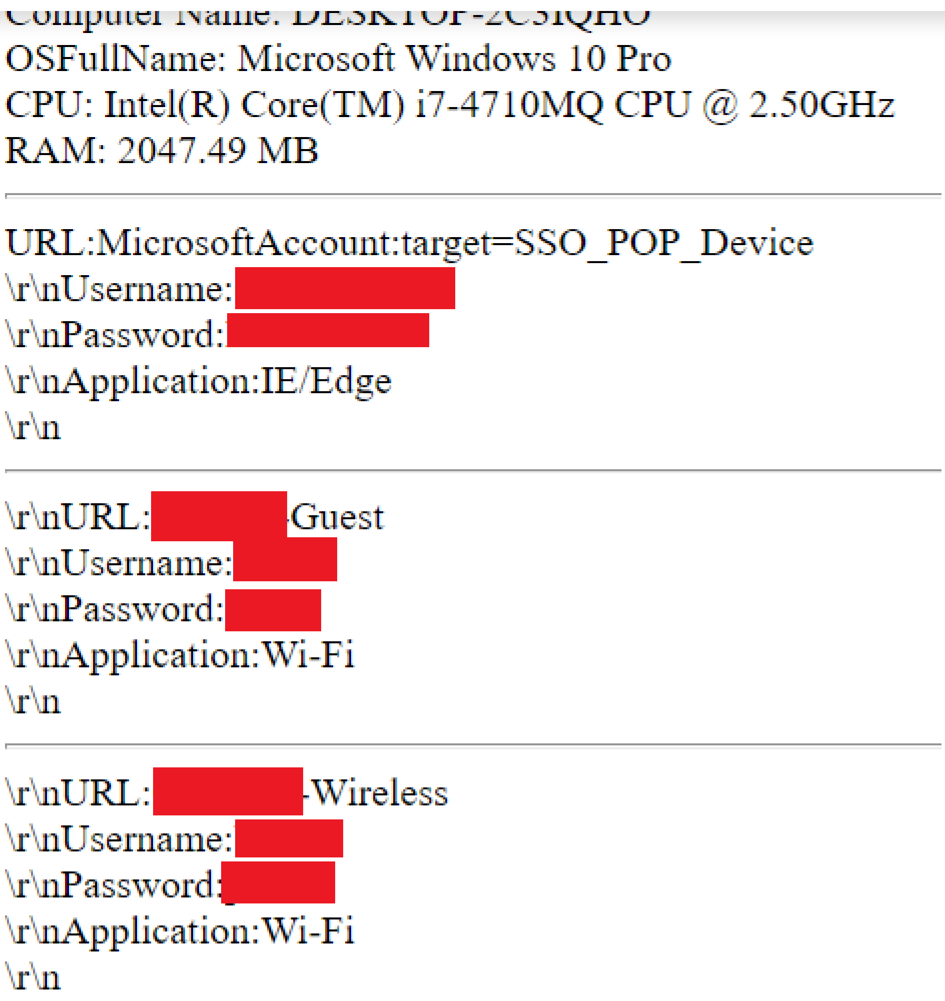
First payload:

```
249a503263717051d62a6d65a5040cf408517dd22f9021e5f8978a819b18063b
```

Second payload:

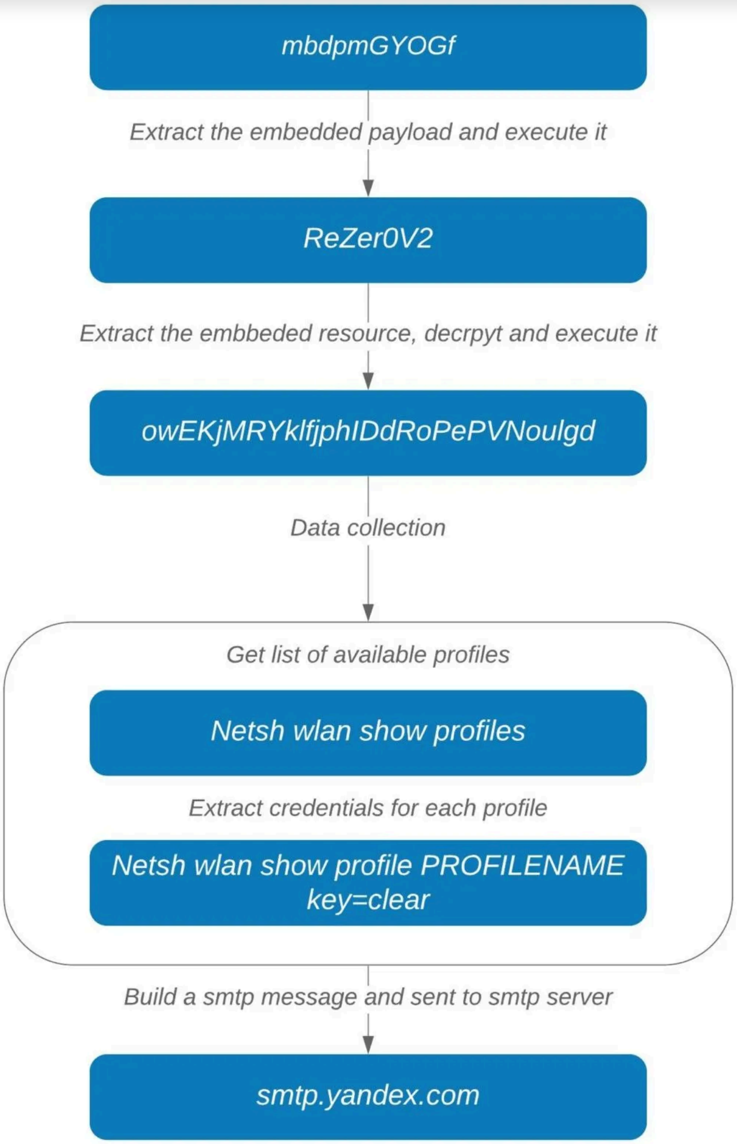
```
63393b114ebe2e18d888d982c5ee11563a193d9da3083d84a611384bc748b1b0
```

Collected information forms the body section of a SMTP message in html format (Figure 8):



```
Computer Name: DESKTOP-2C3IQHO
OSFullName: Microsoft Windows 10 Pro
CPU: Intel(R) Core(TM) i7-4710MQ CPU @ 2.50GHz
RAM: 2047.49 MB
________________________________________
URL:MicrosoftAccount:target=SSO_POP_Device
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:IE/Edge
\r\n
________________________________________
\r\nURL:[redacted]-Guest
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:Wi-Fi
\r\n
________________________________________
\r\nURL:[redacted]-Wireless
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:Wi-Fi
\r\n
```

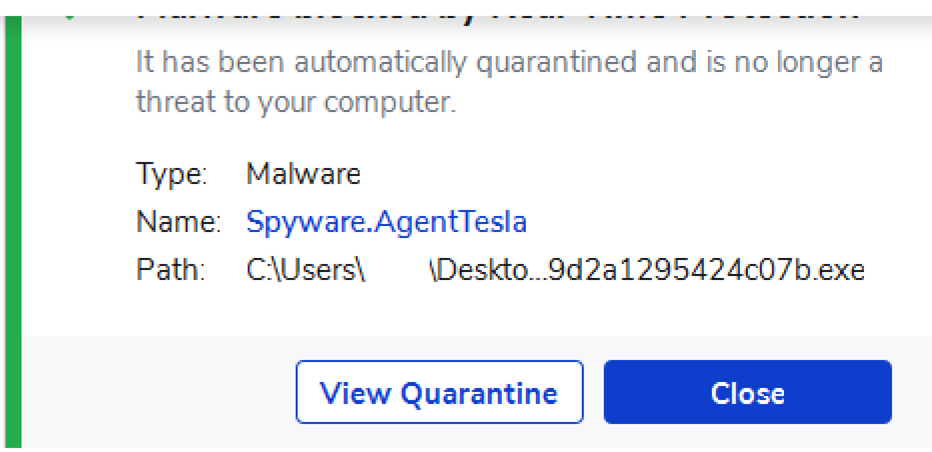
Note: If the final list has less than three elements, it won’t generate a SMTP message. If everything checks out, a message is finally sent via smtp.yandex.com, with SSL enabled (Figure 9):


mbdpmGYOGf
Extract the embedded payload and execute it
ReZer0V2
Extract the embbeded resource, decrpyt and execute it
owEKjMRYklfjphIDdRoPePVNoulgd
Data collection
Get list of available profiles
Netsh wlan show profiles
Extract credentials for each profile
Netsh wlan show profile PROFILENAME key=clear
Build a smtp message and sent to smtp server
smtp.yandex.com

Popular stealer looking to expand

Since AgentTesla added the WiFi-stealing feature, we believe the threat actors may be considering using WiFi as a mechanism for spread, similar to what was observed with Emotet. Another possibility is using the WiFi profile to set the stage for future attacks.

Either way, Malwarebytes users were already protected from this new variant of AgentTesla through our real-time protection technology.



It has been automatically quarantined and is no longer a threat to your computer.

