The Phantom Menace – GhostHook Attack on 64-bit Windows 10

# Overview

Very few users of 64-bit Windows 10 have heard of Microsoft PatchGuard, but most rely on its security guarantees. PatchGuard is a kernel patch protection technology that plays a critical role in “preventing attackers from installing rootkits on systems running Windows 10 64-bit.” [1]

In the past week, however, the unsung guardian has been severely compromised. Researchers from CyberArk Labs has found a way to “bypass PatchGuard protections and gain rootkit abilities on Windows x64 operating systems.” [1]

# How does it work?

GhostHook works only against systems running Intel Processor Trace (PT), “a feature of Intel CPUs that uses dedicated hardware to capture information about current software execution to aid with debugging operations and the detection of malicious code.” [3] By allocating an extremely small buffer, CyberArk researchers were able to cause the CPU to run out of buffer space, and subsequently open a handler that accepts malicious hooks. This results in an exploit where attackers can stealthy patch the Windows kernel and embed rootkits on Windows 10 64-bit.

# Why is this significant?

GhostHook is the first known exploit that give attackers completely control at the kernel level. The attack would be “virtually undetectable by anti-malware tools, host intrusion prevention systems, … and any tool that relies on information from the kernel.” [1] This implies that GhostHook can effectively conceal existing malwares and amplify their effects to catastrophic levels.

# Who was affected?

There haven’t been any reported high-profile cyberattacks that leverage GhostHook. This, however, is not representative of the severity of this vulnerability, since it is only discovered and published last week. Security researchers expect elevating levels of risk in the coming months, as more attackers become aware of and master the published exploit.

# How to defend against such attacks?

According to Dekel from CyberArk, Attackers only needs to “gain local admin rights on a machine to exploit the technique.” [1] There are many methods for experienced attackers to trick users into giving up this level of access, the most common of which is through simple phishing emails. Thus, the best way for users to defend against such attacks is to remain vigilant and security conscious. One should never download untrusted files and click on suspicious links.

# Responses So Far

Microsoft has been informed of the vulnerability, but “the OS maker declined to issue a security update”, on the grounds that GhostHook is only exploitable on an already infested machine. [2] Thus, users should focus on “preventing an attacker from gaining [such] level of access in the first place.” [3]

# Sources

[1] <http://www.darkreading.com/vulnerabilities---threats/ghosthook-foils-windows-10-64-bits-kernel-protection/d/d-id/1329205>

[2] <https://securityintelligence.com/news/ghosthook-attack-reveals-kernel-level-threat-in-64-bit-windows-systems/>

[3] <https://www.bleepingcomputer.com/news/security/new-ghosthook-attack-bypasses-windows-patchguard-protections/>