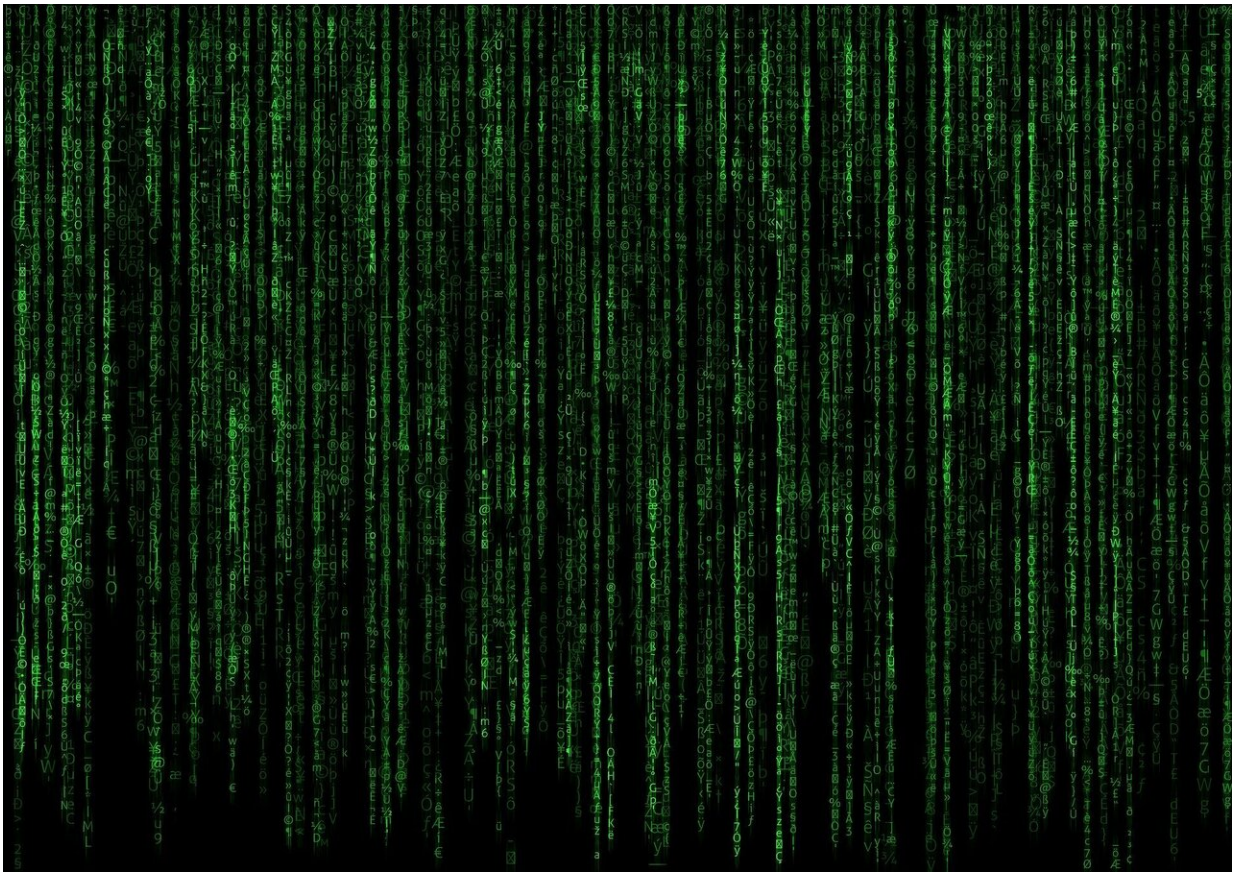
Researcher hacks into 35 major technology firms

February 11 2021, by Peter Grad



Credit: Pixabay/CC0 Public Domain

A Romanian threat researcher detailed in a published report Wednesday how he broke into IT systems belonging to some of the largest

corporations in the world. His assaults successfully targeted Apple, Microsoft, Tesla, PayPal, Netflix and more than 30 other corporations.

Alex Birsan advised the companies in advance that he would be testing the security of their systems, but did not provide them with details beforehand.

Birsan accomplished the tasks by launching a relatively simple attack mode: He replaced private code packages routinely activated by servers with public code packages. When searching for a code package, automated systems used by companies tap into public repositories. If a Javascript, Ruby or Python module is required to execute a particular function, company servers will automatically swap a public module for its own in-house one if it detects an identically named package it believes is a newer version.

His exploit, Birsan told BleepingComputer, exposed "vulnerabilities or design flaws in automated build or installation tools [that] may cause public dependencies to be mistaken for internal dependencies with the exact same name."

Birsan took advantage of this vulnerability by injecting code into packages stored in public repositories such as GitHub. He termed the intentional duplication of names and subsequent swapping of files 'dependency confusion.'

He first had to determine the names companies used for the code files so he could create counterfeit files with the same names, but he found that task to be relatively easy. Shopify, for instance, automatically installed a forged file from Birsan that he correctly guessed was "Shopify-cloud."

"The success rate was simply astonishing," Birsan said an online assessment of his exploits Wednesday.

"We were able to automatically scan millions of domains belonging to the targeted companies and extract hundreds of additional javascript package names which had not yet been claimed on the npm registry," Birsan said.

Such planted by a malicious actor could wreak havoc throughout a company's network, disrupt operations, steal data or attempt to extort money.

Birsan's code was not malicious; he retrieved only basic information about each computer his code impacted including username, hostname and current path of each unique installation. The program notified Birsan when his code was activated by target companies.

"Along with the external IPs, this was just enough data to help security teams identify possibly vulnerable systems based on my reports," Birsan said, "while avoiding having my testing be mistaken for an actual attack."

In return Birsan collected 'bug bounty' cash that companies pay out to researchers who uncover vulnerabilities. The total from several companies that paid him topped $130,000.

Birsan came up with the idea when a colleague, Justin Gardner, examined an internal JavaScript package managing file and wondered what would happen if an identically named file were placed in a public repository. They soon discovered that whichever file had the most recent build number would be tapped by the company's server.

Most of the affected companies were able to quickly patch their systems following notification of the breach.

But Birsan says he believes that dependency confusion on open-source

platforms remains a problem.

"Specifically, I believe that finding new and clever ways to leak internal package names will expose even more vulnerable systems, and looking into alternate programming languages and repositories to target will reveal some additional attack surface for dependency confusion bugs," he said.

More information: medium.com/@alex.birsan/depend … nfusion-4a5d60fec610

Citation: Researcher hacks into 35 major technology firms (2021, February 11) retrieved 25 April 2024 from https://techxplore.com/news/2021-02-hacks-major-technology-firms.html