Linux, Windows Users Targeted With New ACBackdoor Malware

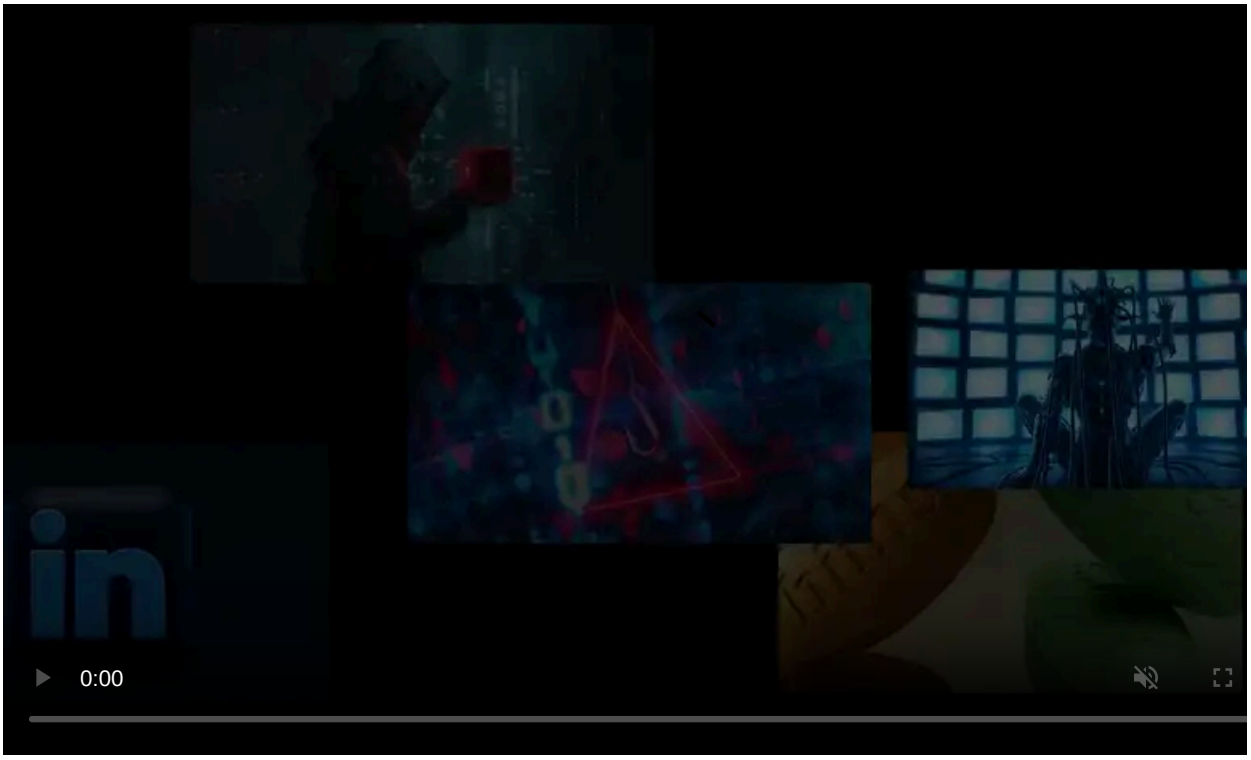
By Sergiu Gatlan

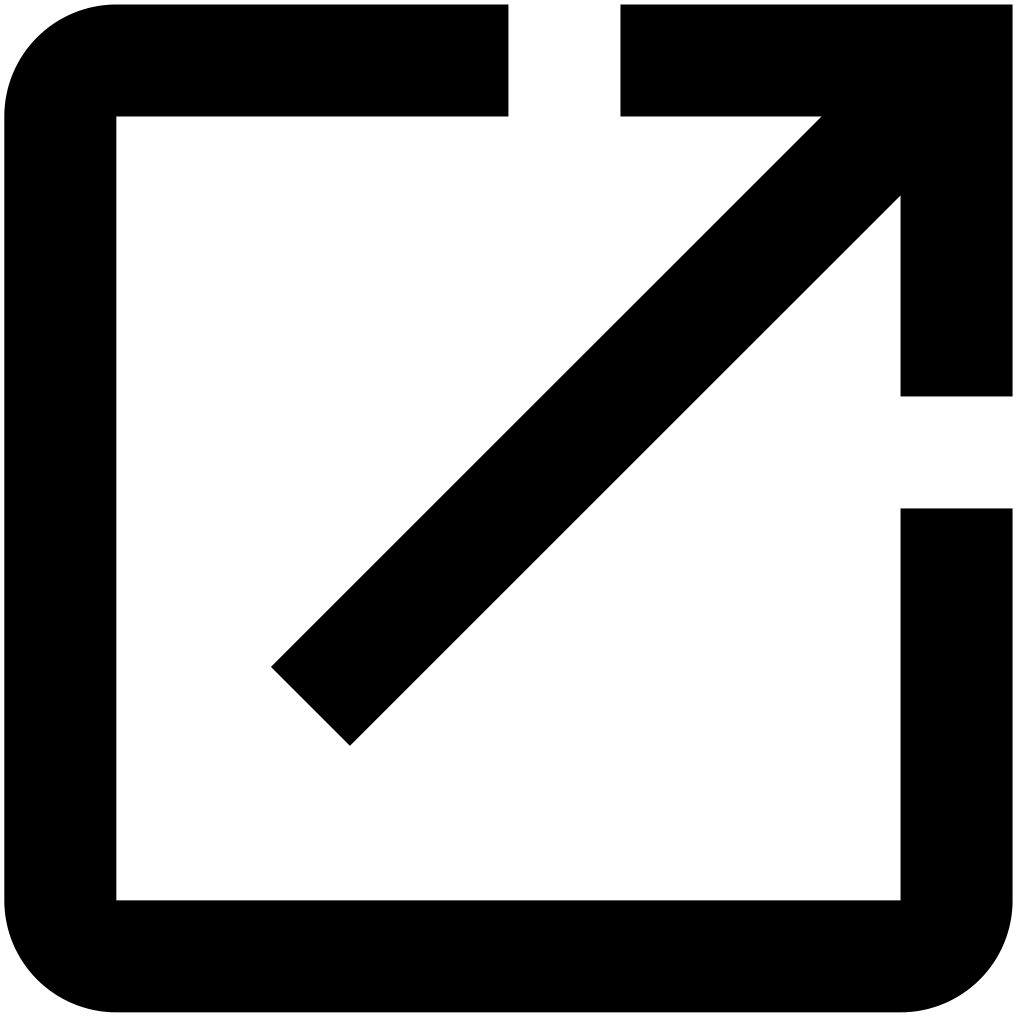
Published: 2019-11-18 · Archived: 2026-04-05 16:52:34 UTC

Researchers have discovered a new multi-platform backdoor that infects Windows and Linux systems allowing the attackers to run malicious code and binaries on the compromised machines.

The malware dubbed ACBackdoor is developed by a threat group with experience in developing malicious tools for the Linux platform based on the higher complexity of the Linux variant as Intezer security researcher Ignacio Sanmillan found.

"ACBackdoor provides arbitrary execution of shell commands, arbitrary binary execution, persistence, and update capabilities," the Intezer researcher found.


0:00



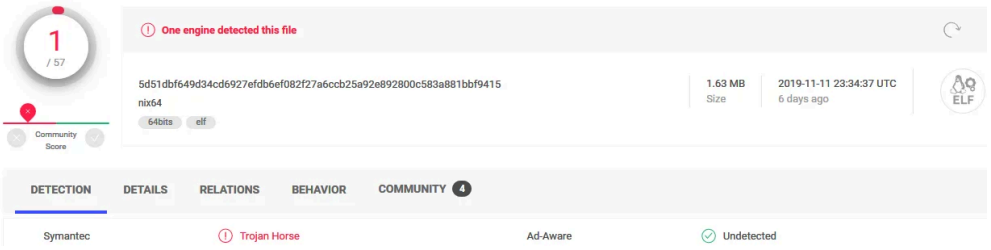
Infection vectors and ported malware

Both variants share the same command and control (C2) server but the infection vectors they use to infect their victims are different: the Windows version is being pushed through malvertising with the help of the Fallout Exploit Kit while the Linux payload is dropped via a yet unknown delivery system.

