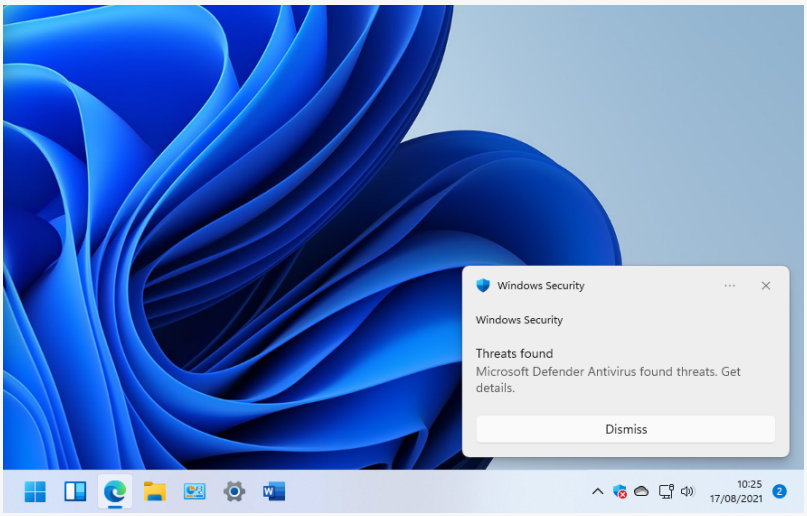
AV-Comparatives warnt davor, dass Malware-Autoren das Interesse an Windows 11 ausnutzen

Microsoft Windows 11 Downloads sind oftmals verseucht, AV-Comparatives rät, nur sichere Downloadquellen zu verwenden.



Windows 11 Malware Warning

INNSBRUCK, TIROL, AUSTRIA, August 18, 2021 /EINPresswire.com/ -- Seit der Ankündigung der nächsten Version von Microsofts Desktop-Betriebssystem Windows 11, im Juni, sind Tech-Enthusiasten auf der ganzen Welt daran interessiert, die neue Plattform auszuprobieren. Wie üblich haben Cyberkriminelle die Gelegenheit genutzt, Malware zu verbreiten. Telangana Today berichtet wie Malware-Autoren gefälschte Installationsprogramme verbreitet haben, die neben dem neuen Windows eine Vielzahl unerwünschter und bösartiger Programme enthalten.

> Microsoft Windows 11 Downloads sind oftmals verseucht. Ich kann nur dazu raten, sichere Downloadquellen zu verwenden, wie z.B. die Quellen von Microsoft direkt."
>
> *Peter Stelzhammer, co-founder, AV-Comparatives*

Warum verwenden die Leute die gefälschten Installer?

Die offiziellen Kanäle von Microsoft ermöglichen es Benutzern, Windows 11 über ihr Insider-Programm in absoluter Sicherheit auszuprobieren. Wenn Sie sich dafür anmelden, können Sie ein vorhandenes Windows 10-System auf eine Vorschauversion des nächsten Betriebssystems aktualisieren. Windows 11 bringt jedoch neue Hardwareanforderungen mit sich, was bedeutet, dass für viele Benutzer die Option zum Upgrade nicht verfügbar ist. Dies gibt Malware-Autoren die Möglichkeit, enttäuschte Technikfans dazu zu bringen, ihre eigenen manipulierten Installer zu verwenden, die einige böse Überraschungen beinhalten.

Wie erkennt man die Fälschungen?

Der Blog von Kaspersky beschreibt die technischen Details der Bedrohungen. Durch das Verständnis des Unterschieds zwischen dem Originalinstallationsprozess von Microsoft und den bösartigen Fälschungen können alarmierte Benutzer ihre Computer schützen. Anstatt den Windows Update-Dienst oder ein vollständiges Windows-Installations-DVD-Image (ISO-Datei) zu verwenden, verwenden die Cyberkriminellen eine andere Installationsmethode.

