

I pirati nord-coreani di Lazarus adesso usano malware “in affitto”

Dic 12, 2019 Marco Schiaffino In evidenza, Malware, News, RSS, Scenario 0

L'utilizzo di un nuovo malware sarebbe il senale di una strana collaborazione tra il gruppo di “hacker di stato” Lazarus e i cyber-criminali di TrickBot.

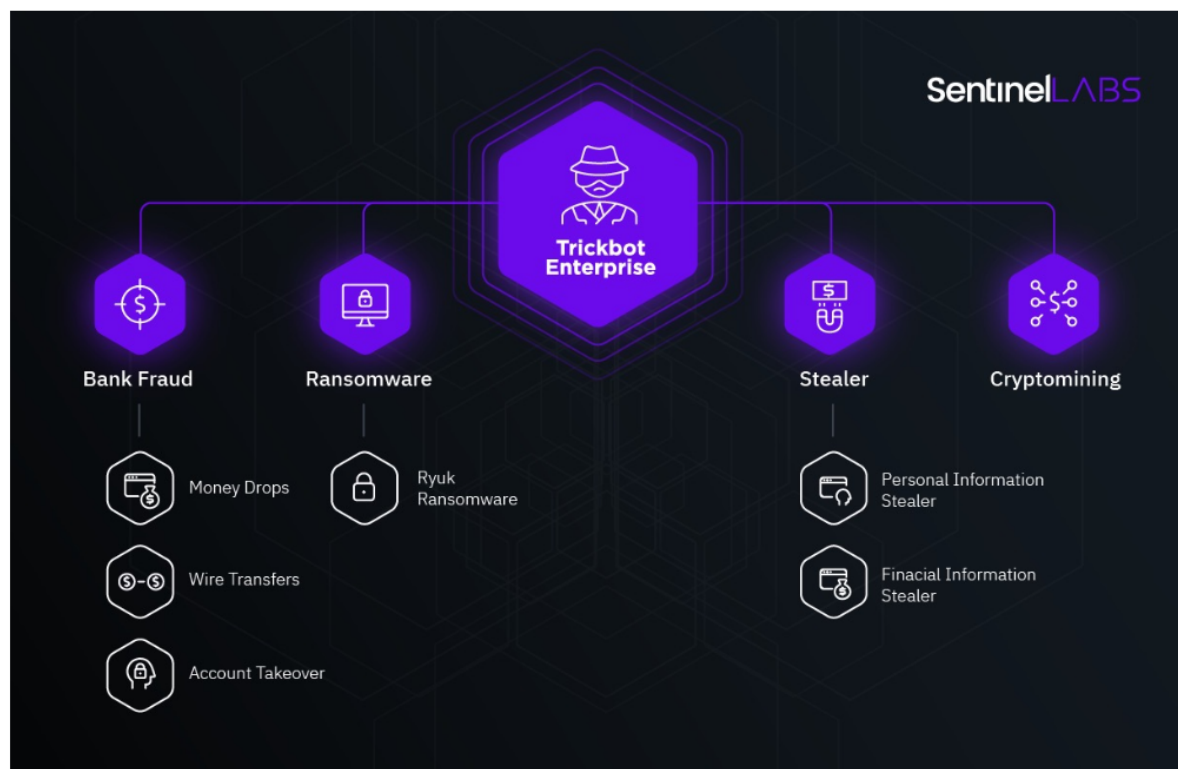
Il mondo della pirateria informatica, ormai da anni, è caratterizzato da forme di collaborazione più o meno strette tra vari gruppi di pirati informatici. Una delle poche “barriere” che vengono considerate invalicabili è quella tra “comuni” cyber-criminali e i gruppi APT, quelli cioè che agiscono per conto di **governi e servizi segreti**. Ora sembra che anche questa distinzione sia caduta.

A segnalarlo sono i ricercatori di **SentinelOne**, che in un report pubblicato sul sito della società di sicurezza spiegano di aver individuato uno stretto rapporto tra il gruppo di cyber-spionaggio **Lazarus** e i pirati informatici di **TrickBot**.

Lazarus, di cui ci è capitato di parlare più volte su **Security Info**, è il gruppo APT che gli esperti di sicurezza considerano da sempre collegato al governo della **Nord Corea** e fino a oggi la sua attività si era caratterizzata per l'utilizzo di strumenti di hacking “fatti in casa”.

Secondo gli analisti di SentinelOne, però, adesso la loro attività sfrutterebbe **Anchor**, un nuovo modulo di spionaggio sviluppato dal gruppo TrickBot.

