OceanLotus ships new backdoor using old tricks

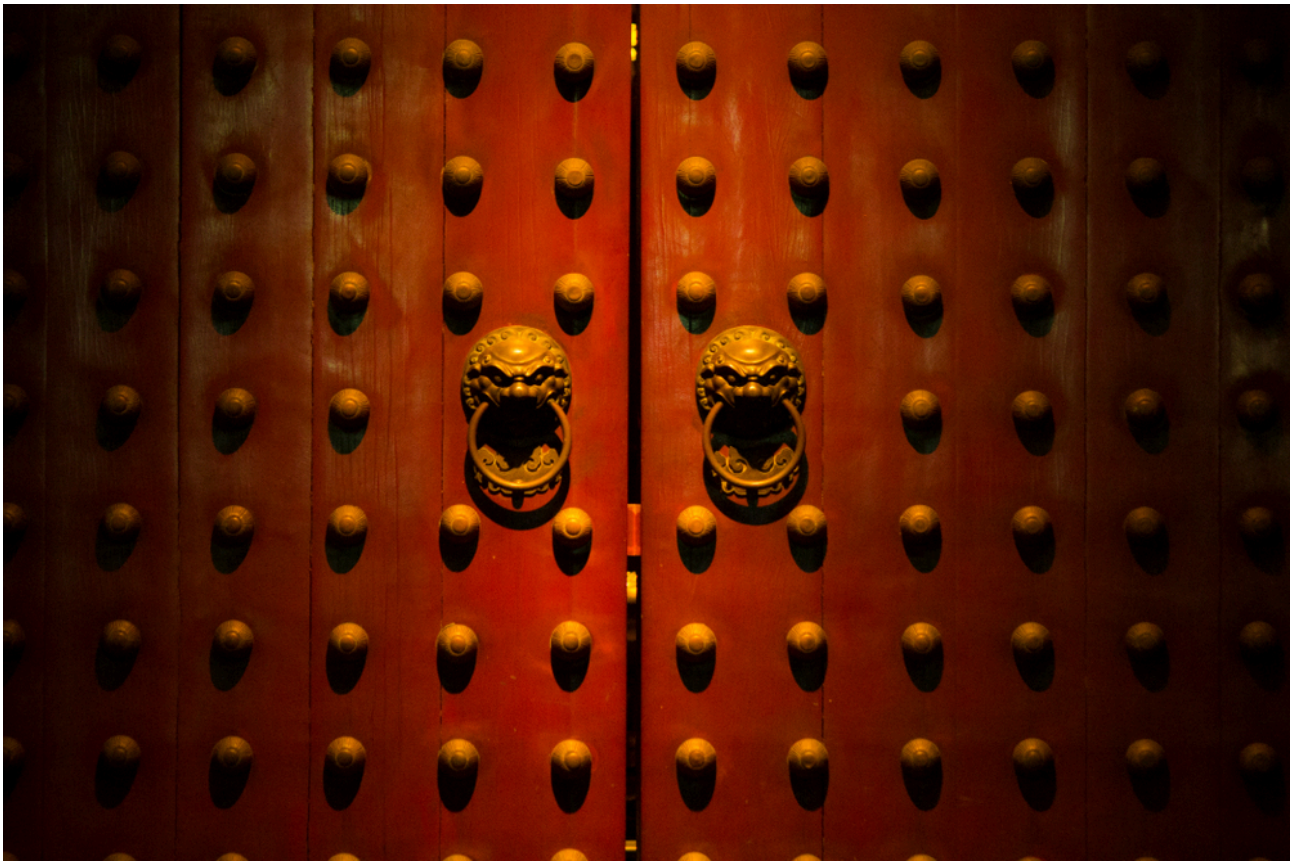
By Tomáš Foltýn

Archived: 2026-04-05 18:58:39 UTC

ESET Research

To smuggle the backdoor onto a targeted machine, the group uses a two-stage attack whereby a dropper package first gains a foothold on the system and sets the stage for the backdoor itself. This process involves some trickery commonly associated with targeted operations of this kind.

13 Mar 2018 • , 4 min. read



ESET researchers have dissected some of the latest additions to the malicious toolkit of the Advanced Persistent Threat (APT) group known as OceanLotus, also dubbed APT32 and APT-C-00.

A prolific purveyor of malware, OceanLotus has its sights set on high-profile corporate and government targets in Southeast Asia, particularly in Vietnam, the Philippines, Laos, and Cambodia. The apparently well-resourced and determined group, is known for integrating its custom-built creations with techniques long known to be successful.

OceanLotus certainly isn't resting on its laurels while pursuing its goals that include cyberespionage, reconnaissance and intellectual property theft. One of the group's latest backdoors is a fully-fledged malicious tool that gives its operators remote access to a compromised machine. The backdoor contains a suite of functionalities, notably a number of tools for file, registry and process manipulation, as well as the loading of additional components.

To smuggle the backdoor onto a targeted machine, the group uses a two-stage attack whereby a dropper package first gains a foothold on the system and sets the stage for the backdoor itself. This process involves some trickery commonly associated with targeted operations of this kind.

The ruse

The attack typically begins with an attempt – most probably via a spearphishing email – to lure the intended victim into running the malicious dropper, which is attached to the email. In order to increase the likelihood that the unsuspecting victim will actually click on it, the malicious executable masquerades as a document or spreadsheet by displaying a fake icon.

When the victim clicks on the attachment, the dropper opens a password-protected document that is intended as a 'red herring' to divert the victim's attention while the dropper goes about its nefarious business. No software exploits are needed.

The attackers use a number of decoy documents. To boost its aura of authenticity, each file has a rather carefully crafted – and usually English – name. ESET detects the files as Win32/TrojanDropper.Agent.RUI.

In addition, OceanLotus is also known to use 'watering hole attacks', which involve the compromise of a website that the victim is likely to visit. In this scenario, the 'prey' is tricked into downloading and executing a fake installer or fake update for popular software from the booby-trapped website. Whatever the method of compromise, ultimately the same backdoor is deployed.

The watering hole technique has probably been used to distribute a dropper called RobototFontUpdate.exe, which is a fake updater for the Roboto Slab regular font and features in our analysis below.

Under the hood

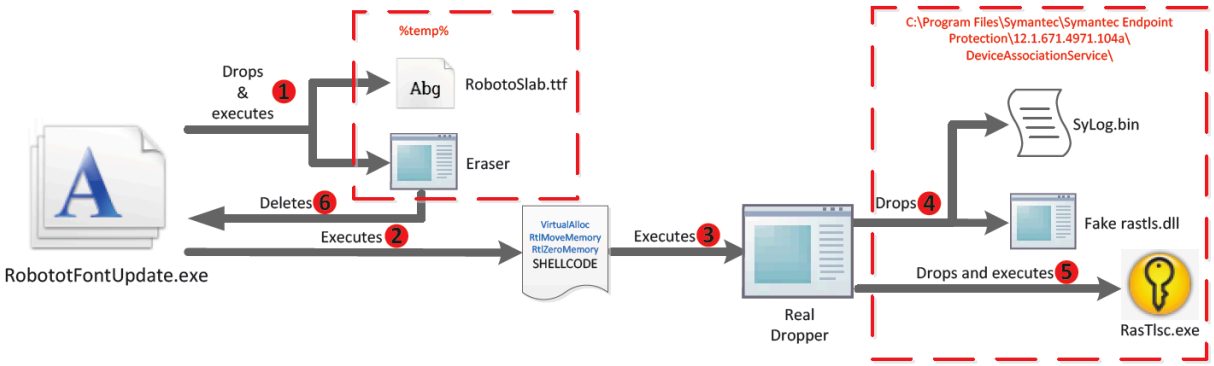


Figure 1. Dropper execution flow

The components of the dropper package are executed in a number of steps; each stage involves a heavy dose of code obfuscation that is designed to shield the malware from detection. To lead researchers and anti-malware software further astray, some garbage code is also included.

