Hackerato l’update automatico di Asus: backdoor su migliaia di PC

Mar 26, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, Minacce, News, RSS 0

L’attacco ha preso di mira ASUS Live Update Utility, per distribuire il malware su 500.000 computer. Ma i pirati puntavano a 600 obiettivi mirati.

Parafrasando Mao, si potrebbe dire “colpirne 500.000 per infettarne 600”. E il fatto che secondo quanto riporta **Kaspersky** i protagonisti dell’attacco si un gruppo di cyber-spioni collegato al governo cinese, non fa che rendere più calzante la citazione.

Secondo gli esperti della società russa, infatti, gli autori di questo clamoroso attacco (battezzato **Operazione ShadowHammer**) che ha preso di mira **Asus** farebbero parte del gruppo **Barium APT**, noto appunto per i suoi legami con Pechino.

L’elemento sconvolgente di tutta questa vicenda riguarda le modalità che i pirati hanno usato per portare il loro attacco, violando addirittura il sistema di aggiornamento automatico (**ASUS Live Update Utility**) di una delle più grandi aziende produttrici di computer del mondo.

Gli hacker, stando alla ricostruzione degli analisti Kaspersky, sarebbero riusciti a impossessarsi di **un certificato digitale di Asus** e avrebbero usato vecchie versioni dei driver dell’azienda taiwanese per crearne una versione contenente una backdoor.

Avrebbero infine caricato i driver infetti sui server ufficiali di Asus che li hanno poi distribuiti come aggiornamento ad almeno 500.000 computer.



Una strategia di attacco decisamente efficace, anche perché aggiornamenti di questo tipo (relativi cioè a driver e firmware) con un certificato digitale valido e provenienza dai server ufficiali aggirano con facilità i controlli dei software antivirus.

L'obiettivo dei pirati, però, non era quello di colpire "a tappeto", ma puntavano a una serie di obiettivi specifici. All'interno del malware che hanno distribuito, infatti, era presente un elenco di circa 600 **MAC Address**, il codice univoco che identifica un dispositivo collegato in rete.

La backdoor nascosta tra le pieghe del codice veniva attivata solo nel caso in cui il MAC Address del computer colpito corrispondeva a uno di quelli in elenco.

Insomma: i pirati sapevano esattamente quali computer volevano colpire e per raggiungerli non hanno esitato a pianificare un attacco clamoroso pur di raggiungere l'obiettivo.

D'altra parte il gruppo Barium APT è conosciuto per aver messo a segno attacchi "supply chain" anche in passato, come nel caso di **ShadowPad** (ne abbiamo parlato in questo articolo) e quello a **CCleaner** (i dettagli in questo articolo).

Resta da capire che rischi corranno gli altri utenti che sono stati colpiti dal malware. Secondo i ricercatori, infatti, potrebbe rimanere al suo posto anche se in uno stato "dormiente". Una prospettiva per nulla rassicurante anche per chi non rientra nel selezionato gruppo di bersagli presi di mira dai pirati.

Secondo i ricercatori, il caso di Asus conferma ancora una volta il livello tecnologico di questo gruppo, che sembra essere in grado di escogitare strategie sempre più raffinate per raggiungere i suoi scopi.

Please follow and like us:



Falle di sicurezza in Java Card. A rischio anche le carte Bancomat

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/03/26/hackerato-lupdate-automatico-di-asus-backdoor-su-migliaia-di-pc/