Type: Malware
Name: Spyware.AgentTesla
Path: C:\Users\ \Deskto...9d2a1295424c07b.exe

Indicators of compromise

AgentTesla samples:

```
91b711812867b39537a2cd81bb1ab10315ac321a1c68e316bf4fa84badbc09b
dd4a43b0b8a68db65b00fad99519539e2a05a3892f03b869d58ee15fdf5aa044
27939b70928b285655c863fa26efded96bface9db46f35ba39d2a1295424c07b
```

First payload:

```
249a503263717051d62a6d65a5040cf408517dd22f9021e5f8978a819b18063b
```

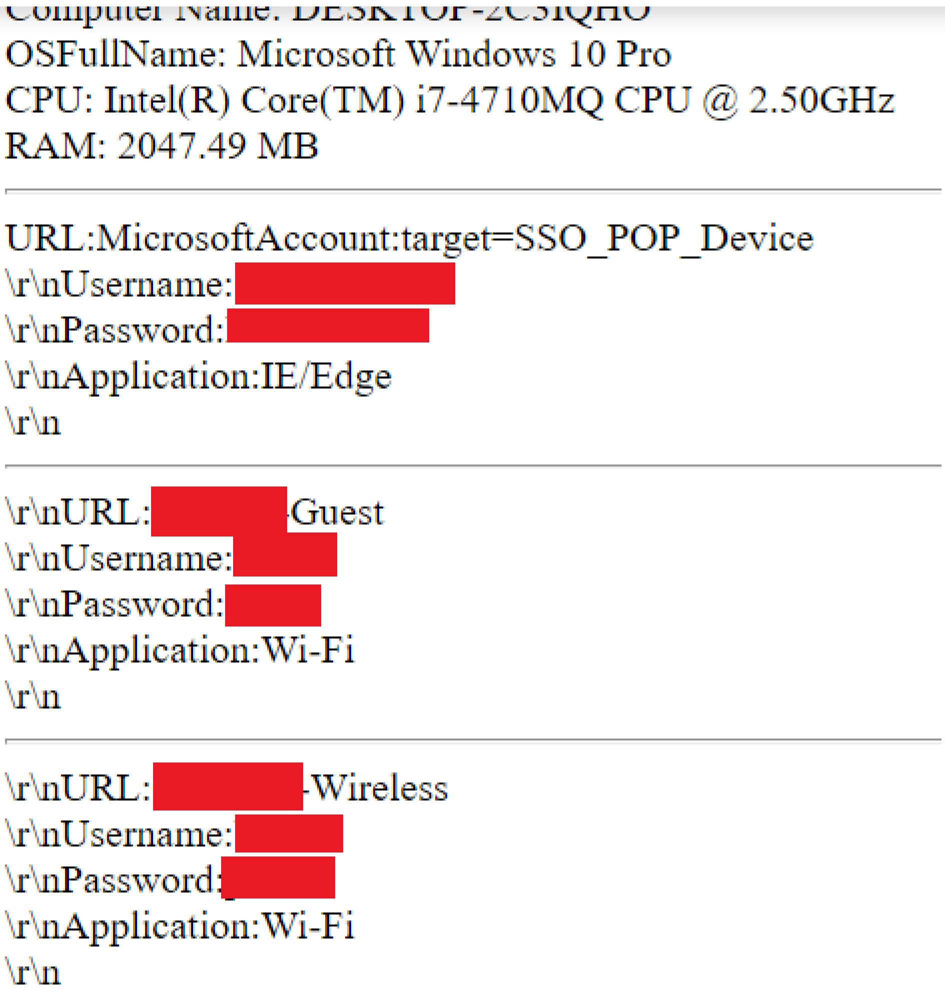
Second payload:

```
63393b114ebe2e18d888d982c5ee11563a193d9da3083d84a611384bc748b1b0
```

For example, in Figure 5, “119216” is decrypted into “wlan show profile name=” and “119196” is decrypted into “key=clear”.

In addition to WiFi profiles, the executable collects extensive information about the system, including FTP clients, browsers, file downloaders, and machine info (username, computer name, OS name, CPU architecture, RAM) and adds them to a list (Figure 7).

Collected information forms the body section of a SMTP message in html format (Figure 8):



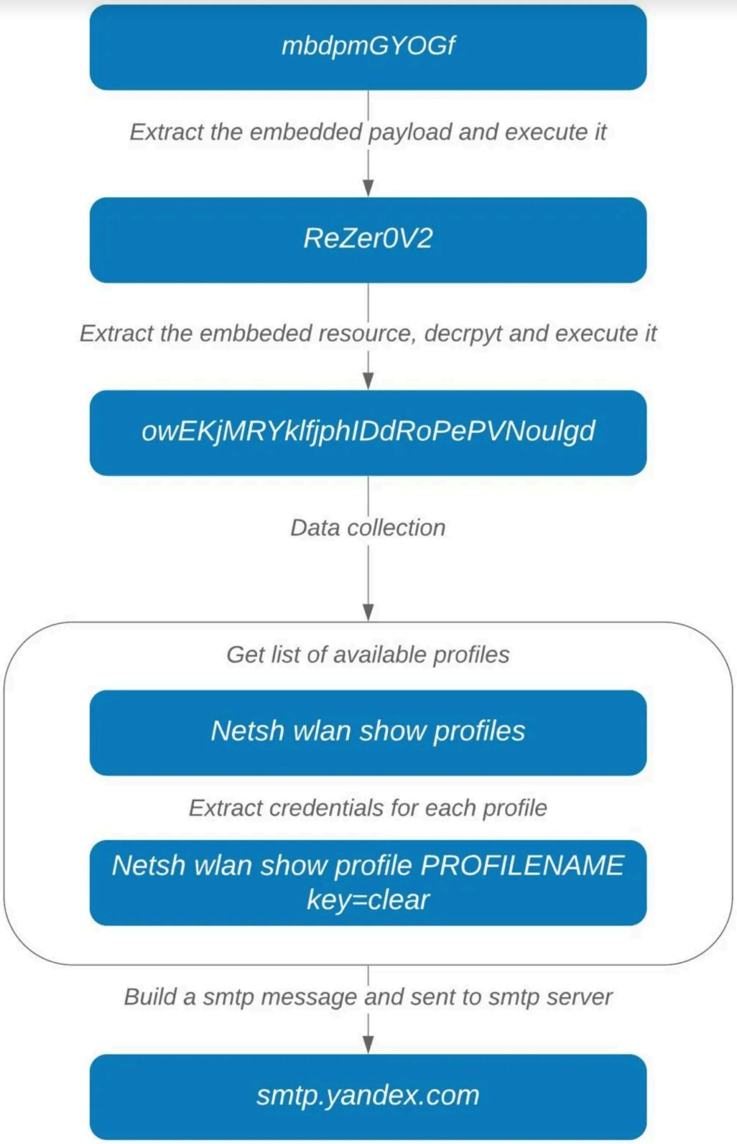
```
Computer Name: DESKTOP-2C5IQHO
OSFullName: Microsoft Windows 10 Pro
CPU: Intel(R) Core(TM) i7-4710MQ CPU @ 2.50GHz
RAM: 2047.49 MB

URL:MicrosoftAccount:target=SSO_POP_Device
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:IE/Edge
\r\n

\r\nURL:[redacted]-Guest
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:Wi-Fi
\r\n

\r\nURL:[redacted]-Wireless
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:Wi-Fi
\r\n
```

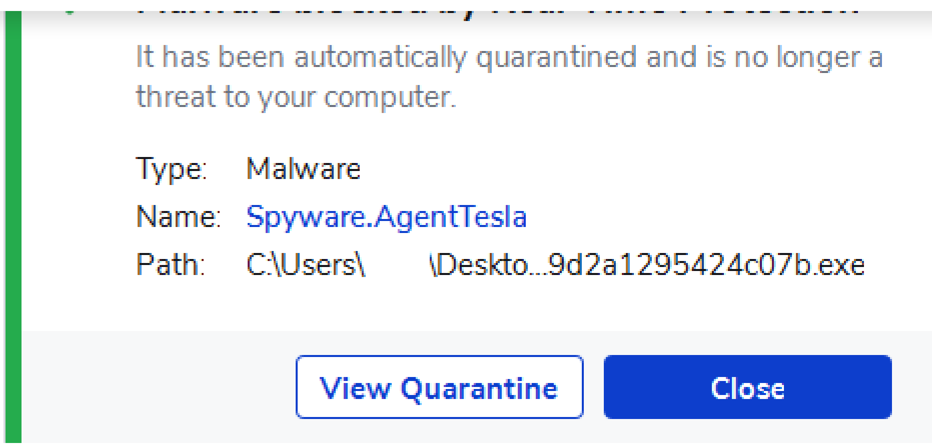
Note: If the final list has less than three elements, it won't generate a SMTP message. If everything checks out, a message is finally sent via smtp.yandex.com, with SSL enabled (Figure 9):


mbdpmGYOGf
Extract the embedded payload and execute it
ReZer0V2
Extract the embbeded resource, decrpyt and execute it
owEKjMRYklfjphIDdRoPePVNoulgd
Data collection
Get list of available profiles
Netsh wlan show profiles
Extract credentials for each profile
Netsh wlan show profile PROFILENAME key=clear
Build a smtp message and sent to smtp server
smtp.yandex.com

Popular stealer looking to expand

Since AgentTesla added the WiFi-stealing feature, we believe the threat actors may be considering using WiFi as a mechanism for spread, similar to what was observed with Emotet. Another possibility is using the WiFi profile to set the stage for future attacks.

