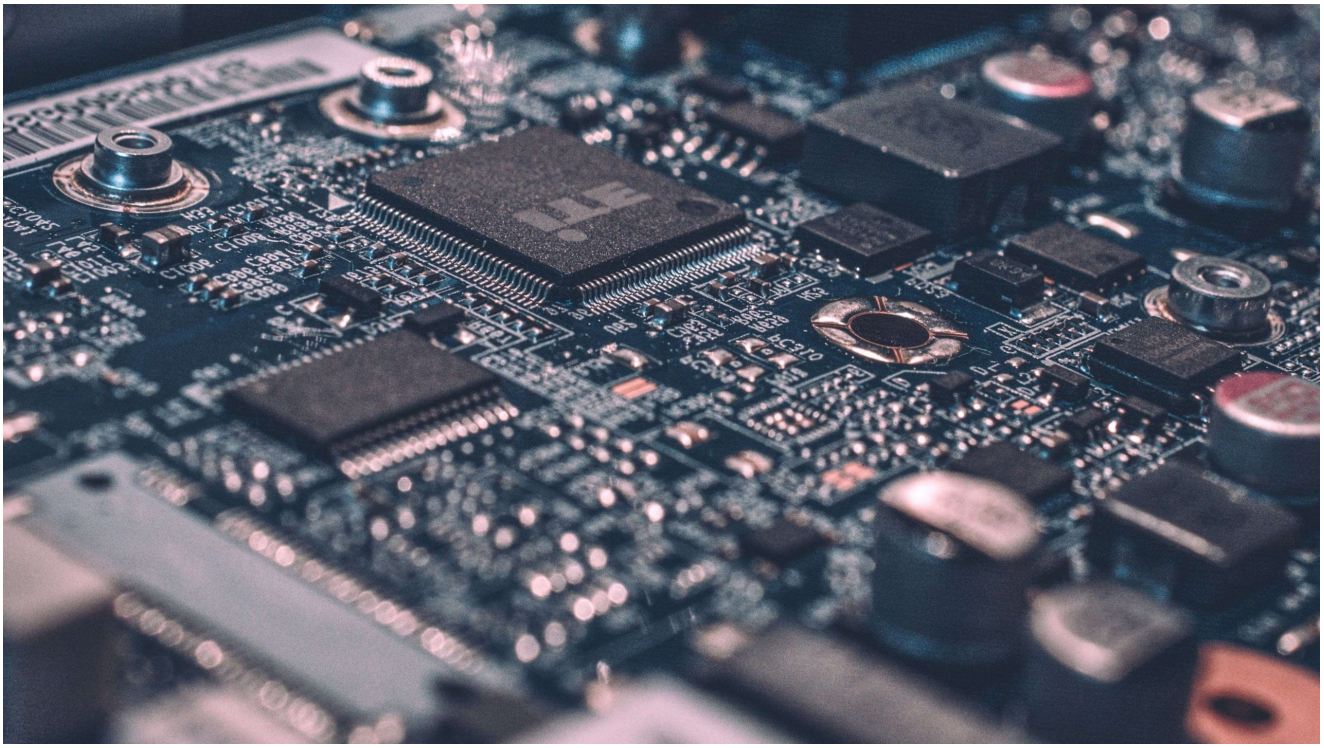
First Fully Weaponized Spectre Exploit Discovered Online

therecord.media/first-fully-weaponized-spectre-exploit-discovered-online/

March 1, 2021



A fully weaponized exploit for the Spectre CPU vulnerability was uploaded on the malware-scanning website VirusTotal last month, marking the first time a working exploit capable of doing actual damage has entered the public domain.

The exploit was discovered by French security researcher Julien Voisin. It targets Spectre, a major vulnerability that was disclosed in January 2018.

According to its website, the Spectre bug is a hardware design flaw in the architectures of Intel, AMD, and ARM processors that allows code running inside bad apps to break the isolation between different applications at the CPU level and then steal sensitive data from other apps running on the same system.

The vulnerability, which won a Pwnie Award in 2018 for one of the best security bug discoveries of the year, was considered a milestone moment in the evolution and history of the modern CPU.

Its discovery, along with the Meltdown bug, effectively forced CPU vendors to rethink their approach to designing processors, making it clear that they cannot focus on performance alone, to the detriment of data security.

Software patches were released at the time, but the Meltdown and Spectre disclosures forced Intel to rethink its entire approach to CPU designs going forward.

Initial Spectre PoCs were all benign

At the time, the teams behind the Meltdown and Spectre bugs published their work in the form of research papers and some trivial proof-of-concept code to prove their attacks.

Shortly after the Meltdown and Spectre publications, experts at AV-TEST, Fortinet, and Minerva Labs spotted a spike in VirusTotal uploads for both CPU bugs.

While initially there was a fear that malware authors might be experimenting with the two bugs as a way to steal data from targeted systems, the exploits were classified as harmless variations of the public PoC code published by the Meltdown and Spectre researchers and no evidence was found of in-the-wild attacks.

