Le vie per il ransomware sono infinite

Secondo l'**Osservatorio Cybersecurity di Exprivia** sono stati individuati in Italia 58 attacchi ransomware dall'inizio della pandemia.

Ad oggi, i **metodi più efficaci per diffondere ransomware** sono:

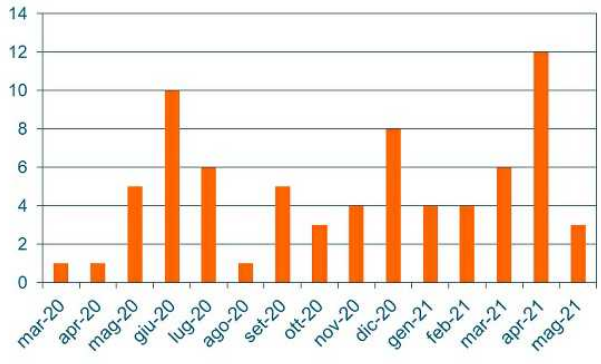
- tramite gli **allegati presenti nell'email**;
- tramite **link che reindirizzano l'utente verso siti malevoli**.

Esiste un forte legame tra il ransomware ed il **protocollo RTP**, ovvero il **Remote Desktop Protocol**.

Il Remote Desktop Protocol (RDP) è un protocollo della suite di Windows che permette l'accesso alle workstations in maniera grafica, utilizzato per default attraverso la **porta 3389**.

RDP è una funzionalità del sistema operativo server che permette all'amministratore IT di **accedere ai desktops aziendali da remoto**, per distribuire rapidamente aggiornamenti e patch software o compiere altre attività, senza dover operare su ogni singolo PC. Questa funzionalità però può anche essere sfruttata dagli aggressori, non per distribuire aggiornamenti ma malware.

Durante la pandemia l'utilizzo di questo protocollo è sensibilmente aumentato, in quanto utilizzato dagli utenti per accedere ai sistemi da remoto. Gli attaccanti a loro volta hanno provato a sfruttare tecniche di **brute-force** per ottenere l'accesso a questi sistemi.



Attraverso i sistemi acceduti è possibile eseguire attacchi brute force per poter ottenere l'accesso ai dispositivi. Di conseguenza, una volta all'interno del perimetro aziendale, i malintenzionati potranno utilizzare metodi di **privilege escalation** e/o eseguire **movimenti laterali** per acquisire indebitamente dei privilegi.

L'accesso illecito ai sistemi è funzionale alla diffusione dei ransomwares. In caso in cui gli attacchi a forza bruta non abbiamo successo, l'attaccante può infatti sfruttare, soprattutto quando i sistemi non sono aggiornati, vulnerabilità presenti sul protocollo, come:

- **CVE-2020-0609**, **CVE-2020-0610**: queste due vulnerabilità permettono l'esecuzione di codice in modalità remota su Windows Remote Desktop Gateway (RD Gateway) quando un utente malintenzionato non autenticato si connette al sistema di destinazione tramite RDP e invia richieste appositamente create al server RD Gateway di destinazione. Il successo...

LE NOTIZIE PIÙ LETTE

Ultimi 7 giorni | Mese

1. Il Decalogo del Security Manager (parte II)
2. Le vie per il ransomware sono infinite
3. Axon: l'innovazione tecnologica che garantisce pubblica sicurezza
4. 48% aziende italiane pro smartworking ma serve più innovazione
5. Dahua: Nuovi Server IVSS serie M per analisi video AI al top
6. Nebbiogeno UFO: Sistema unico contro Furti e Rapine
7. Sicurezza Urbana: quali sinergie tra Comuni e Istituti di Vigilanza?
8. Ajax protegge dagli incendi la stazione "Vernadsky" in Antartide
9. Convenzione CEI e Confartigianato 2021/2022
10. Futuro del lavoro? Ibrido, intelligente e sicuro

Le vie per il ransomware sono infinite

Secondo l'Osservatorio Cybersecurity di Exprivia sono stati individuati in Italia 58 attacchi ransomware dall'inizio della pandemia.

Ad oggi, i metodi più efficaci per diffondere ransomware sono:

• tramite gli allegati presenti nell'email;
• tramite link che reindirizzano l'utente verso siti malevoli.

Esiste un forte legame tra il ransomware ed il protocollo RTP, ovvero il Remote Desktop Protocol.

Il Remote Desktop Protocol (RDP) è un protocollo della suite di Windows che permette l'accesso alle workstations in maniera grafica, utilizzato per default attraverso la porta 3389.

RDP è una funzionalità del sistema operativo server che permette all'amministratore IT di accedere ai desktops aziendali da remoto, per distribuire rapidamente aggiornamenti e patch software o compiere altre attività, senza dover operare su ogni singolo PC. Questa funzionalità però può anche essere sfruttata dagli aggressori, non per distribuire aggiornamenti ma malware.