Either way, Malwarebytes users were already protected from this new variant of AgentTesla through our real-time protection technology.



It has been automatically quarantined and is no longer a threat to your computer.

Type: Malware
Name: Spyware.AgentTesla
Path: C:\Users\ \Deskto...9d2a1295424c07b.exe

Indicators of compromise

AgentTesla samples:

```
91b711812867b39537a2cd81bb1ab10315ac321a1c68e316bf4fa84badbc09b
dd4a43b0b8a68db65b00fad99519539e2a05a3892f03b869d58ee15fdf5aa044
27939b70928b285655c863fa26efded96bface9db46f35ba39d2a1295424c07b
```

First payload:

```
249a503263717051d62a6d65a5040cf408517dd22f9021e5f8978a819b18063b
```

Second payload:

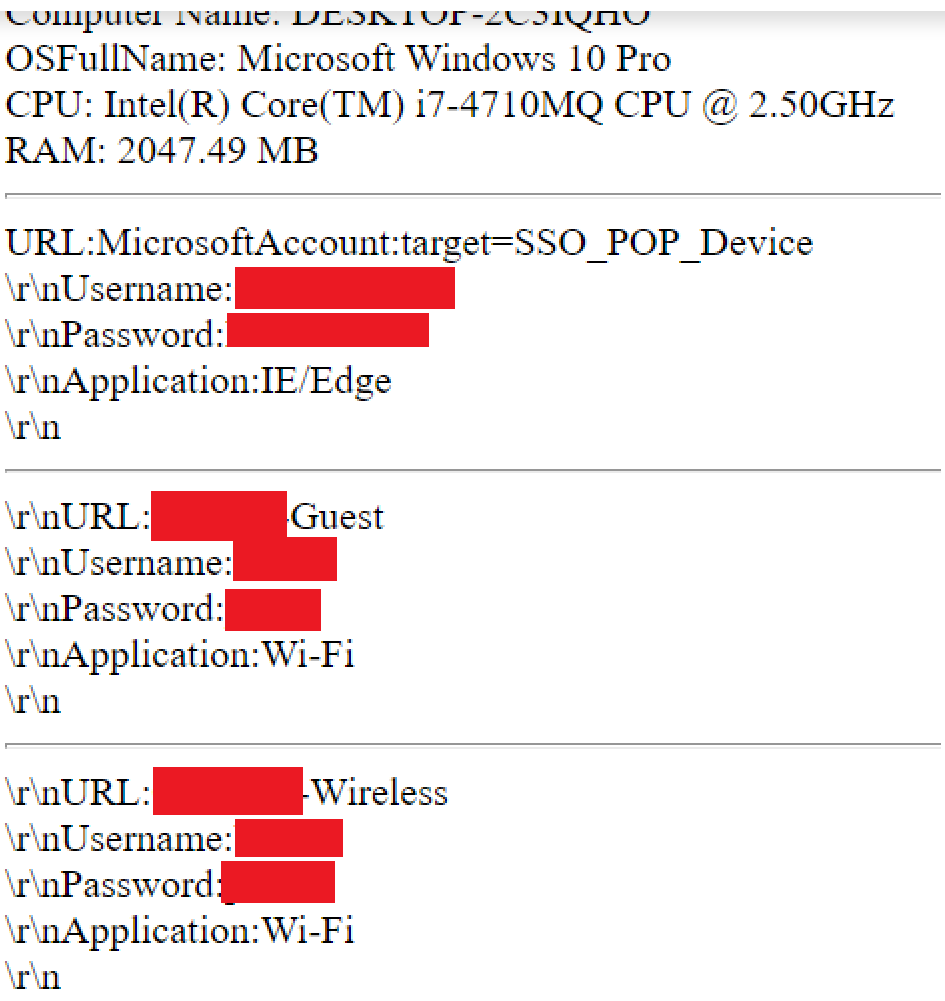
```
63393b114ebe2e18d888d982c5ee11563a193d9da3083d84a611384bc748b1b0
```

String encryption

For example, in Figure 5, “119216” is decrypted into “wlan show profile name=” and “119196” is decrypted into “key=clear”.

In addition to WiFi profiles, the executable collects extensive information about the system, including FTP clients, browsers, file downloaders, and machine info (username, computer name, OS name, CPU architecture, RAM) and adds them to a list (Figure 7).

Collected information forms the body section of a SMTP message in html format (Figure 8):



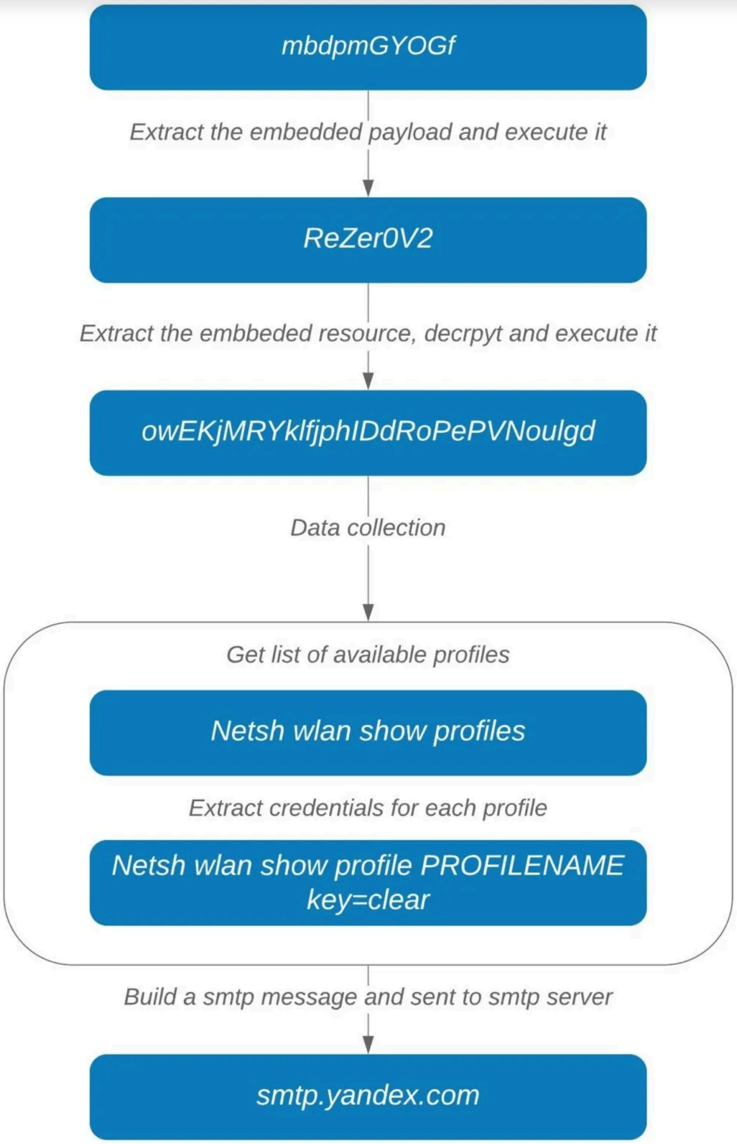
```
Computer Name: DESKTOP-2C3IQHO
OSFullName: Microsoft Windows 10 Pro
CPU: Intel(R) Core(TM) i7-4710MQ CPU @ 2.50GHz
RAM: 2047.49 MB
```

```
URL:MicrosoftAccount:target=SSO_POP_Device
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:IE/Edge
\r\n
```

```
\r\nURL:[redacted]-Guest
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:Wi-Fi
\r\n
```

```
\r\nURL:[redacted]-Wireless
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:Wi-Fi
\r\n
```

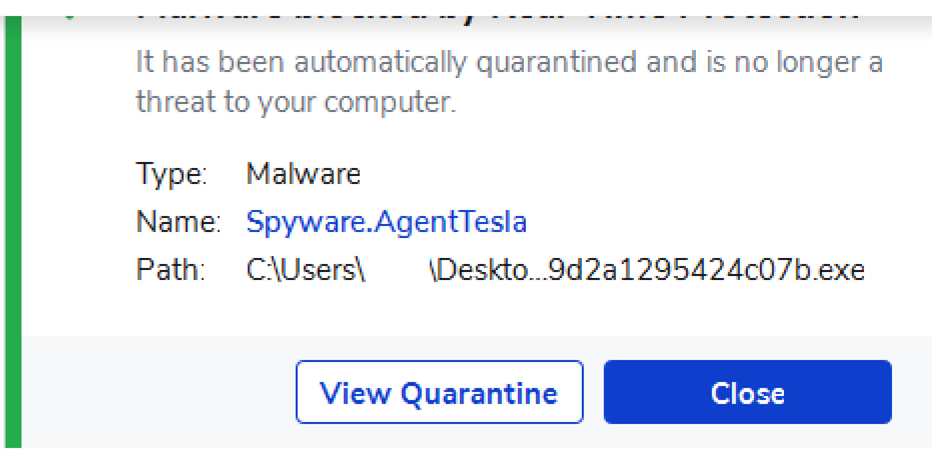
Note: If the final list has less than three elements, it won't generate a SMTP message. If everything checks out, a message is finally sent via smtp.yandex.com, with SSL enabled (Figure 9):


mbdpmGYOGf
Extract the embedded payload and execute it
ReZer0V2
Extract the embbeded resource, decrpyt and execute it
owEKjMRYklfjphIDdRoPePVNoulgd
Data collection
Get list of available profiles
Netsh wlan show profiles
Extract credentials for each profile
Netsh wlan show profile PROFILENAME key=clear
Build a smtp message and sent to smtp server
smtp.yandex.com

Popular stealer looking to expand

Since AgentTesla added the WiFi-stealing feature, we believe the threat actors may be considering using WiFi as a mechanism for spread, similar to what was observed with Emotet. Another possibility is using the WiFi profile to set the stage for future attacks.