If run with administrator privileges, the dropper creates a Windows service that establishes persistence on the system (so that the malware will survive a reboot). Otherwise, the same goal is achieved by tampering with the operating system's registry.

In addition, the package drops an application whose sole purpose is to delete the 'lure document' once it fulfills its mission.

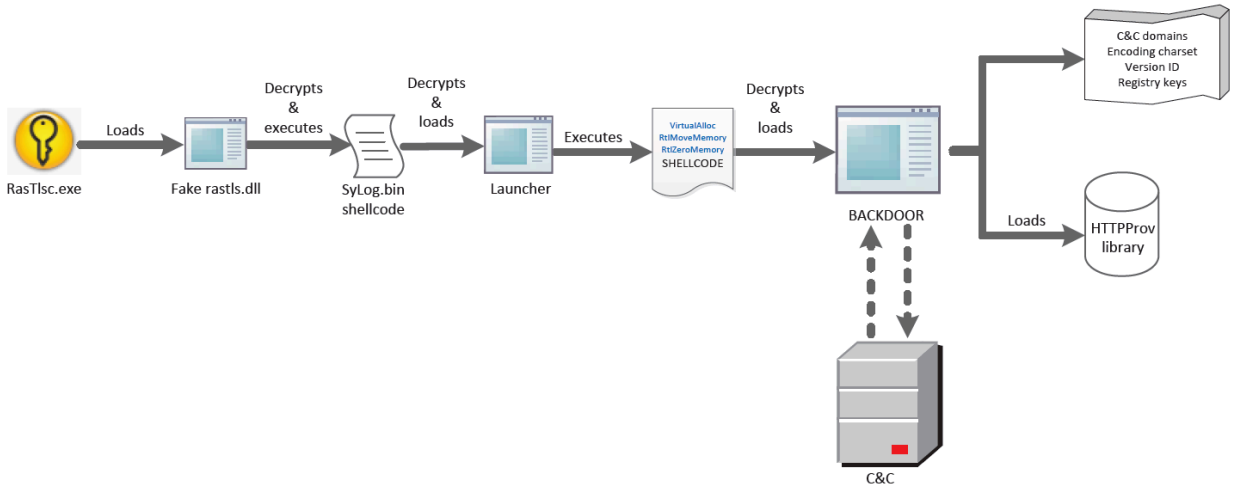


Figure 2. Backdoor execution flow

Importantly, two more files are dropped and come into play during this stage – a digitally-signed executable from a major, legitimate software developer and a malicious Dynamic Link Library (DLL) named after one used by the legitimate executable.

The two files figure in a tried-and-tested trick called 'DLL side-loading', which consists in co-opting a legitimate application's library-loading process by planting a malicious DLL inside the same folder as the signed executable. This is a way to remain under the radar, since a trusted application with a valid signature is less likely to arouse suspicion.

In campaigns utilizing these new OceanLotus tools, we have seen deployed, among others, the genuine signed executables RasTlsc.exe from Symantec and mcoemcpy.exe from McAfee. When run, these programs call, respectively, the maliciously supplied rastls.dll (detected by ESET as Win32/Salgorea.BD) and McUtil.dll (detected as Win32/Korplug.MK).

