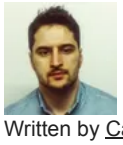
New espionage malware found targeting Russian-speaking users in Eastern Europe

zdnet.com/article/new-espionage-malware-found-targeting-russian-speaking-users-in-eastern-europe/

Home Innovation Security
New Attor malware seems to be the work of one of the world's most sophisticated espionage players.



Written by Catalin Cimpanu, Contributor on Oct. 10, 2019

-
-
-
-
-

Security researchers have discovered an advanced malware strain that's been deployed to spy on diplomats and Russian-speaking users in Eastern Europe.

See als

10 dangerous app vulnerabilities to watch out for (free PDF)

The malware, named Attor, has been used in attacks since 2013 but was only discovered last year, according to an ESET report published today.

ESET said the malware bears the signs of a targeted espionage campaign perpetrated by a skilled actor, with a very narrow focus on a small selection of targets.

Targeting diplomats and Russian-speaking users`

An analysis of the malware and its features shows that Attor's creators specifically designed it to target Russian-speaking users.

"Our conclusion is that Attor is specifically targeting Russian-speakers, which is further supported by the fact that most of the targets are located in Russia," said ESET malware analyst Zuzana Hromcová.

"Other targets are located in Eastern Europe, and they include diplomatic missions and governmental institutions," she added.

Image: ESET

Furthermore, the theory that this malware was designed to target Russian users first and foremost is supported by some of Attor's features that include the targeting of popular Russian apps and services -- such as social networks Odnoklassniki and VKontakt, VoIP provider Multifon, IM apps Qip and Infium, search engine Rambler, email clients Yandex and Mail.ru, and payment system WebMoney.

Attor was designed by skilled malware coders

In addition, the ESET report paints a pretty clear picture that Attor is not your run-of-the-mill malware. The malware uses a highly-modularized architecture and is designed around a central component, called a dispatcher.

This is not strange, as most malware uses a modularized structure. However, Attor shows its sophistication by the use of encryption to hide the modules, something seen only on very rare occasions, and in malware strains usually developed by nation-state hacker groups.

"Attor's plugins are delivered to the compromised computer as DLLs, asymmetrically encrypted with RSA," Hromcová said. "The plugins are only fully recovered in memory, using the public RSA key embedded in the dispatcher. As a result, it is difficult to obtain Attor's plugins, and to decrypt them without access to the dispatcher."

Over the course of the past year, Hromcová and other ESET researchers have spent months toiling over Attor to decipher its secrets. Eventually, they had a breakthrough.

"We were able to recover eight of Attor's plugins," she said.

The Slovak researcher said they found a module for taking screenshots, one for recording audio, one to upload files to a remote server, one for setting up a SOCKS proxy to disguise its traffic, a keyboard and clipboard logger, an installer watchdog, a device monitor, and a module to support communications via the Tor network.

Image: ESET

The GSM fingerprinting module

Of all the plugins, by a very wide margin, the most interesting one was the module that performed device monitoring.

This module, found in many other malware strains, usually works by creating a fingerprint of devices a user connects to a computer or laptop. For example, POS malware uses similar modules to detect when certain types of devices are connected, so they can watch for incoming data streams that may contain payment card data.

Other malware strains uses similar modules to detect when users plug in a USB thumb drive, to plant malware-laced files on its storage.

However, Attor's device monitor module was specifically designed to detect when users connected modems and older phones to their devices. When this happened, Attor would collect info about the files present on each device.

"[This module] is responsible for collection of metadata, not the files themselves, so we consider it a plugin used for device fingerprinting, and hence likely used as a base for further data theft," Hromcová said.

But there was more. Attor's device monitoring module also included a very strange function that used ancient AT commands to fingerprint GSM-capable devices.

"Whenever a modem or a phone device is connected to a COM port, Device monitor uses AT commands to communicate with the device, via the associated serial port," Hromcová said.

AT commands were developed in the 80s as a way to control with early versions of internet modems. They are still supported today, even on modern high-end smartphones -- all of which come with modems to be able to connect to a telco provider's LTE network.

The Attor device monitor module used these ancient commands to determine when targets were connecting GSM equipment to their computers.

But here's the catch. The Attor gang was completely ignoring modern smartphones connected via USB. Stealing or planting malware on smartphones via the USB port would have been much easier than using AT commands via old serial ports.

Malware targeting spies?

ESET speculates that Attor creators specifically created this module to target users who employed older mobile handsets -- or even a custom GSM-capable platform used by one of their targets.

"In this scenario, it is possible the attackers have learned about the victim's use of these devices using some other reconnaissance techniques," Hromcová said.

Many diplomatic and intelligence operations use custom GSM-capable platforms for secure communications -- showing just how targeted this malware really was.

While ESET didn't provide any thoughts on who might have developed and deployed Attor, it is clear that this malware was used by some of the world's most sophisticated espionage players.

More in ESET's 32-page Attor report [PDF].

The world's most famous and dangerous APT (state-developed) malware