Durante la pandemia l'utilizzo di questo protocollo è sensibilmente aumentato, in quanto utilizzato dagli utenti per accedere ai sistemi da remoto. Gli attaccanti a loro volta hanno provato a sfruttare tecniche di brute-force per ottenere l'accesso a questi sistemi.Attraverso i sistemi acceduti è possibile eseguire attacchi brute force per poter ottenere l'accesso ai dispositivi. Di conseguenza, una volta all'interno del perimetro aziendale, i malintenzionati potranno utilizzare metodi di privilege escalation e/o eseguire movimenti laterali per acquisire indebitamente dei privilegi.

L'accesso illecito ai sistemi è funzionale alla diffusione dei ransomwares. In caso in cui gli attacchi a forza bruta non abbiamo successo, l'attaccante può infatti sfruttare, soprattutto quando i sistemi non sono aggiornati, vulnerabilità presenti sul protocollo, come:

• CVE-2020-0609, CVE-2020-0610: queste due vulnerabilità permettono l'esecuzione di codice in modalità remota su Windows Remote Desktop Gateway (RD Gateway) quando un utente malintenzionato non autenticato si connette al sistema di destinazione tramite RDP e invia richieste appositamente predisposte. Questa vulnerabilità è una pre-autenticazione e non richiede l'interazione dell'utente.
• CVE-2019-0708: conosciuta anche come BlueKeep, questa vulnerabilità permette l'esecuzione di codice in modalità remota a Servizi Desktop remoto. Un utente malintenzionato non autenticato si connette al sistema di destinazione tramite RDP e invia richieste appositamente predisposte. Questa vulnerabilità è di pre-autenticazione, quindi non richiede l'interazione dell'utente.

Sfruttando con successo questa vulnerabilità, un utente malintenzionato potrebbe eseguire codice arbitrario sul sistema di destinazione. L'attaccante potrebbe anche installare programmi; visualizzare, modificare o eliminare i dati o creare nuovi account.

• CVE-2019-1181, CVE-2019-1182: Queste due vulnerabilità, simili alla CVE-2019.0708 (BlueKeep), sono "wormable", il che significa che qualsiasi malware futuro che le sfrutta potrebbe propagarsi da un computer vulnerabile a un computer vulnerabile senza l'interazione dell'utente. Anche queste due vulnerabilità sono prive di autenticazione.

Vulnerabilità, come quelle elencate precedentemente, permettono l'accesso ai dispositivi evitando di inserire le credenziali, il che lo rendono un protocollo non molto sicuro, soprattutto quando queste non sono aggiornate.

L'osservatorio ha anche notato una grande presenza di dispositivi connessi online che usano il protocollo RDP, ben 38.119, con maggior presenza al Nord Italia. Questo è un dato molto allarmante in relazione a quanto detto finora.L'attacco ransomware è uno degli attacchi che assicura molto spesso un guadagno diretto, qualora l'azienda paghi il riscatto. Questo, porta gli attaccanti ad ottenere guadagni sempre maggiori, che possono essere sfruttati per finanziare attacchi sempre più sofisticati. Si ricorda che nel darkweb c'è un vero e proprio mercato per ottenere:

• informazioni su persone: per proseguire con attacchi di phishing;

• credenziali rubate: per proseguire con attacchi brute force;

• malware: per proseguire con malware sempre più moderni con arsenali sempre più ricchi, compresa la documentazione.

Questo porta ad una catena nella quale gli attaccanti si ritrovano ad avere budget maggiori rispetto ad aziende sempre più indifese che, molto spesso intervengono dopo aver subito un attacco o peggio ancora che pagano il riscatto per riavere subito i dati non più accessibili. Il gap tra attacco e difesa diventa così sempre più grande.

CONCLUSIONI

Per diminuire il range di attacchi si consiglia di chiudere la porta 3389. In caso in cui questo non fosse possibile, si consiglia o di filtrare questa porta attraverso dispositivi firewall, o di monitorare questi dispositivi attraverso IDS/IPS o SIEM, in maniera da poter intervenire subito in caso di anomalia.

Un'altra valida soluzione è spostare questi dispositivi esposti in rete, all'interno delle proprie reti aziendali, fornendo agli utenti che devono accedere a questi dispositivi una connessione VPN, in maniera da offrire una maggiore protezione, in quando l'attaccante dovrebbe superare un altro step, prima di poter raggiungere questi dispositivi. Infine è possibile configurare l'autenticazione a livello di rete (NLA).

a cura di Andrea Pastore,
CyberSecurity Researcher Exprivia

15.06.2021