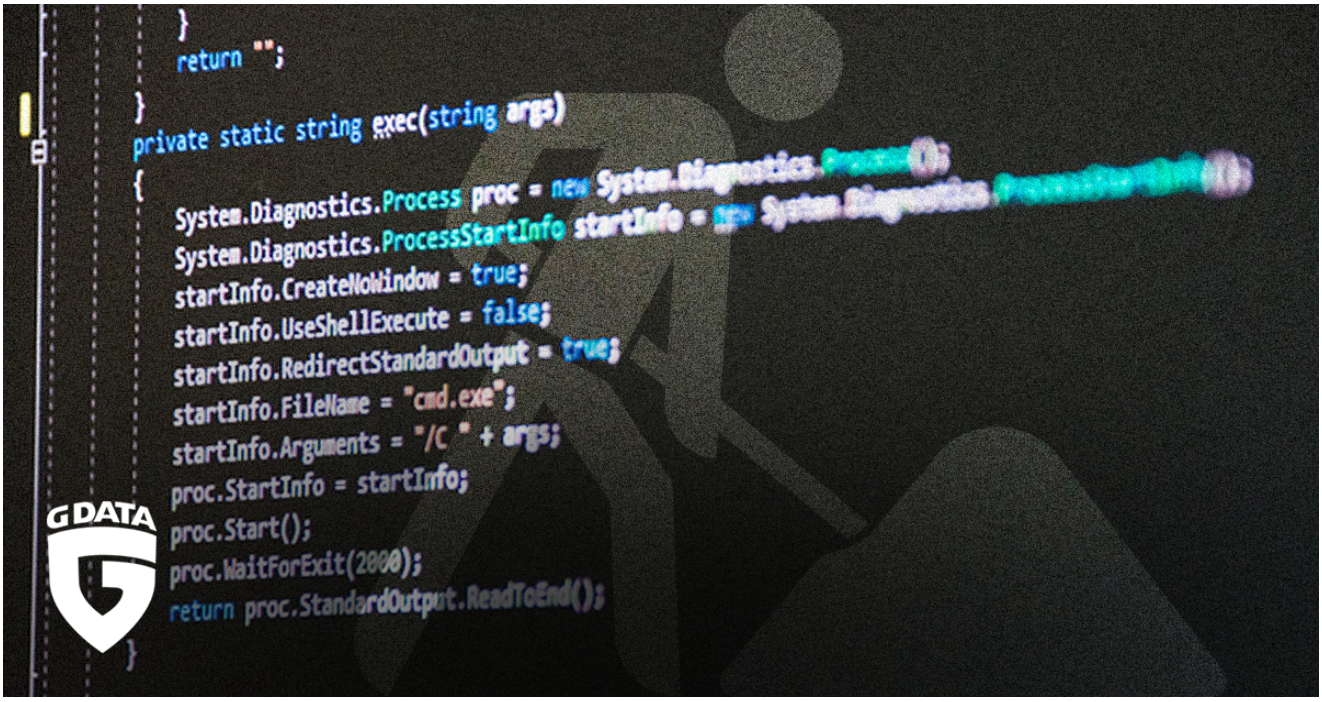
Rurktar - Spyware under Construction

gdatasoftware.com/blog/2017/07/29896-rurktar-spyware-under-construction



The development of any kind of software takes time. Not every function that is planned for the final product is implemented right from the start. It does not come as a surprise that this is also true for the development of malware. At the G DATA Security Labs, a file has sparked the interest of our researchers - this file is interesting for a number of reasons.

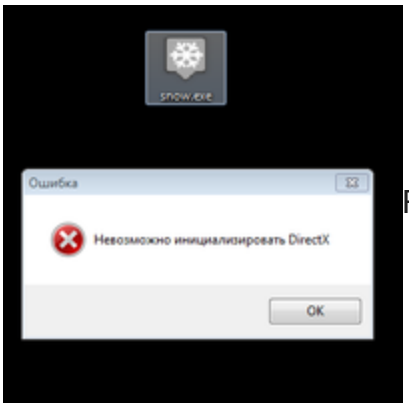
Who commissioned it?

The new espionage tool which was was christened "Rurktar" allows some conclusions as to its origin. It is very likely that it originates from Russia. There is quite some evidence to support this: some of the internal error messages of Rurktar are in Russian. Also, the IP addresses used for remote control of the spyware are located in Russia.

It is not 100 per cent clear whether Rurktar is the work of a single individual or a development team. What we can say, though, is that a Dropbox folder is used as a working directory. There are several possible reasons for this. One of them is that several developers are cooperating here and consolidate their work through a Dropbox. What Dropbox can also be used for by a single individual is a crude and very basic versioning system - some

Dropbox accounts offer the possibility of restoring earlier versions of a file. Therefore, it can be used to track changes, but it is not ideal from a developer's stand point. Using Dropbox as a backup is, of course, also a possibility to be considered here.

Objectives



Rurktar error message in Russian

Although not all of the functions are omplemented yet, it is relatively safe to say that Rurktar is intended for use in targeted spying operations. The functions that are already implemented allow reconnaissance of a network infrastructure, they can check whether or not a particular machine is reachable, take screen shots and even download specific files from an infected machine. It is also possible to delete files from or upload files to a machine. All of this points to industrial espionage - the functions that have been described so far do not have any practical application for large-scale operations, such as ransomware schemes.

Prevalence

As the spyware is still in a development state and not operational yet, it has not spread very widely.
Those few IP addresses that have been linked to Rurktar so far could just as well only have been used for testing purposes by the developer(s). This, however, can and will change as development work progresses. The IP addresses used for remote controlling Rurktar will see more diversity and not only be confined to Russia but to other countries as well. This is also due to the fact that other actors will start using or repurposing the malware either entirely or in parts. Past experiences have shown that many malidious programs are used by so-called "script kiddies" who intend to cobble together new malware using readily available parts while having only minimal coding skills. This has happened, for instance, with the "HiddenTear" ransomware, which was originally designed for training and education. It had some flaws in its cryptographic components (which had also been documented by the developer) - but this did not keep some from using the flawed encryption components to create "real" ransomware.

The versions of Rurktar which are known so far are detected by all G DATA solutions as **MSIL.Backdoor.Rurktar.A**.

"Coming soon"?

Many functions and configuration parameters are defined but not implemented yet. The following table shows a small excerpt:

Configuration	Functionality
Debug	If enabled, a logfile "RCS.log" gets written to the hard drive.
Port	The port which the malware connects to
IP	The IP which the malware connects to
FriendlyID	Default return value which is being used if no UUID could be enumerated.
CaptureMode	Not implemented yet
CaptureStart	Not implemented yet
CaptureMonikerString	Not implemented yet
ACaptureMonikerString	Not implemented yet
VideoCap	Not implemented yet

Feature & configuration list of Rurktar - not all functions are implemented yet.

Detailled information

You can read up on further technical information in Nathan Stern's detailed analysis report. The report is downloadable using the link below.

- Malware
- Exploits
- Vulnerabilities

Related articles:

It's Educational - On the No 1 Argument for Open Source Ransomware

Researchers have published several ransomware projects in the name of education and freedom of knowledge. The question of their usefulness sparks…