Bug hunter finds cryptocurrency-mining botnet on DOD network

Monero-mining botnet infects one of the DOD's Jenkins servers.

By Catalin Cimpanu for Zero Day | February 5, 2020 -- 19:42 GMT (11:42 PST) | Topic: Security

Image: Dmitry Moraine

A security researcher hunting for bug bounties discovered last month that a cryptocurrency-mining botnet had found a home and burrowed inside a web server operated by the US Department of Defense (DOD).

The issue was discovered and reported (https://hackerone.com/reports/768266) via the DOD's official bug bounty program by Indian security researcher Nitesh Surana (https://twitter.com/ideaengine007).

Initially, the bug report was filed in relation to a misconfigured Jenkins automation server (https://en.wikipedia.org/wiki/Jenkins_(software)) running on an Amazon Web Services (AWS) server associated with a DOD domain.

Surana discovered that anyone could access the Jenkins server without login credentials.

Full access was apparently possible, including to the filesystem. Surana says the /script folder, part of the Jenkins installation, was also open to anyone.

This folder is where users upload files which the Jenkins server reads and executes automatically at regular intervals.

Surana informed the DOD that an attacker could upload malicious files inside this folder and install a permanent backdoor or take over the entire server.

SERVER ALREADY HACKED BEFORE RESEARCHER'S REPORT

The DOD secured the vulnerable server, but when revisiting his findings, Surana also realized that the Jenkins server had already been compromised even before he found it.

The researcher said he tracked down the clues he found to a malware operation specialized in hacking cloud servers and installing Monero-mining malware.

ZDNet searched for the Monero wallet address that this botnet was using to collect funds. Google results (https://www.google.com/search?q=%2246sfbbM3XSjBo54d5a8PYUU5yQ31x6Rpv6tBhe22Cd7VYeJUyFUhzBF5rTf1oTB1d8MqgHxX5RbbEEKZd8fBAAr show tens of mentions of this address going back as far as August 2018.

Most mentions are from Chinese users, who reported finding a Monero miner on their cloud servers [1 (https://blog.verysu.com/mobile/article/398), 2 (https://www.52pojie.cn/thread-1079327-1-1.html), 3 (https://cloud.tencent.com/developer/news/304639), 4 (https://github.com/xmrig/xmrig/issues/1470), 5 (https://www.cnblogs.com/mybxy/p/12144154.html), 6 (https://bbs.csdn.net/topics/395440908?list=74194821)].

Using the XMRHunter service, we found that the Monero address currently holds 35.4 Monero coins, worth just over $2.700. However, past funds could have been withdrawn to other

accounts at regular intervals, so we can't accurately estimate this botnet's operation just on this address.

