5G e cybersecurity, tra attacchi DDoS e Botnet cosa c’è in agguato?

La crescita e lo sviluppo delle nuove reti **5G** è sicuramente un argomento caldo, ma come con l’avvento di qualsiasi nuova tecnologia si sono sollevati alcuni dubbi sulla sua introduzione – e non solo di carattere strutturale –, dubbi ribaditi anche in un recente report dell’Unione Europea.

A differenza delle precedenti connessioni come 3G e 4G il network loro erede sarà – per la maggior parte – basato su software e virtualizzato.

L’avvento del 5G

Questo rappresenta una grossa frattura rispetto al passato, dove i network erano storicamente confinati e limitati dall’hardware a loro disposizione, trasformando le funzioni del network tradizionale in funzioni virtuali, il tutto orchestrato attraverso un software di controllo.

Sempre parte del pacchetto di novità introdotto con il 5G sarà l’uso massiccio della tecnologia di ***Edge Computing*** dove le applicazioni, l’attività di archiviazione e tutte le funzioni di controllo saranno obbligate ad operare relativamente vicine agli end user e ai vari endpoint IoT.

Questo è un *paradigm shift* non indifferente, dall’architettura centralizzata del network 4G stiamo passando a un’architettura diffusa e – in maniera più preoccupante – creando un perimetro d’attacco decisamente più ampio per i Criminal Hacker.

Stiamo correndo il rischio di esporre i network mobile a insidie mai riscontrate prima. Il report pubblicato dall'Unione Europea ha messo in guardia sui vari rischi legati ai fornitori e alla fase di sviluppo software, in particolare per quanto riguarda la catena dei fornitori.

Il rischio di delegare troppo all'IoT

L'inevitabile proliferazione dei software per sostenere e portare avanti l'infrastruttura 5G è, come anticipato una delle maggiori preoccupazioni dell'UE.

Il problema infatti non è insisto nella sicurezza della tecnologia 5G in sé e per sé, nonostante alcuni esempi pratici della sua possibile vulnerabilità di questa tecnologia – come la possibilità per possibili attaccanti di utilizzare ripetitori "falsi" virtuali per dirottare il traffico e sottrarre informazioni -. In generale, infatti, il 5G può vantare una maggiore capacità di crittografare i dati e un superiore algoritmo di verifica della legittimità degli utenti connessi rispetto al suo antenato.

Ma il vero punto debole dal punto di vista della Cybersecurity del 5G è sicuramente il traffico di dati tra i tantissimi *endpoint* ***IoT*** connessi a Internet grazie a questa tecnologia. Stiamo parlando di una mole e di una varietà di device – che spaziano dalle auto ai robot industriali fino ai semplici oggetti di domotica – impressionante e soprattutto che opera secondo una moltitudine di standard di sicurezza fin troppo variegata. Secondo le stime più conservative di Gartner questi arriveranno ad essere circa 25 miliardi entro la fine del prossimo anno.

Tutti questi, naturalmente, passeranno a breve sulle nuove reti 5G fornendo di fatto ai Criminal hacker una superfice d'attacco senza precedenti. Non è una novità d'altronde che

non ci sia bersaglio più ambito da questi gruppi delle new entry nel mondo della tecnologia, sia perché tra i Criminal Hacker vige una certa competizione sia perché le nuove tecnologie sono sempre le più vulnerabili.

C'è anche un'altra grande questione legata alla provenienza e all'affidabilità dei vari produttori dei device IoT – non che i grandi nomi del settore tech siano immuni a questi "scivoloni" – provenienti in particolar modo dal sud-est asiatico. Affidereste la sicurezza dei vostri dati a uno dei più disparati mobile che si possono acquistare su siti di e-commerce come Aliexpress?

5G: il rischio DDoS e Botnet

I Criminal Hacker possiedono già l'abilità di scannerizzare centinaia di migliaia di device in cerca di possibili falle – anche le più banali come quelle legate alle password di default che non vengono cambiate al momento della messa in commercio del prodotto (da "admin" a "guest").

