May, 2017

Operation Cloud Hopper & RedLeaves

What you need to know and how to stay protected

LIFARS
your digital world, **secured**

Contents

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com

Overview

Cloud Hopper is a recent Malware campaign that has been targeting MSPs (Managed Service Providers). This campaign is linked to APT10, a Chinese threat actor. There have been a few reports where Japanese organizations have been targeted using ChChes malware under the umbrella of this campaign.

In this campaign, various malware payloads such as RedLeaves and PlugX have been used for implanting a backdoor. APT10 basically uses a side-dynamic link library (DLL) file to load and execute the main payload.

RedLeaves is a new fully-developed backdoor whose activity was first recorded by Japan's CERT in June 2016, while PlugX is a common espionage tool used by many hackers. The first instance of PlugX was recorded in 2014.

Who is APT10?

APT10, also known as menuPass team, Red Apollo, and Stone Panda, is a China-based threat actor which has been predominantly targeting MSPs as well as Japanese organizations in the last 12 months. The first activity of this group was recorded in 2009 when it targeted Western Defense Companies.

APT10, through Cloud Hopper, has targeted and breached a large number of MSPs successfully. After this success, they have an unconditional and unprecedented access to these service providers as well as their clients across the world. Over the past year APT10 has significantly increased their capability and scale of their attacks, and have now shifted to open-source malware, hence making the attacks even more sophisticated.

What is RedLeaves?

RedLeaves, as mentioned, is a malware payload, which consists of three parts:

- **An executable file (.exe):** It is a signed, legitimate application which reads the DLL file in the same folder
- **A Loader File (.dll):** It is a DLL file which is loaded file by the application
- **An Implant ShellCode (.data):** It contains encoded data for RedLeaves which is read by the loader

RedLeaves creates these 3 files in %TEMP% folder, and are bound together to get executed as soon as the legitimate application runs. It is a Remote Administration Trojan (RAT), which has been built in Visual C++ and it excessively makes use of thread generation technique during the execution.

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com

How does RedLeaves operate?