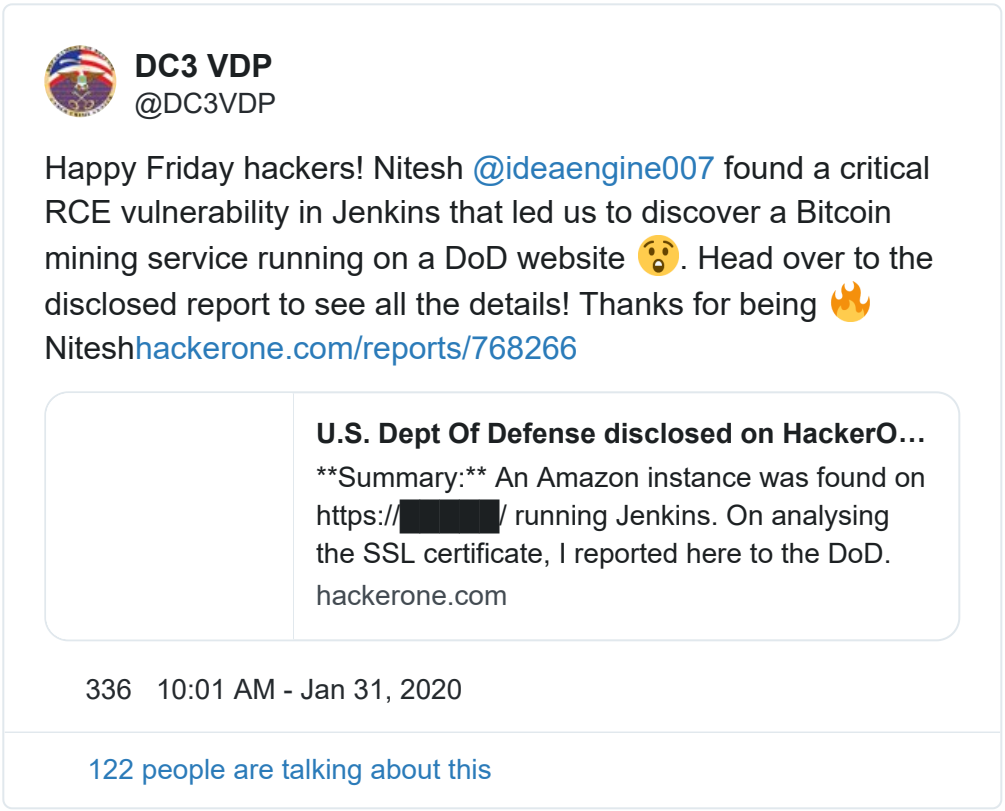
DOD RUNS A BUG BOUNTY PROGRAM ON HACKERONE

Surana reported his findings through the DOD's official bug bounty program (https://hackerone.com/deptofdefense), hosted on the HackerOne platform.

The DOD has been running a bug bounty program for years.

The most recent DOD bug-hunting drive ended last month, during which the department paid $275,000 to security researchers (https://www.helpnetsecurity.com/2020/01/17/department-of-defense-hackerone/) for their work in finding bugs in US Army-related web servers.

Due to the sensitive nature of the DOD infrastructure, Surana's report was redacted to remove the name and URL of the DOD server that was compromised by the coin-mining botnet. The researcher told ZDNet he was not awarded a bounty for his report, but this was one of the rare cases where a researcher's findings were made public.



Threat Intelligence Index Report from IBM X-Force

The Tonya Hall Innovation Show

Follow

07:31

SECURITY

FBI recommends passphrases over password complexity (https://www.zdnet.com/article/fbi-recommends-passphrases-over-password-complexity/)

Cisco unveils SecureX cloud platform for improved security visibility (https://www.zdnet.com/article/cisco-unveils-securex-cloud-platform-for-improved-security-visibility/)

Forget passwords: Secure yourself with a passphrase and these tools (https://www.zdnet.com/article/forget-passwords-secure-yourself-with-a-passphrase-and-these-tools/)

Scam, spam and phishing texts: How to spot SMS fraud and stay safe (https://www.zdnet.com/article/scam-spam-and-phishing-texts-how-to-spot-sms-fraud-and-stay-safe/)

Cybersecurity: Do these ten things to keep your networks secure from hackers (https://www.zdnet.com/article/cybersecurity-do-these-ten-things-to-keep-your-networks-secure-from-hackers-hospitals-told/)

Threat Intelligence Index Report from IBM X-Force (ZDNet YouTube) (https://www.youtube.com/watch?v=dyoPsJYr_rg)

Best home security of 2020: Professional monitoring and DIY (CNET) (https://www.cnet.com/how-to/best-home-security-systems-for-2020/?ftag=CMG-01-10aaa1b)

How to set up secure credential storage for Docker (TechRepublic) (https://www.techrepublic.com/article/how-to-setup-secure-credential-storage-for-docker/?ftag=CMG-01-10aaa1b)

RELATED TOPICS: GOVERNMENT - US | SECURITY TV | DATA MANAGEMENT | CXO | DATA CENTERS

By Catalin Cimpanu for Zero Day | February 5, 2020 -- 19:42 GMT (11:42 PST) | Topic: Security

SHOW COMMENTS