Extortionware – dal Dark Web "la strategia della vergogna"

Pubblicato da **Annamaria Gigante** | 15/06/2021

I crimini informatici sono fenomeni in continua crescita; ciò in ragione del fatto che il rischio associato alla commissione del reato è basso rispetto ai guadagni che ne derivano. Infatti il cyber crime è oggi un business globale da 600 miliardi di dollari che rappresenta lo 0,8% del PIL mondiale.

Sono vecchie notizie, ormai, le truffe di phishing e il furto di identità, attualmente le minacce più gravi per le organizzazioni sono il **ransomware** e l'**extortionware**.

Qual è la differenza tra ransomware ed extortionware? E quali misure adottare per evitare di diventare una vittima del crimine informatico?

Il **ransomware** è la forma più comune di crimine informatico e forse la più efficace. Consiste in un tipo di malware che blocca un sistema informatico fino a quando la vittima non paga l'estorsione per il codice chiave necessario a sbloccare il dispositivo. Di solito, la vittima deve pagare in Bitcoin o tramite un altro metodo difficile da rintracciare. Il problema è che non c'è niente che impedisca al criminale di tornare ad estorcere, chiedendo per la seconda volta un riscatto più costoso, oltre che continuare a danneggiare la produttività e la reputazione della vittima.

Il ransomware si è evoluto in maniera evidente. I criminali un tempo operavano in solitaria o in piccoli gruppi, mettendo nel mirino singoli utenti a caso tramite siti web o attacchi via email. Ma negli ultimi anni sono diventati più raffinati e ambizioni e si sono ben organizzati. Fino al 2019 i dati venivano semplicemente cifrati per complicare le operazioni di un'azienda, mentre più recentemente tali dati vengono scaricati dagli hacker stessi. Questo ha significato un netto aumento nelle richieste di riscatto perché la minaccia di rivendita dei dati a terzi è percepita come più seria.

Per mezzo dell'**extortionware** i ricattatori utilizzano la psicologia della paura e della vergogna per motivare le vittime. In questi casi, il criminale informatico afferma di essere stato all'interno del computer della vittima, di aver scattato schermate di foto o ricerche imbarazzanti e di aver registrato video abbozzati utilizzando la sua fotocamera. Minaccerà di inviare gli screenshot e le foto a tutti i nomi in rubrica o di pubblicarli sui social media a meno di un pagamento, alquanto costoso.

È fondamentalmente un ricatto informatico, un tipo di crimine particolarmente insidioso che non colpisce solo gli individui, ma danneggia anche le aziende. Gli hacker rubano dati sensibili dallo storage di un'azienda e minacciano di esporli a meno che non vengano ripagati. Molte volte, l'hacker non ha alcuna prova e sta semplicemente bluffando. La parte davvero pericolosa è che le e-mail degli hacker spesso rivelano di aver protetto la password della vittima e questo.

# Extortionware – dal Dark Web “la strategia della vergogna”

I crimini informatici sono fenomeni in continua crescita; ciò in ragione del fatto che il rischio associato alla commissione del reato è basso rispetto ai guadagni che ne derivano. Infatti il cyber crime è oggi un business globale da 600 miliardi di dollari che rappresenta lo 0,8% del PIL mondiale.

Sono vecchie notizie, ormai, le truffe di phishing e il furto di identità, attualmente le minacce più gravi per le organizzazioni sono il ransomware e l'extortionware.

Qual è la differenza tra ransomware ed extortionware? E quali misure adottare per evitare di diventare una vittima del crimine informatico?

Il ransomware è la forma più comune di crimine informatico e forse la più efficace. Consiste in un tipo di malware che blocca un sistema informatico fino a quando la vittima non paga l'estorsione per il codice chiave necessario a sbloccare il dispositivo. Di solito, la vittima deve pagare in Bitcoin o tramite un altro metodo difficile da rintracciare. Il problema è che non c'è niente che impedisca al criminale di tornare ad estorcere, chiedendo per la seconda volta un riscatto più costoso, oltre che continuare a danneggiare la produttività e la reputazione della vittima.

Il ransomware si è evoluto in maniera evidente. I criminali un tempo operavano in solitaria o in piccoli gruppi, mettendo nel mirino singoli utenti a caso tramite siti web o attacchi via email. Ma negli ultimi anni sono diventati più raffinati e ambizioni e si sono ben organizzati. Fino al 2019 i dati venivano semplicemente cifrati per complicare le operazioni di un’azienda, mentre più recentemente tali dati vengono scaricati dagli hacker stessi. Questo ha significato un netto aumento nelle richieste di riscatto perché la minaccia di rivendita dei dati a terzi è percepita come più seria.

Per mezzo dell’extortionware i ricattatori utilizzano la psicologia della paura e della vergogna per motivare le vittime. In questi casi, il criminale informatico afferma di essere stato all'interno del computer della vittima, di aver scattato schermate di foto o ricerche imbarazzanti e di aver registrato video abbozzati utilizzando la sua fotocamera. Minaccerà di inviare gli screenshot e le foto a tutti i nomi in rubrica o di pubblicarli sui social media a meno di un pagamento, alquanto costoso.

È fondamentalmente un ricatto informatico, un tipo di crimine particolarmente insidioso che non colpisce solo gli individui, ma danneggia anche le aziende. Gli hacker rubano dati sensibili dallo storage di un'azienda e minacciano di esporli a meno che non vengano ripagati. Molte volte, l'hacker non ha alcuna prova e sta semplicemente bluffando. La parte davvero pericolosa è che le e-mail degli hacker spesso rivelano di aver protetto la password della vittima e questo, spesso, è sufficiente per creare seri danni.

Difendersi da queste minacce è difficile, ma non impossibile.

Le misure preventive fanno molto:

tenere i backup dei dati aziendali aiuta la società a recuperare da attacchi ransomware complessi ma non basta nel caso in cui gli hacker utilizzino tattiche estorsive. Per i dipendenti è consigliato di non conservare alcun dato o file che potrebbe danneggiare la reputazione di un'azienda sui server societari. Da qui l'importanza della formazione che dovrebbe essere impartita dall'azienda stessa a tutto il personale;
per ridurre al minimo il rischio di pubblicare dati non crittografati su Internet come mezzo di estorsioni, le aziende dovrebbero utilizzare la crittografia;
come programma completo di sicurezza delle informazioni le aziende dovrebbero adottare una pianificazione del ripristino di emergenza.
Purtroppo, la mancanza di denunce da parte delle vittime e la cultura dell'insabbiamento rende molto complesso stimare il potenziale economico dei danni; importante è conoscere bene il fenomeno per essere meno vulnerabili.

Di Annamaria Gigante, Event & Communication Specialist presso Exprivia Spa e membro della community Women for Security

Fonti:

https://alpinesecurity.com/blog/cyber-extortion-ransomware-vs-extortionware/
https://www.difesaesicurezza.com/cyber/cybercrime-lascesa-dellextortionware-variante-social-engineering-del-ransomware/

https://searchsecurity.techtarget.com/answer/Whats-the-difference-between-extortionware-and-ransomware