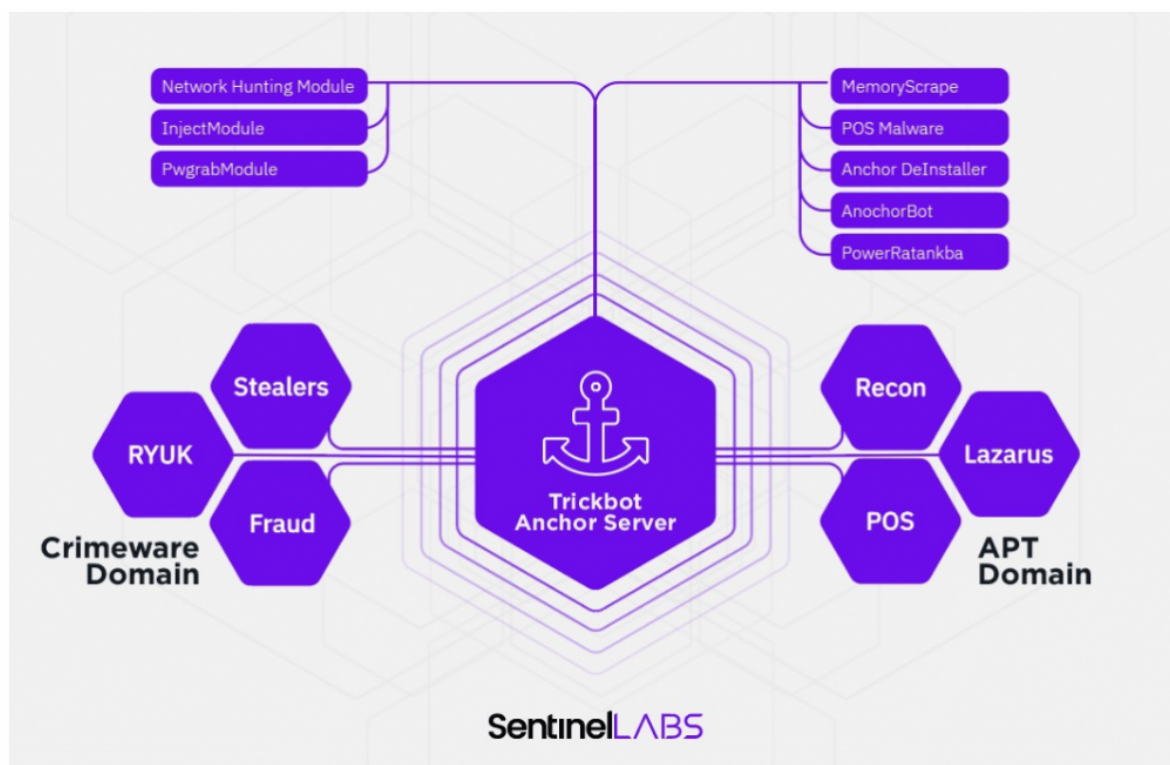
Quest'ultimo è un soggetto ben conosciuto, che fa parte però di quella "delinquenza comune" normalmente attiva in settori orientati alla raccolta di credenziali bancarie e attacchi a soggetti che operano nella finanza.



In quest'ottica, il fatto che usi la formula del **malware as a service**, cioè che affitti ad altri criminali i suoi software, non stupisce più di tanto. Tanto più che la gang è nota per fornire servizi personalizzati in base alle esigenze dei suoi clienti.

Il nuovo modulo, però, sembra pensato proprio per chi vuole guadagnare un livello di elevata persistenza sulla macchina compromessa senza dare troppo nell'occhio. **Qualcosa, cioè, che può interessare principalmente a hacker che puntano ad attacchi mirati e allo spionaggio.**

In realtà, come spiegano i ricercatori nel report, Anchor consiste di una collezione di strumenti estremamente evoluti che, molto probabilmente, sono stati pensati in origine per "clienti" interessati a colpire bersagli di alto livello del settore finanziario.



L'interessamento del gruppo Lazarus è probabilmente dovuto a una semplice intuizione: lo stesso set di strumenti può essere utilizzato per portare avanti attività di spionaggio. **Il modulo, infatti, integra sistemi per cancellare le tracce dell'attacco e per offuscare l'attività del malware che si prestano alla perfezione a questo tipo di attività.**

Insomma: è probabile che i pirati di TrickBot non avessero assolutamente idea che il loro nuovo "prodotto" avrebbe potuto suscitare l'interesse di un gruppo di hacker di stato. Considerato che il detto "pecunia non olet" si applica benissimo anche ai bassifondi del Web, la strana alleanza tra TrickBot e Lazarus non deve stupire più di tanto.

Condividi l'articolo

Progetto Blackfin: F-Secure cambia la logica dell'intelligenza artificiale

Articoli correlati

Altro in questa categoria

<https://www.securityinfo.it/2019/12/12/i-pirati-nord-coreani-d-i-lazarus-adesso-usano-malware-in-affitto/>