> Meltdown and Spectre always seemed vulnerabilities where for most people and orgs the cure was going to be worse than the disease. https://t.co/aPOvGD2GSF
>
> — Martijn Grooten (@martijn_grooten) March 28, 2018

But today, Voisin said he discovered new Spectre exploits—one for Windows and one for Linux—different from the ones before. In particular, Voisin said he found a Linux Spectre exploit capable of dumping the contents of ***/etc/shadow***, a Linux file that stores details on OS user accounts.

Such behavior is clearly malicious; however, there is no evidence that the exploit was used in the wild, as it could have also been uploaded on VirusTotal by a penetration tester as well.

Exploits linked to Immunity's CANVAS tool

But the most interesting part of Voisin's discovery is in the last paragraph of his blog, where he hints that he may have discovered who may be behind this new Spectre exploit.

"Attribution is trivial and left as an exercise to the reader," the French security researcher said in a mysterious ending.

But while Voisin did not want to name the exploit author, several people were not as shy. Security experts on both Twitter and news aggregation service HackerNews were quick to spot that the new Spectre exploit might be a module for CANVAS, a penetration testing tool developed by Immunity Inc.

"If you are a paid subscriber, you get extra bits [of information] from VirusTotal. One of which is you can see what files are 'parents' of the sample," said a HackerNews user today.

“In this case, there are a bunch of zip files that contain this file, all named Immunity Canvas or similar. Canvas is a pentesting tool where they publish exploits, so I guess he’s saying you can attribute it to Immunity.”

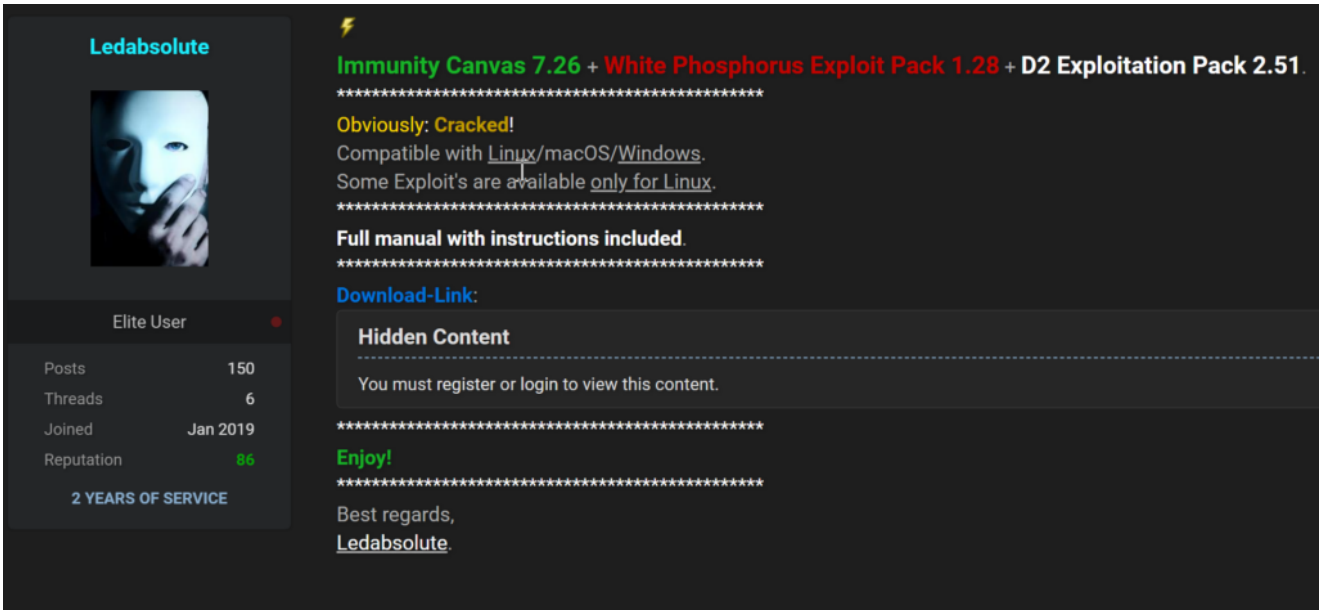
An Immunity spokesperson did not return a request for comment from *The Record* before this article’s publication to confirm that the Spectre exploits uploaded on VirusTotal last month are indeed Canvas modules.

However, in a tweet today from Dave Aitel, the former Immunity CEO appears to confirm that Voisin’s discovery is indeed the CANVAS Spectre module that his former company was touting back in February 2018.

