Cyber crime, cosa ci riserva il futuro?



L’ultimo rapporto FortiGuard Labs, partendo da un’attenta osservazione degli sviluppi significativi nel panorama delle minacce informatiche nel 2020 a livello globale, comprendendone dinamiche e trend, riporta delle previsioni molto verosimili sui nuovi strumenti e strategie che potrebbero essere disponibili ai criminal hacker nel breve e nel lungo termine.

Tale scenario, come si evince dal documento “Cyber Threat Predictions for 2021”, risulta principalmente influenzato dalle evoluzioni implementative che subiranno i malware e gli attacchi informatici in genere alla luce delle nuove potenzialità offerte dal 5G, dal quantum computing e dall’intelligenza artificiale (AI) e machine learning (ML), tutte opportunità sfruttabili anche dal cyber crime.

Ecco alcuni spunti interessanti che aziende ed organizzazioni

dovrebbero prendere seriamente in considerazione.

Evoluzione del malware e dell’ingegneria sociale

Gli smart worker con le loro risorse domestiche, continueranno a rappresentare, per i criminali informatici, degli obiettivi sensibili da utilizzare come teste di ponte preferenziali per sferrare attacchi, attentamente coordinati, alle reti aziendali. Il malware avanzato del prossimo futuro potrebbe anche essere in grado di carpire dati sensibili e ricavare preferenze e abitudini delle vittime attraverso gli Edge Access Trojan (EAT) ovvero una nuova entità spyware distribuita e capace d’intercettazioni e compromissioni più invasive.

In tal senso non fa eccezione nemmeno il mercato degli strumenti cyber estorsivi con le famiglie dei ransomware che continueranno a evolversi e a colpire i sistemi di tecnologia operativa (OT) e in particolare le infrastrutture critiche che, coinvolgendo maggiormente i sistemi IT e estendendo la superfice di attacco, mettono a rischio ancor più dati, dispositivi e spesso, in base ai settori, anche vite umane.

Anche i dispositivi IoT e i sistemi domestici, che interagiscono con gli utenti, non saranno più dei semplici bersagli, ma rappresenteranno loro stessi dei canali di attacco più insidiosi, rendendo più efficace anche il social engineering.

Gli attacchi swarm-based e il 5G

La trasformazione digitale in atto in questi anni ha esteso, e in modo particolare durante questa fase emergenziale, ciò che tradizionalmente viene definito perimetro di rete con nuovi ambienti cloud, smart e IoT ciascuno dei quali, portando con sé dei rischi intrinseci che vanno ad aggiungersi a quelli

preesistenti, hanno finito con l'esporre maggiormente la superfice di rete estesa potenzialmente attaccabile. Di conseguenza, il cyber crime sta evolvendo le proprie strategie offensive contro questi ambienti cercando di sfruttare la velocità e la scalabilità offerte dal 5G, aprendo delle opportunità per minacce più avanzate e il dispiegamento di attacchi swarm-based. I criminali informatici, in tal senso, stanno compiendo notevoli progressi per compromettere e dirottare i dispositivi abilitati per il 5G anche se con tecnologie che richiedono comunque una certa potenza di elaborazione per abilitare i singoli swarmbot e condividere in modo efficiente le informazioni.

Innovazioni nelle prestazioni di elaborazione a scopo di lucro

Il rapporto stilato prevede anche l'evolversi di altri tipi di attacchi che, attraverso l'amplificazione delle prestazioni di elaborazione e di connettività, avranno l'unico scopo di accrescere i profitti illeciti dei criminal hacker coinvolgendo e sfruttando nuovi ambiti per migliorare l'efficienza del cryptomining, estendere su larga scala il bacino dei target e scardinare gli algoritmi di crittografia asimmetrica.

La potenza di elaborazione assumerà un valore sempre più prezioso qualora si volessero scalare attacchi futuri basati sul machine learning e l'intelligenza artificiale in grado di gestire enormi quantità di dati e consentire anche un maggiore rendimento del mining.

Anche la connettività dei sistemi satellitari e delle telecomunicazioni in generale potrebbe essere una ulteriore arma interessante per i criminali informatici. Una compromissione delle stazioni base e la successiva diffusione di malware attraverso le reti satellitari potrebbero dare agli aggressori la possibilità di prendere di mira milioni di

utenti connessi su larga scala e infliggere attacchi DDoS devastanti.

Dal punto di vista della sicurezza informatica, infine, il quantum computing è candidato a generare un nuovo rischio. Anche se non alla portata di tutti, l'enorme potenza di calcolo dei computer quantistici, infatti, potrebbe rendere risolvibili alcuni algoritmi di crittografia asimmetrica. Di conseguenza, le organizzazioni dovrebbero quanto prima adottare delle strategie di agilità crittografica elaborando algoritmi crittografici più resistenti.

Le future armi di difesa

Sicuramente l'evoluzione dell'intelligenza artificiale, potenziando le future tecnologie capaci di prevedere e reagire con nodi di apprendimento locali (machine learning), sarà fondamentale per la difesa contro queste tipologie di attacchi in continua evoluzione e con velocità di propagazione sempre più performanti.

Con questo tipo di approccio sarà possibile, fornendo ai sistemi d'intelligenza artificiale informazioni sulle tattiche, tecniche e procedure (TTP) degli attori delle minacce e dettagliate mappe sinottiche, rilevare i modelli di attacco e intervenire in modo proattivo offuscando gli obiettivi sensibili.

Purtroppo è solo questione di tempo ed è ragionevole pensare che molte di queste tendenze del crimine informatico diventeranno gradualmente realtà, anche tramite risorse mercificate e rese disponibili nei marketplace underground.

Pertanto, come dicono gli stessi ricercatori, sarà necessaria un'attenta combinazione di tecnologie, di persone, di formazione e di partnership per proteggersi dal cyber crime del futuro.

Cyber crime, cosa ci riserva il futuro?