Logo AV-Comparatives

Die von ihnen bereitgestellte Installationsdatei ist viel kleiner als jedes echte Microsoft Windows-Setup-Programm (2 GB statt 5 GB). Das ist schon ein Hinweis an sich. Wenn ein solches Installationsprogramm ausgeführt wird, ähnelt es zunächst einem echten Microsoft-Setup-Assistenten, liefert dann jedoch weitere Beweise dafür, dass es sich nicht um einen solchen handelt. Aufgrund seiner geringen Größe kann es die Installation nicht selbst abschließen, sondern muss ein zusätzliches Setup-Programm herunterladen. Darüber hinaus wird der sekundäre Installer den Benutzer selbst ermutigen, zusätzliche Software zu installieren, indem er behauptet, dass dies z.B. ein Download-Manager ist. All dies ist völlig anders als ein echtes Windows-Installationsprogramm.

Kaspersky weist darauf hin, dass es eine Reihe verschiedener gefälschter Windows 11-Installationsprogramme gibt, die jeweils ihre eigene unerwünschte Software installieren. Dabei kann es sich um relativ harmlose Adware, aber auch um hochgradig bösartige Software zum Diebstahl von Passwörtern oder um jede Art von Malware handeln.

Wie kann ich Windows 11 sicher testen?

Sehr vernünftigerweise rät Kaspersky den Benutzern, nur den offiziellen Upgrade-Prozess von Microsoft zu verwenden, wenn sie Windows 11 ausprobieren möchten Ausführung. Während Microsoft die aktuellen Hardwarebeschränkungen von Windows 11 strikt auf physischen PCs durchsetzt, hat sie sie für Installationen auf einer virtuellen Maschine gelockert. Das bedeutet, dass Sie durch Virtualisierung das neue Betriebssystem sicher ausprobieren können.

Kaspersky rät Benutzern auch, keine Vorschau-Builds – auch keine absolut sicheren, echten Microsoft-Builds – auf dem Hauptcomputer zu verwenden, den Sie täglich verwenden. Microsoft selbst macht dasselbe. Dies liegt daran, dass Vorschau-Builds aufgrund ihrer Natur nicht so zuverlässig sind wie das fertige Produkt. Durch die Verwendung einer virtuellen Maschine können Sie Windows 11 sicher und ohne das Risiko einer Destabilisierung des Computers, den Sie täglich verwenden, ausprobieren. Es gibt gute, kostenlose Virtualisierungsprogramme. Sie müssen zunächst Windows 10 auf einer virtuellen Maschine installieren, sich für das Windows-Insider-Programm registrieren und dann den Release-Kanal auswählen, der für Windows 11-

Builds am besten zu Ihnen passt.

Dies kann länger dauern als die Verwendung eines gefälschten Windows 11-Installationsprogramms, garantiert Ihnen jedoch eine sichere und zuverlässige Möglichkeit, einen echten Build des neuen Betriebssystems auszuprobieren.
Was muss ich sonst noch tun, um meinen PC zu schützen?

Kasperskys Blog zeigt Benutzern nicht nur, wie sie gefälschte Windows 11-Installationsprogramme vermeiden können, sondern empfiehlt auch, immer ein zuverlässiges Antivirenprogramm auf Ihrem Computer auszuführen und es niemals zu deaktivieren. AV-Comparatives stimmt diesem Rat voll und ganz zu. Unsere Testberichte können Ihnen helfen, eine effektive und zuverlässige Antivirenlösung zu finden, die Ihren Computer sicher hält. Diese können kostenlos und ohne Registrierung von www.av-comparatives.org heruntergeladen werden. Übrigens, echte Vorschau-Builds von Windows 11 werden mit integriertem Microsoft Windows Defender Antivirus geliefert.

AV-Comparatives ist ein unabhängiges Testlabor mit Sitz in Innsbruck, Österreich, und testet seit 2004 öffentlich Computersicherheitssoftware. Es ist nach ISO 9001:2015 für den Geltungsbereich „Unabhängige Tests von Anti-Virus-Software“ zertifiziert. Darüber hinaus besitzt es die EICAR-Zertifizierung als „Trusted IT-Security Testing Lab“.

QUELLEN

https://telanganatoday.com/beware-you-could-be-downloading-a-windows-11-malwarehttps://telanganatoday.com/beware-you-could-be-downloading-a-windows-11-malware

Peter Stelzahmmer
AV-Comparatives
+43 664 1611444
p.stelzhammer@av-comparatives.org
Visit us on social media:
Facebook
Twitter
LinkedIn