Either way, Malwarebytes users were already protected from this new variant of AgentTesla through our real-time protection technology.



It has been automatically quarantined and is no longer a threat to your computer.

Type: Malware
Name: Spyware.AgentTesla
Path: C:\Users\ \Deskto...9d2a1295424c07b.exe

Indicators of compromise

AgentTesla samples:

```
91b711812867b39537a2cd81bb1ab10315ac321a1c68e316bf4fa84badbc09b
dd4a43b0b8a68db65b00fad99519539e2a05a3892f03b869d58ee15fdf5aa044
27939b70928b285655c863fa26efded96bface9db46f35ba39d2a1295424c07b
```

First payload:

```
249a503263717051d62a6d65a5040cf408517dd22f9021e5f8978a819b18063b
```

Second payload:

```
63393b114ebe2e18d888d982c5ee11563a193d9da3083d84a611384bc748b1b0
```

In the next step for each wireless profile, the following command is executed to extract the profile's credential: "netsh wlan show profile PRPFILENAME key=clear" (Figure 5).

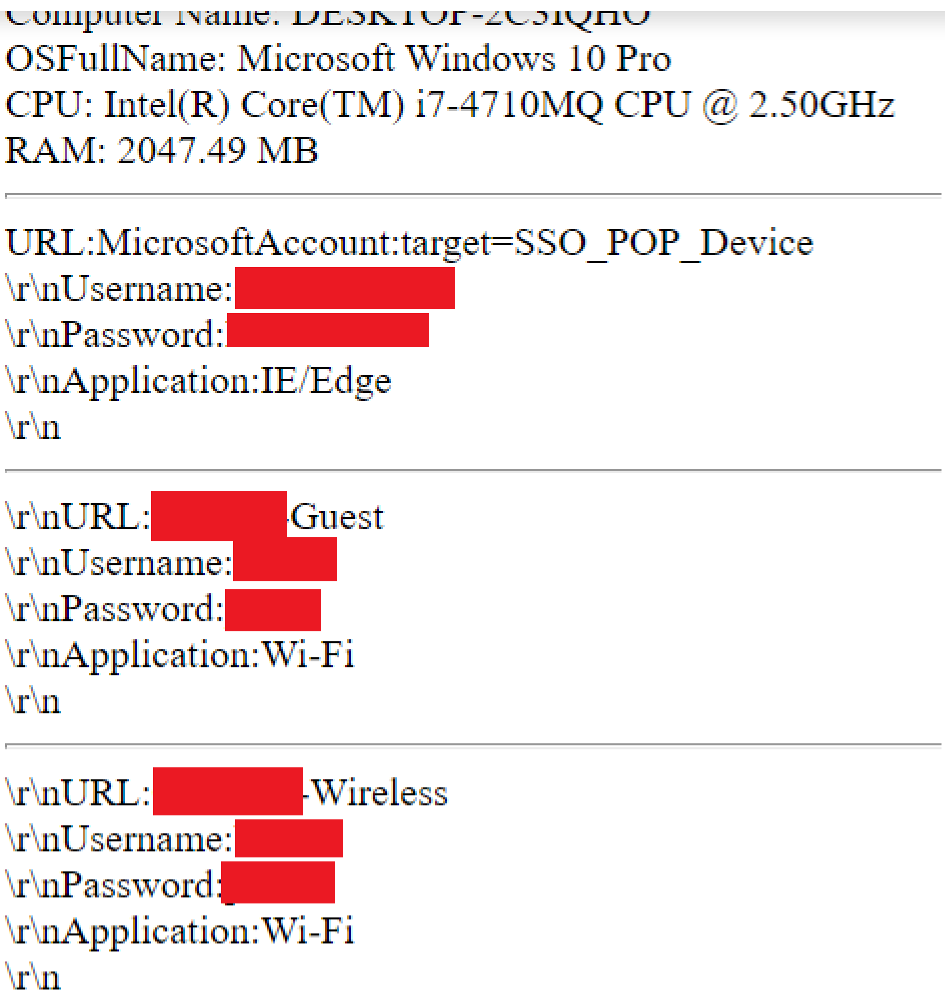
String encryption

All the strings used by the malware are encrypted and are decrypted by Rijndael symmetric encryption algorithm in the ".u200E" function. This function receives a number as an input and generates three byte arrays containing input to be decrypted, key and IV (Figure 6).

For example, in Figure 5, “119216” is decrypted into “wlan show profile name=” and “119196” is decrypted into “key=clear”.

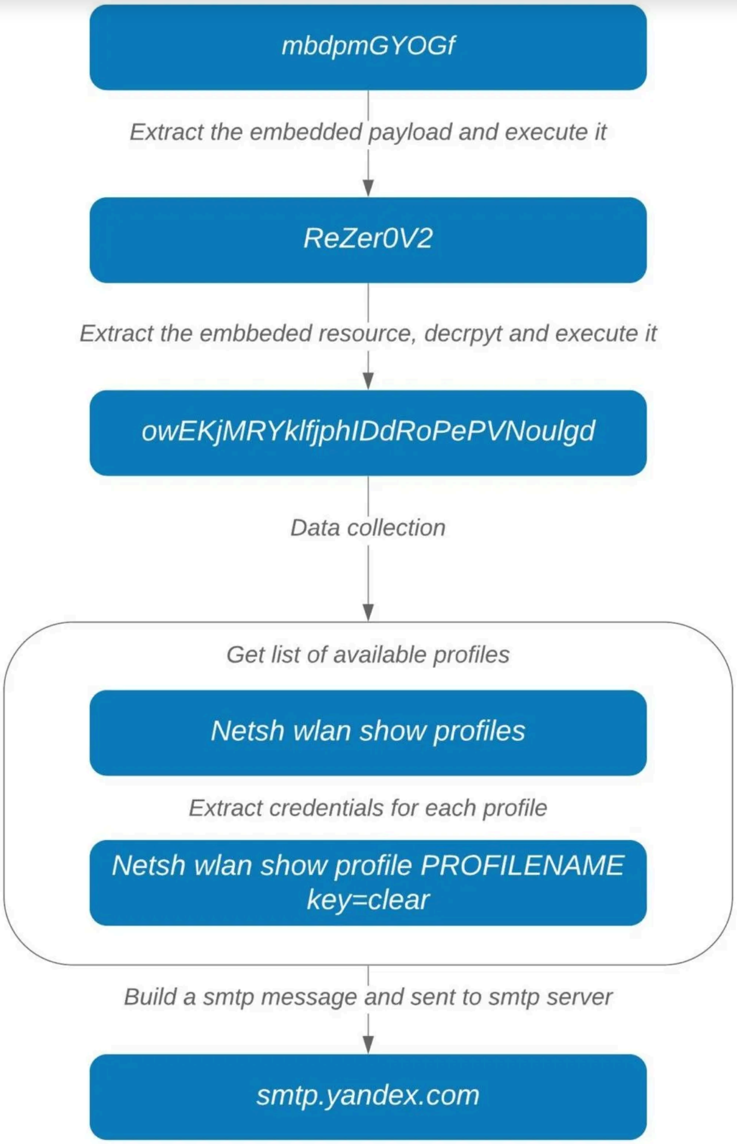
In addition to WiFi profiles, the executable collects extensive information about the system, including FTP clients, browsers, file downloaders, and machine info (username, computer name, OS name, CPU architecture, RAM) and adds them to a list (Figure 7).

