Linux, Windows Users Targeted With New ACBackdoor Malware

bleepingcomputer.com/news/security/linux-windows-users-targeted-with-new-acbackdoor-malware/

Sergiu Gatlan

By
Sergiu Gatlan

- November 18, 2019
- 02:23 PM
- 6

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.

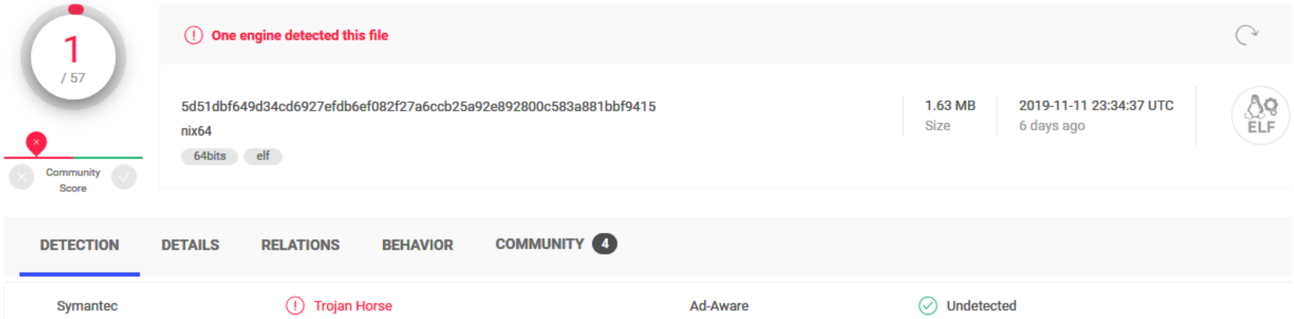
Infection vectors and ported malware

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.



One engine detected this file

5d51dbf649d34cd6927efdb6ef082f27a6ccb25a92e892800c583a881bbf9415
nix64
64bits elf

1.63 MB
Size

2019-11-11 23:34:37 UTC
6 days ago

Symantec ⓘ Trojan Horse Ad-Aware ✓ Undetected

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.

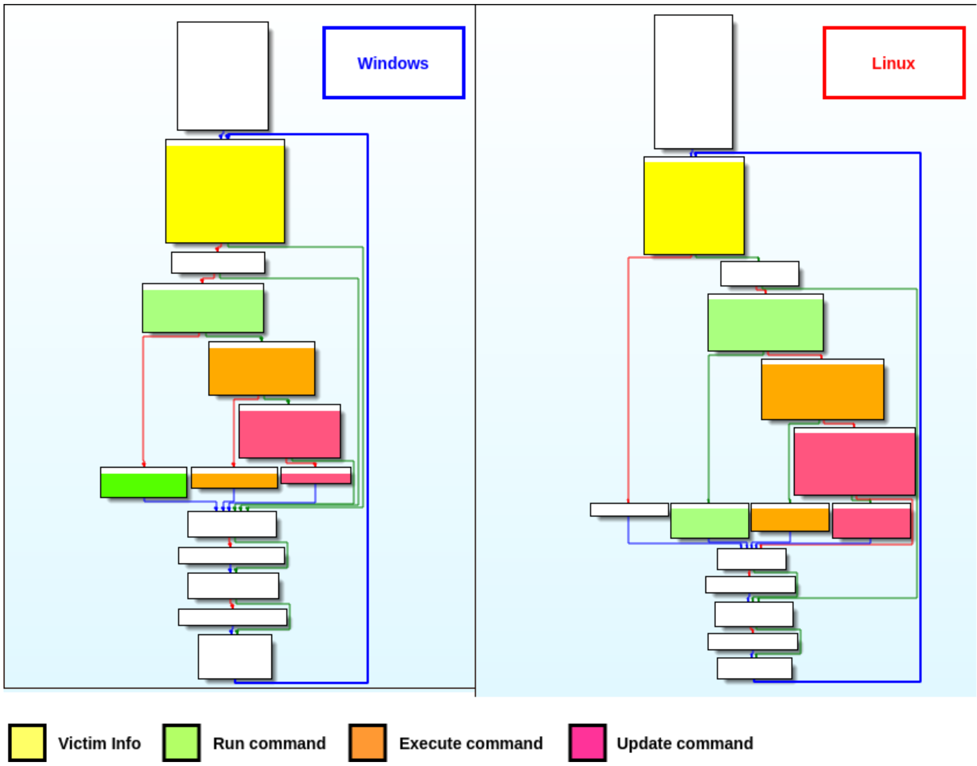
"The Linux implant has noticeably been written better than the Windows implant, highlighting the implementation of the persistence mechanism along with the different backdoor commands and additional features not seen in the Windows version such as independent process creation and process renaming," the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

Related Articles:

Malicious PyPI package opens backdoors on Windows, Linux, and Macs

Microsoft: Sysrv botnet targets Windows, Linux servers with new exploits

New cryptomining malware builds an army of Windows, Linux bots

BPFDoor malware uses Solaris vulnerability to get root privileges

BPFDoor: Stealthy Linux malware bypasses firewalls for remote access

- Backdoor
- Exploit Kit
- Fallout Exploit Kit
- Linux
- Malware
- Windows

Sergiu Gatlan

Sergiu Gatlan is a reporter who covered cybersecurity, technology, Apple, Google, and a few other topics at Softpedia for more than a decade. Email or Twitter DMs for tips.

- Previous Article
- Next Article

Comments

-
  buddy215 - 2 years ago
  -
  -

  As I read this....this malware targets Flash Player that hasn't been updated with the December 2018 Flash Player security update. Am I right about that? To further clarify...that is what is targeted on a Linux machine...right?

-
  serghei - 2 years ago
    -
    -

  Nope, that is the Windows variant.

  "the Linux payload is dropped via a yet unknown delivery system"
-
  buddy215 - 2 years ago
    -
    -

  Thanks
-
  ElliotAlderson - 2 years ago
    -
    -

  “the Linux payload is dropped via a yet unknown delivery system.”

  A total non-story then !!!

-

  Al_Capella - 2 years ago

"“the Linux payload is dropped via a yet unknown delivery system.” A total non-story then !!!"

Linux getting infected by backdoor malware is a total non-story? Maybe you're confused by the term "dropped." "Dropped" means loaded into the victim system.

-
  Mike_Walsh - 2 years ago

  Well, totally as expected, I see the Linux/Unix variant is being targeted at Ubuntu. Predictable, bog-standard practice; target the largest user-base.

  It won't know WHAT the hell to make of Puppy Linux, then. Pup loads from 'read-only' files, on a 'locked' CD that physically CANNOT be tampered with. When running in permanent 'Live' mode, with nothing saved from the session; at shutdown, the entire session contents simply go poooff!!.....and disappear into cyber-space.

  And Puppy's initrd is like nothing you've ever even imagined. 16+aufs file-system layers, controlled a script that's like so much gibberish even to veteran Linux users.... Nope; nothing 'standard' there, by a long chalk.

  Figure out a way round THAT one, threat actors..... These idiots will soon come to realize that the 'geek' community won't be quite as susceptible to their drivel as they would like them to be, given that most of us know our systems inside out.....and stuff like this will stick out like a sore thumb.

  It's times like this I'm glad NOT to be one of 'the crowd', using bog-standard, 'mainstream' distros...!!

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: