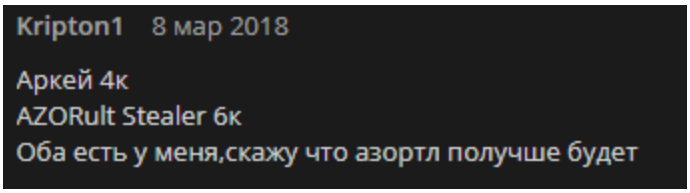
AZORult++: Rewriting history

SL securelist.com/azorult-analysis-history/89922/

Authors

Expert Alexander Eremin

The AZORult Trojan is one of the most commonly bought and sold stealers in Russian forums. Despite the relatively high price tag ($100), buyers like AZORult for its broad functionality (for example, the use of .bit domains as C&C servers to ensure owner anonymity and to make it difficult to block the C&C server), as well as its high performance. Many comment leavers recommend it.



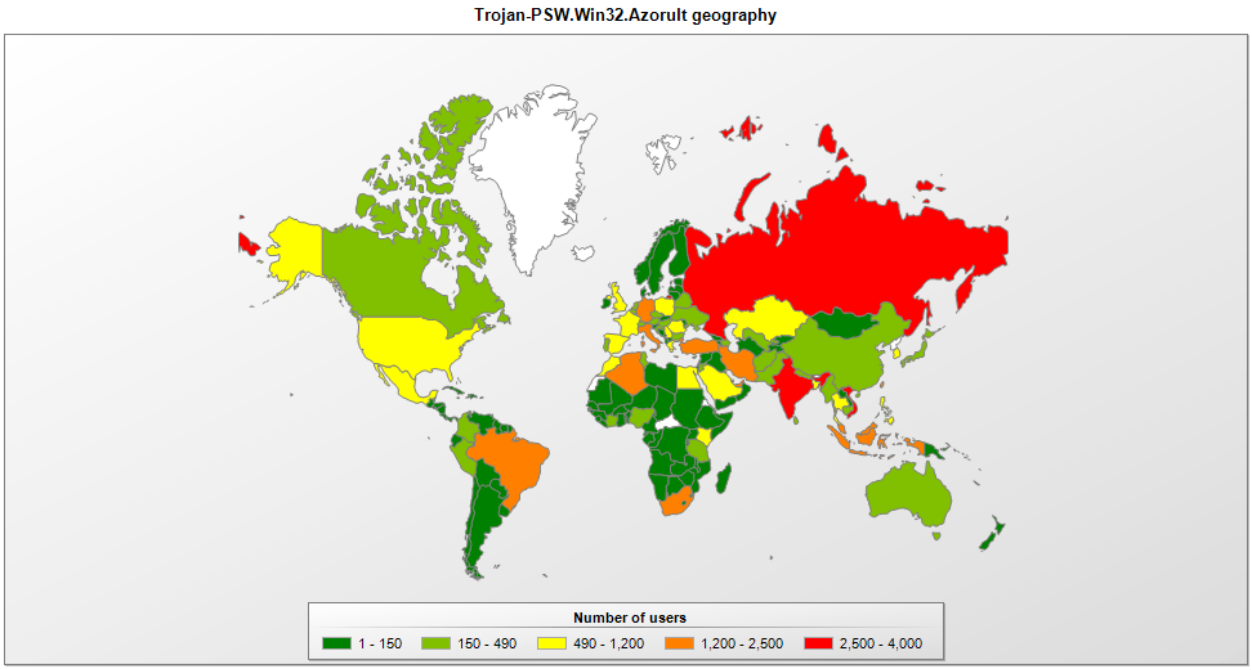
But at the back end of 2018, the main seller, known under the handle CrydBrox, stopped selling the malware:

“All software has a shelf life. It’s run out for AZORult.
It is with joy and sadness that I announce that sales are closed forever.”

Some attribute the move to AZORult 3.2 having become too widely available, likewise the source code of the botnet control panel. This version of the malware spread to other forums where even users without special skills can download and configure it for their own purposes. So the imminent demise of AZORult was apparently down to a lack of regular updates and its overly wide distribution. Yet the story of AZORult does not end there.