The latest version of this exploit kit, analyzed by researcher nao_sec in September, targets the CVE-2018-15982 (Flash Player) and the CVE-2018-8174 (Microsoft Internet Explorer VBScript Engine) vulnerabilities to infect visitors of attacker-controlled sites with malware.

Luckily, "the Windows variant of this malware does not represent a complex threat in terms of Windows malware," Sanmillan says.

ACBackdoor's Windows version also seems to have been ported from the Linux one seeing that the researcher discovered that they share several Linux-specific strings like paths belonging to a Linux file system or kernel thread process names.



ACBackdoor Linux variant detection rate

Besides infecting victims via an unknown vector, the Linux malicious binary is detected by only one of the anti-malware scanning engines on VirusTotal at the time this article was published, while the Windows one is detected by 37 out of 70 engines.

The Linux binary is also more complex and has extra malicious capabilities, although it shares a similar control flow and logic with the Windows version.

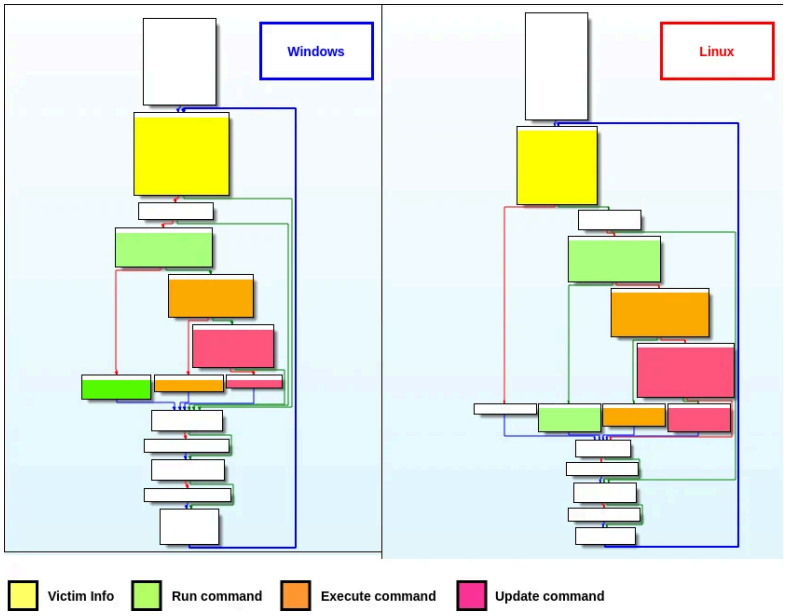
"The Linux implant has noticeably been written better than the Windows implant, highlighting the implementation of the persistence mechanism along with the different backdoor commands and additional features not seen in the Windows version such as independent process creation and process renaming," the report states.

Backdoor malicious capabilities

After it infects a victim's computer, the malware will start collecting system information including its architecture and MAC address, using platform-specific tools to do it, with Windows API functions on Windows and uname UNIX program commonly used to print system info.

Once it's done with the info harvesting tasks, ACBackdoor will add a registry entry on Windows, and create several symbolic links as well as an initrd script on Linux to gain persistence and get automatically launched on system startup.

The backdoor will also attempt to camouflage itself as MsMpEng.exe process, the of Microsoft's Windows Defender antimalware and antispyware utility, while on Linux it will disguise as the Ubuntu UpdateNotifier utility and will rename its process to *[kworker/u8:7-ev]*, a Linux kernel thread.



Windows and Linux variants control flows *(Intezer)*

To communicate with its C2 server, both malware variants use Hypertext Transfer Protocol Secure (HTTPS) as a communication channel, with all the collected information being sent as a BASE64 encoded payload.

ACBackdoor can receive the info, run, execute, and update commands from the C2 server, allowing its operators to run shell commands, to execute a binary, and to update the malware on the infected system.

"Because there is no attributable information documented on this backdoor, there is a possibility that some known Linux-based threat group is updating its toolset," Sanmillan concludes.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
