Autostrada degli attacchi

Un esame approfondito del traffico DNS dannoso

Akamai

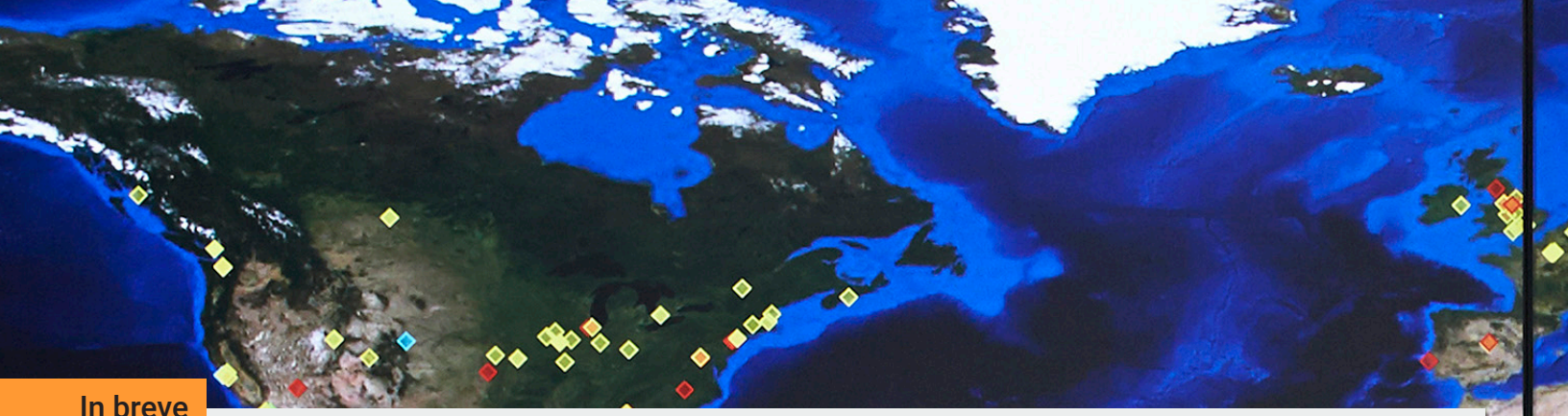
Sommario

DNS (Domain Name Server): un'autostrada per il traffico degli attacchi

Il DNS (Domain Name System) è stato una parte fondamentale dell'infrastruttura Internet sin dai suoi primissimi esordi. Gran parte del nostro utilizzo di Internet, sia a casa che al lavoro, deve essere facilitato tramite il DNS per consentirci di navigare correttamente verso la nostra destinazione sul World Wide Web. Non sorprende che gli autori di attacchi spesso scelgano di sfruttare questa infrastruttura per facilitare i propri attacchi, sia che si tratti di una minaccia che accede ai server di comando e controllo (C2) per attendere i comandi o di un'esecuzione di codice remoto che raggiunge un dominio per scaricare file dannosi su un computer. A causa della sua ubiquità, il DNS è diventato una parte importante dell'infrastruttura di attacco.

In qualità di azienda di servizi per la sicurezza, Akamai dispone di un punto di osservazione che ci consente di esaminare e proteggere le aziende, nonché gli utenti privati, dal traffico DNS dannoso che potrebbe comportare la compromissione del sistema e il furto di informazioni. In questo rapporto, forniremo un'analisi del traffico dannoso che prende di mira utenti privati e aziende in tutto il mondo. Un'analisi approfondita del traffico DNS dannoso, che include la correlazione con gruppi o strumenti di criminali, può fornire alle organizzazioni informazioni importanti sulle minacce più diffuse per le loro attività. Pertanto, queste informazioni possono aiutare i professionisti della sicurezza a valutare la propria strategia di difesa e condurre valutazioni delle lacune per contrastare le tecniche e le metodologie utilizzate contro di loro. In caso contrario, potrebbero verificarsi violazioni che comportano perdite di dati riservati, perdite finanziarie o sanzioni dovute a violazioni della conformità. Con un aumento annuale previsto dei costi del cybercrimine fino a 10,5 mila miliardi di dollari entro il 2025, le organizzazioni devono essere preparate anche prima che si verifichino gli attacchi.