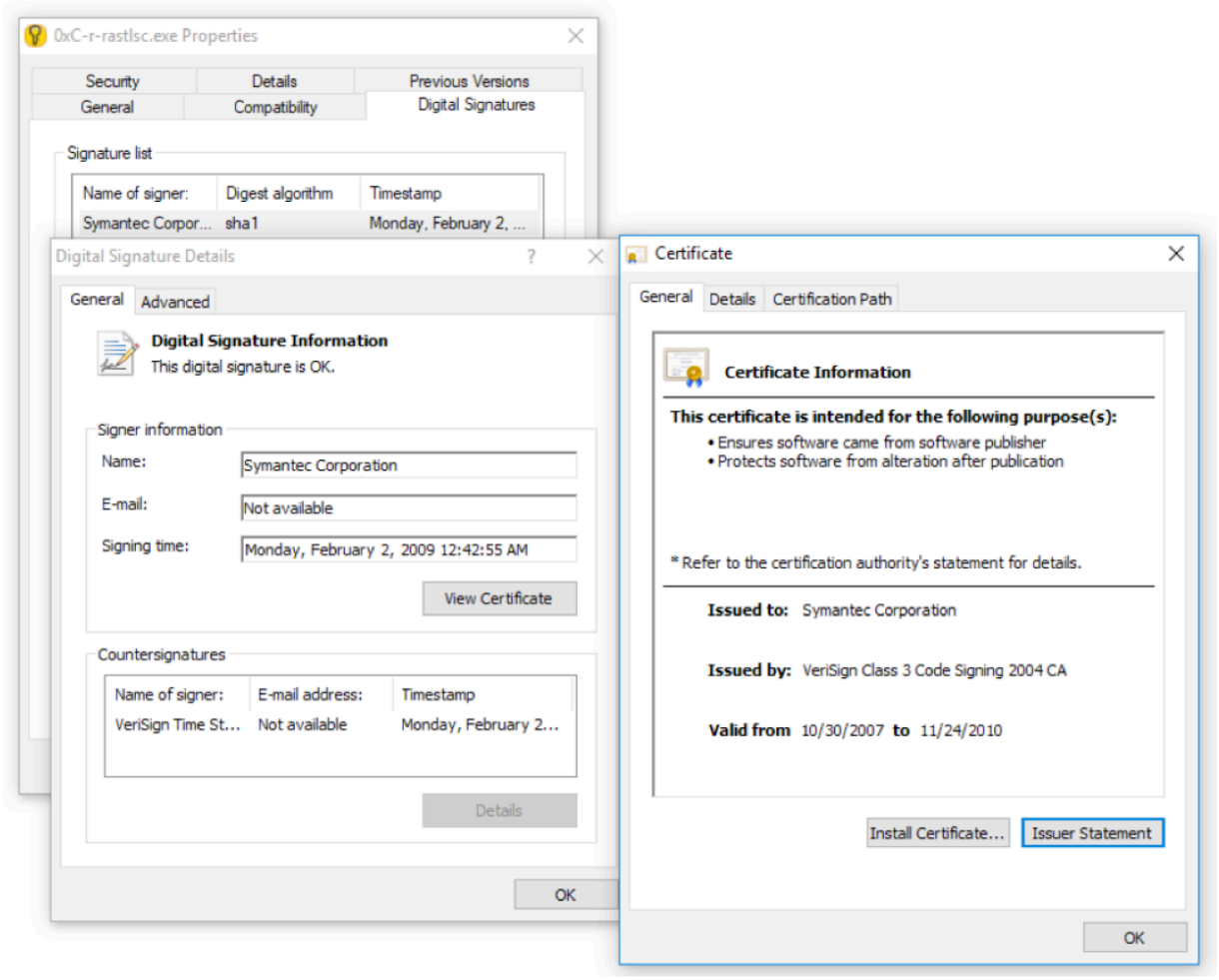


Figure 3. Symantec rastlsc.exe digital signature

The backdoor opens

Once decrypted, the backdoor takes a fingerprint of the system. It sends home various data, such as the computer and user names and the operating system version, before waiting for commands to carry out its main mission.

A number of domain names and IP addresses are used for the command-and-control (C&C) infrastructure. All communication with the C&C servers is encrypted. It can be readily unscrambled, however, as the decryption key is prepended to the data.

Our deep dive (see the link below) into OceanLotus's latest marauding campaigns shows that the group isn't letting up in its efforts and combines legitimate code and publicly available tools with its own harmful creations. The group clearly goes to great lengths in order to bypass detection for its malware and, ultimately, to 'muddy the waters' for researchers.

A detailed analysis may be read in the white paper: *OceanLotus: Old techniques, new backdoor*