Collected information forms the body section of a SMTP message in html format (Figure 8):



```
Computer Name: DESKTOP-2C3IQHO
OSFullName: Microsoft Windows 10 Pro
CPU: Intel(R) Core(TM) i7-4710MQ CPU @ 2.50GHz
RAM: 2047.49 MB
________________________________________
URL:MicrosoftAccount:target=SSO_POP_Device
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:IE/Edge
\r\n
________________________________________
\r\nURL:[redacted]-Guest
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:Wi-Fi
\r\n
________________________________________
\r\nURL:[redacted]-Wireless
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:Wi-Fi
\r\n
```

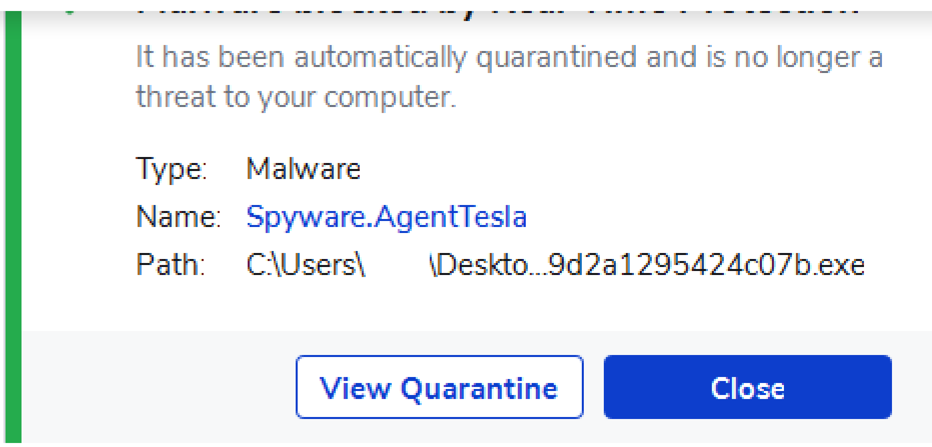
Note: If the final list has less than three elements, it won’t generate a SMTP message. If everything checks out, a message is finally sent via smtp.yandex.com, with SSL enabled (Figure 9):


mbdpmGYOGf
Extract the embedded payload and execute it
ReZer0V2
Extract the embbeded resource, decrpyt and execute it
owEKjMRYklfjphIDdRoPePVNoulgd
Data collection
Get list of available profiles
Netsh wlan show profiles
Extract credentials for each profile
Netsh wlan show profile PROFILENAME key=clear
Build a smtp message and sent to smtp server
smtp.yandex.com

Popular stealer looking to expand

Since AgentTesla added the WiFi-stealing feature, we believe the threat actors may be considering using WiFi as a mechanism for spread, similar to what was observed with Emotet. Another possibility is using the WiFi profile to set the stage for future attacks.

Either way, Malwarebytes users were already protected from this new variant of AgentTesla through our real-time protection technology.



It has been automatically quarantined and is no longer a threat to your computer.

Type: Malware
Name: Spyware.AgentTesla
Path: C:\Users\ \Deskto...9d2a1295424c07b.exe

Indicators of compromise

AgentTesla samples:

```
91b711812867b39537a2cd81bb1ab10315ac321a1c68e316bf4fa84badbc09b
dd4a43b0b8a68db65b00fad99519539e2a05a3892f03b869d58ee15fdf5aa044
27939b70928b285655c863fa26efded96bface9db46f35ba39d2a1295424c07b
```

First payload:

```
249a503263717051d62a6d65a5040cf408517dd22f9021e5f8978a819b18063b
```

Second payload:

```
63393b114ebe2e18d888d982c5ee11563a193d9da3083d84a611384bc748b1b0
```

To collect wireless profile credentials, a new “netsh” process is created by passing “wlan show profile” as argument (Figure 4). Available WiFi names are then extracted by applying a regex: “All User Profile * : (?.*)”, on the stdout output of the process.

In the next step for each wireless profile, the following command is executed to extract the profile's credential: "netsh wlan show profile PRPFILENAME key=clear" (Figure 5).

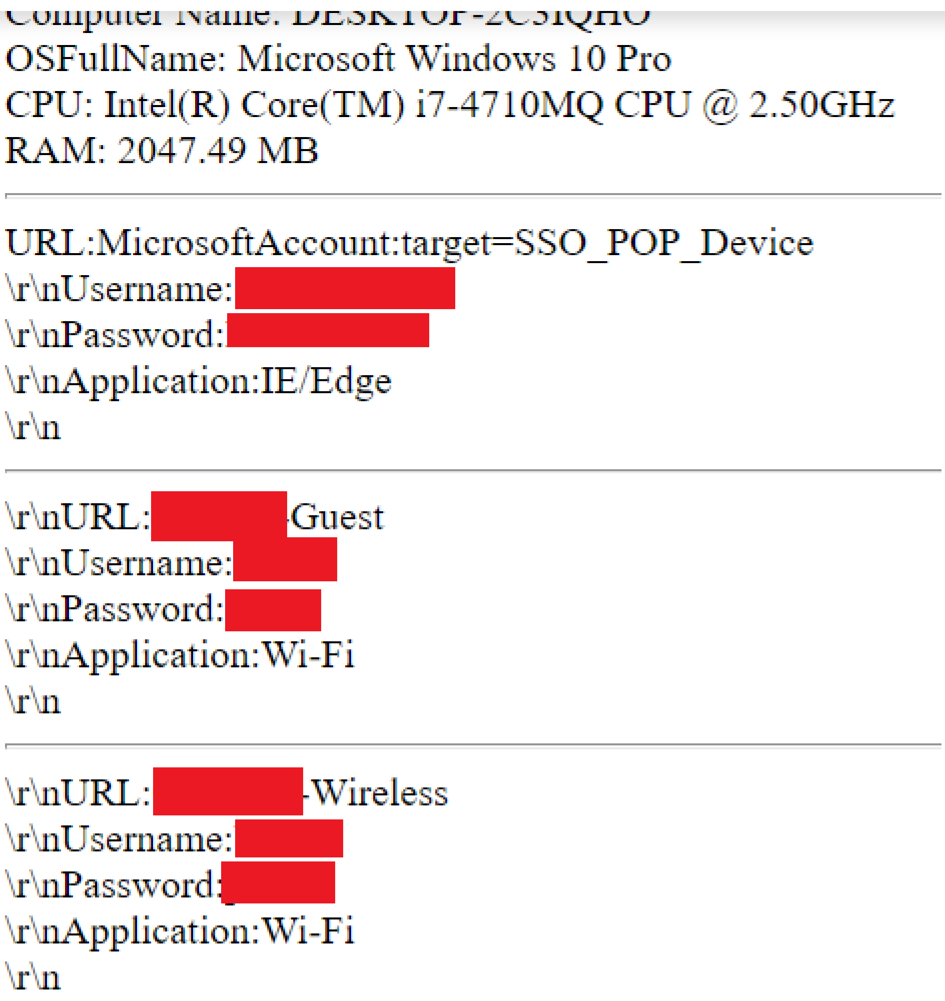
String encryption

All the strings used by the malware are encrypted and are decrypted by Rijndael symmetric encryption algorithm in the ".u200E" function. This function receives a number as an input and generates three byte arrays containing input to be decrypted, key and IV (Figure 6).

For example, in Figure 5, “119216” is decrypted into “wlan show profile name=” and “119196” is decrypted into “key=clear”.

In addition to WiFi profiles, the executable collects extensive information about the system, including FTP clients, browsers, file downloaders, and machine info (username, computer name, OS name, CPU architecture, RAM) and adds them to a list (Figure 7).

Collected information forms the body section of a SMTP message in html format (Figure 8):



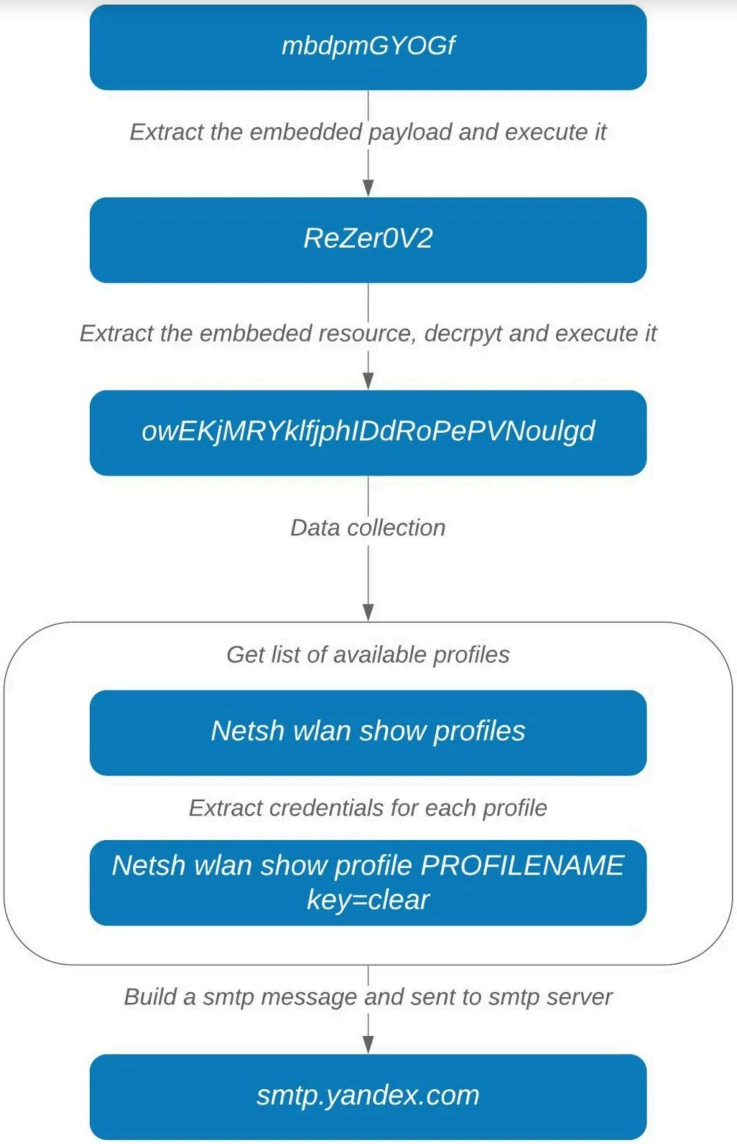
```
Computer Name: DESKTOP-2C3IQHO
OSFullName: Microsoft Windows 10 Pro
CPU: Intel(R) Core(TM) i7-4710MQ CPU @ 2.50GHz
RAM: 2047.49 MB

URL:MicrosoftAccount:target=SSO_POP_Device
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:IE/Edge
\r\n

\r\nURL:[redacted]Guest
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:Wi-Fi
\r\n

\r\nURL:[redacted]-Wireless
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:Wi-Fi
\r\n
```