In a nutshell

AZORult is a Trojan stealer that collects various data on infected computers and sends it to the C&C server, including browser history, login credentials, cookies, files from folders as specified by the C&C server (for example, all TXT files from the Desktop folder), cryptowallet files, etc.; the malware can also be used as a loader to download other malware. Kaspersky Lab products detect the stealer as Trojan-PSW.Win32.Azorult. Our statistics show that since the start of 2019, users in Russia and India are the most targeted.



Geography of users attacked by Trojan-PSW.Win32.Azorult, 01.01.2019 — 03.18.2019

From Delphi to C++

In early March 2019, a number of malicious files detected by our products caught the eye. Although similar to AZORult already known to us, unlike the original malware, they were written not in Delphi, but in C++. A clear hint at the link between them comes from a section of code left by the developer.

```
F:\orders\cpp\azorult_new\Release\azorult_new.pdb
```

It appears that the acolytes of CrydBrox, the very one who pulled the plug on AZORult, decided to rewrite it in C++; this version we call AZORult++. The presence of lines containing a path to debugging files likely indicates that the malware is still in development, since developers usually try to remove such code as soon as feasible.

AZORult++ starts out by checking the language ID through a call to the GetUserDefaultLangID() function. If AZORult++ is running on a system where the language is identified as Russian, Armenian, Azerbaijani, Belarusian, Georgian, Kazakh, Tajik, Turkmen, or Uzbek, the malware stops executing.

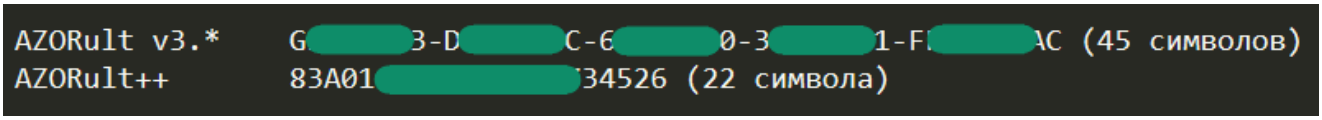
```
result = GetUserDefaultLangID();
if ( result == russian
  || result == armenian
  || result == azerbaijani
  || result == azerbaijani_2
  || result == belarusian
  || result == georgian
  || result == kazakh
  || result == tajik
  || result == turkmen
  || result == uzbek
  || result == uzbek_2 )
{
  ExitProcess(0);
}
return result;
```

A more detailed analysis reveals that the C++ version is deficient compared to AZORult 3.3, the last iteration to be sold. In particular, there is no loader functionality and no support for stealing saved passwords from many of the browsers supported by AZORult 3.3. At the same time, many signature features of the Delphi-based version 3.3 are present in AZORult++, including the algorithm for communication with the C&C server, the command format, the structure and method of storing harvested data, and encryption keys.

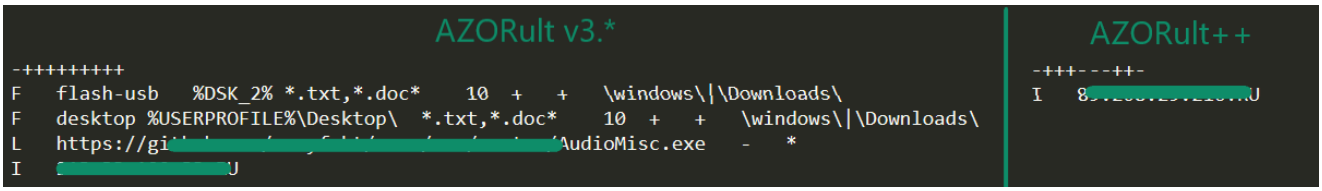
Like AZORult 3.3, AZORult++ uses an XOR operation with a 3-byte key to encrypt data sent to the C&C server. What's more, this key we had already encountered in various modifications of version 3.3.

