ESET Threat Report 2022: il focus è sul conflitto in Ucraina

https://www.hwupgrade.it/i/n/Eset_Report_720.jpg,

Calano gli attacchi RDP e quelli scagliati contro SQL, mentre si nota un ritorno di Emotet. Se prima del conflitto la maggior parte degli attacchi ransomware evitavano bersagli russi, ora la situazione si è ribaltata

di Alberto Falchi pubblicata il **03 Giugno 2022**, alle **17:41** nel canale Security

ESET

Dopo anni in cui gli attacchi RDP (Remote Desktop Protocol) continuavano a crescere, nei primi sei mesi del 2022 è stato registrato un calo del 43%. In calo anche attacchi rivolti ai database SQL (-64%) e al protocollo SMB (-26%). Sono alcuni dei dati che emergono dal **Threat Report T1 2022** di ESET, che però sottolinea come **la maggior parte degli attacchi in questo periodo abbia avuto origine in Russia.**

Timeline of the attacks detected by ESET researchers around the time of the Russian invasion of Ukraine

Secondo i ricercatori di ESET, è probabile che questi cambiamenti nello scenario delle minacce informatiche siano legati proprio al conflitto in Ucraina e il report è incentrato proprio su questo tema. Va anche sottolineato che ESET ha la sua sede in zone vicine a quelle che sono attualmente scenari di guerra: *"Ci sentiamo fortemente coinvolti da quanto accade proprio al di là dei confini orientali della Slovacchia, dove ESET ha il suo quartier generale e diversi uffici, e dove gli ucraini stanno combattendo per le loro vite e la loro sovranità"*, afferma **Roman Kováč**, Chief Research Officer di ESET.

Come la guerra in Ucraina sta modificando lo scenario delle minacce informatiche

Oltre al calo degli attacchi RDP e contro SQL, ESET nel suo report ha notato un importante cambiamento di tendenza: se gli attacchi ransomware prima della guerra raramente venivano lanciati contro obiettivi russi, ora accade il contrario e **la Russia è il paese più bersagliato dal ransomware**. Anche i wiper, malware che distruggono i dati delle vittime, lanciati contro realtà russe sono cresciuti di molto e in molti casi non si tratta di attacchi scagliati da "professionisti", ma da persone meno esperte, probabilmente come reazione all'attacco, come suggerisce anche il fatto che sono state trovate varianti di lock screen contenenti il saluto nazionale ucraino "Slava Ukraini!". (Gloria all'Ucraina!).

Non che la Russia stia a guardare: **ESET ha rilevato un attacco a un provider di energia ucraino che faceva leva su Industroyer2**, variante del malware Industroyer che prende di mira i sistemi industriali ICS.

Ma l'incremento degli attacchi contro obiettivi russi non è l'unico effetto rilevato da ESET, che sottolinea come subito dopo lo scoppio del conflitto siano state avviate numerose campagne di spam e phishing che cercavano di approfittare delle persone che sostenevano l'Ucraina.

Il ritorno di Emotet

Fra le altre evidenze del rapporto, va sottolineato **il ritorno di Emotet:** gli operatori della botbet Emotet hanno lanciato diverse campagne di spam nei primi sei mesi del 2022, con una

crescita dei rilevamenti di oltre cento volte.

“*Possiamo confermare che Emotet, il famigerato malware diffuso principalmente tramite e-mail di spam, è tornato dopo i tentativi di rimozione dello scorso anno ed è di nuovo in crescita nella nostra telemetria*“, spiega Kováč. Tuttavia, le campagne che si basavano su macro dannose potrebbero essere state le ultime, vista la recente mossa di Microsoft di disabilitare le macro da Internet per impostazione predefinita nei programmi Office. In seguito a questo cambiamento, gli operatori di Emotet hanno iniziato a testare altri vettori di compromissione su campioni di vittime molto più piccoli.

Read More