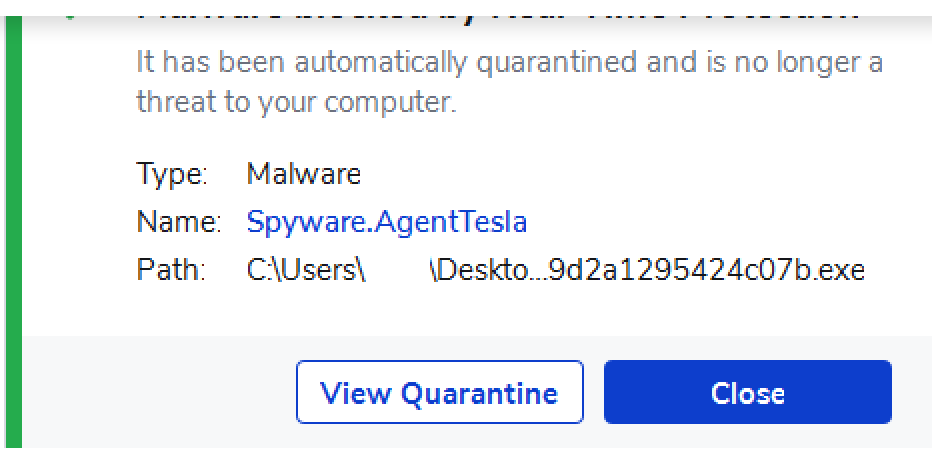
Note: If the final list has less than three elements, it won't generate a SMTP message. If everything checks out, a message is finally sent via smtp.yandex.com, with SSL enabled (Figure 9):


mbdpmGYOGf
Extract the embedded payload and execute it
ReZer0V2
Extract the embbeded resource, decrpyt and execute it
owEKjMRYklfjphIDdRoPePVNoulgd
Data collection
Get list of available profiles
Netsh wlan show profiles
Extract credentials for each profile
Netsh wlan show profile PROFILENAME key=clear
Build a smtp message and sent to smtp server
smtp.yandex.com

Popular stealer looking to expand

Since AgentTesla added the WiFi-stealing feature, we believe the threat actors may be considering using WiFi as a mechanism for spread, similar to what was observed with Emotet. Another possibility is using the WiFi profile to set the stage for future attacks.

Either way, Malwarebytes users were already protected from this new variant of AgentTesla through our real-time protection technology.



It has been automatically quarantined and is no longer a threat to your computer.

Type: Malware
Name: Spyware.AgentTesla
Path: C:\Users\ \Deskto...9d2a1295424c07b.exe

Indicators of compromise

AgentTesla samples:

```
91b711812867b39537a2cd81bb1ab10315ac321a1c68e316bf4fa84badbc09b
dd4a43b0b8a68db65b00fad99519539e2a05a3892f03b869d58ee15fdf5aa044
27939b70928b285655c863fa26efded96bface9db46f35ba39d2a1295424c07b
```

First payload:

```
249a503263717051d62a6d65a5040cf408517dd22f9021e5f8978a819b18063b
```

Second payload:

```
63393b114ebe2e18d888d982c5ee11563a193d9da3083d84a611384bc748b1b0
```

The second payload (owEKjMRYkIfjPazjphIDdRoPePVNoulgd) is the main component of AgentTesla that steals credentials from browsers, FTP clients, wireless profiles, and more (Figure 3). The sample is heavily

To collect wireless profile credentials, a new “netsh” process is created by passing “wlan show profile” as argument (Figure 4). Available WiFi names are then extracted by applying a regex: “All User Profile * : (?.*)”, on the stdout output of the process.

In the next step for each wireless profile, the following command is executed to extract the profile's credential: "netsh wlan show profile PRPFILENAME key=clear" (Figure 5).

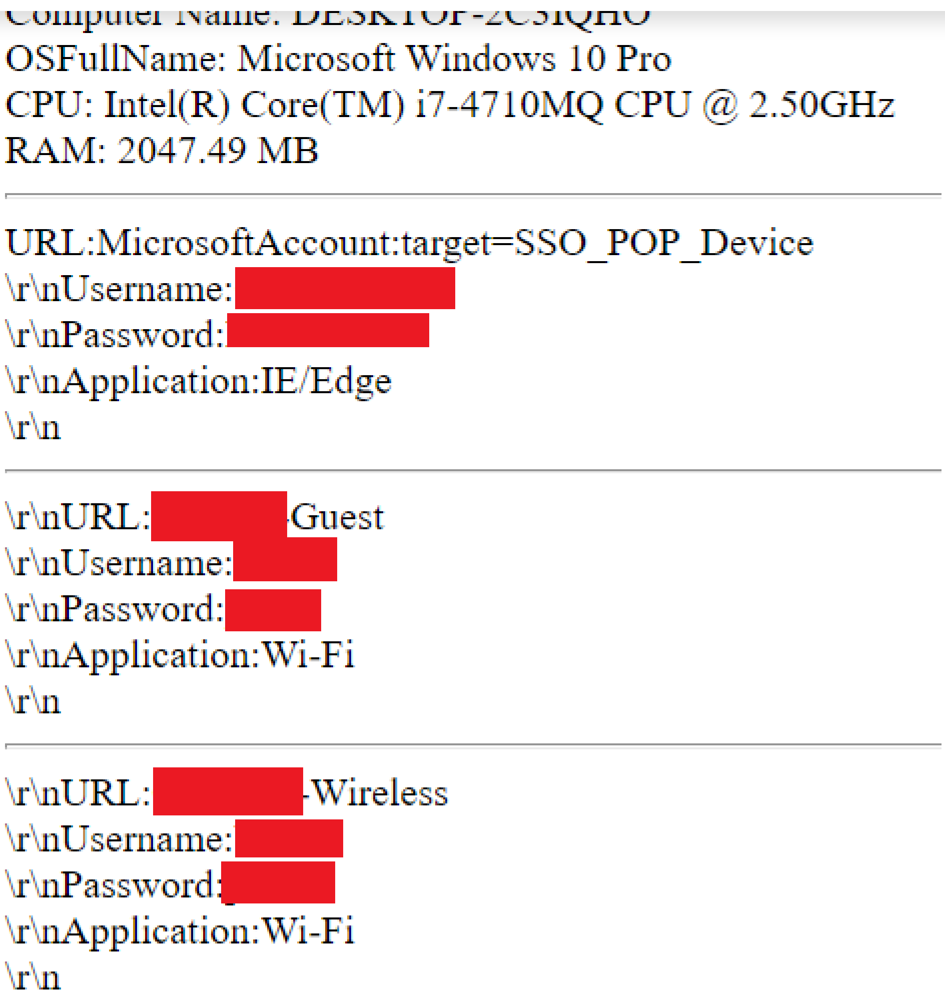
String encryption

All the strings used by the malware are encrypted and are decrypted by Rijndael symmetric encryption algorithm in the ".u200E" function. This function receives a number as an input and generates three byte arrays containing input to be decrypted, key and IV (Figure 6).

For example, in Figure 5, “119216” is decrypted into “wlan show profile name=” and “119196” is decrypted into “key=clear”.

