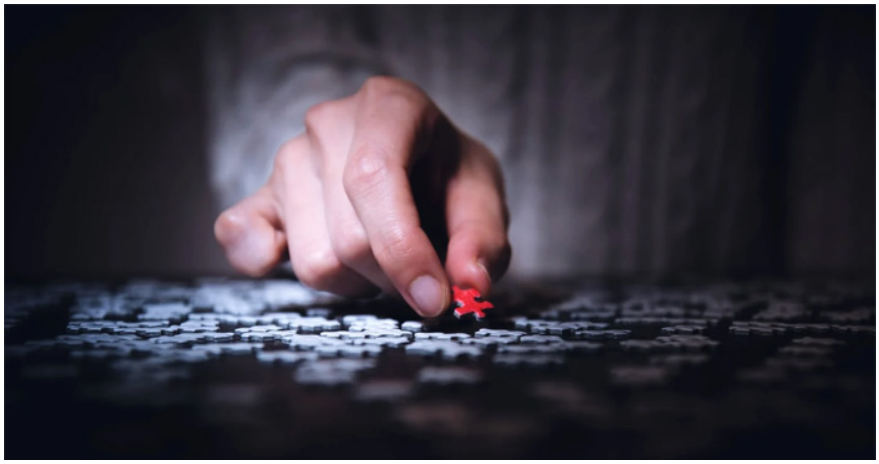
Detecting new culprits attacking Windows 10

Kaspersky security researchers have discovered a new culprit - PuzzleMaker - who used the Google Chrome and Windows 10 zero-day exploit chain in highly targeted attacks against multiple companies all around the world.

According to Kaspersky, the attacks coordinated by PuzzleMaker were first discovered in mid-April when the first victims' networks were compromised.

The zero-day exploit chain used a remote code execution vulnerability in Google Chrome's V8 JavaScript engine to gain access to targeted systems.

Next, PuzzleMaker used custom-tuned privileged exploit enhancement to compromise the latest versions of Windows 10 by abusing an information disclosure vulnerability in the Windows kernel (CVE-2021-31955) and Windows NTFS privilege escalation bug (CVE-2021 -31956), both fixed in the June Tuseday Patch.



Attackers have abused the Windows Notification Facility (WNF) along with the CVE-2021-31956 vulnerability to execute system-privileged malware modules on compromised Windows 10 systems.

"When attackers use both Chrome and Windows exploits to gain a foothold in the targeted system, the stager module loads and executes a more sophisticated dropper malware from a remote server. The dropper then installs two executables disguised as legitimate Microsoft Windows operating system files.The second of these two executables is a remote shell module that can download and upload files. , create a process, sleep for a certain period of time and delete itself from the infected system', the researchers informed.

This is not the first Chrome zero-day exploit that has become popular in recent months.

Project Zero, Google's zero-day bug hunting team, has revealed a large-scale operation in which a group of hackers used 11 zero-day vulnerabilities to attack Windows, iOS and Android users within a year. .

The attacks took place in two separate campaigns, in February and October 2020, with at least dozens of websites hosting two exploit servers, each targeting iOS and Windows users. or Android.

Project Zero researchers collected a large amount of information from the mining servers used in the two campaigns, including:

1. renderer exploits for four bugs in Chrome, one of which is still a zero-day bug at the time of discovery
2. two sandbox escape exploits abuse three zero-day vulnerabilities in Windows
3. "privilege escalation suite" includes publicly known exploits for n-day vulnerabilities for older Android versions
4. a full exploit chain targeting Windows 10 has been fully patched with Google Chrome
5. two partial chains targeting two different fully patched Android devices running Android 10 using Google Chrome and Samsung Browser
6. several RCE exploits for iOS 11-13 and one privilege escalation exploit for iOS 13 (with exploits present on iOS 14.1)

Boris Larin, senior security researcher at the Global Research and Analysis Group (GReAT), said: 'Overall, towards the end of the year, we have seen several waves of high-threat threat activity. level is driven by zero-day exploits. It reminds us that zero-day vulnerabilities continue to be the most effective method of infecting targets."