Examples of different versions of AZORult in operation (data encrypted using XOR)

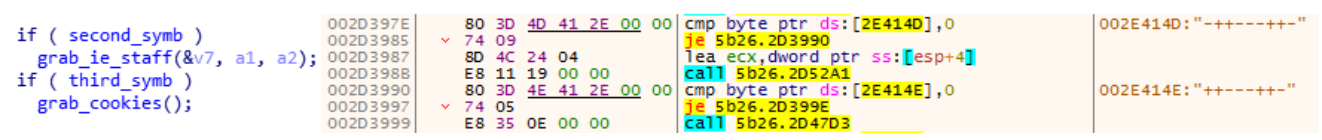
The malware collects stolen data in RAM and does not write to the hard drive to keep its actions hidden. A comparison of the data sent in the first packet (the ID of the infected device) shows that AZORult++ uses a shorter string than AZORult 3.3 for identification:



The server response also contains far less data. In version 3.3, the response contained a command in the form “++++-+–+-“, specifying the bot configuration and a link for downloading additional malware, plus several binary files needed for the stealer to work. The string “++++-+–+-” is parsed by the Trojan character-by-character; “+” in a specific position signifies a command to execute certain actions (for example, harvesting of cryptowallet files). The current version of AZORult++ employs a shorter, yet similar command:



It is worth mentioning separately that the resulting configuration string is not processed correctly; the code execution does not depend on the value “+” or “-” in the string, since the characters are checked against \x00 for a match. In other words, the resulting command does not affect the stealer’s behavior:



This seems to be an error on the part of the developer, which suggests again that the project is in the very early stages of development. Going forward, these bugs are expected to be eliminated and the functionality of AZORult++ expanded.

++ up the sleeve

For all its flaws, AZORult++ could actually be more dangerous than its predecessor due to its ability to establish a **remote connection to the desktop**. To do so, AZORult++ creates a user account using the NetUserAdd() function (username and password are specified in the AZORult++ code), before adding this account to the Administrators group:

```
if ( AllocateAndInitializeSid(
       &pIdentifierAuthority,
       2u,
       SECURITY_BUILTIN_DOMAIN_RID,
       DOMAIN_ALIAS_RID_ADMINS,
       0,
       0,
       0,
       0,
       0,
       0,
       &pSid)
  && LookupAccountSidW(0, pSid, &Name, &cchName, &ReferencedDomainName, &cchReferencedDomainName, &peUse) )
{
  *buf = &domain_and_name;
  NetLocalGroupAddMembers(0, &Name, 3u, buf, 1u);
}
```

Next, AZORult++ hides the newly created account by setting the value of the *Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\Userlist* registry key to 0. Likewise, through setting registry key values, a Remote Desktop Protocol (RDP) connection is allowed:

```
(v3, L"SYSTEM\\CurrentControlSet\\Control\\Terminal Server", 0, L"fDenyTSConnections", 0);
(v4, L"SYSTEM\\CurrentControlSet\\Control\\Terminal Server\\WinStations\\RDP-Tcp", 0, L"SecurityLayer", 1);
(v5, L"SYSTEM\\CurrentControlSet\\Control\\Terminal Server\\WinStations\\RDP-Tcp", 0, L"UserAuthentication", 0);
```

The malicious cherry on the cake is a call to ShellExecuteW() to open a port to establish a remote connection to the desktop:

```
ShellExecuteW(0, L"open", L"cmd", L"/c netsh firewall add portopening TCP 3389 \"Remote Desktop\"", 0, 0);
```

After that, the infected computer is ready to accept the incoming RDP connection, which allows the cybercriminal — armed with the victim's IP address and account information — to connect to the infected computer and seize complete control of it.

Conclusion

During development, AZORult underwent several changes related to the expansion of its functionality. Moreover, despite its many flaws, the C++ version is already more threatening than its predecessor due to the ability to establish a remote connection to the desktop. Because AZORult++ is likely still in development, we should expect its functionality to expand and bugs to be eliminated, not to mention attempts to distribute it widely under a name that buyers will recognize.

IoC

C&C servers
http://ravor.ac[.]ug
http://daticho.ac[.]ug

MD5
08EB8F2E441C26443EB9ABE5A93CD942
5B26880F80A00397BC379CAF5CADC564
B0EC3E594D20B9D38CC8591BAFF0148B
FE8938F0BAAF90516A90610F6E210484

- Data theft
- Malware Descriptions
- Trojan
- Trojan-stealer

Authors

Alexander Eremin

AZORult++: Rewriting history

Your email address will not be published. Required fields are marked *