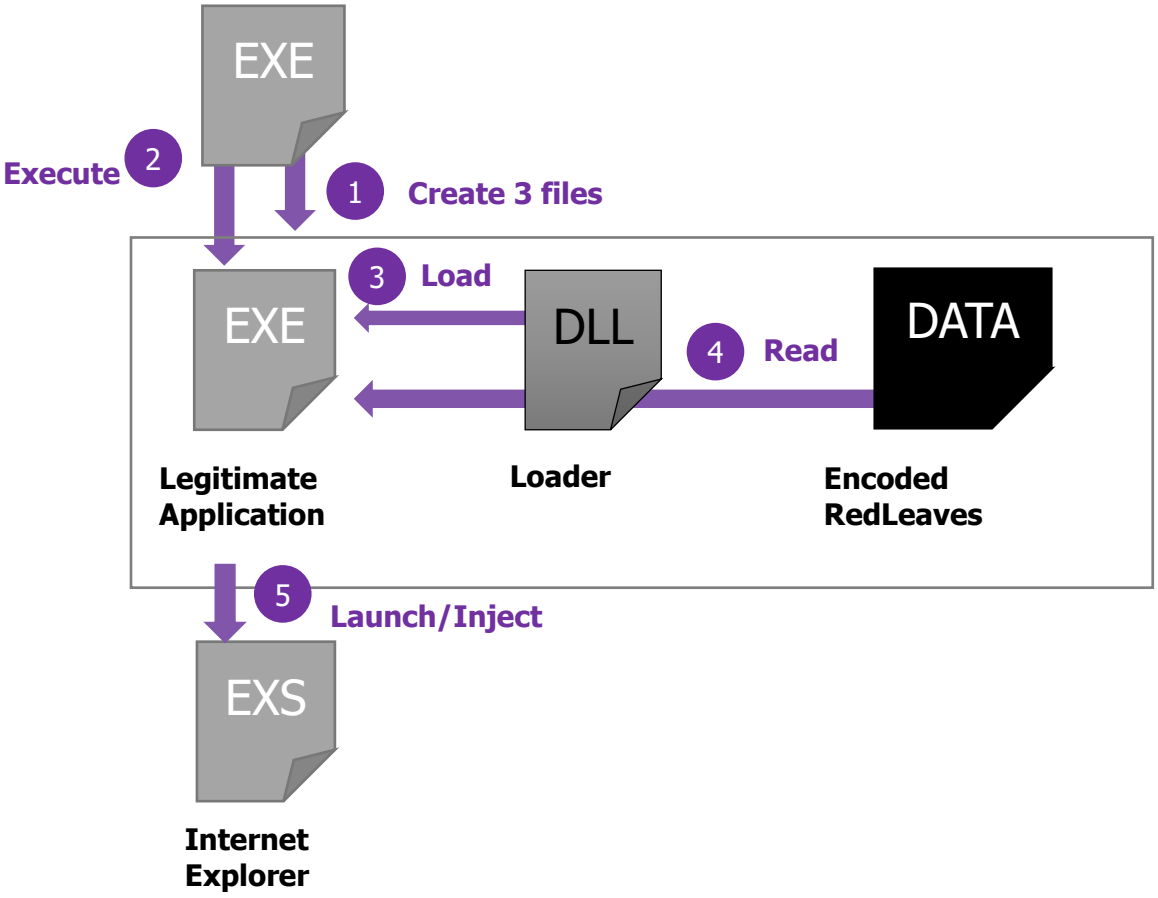

Figure 1: Flow of Events, Source: JPCERT

Step-1: With the help of DLL hijacking, the so-called legitimate application gets executed

Step-2: The application loads the loader into the same folder

Step-3: The loader then decodes the encoded RedLeaves data present in ShellCode file and prepares it for execution

Step-4: After execution, RedLeaves starts a process in a particular browser, most preferably Internet Explorer. The browser chosen depends on its configuration,

Step-5: RedLeaves injects into the said process and keeps on running in the backend

COMMAND & CONTROL (C2)

Command & Control transpires in RedLeaves by using RC4 Cipher technique over Port #443 to the domains that repetitively change the IP addresses. These domains spoof the original websites while keeping a special focus on the websites providing the services related to Windows update. The domains used by RedLeaves use dynamic DNS services, hence they become even more complex to be tracked down.

Capabilities of RedLeaves

According to an in-depth study by US-CERT, RedLeaves is capable of performing following typical RAT functions:

1. SYSTEM ENUMERATION

RedLeaves gathers following fields of information from a victim system and sends it back to its C2:

- Name & Architecture of the system
- Major & Minor versions of the Operating System
- Specifications about the processor
- Amount of the memory available in the system,
- Language of the user,
- Group permissions & Privileges of the user,
- IP Address
- System Uptime
- Primary Drive Storage Utilization

2. COMMAND EXECUTION

When a command containing a "/c" is passed on to cmd.exe, RedLeaves has the capability to execute the command inside a command shell itself.

"cmd.exe /c <command>"

3. COMMAND WINDOW GENERATION

RedLeaves also has the ability to execute a command, which has been generated and passed through a named pipe. The command window is then piped back to C2 as a

remote shell or as a threat or a process that can communicate with that particular pipe. RedLeaves uses *mutexRedLeavesCMDSimulatorMutex* to perform this function.

4. FILE SYSTEM ENUMERATION

RedLeaves collects data in each specified directory where it gathers the following information:

- File names
- Last write file names
- File size

5. NETWORK TRAFFIC COMPRESSION AND ENCRYPTION

Before sending the data from a victim system, RedLeaves uses Lempel–Ziv–Oberhumer (LZO) Algorithm. It is a lossless data compression algorithm. This algorithm is known for its speedy decompression. This data is then ciphered with the help of RC4 (Rivest Cipher 4) before being sent back to C2. Whenever RedLeaves is connected to its C2 over Port #443, the connection is not secure. The data being transferred is not encrypted as there is no SSL Handshake taking place. Thus, the data being transferred through the named pipe is the ciphertext generated by the RC4 algorithm.

Security best practices

As mentioned, RedLeaves is a new type of malware that has been in the news since mid-2016. It targets a system through simple email attachments. To make sure that your systems are safe and secure, you can use the directory containing a list of destination websites as given by US-CERT. You can access this directory via this link. Meanwhile, the investigation is still going on, you can follow these best practices:

- Creating an insider threat program and information sharing program
- Completing independent security audit
- Implementing platforms for vulnerability assessment and remediation program
- Encrypting all the data in transit and stored in the storage devices connected to the network
- Maintaining a network & system documentation that should necessarily include asset (owners & type), network diagrams, and an immediate incident response plan