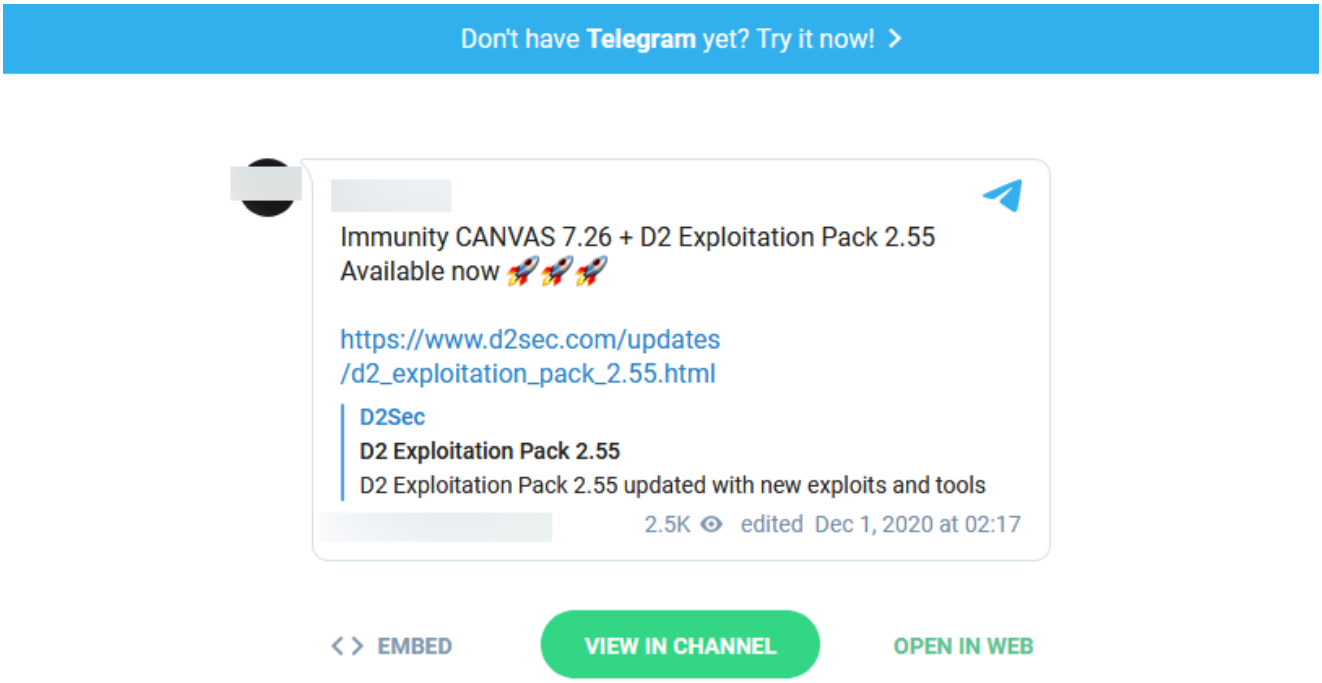
> Just some random video that MAY or MAY NOT be interesting to you! 🙂 https://t.co/bc6BfMLi4P
>
> — daveaitel (@daveaitel) March 1, 2021

> For those who have been asking, our SPECTRE exploit dumping /etc/shadow is now available to our Canvas Early Update clients.https://t.co/CEqGfTXa2R#spectre #meltdown pic.twitter.com/SbESP69Fo6
>
> — Immunity Inc. (@Immunityinc) February 1, 2018

Furthermore, shortly after this this article went live, a source in the cybersecurity community who did not want to be named effectively confirmed our report by pointing *The Record* to a post on an underground hacking forum where a threat actor had published a cracked version of the Immunity CANVAS v7.26 pen-testing tool, along with cracked copies of White Phosphorus and D2, two CANVAS expansion packs that contained two different sets of exploits for various vulnerabilities. Among the vulnerabilities there was also an exploit for CVE- 2017-5715, the vulnerability ID for the Spectre bug.



Dmitry Smilyanets, cyber threat intelligence expert for Recorded Future, told *The Record* that cracked versions of this pen-testing toolkit have been shared in private Telegram channels for months, since at least October 2020, if not earlier.



These new revelations suggest that these cracked CANVAS versions are most likely the source of the CANVAS Spectre modules that were uploaded on VirusTotal on February 3.

The fact that Immunity had a fully working and fully weaponized Spectre exploit is not a surprise for industry experts, as Aitel's company was also among the first to put together a fully weaponized exploit for the BlueKeep vulnerability back in 2019, which it publicly advertised at the time, as a way to boast CANVAS' superior penetration-testing features.

Last "patch now" warning!

Copies of this Spectre exploit are now making the rounds in Discord and Telegram channels run by security researchers, and it's only a matter of time until they hit GitHub and become broadly available to everyone, including malware authors.

If the exploit code can be weaponized as part of an actual attack still remains to be seen as this is no run-of-the-mill vulnerability, but ready-made exploits that enter the public domain are often abused as it's easier for threat actors to adapt code written by someone else than write their own from scratch.

Voisin's discovery is about as close the Spectre doomsday clock can tick close to midnight before attacks get underway, if they haven't already.

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.