PLATINUM Hackers Hijack Windows Hotpatching to Stay Hidden

By The Hacker News

Published: 2016-04-28 · Archived: 2026-04-05 22:51:55 UTC

In Brief

The Microsoft's Windows Defender Advanced Threat Hunting team detected that a cyber espionage group of hackers, known as PLATINUM, has found a way to turn the Windows's Hotpatching technique (a way of updating the operating system without requiring a restart) to hide its malware from Antivirus products.

PLATINUM group has been active since 2009 and launching large-scale attacks against governmental organizations, intelligence agencies, defense institutes and telecommunication providers in South and Southeast Asia.

Practically speaking, the most important thing for a sophisticated APT hacker and a cyber-espionage group is to remain undetected for the longest possible period.

Well, that's exactly what an APT (Advanced Persistent Threat) group has achieved.

The Microsoft's **Windows Defender Advanced Threat Hunting** team has discovered that an APT group, dubbed Platinum, has been spying on high-profile targets by abusing a "*novel*" technique called **Hotpatching**.

Introduced in Windows Server 2003, the Hotpatching feature allows Microsoft to upgrade applications or the operating system in the running system without having to reboot the computer by inserting the new, updated code into a server.

The Platinum hacking group has often used the spear-phishing technique to penetrate initially the targeted networks, used numerous zero-day vulnerabilities in attacks, and has taken many efforts to hide its attacks.

The latest report released by Microsoft said the Platinum group abused the Windows' hotpatching feature, allowing it to inject malicious code into running processes without having to reboot the server and then later hide backdoors and other malware from installed antivirus solution.

> "If the tool fails to inject code using hot patching, it reverts to attempting the other more common code injection techniques into common Windows processes, primarily targeting winlogon.exe, lsass.exe, and svchost.exe," Microsoft said in its report.

The hotpatching technique works against Windows Server 2003 Service Pack 1, Windows Server 2008, Windows Server 2008 R2, Windows Vista, and Windows 7. Platinum abused the technique in real-world attacks to hide its efforts from analysis.

The group has been using the Hotpatching technique to install the Dipsing, Adbupd and JPIN backdoors on networks belonging to governmental organizations, including defense organizations, intelligence agencies, diplomats and Internet Service Providers (ISPs) and then to steal sensitive data.

The goal of the attacks doesn't appear to have been immediate financial gain; rather the Platinum APT group is up to a broader economic espionage campaign using stolen information.

The group has been targeting countries in South and Southeast Asia since at least 2009, with Malaysia being its biggest victim, following Indonesia, China, and India.

Though the Platinum group is still active, there is still a way for organizations and companies to avoid infection.

Microsoft's security experts explain that the hotpatching technique requires admin-level permissions, so the threat actors are sending spear-phishing emails that come with boobytrapped Office documents to infect each target.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.

Source: https://thehackernews.com/2016/04/windows-hotpatching-malware.html