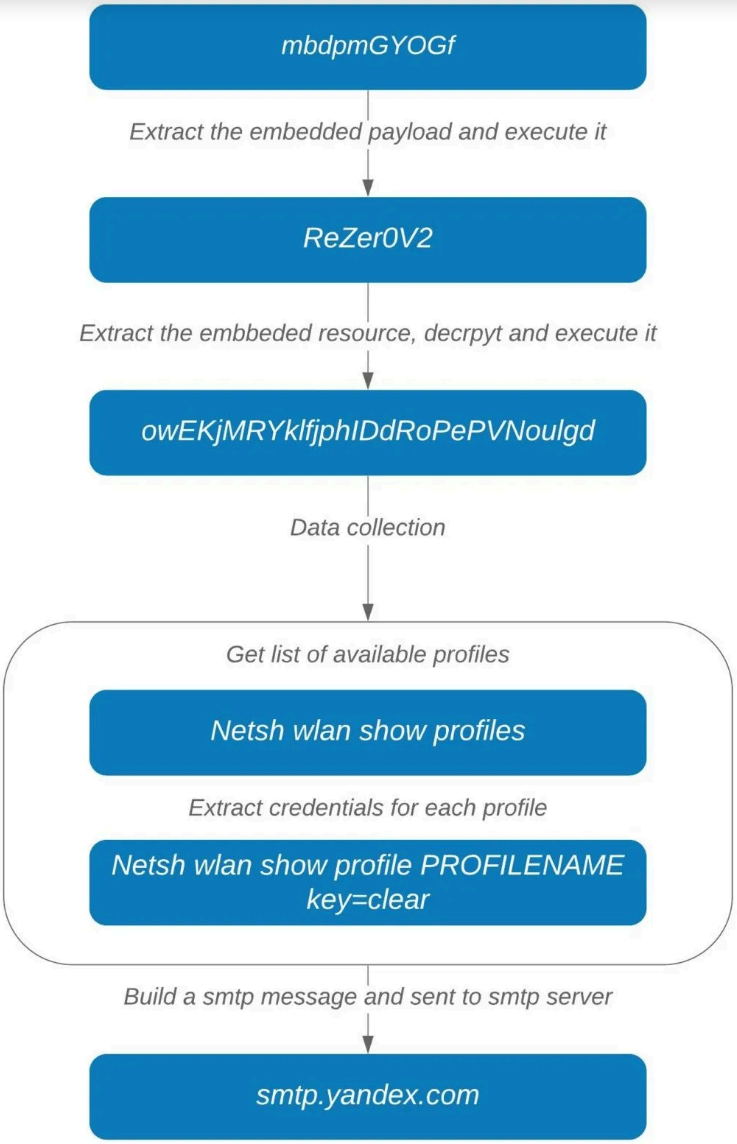
In addition to WiFi profiles, the executable collects extensive information about the system, including FTP clients, browsers, file downloaders, and machine info (username, computer name, OS name, CPU architecture, RAM) and adds them to a list (Figure 7).

Collected information forms the body section of a SMTP message in html format (Figure 8):



```
Computer Name: DESKTOP-2C5IQHO
OSFullName: Microsoft Windows 10 Pro
CPU: Intel(R) Core(TM) i7-4710MQ CPU @ 2.50GHz
RAM: 2047.49 MB
________________________________________
URL:MicrosoftAccount:target=SSO_POP_Device
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:IE/Edge
\r\n
________________________________________
\r\nURL:[redacted]-Guest
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:Wi-Fi
\r\n
________________________________________
\r\nURL:[redacted]-Wireless
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:Wi-Fi
\r\n
```

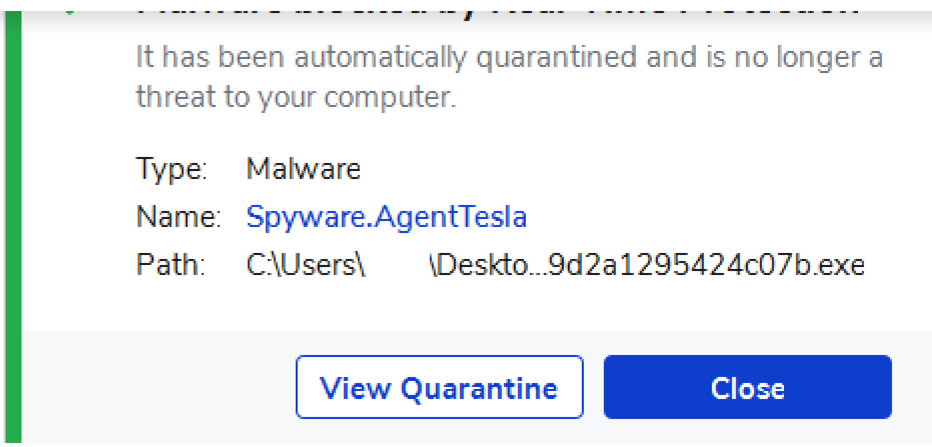
Note: If the final list has less than three elements, it won't generate a SMTP message. If everything checks out, a message is finally sent via smtp.yandex.com, with SSL enabled (Figure 9):


mbdpmGYOGf
Extract the embedded payload and execute it
ReZer0V2
Extract the embbeded resource, decrpyt and execute it
owEKjMRYklfjphIDdRoPePVNoulgd
Data collection
Get list of available profiles
Netsh wlan show profiles
Extract credentials for each profile
Netsh wlan show profile PROFILENAME key=clear
Build a smtp message and sent to smtp server
smtp.yandex.com

Popular stealer looking to expand

Since AgentTesla added the WiFi-stealing feature, we believe the threat actors may be considering using WiFi as a mechanism for spread, similar to what was observed with Emotet. Another possibility is using the WiFi profile to set the stage for future attacks.

Either way, Malwarebytes users were already protected from this new variant of AgentTesla through our real-time protection technology.



It has been automatically quarantined and is no longer a threat to your computer.

Type: Malware
Name: Spyware.AgentTesla
Path: C:\Users\ \Deskto...9d2a1295424c07b.exe

Indicators of compromise

AgentTesla samples:

```
91b711812867b39537a2cd81bb1ab10315ac321a1c68e316bf4fa84badbc09b
dd4a43b0b8a68db65b00fad99519539e2a05a3892f03b869d58ee15fdf5aa044
27939b70928b285655c863fa26efded96bface9db46f35ba39d2a1295424c07b
```

First payload:

```
249a503263717051d62a6d65a5040cf408517dd22f9021e5f8978a819b18063b
```

Second payload:

```
63393b114ebe2e18d888d982c5ee11563a193d9da3083d84a611384bc748b1b0
```

This executable (ReZer0V2) also has a resource that is encrypted. After doing several anti-debugging, anti-sandboxing, and anti-virtualization checks, the executable decrypts and injects the content of the resource into itself (Figure 2).

The second payload (owEKjMRYkIfjPazjphIDdRoPePVNoulgd) is the main component of AgentTesla that steals credentials from browsers, FTP clients, wireless profiles, and more (Figure 3). The sample is heavily obfuscated to make the analysis more difficult for researchers.

To collect wireless profile credentials, a new “netsh” process is created by passing “wlan show profile” as argument (Figure 4). Available WiFi names are then extracted by applying a regex: “All User Profile * : (?.*)”, on the stdout output of the process.

In the next step for each wireless profile, the following command is executed to extract the profile's credential: "netsh wlan show profile PRPFILENAME key=clear" (Figure 5).

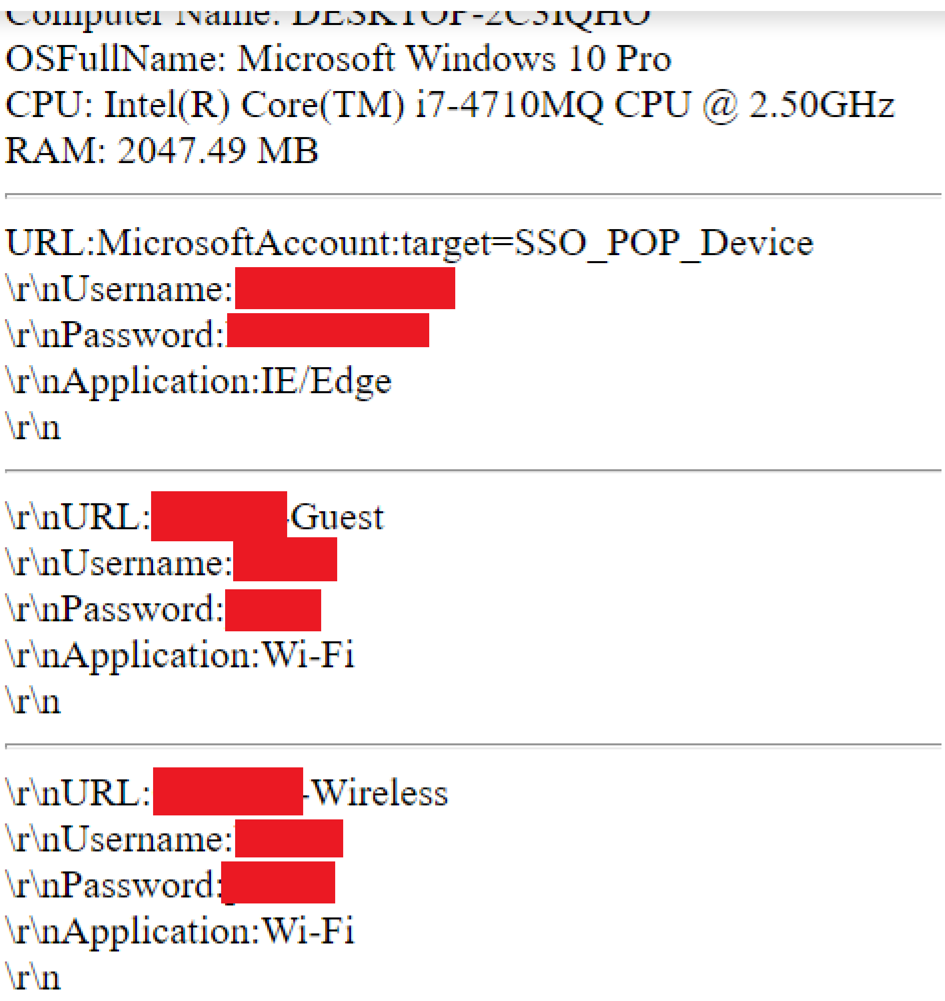
String encryption

All the strings used by the malware are encrypted and are decrypted by Rijndael symmetric encryption algorithm in the ".u200E" function. This function receives a number as an input and generates three byte arrays containing input to be decrypted, key and IV (Figure 6).

