IT IS IDENTIFIED ATTACKS OF THE CIBERCRIMINAL LAZARUS GROUP DIRECTED TO ORGANIZATIONS IN RUSSIA

securitysummitperu.com/articulos/se-identifico-ataques-del-grupo-cibercriminal-lazarus-dirigidos-a-organizaciones-en-rusia

20 de febrero de 2019

Security researchers have concluded that the cybercriminal group sponsored by the state of North Korea, Lazarus, would be conducting suspicious activities aimed at companies based in Russia. This is based on the connections discovered between the tactics, techniques and tools detected and the way of operation of the group also known as Hidden Cobra.

Services Affected

• Microsoft Windows Operating Systems

Technical details

The Lazarus campaign aimed at Russia uses malicious Office documents delivered as ZIP files, along with a PDF document called NDA_USA.pdf that contains a StarForce Technologies agreement, which is a Russian software company that provides copy protection software.

The security community believes that Lazarus is divided into at least two subdivisions: the first called Andariel, which focuses on attacking the government and organizations of South Korea, and the second, Bluenoroff, whose main focus is monetization and campaigning. global espionage.

This incident, however, represents an unusual victim choice by the North Korean threat actor. In general, these attacks reflect geopolitical tensions between the Democratic People's Republic of Korea (DPRK) and nations such as the United States, Japan and South Korea.

Infection chain

The main infection flow consists of the following three main steps:

1. A ZIP file containing two documents: a benign decoy PDF document and a malicious Word document with macros.

2. The malicious macro downloads a VBS script from a Dropbox URL, followed by the execution of the VBS script.

3. The VBS script downloads a CAB file from the server in the download area, extracts the embedded EXE file (KEYMARBLE) with the Windows "expand.exe" utility, and finally executes it.

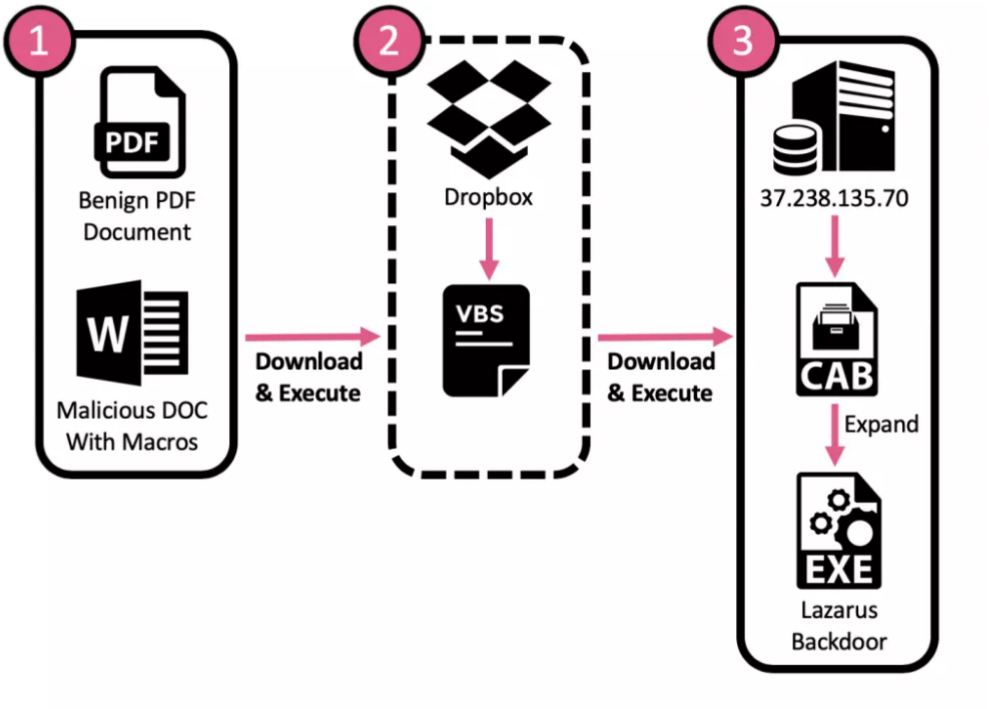


Figure 1 : Sequence of infection of the KEymarble malware of Lazarus.

KEYMARBLE

This malware is a remote administration tool (RAT) that provides its operators with a basic functionality to retrieve information from the victim's computer. Once executed, it performs several initializations, contacts a Command and Control server (C & C) and waits indefinitely to receive new commands. Each received command is processed by the backdoor and is handled within an appropriate function, which in turn collects an information or performs an action on the target computer.

Indicators of Commitment (IoC)

IP

194 [.] 45 [.] 8 [.] 41
37 [.] 238 [.] 135 [.] 70

Hashes

MD5 : dc3fff0873c3e8e853f6c5e01aa94fcf
SHA256 : 1c4745c82fdcb9d05e210eff346d7bee2f087357b17bfcf7c2038c854f0dee61

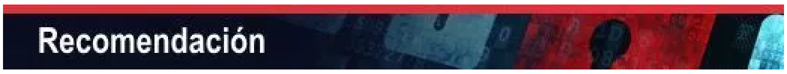
MD5 : 704d491c155aad996f16377a35732cb4
SHA256 : e23900b00ffd67cd8dfa3283d9ced691566df6d63d1d46c95b22569b49011f09

MD5 : 2b68360b0d4e26d2b5f7698fe324b87d
SHA256 :
49a23160ba2af4fba0186512783482918b07a32b0e809de0336ba723636ae3b6

MD5 : a7be38e8f84c5ad9cce30d009dc31d32
SHA256 : f4bdf0f967330f9704b01cc962137a70596822b8319d3b35404eafc9c6d2efe7

MD5 : 7646d1fa1de852bb99c621f5e9927221
SHA256 : 9894f6993cae186981ecb034899353a04f1a9b009bdf265cecda9595b725ee20

MD5 : 22d53ada23b2625265cdbddc8a599ee0
SHA256 :
8e099261929b1b09e9d637e8d054d5909b945b4157f29337977eb7f5fb835e5d



It is recommended that our clients follow the following preventive actions to reduce risks:

For information security personnel:

• Maintain a protocol of strict updates of operating systems, antivirus and all applications that run on them.

• Constantly raise awareness among users on issues related to computer security.

• Restrict the ability (permissions) of users to install and run unwanted software applications. Do not add users to the local administrators group unless it is necessary.

• Block the indicators of commitments (IOC) shown, in the security devices of your infrastructure.

** Before blocking the IOCs, it is important that previously in the development environment, validation and confirmation be made at the level of internal and external services, in order to apply the changes in a controlled manner.

For end users:

• Verify the account information that sends you an email, the name and address of the recipient to identify if they are suspicious.

• Do not open emails of dubious origin (unknown sender), or click on links, or download unknown attachments.

• To detect a spam or phishing email report immediately to the information security managers of your institution.

• Scan all software downloaded from the Internet before execution.

• Visit secure web pages (https), and verify the digital certificate with a click on the padlock on the status bar.

Sources

- Source 1: North Korea Turns Against New Targets ?!
- Source 2: North Korean APT Lazarus Targets Russian Entities with KEYMARBLE Backdoor

If you have any questions, do not hesitate to contact us: informes@securesoftcorp.com