Non è solo una previsione di catastrofismo tecnologico; non è passato molto tempo dall'attacco "**Mirai Botnet**" del 2016 che aveva sfruttato debolezze di questo genere trovate in migliaia di device "connessi" come fotocamere, router e videocamere per prenderne il controllo e "abbattere" siti come **Twitter, il New York Times e Spotify.**

I criminali, nel dettaglio, avevano utilizzato un "merge" di due tecniche differenti, ma comunque conosciute: prima un botnet – che appunto prende il controllo dei dispositivi IoT e li utilizza per sferrare un Cyber attacco – e successivamente un DDoS, in grado di sovraccaricare il network bersaglio con un numero eccessivo di richieste.

Cosa c’è in agguato?

Il rischio, in futuro, potrebbe essere che quando i Criminal Hacker riescono a violare un dispositivo collegato al 5G, la velocità della rete permetterà loro di estrarre e scaricare informazioni, compresi i dati personali e le informazioni sui clienti, molto più velocemente di prima.

La probabilità di trovare un dispositivo IoT che non è stato settato propriamente, o con una password debole, come accennato, è al momento piuttosto alto. Come se non bastasse, poiché i dispositivi IoT si collegano direttamente alla rete mobile, i Criminal Hacker non dovranno aggirare il framework di sicurezza – tradizionalmente più resiliente – delle reti domestiche o aziendali. C’è anche il rischio che le case che utilizzano dispositivi di domotica 5G diventino più vulnerabili.

Se il software di sicurezza di frigoriferi, allarmi anti-fumo e altri dispositivi “intelligenti” connessi a Internet non viene aggiornato regolarmente, una singola falla potrebbe esporre un’enorme quantità di dati. Anche le aziende dovranno necessariamente mettersi in guardia dai potenziali rischi nel caso in cui i dipendenti utilizzano reti 5G piuttosto che le loro reti aziendali per inviare dati riservati.

Ci sono anche alcuni problemi “*legacy*” che si trascinano dal tempo della prima implementazione del 3G. La nuova tecnologia utilizza ancora la **Authentication and Key Agreement (AKA) u**n sistema virtuale che permette ai vari network di identificarsi correttamente.

3 macro aree di criticità

Nel 5G questo sistema ha due criticità ancora latenti: permette a un Threat actor di spostare la propria fattura e il conto del consumo di traffico su un altro ignaro utente e – in

maniera più preoccupante – permette il tracking dei dispositivi vicini.

C'è anche un fattore stressogeno più umano: l'effort necessario in termini di costo e ore di lavoro per implementare la nuova soluzione rispetto al 4G che alcuni team IT incaricati potrebbero essere più proni ad errori in fase di rollout, causando falle e problematiche di sicurezza non volute.

Riassumendo possiamo dire che ci sono tre macroaree di criticità legate all'introduzione del 5G che potrebbero introdurre una nuova dimensione di Cyber risk:

- L'insieme delle tecnologie che danno vita al 5G non è ancora sufficientemente testato;
- Permette accesso e movimento di una quantità enormemente più grande di dati e di conseguenza amplia la superfice d'attacco
- È una scommessa, molto più del 4G verrà utilizzato come base per applicazioni "mission-critical" (d'importanza centrale per il funzionamento di un dato servizio).

Sembra una strada senza uscita, ma in realtà quello che deve accompagnare l'implementazione del 5G e una maggiore e rinnovata attenzione agli standard di sicurezza adottati dai produttori che devono essere necessariamente rinforzati e condivisi.

"Yoda: Vittoria? Vittoria, tu la chiami, maestro Obi-Wan? No, non vittoria. Su tutto l'ombra del lato oscuro è calata. Cominciata la Guerra dei Cloni è." (Star War)

Le novità sono sempre eccitanti, ma forse con il 5G dobbiamo adottare un approccio più cauto e misurato.

https://www.key4biz.it/5g-e-cybersecurity-tra-attacchi-ddos-e-botnet-cosa-ce-in-agguato/279892/