For example, in Figure 5, “119216” is decrypted into “wlan show profile name=” and “119196” is decrypted into “key=clear”.

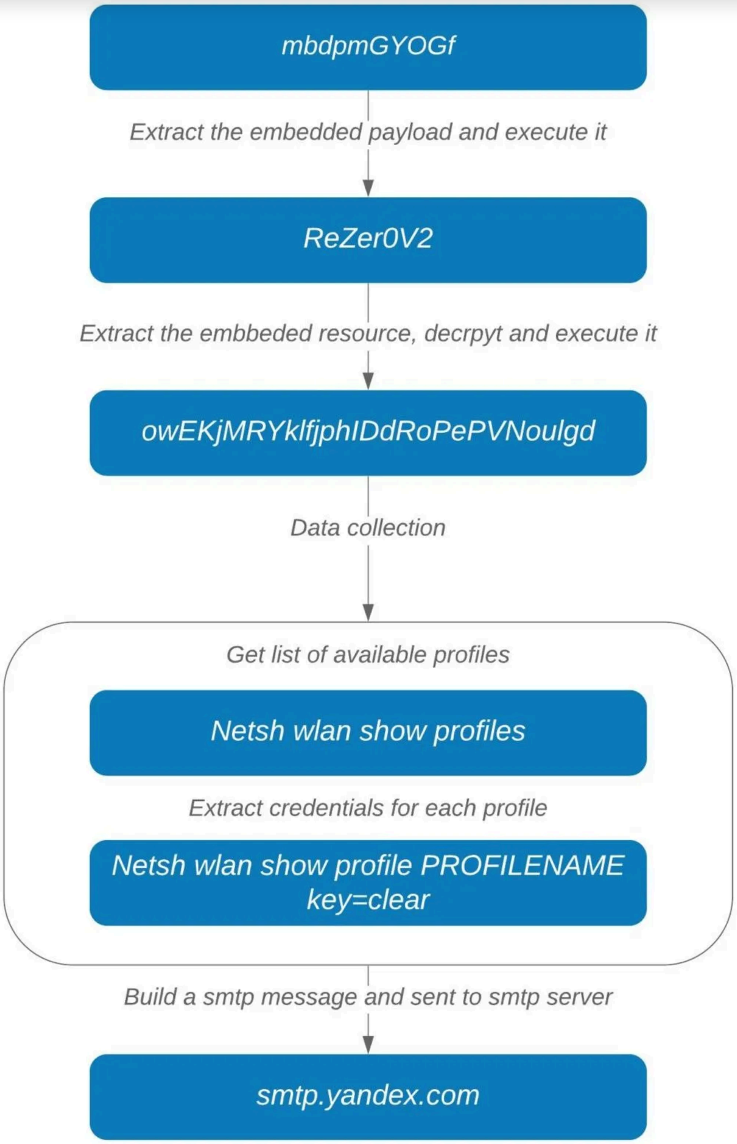
In addition to WiFi profiles, the executable collects extensive information about the system, including FTP clients, browsers, file downloaders, and machine info (username, computer name, OS name, CPU architecture, RAM) and adds them to a list (Figure 7).

Collected information forms the body section of a SMTP message in html format (Figure 8):



```
Computer Name: DESKTOP-2C3IQHO
OSFullName: Microsoft Windows 10 Pro
CPU: Intel(R) Core(TM) i7-4710MQ CPU @ 2.50GHz
RAM: 2047.49 MB
________________________________________
URL:MicrosoftAccount:target=SSO_POP_Device
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:IE/Edge
\r\n
________________________________________
\r\nURL:[redacted]Guest
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:Wi-Fi
\r\n
________________________________________
\r\nURL:[redacted]-Wireless
\r\nUsername:[redacted]
\r\nPassword:[redacted]
\r\nApplication:Wi-Fi
\r\n
```

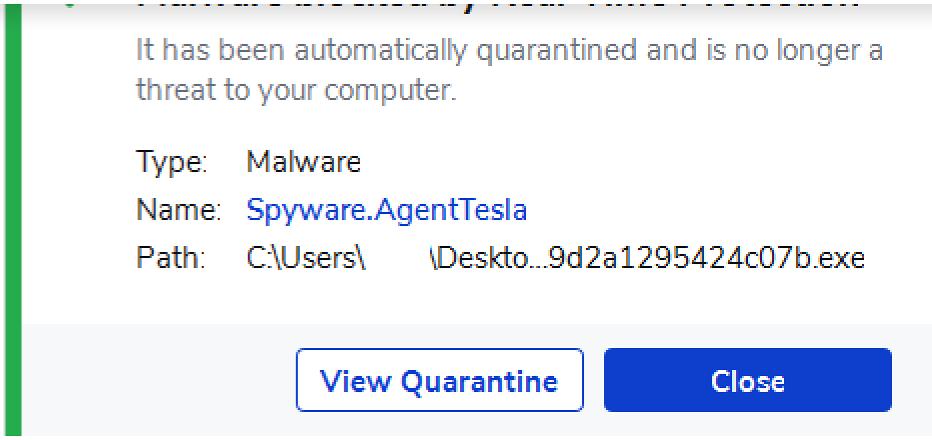
Note: If the final list has less than three elements, it won't generate a SMTP message. If everything checks out, a message is finally sent via smtp.yandex.com, with SSL enabled (Figure 9):


mbdpmGYOGf
Extract the embedded payload and execute it
ReZer0V2
Extract the embbeded resource, decrpyt and execute it
owEKjMRYklfjphIDdRoPePVNoulgd
Data collection
Get list of available profiles
Netsh wlan show profiles
Extract credentials for each profile
Netsh wlan show profile PROFILENAME key=clear
Build a smtp message and sent to smtp server
smtp.yandex.com

Popular stealer looking to expand

Since AgentTesla added the WiFi-stealing feature, we believe the threat actors may be considering using WiFi as a mechanism for spread, similar to what was observed with Emotet. Another possibility is using the WiFi profile to set the stage for future attacks.

Either way, Malwarebytes users were already protected from this new variant of AgentTesla through our real-time protection technology.



It has been automatically quarantined and is no longer a threat to your computer.

Type: Malware
Name: Spyware.AgentTesla
Path: C:\Users\ \Deskto...9d2a1295424c07b.exe

Indicators of compromise

AgentTesla samples:

```
91b711812867b39537a2cd81bb1ab10315ac321a1c68e316bf4fa84badbc09b
dd4a43b0b8a68db65b00fad99519539e2a05a3892f03b869d58ee15fdf5aa044
27939b70928b285655c863fa26efded96bface9db46f35ba39d2a1295424c07b
```

First payload:

```
249a503263717051d62a6d65a5040cf408517dd22f9021e5f8978a819b18063b
```

Second payload:

```
63393b114ebe2e18d888d982c5ee11563a193d9da3083d84a611384bc748b1b0
```

SHARE THIS ARTICLE

RELATED ARTICLES

your calls to the bank

October 31, 2024 - Android malware FakeCall can intercept calls to the bank on infected devices and redirect the target to the criminals.

CONTINUE READING

0 Comments

Apple | News

Patch now! New Chrome update for two critical vulnerabilities

October 30, 2024 - Chrome issued a security update that patches two critical vulnerabilities. One of which was reported by Apple

CONTINUE READING

0 Comments

Apple issues patches for several vulnerabilities

October 29, 2024 - Apple has issued patches for several of its operating systems. The ones for iOS and iPadOS deserve your immediate attention.

CONTINUE READING

0 Comments

Cybercrime | News

Europol warns about counterfeit goods and the criminals behind them

October 28, 2024 - There is a whole ecosystem behind the sales and distribution of counterfeit goods. Best to tay away from them.

CONTINUE READING

0 Comments

October 27)

October 28, 2024 - A list of topics we covered in the week of October 21 to October 27 of 2024

CONTINUE READING

0 Comments

ABOUT THE AUTHOR

Hossein Jazi

Special interest in tracking APTs

Cybersecurity info you can't live without

Want to stay informed on the latest news in cybersecurity? Sign up for our newsletter and learn how to protect your computer from threats.

Email Address

Email Address

Sign Up

FOR PERSONAL

Windows Antivirus

Mac Antivirus

Android Antivirus

Free Antivirus

VPN App (All Devices)

Malwarebytes for iOS

SEE ALL

FOR BUSINESS

Small Businesses

Mid-size Businesses

Larger Enterprise

Endpoint Protection

Endpoint Detection & Response (EDR)

Managed Detection & Response (MDR)

COMPANY

About Us

Contact Us

Careers

News and Press

Blog

Scholarship

FOR PARTNERS

Managed Service Provider (MSP) Program

Resellers

MY ACCOUNT

Sign In

Malwarebytes LABS

SOLUTIONS

Digital Footprint Scan

Rootkit Scanner

Trojan Scanner

Virus Scanner

Spyware Scanner

Password Generator

Anti Ransomware Protection

LEARN

Malware

Hacking

Phishing

Ransomware

Computer Virus

Antivirus

What is VPN?

ADDRESS

One Albert Quay
2nd Floor
Cork T12 X8N6
Ireland

Malwarebytes LABS

Privacy

Terms of Service

Accessibility

Imprint