Analizzando il traffico DNS dannoso di utenti aziendali e privati, siamo stati in grado di individuare diversi attacchi e campagne nel processo, come la diffusione di FluBot, un malware basato su Android che si sposta da un paese all'altro in tutto il mondo, nonché la prevalenza di vari gruppi di criminali informatici che prendono di mira le imprese. Forse l'esempio migliore è la significativa presenza di traffico C2 relativo agli IAB (Initial Access Broker) che violano le reti aziendali e monetizzano l'accesso vendendolo ad altri, come i gruppi RaaS (Ransomware as a Service). Abbiamo individuato queste attività sull'autostrada di informazioni che è il DNS e le condividiamo a beneficio dei nostri lettori.



In breve

Secondo i nostri dati, tra il 10% e il 16% delle organizzazioni ha rilevato la presenza di traffico C2 sulla propria rete in un dato trimestre. La presenza di traffico C2 nella rete indica la possibilità di un attacco o una violazione in corso e le minacce vanno dalle botnet che rubano informazioni agli IAB.

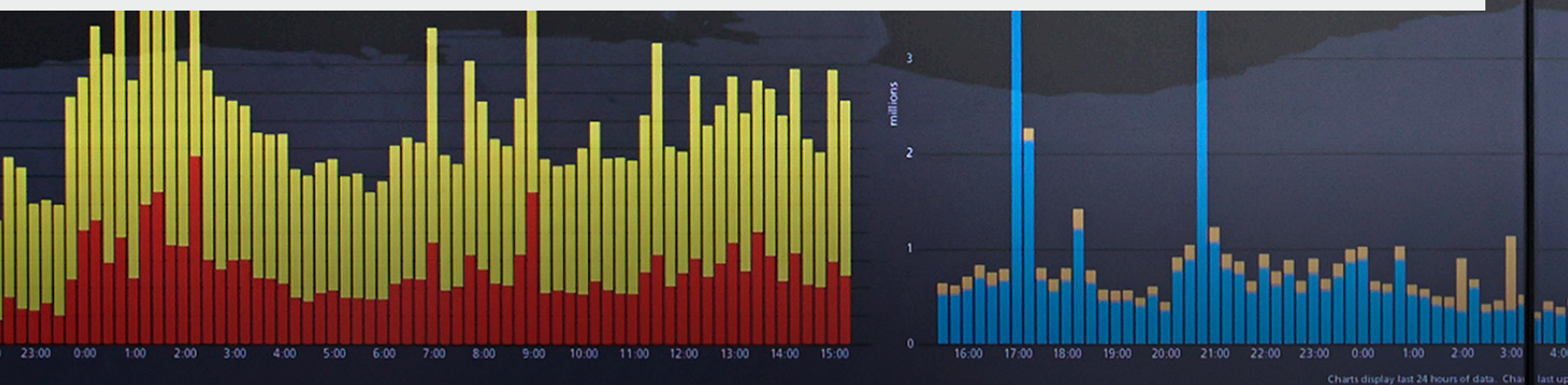
Il 26% dei dispositivi colpiti ha raggiunto i domini C2 IAB noti, inclusi i domini relativi a Emotet e Qakbot. Gli IAB rappresentano un grosso rischio per le aziende perché, dopo l'iniziale violazione, il loro scopo principale è quello di vendere le credenziali di accesso ai gruppi di ransomware e cybercriminali.

I NAS (Network Attached Storage) sono soggetti agli exploit perché è meno probabile che siano aggiornati con patch e contengono dati preziosi. I nostri dati mostrano che gli autori di attacchi stanno abusando di questi dispositivi tramite QSnatch, con il 36% dei dispositivi interessati nelle reti aziendali che accedono ai domini C2 correlati a questa minaccia.

Il 30% delle organizzazioni interessate opera nel settore della produzione, il doppio rispetto al secondo maggiore segmento verticale, sottolineando le implicazioni concrete degli attacchi informatici, quali problemi della supply chain e interruzioni alle attività quotidiane. Normative come la direttiva sulla sicurezza delle reti e dell'informazione 2 (NIS2) potrebbero aiutare a ridurre gli attacchi contro settori essenziali o infrastrutture critiche come la produzione.

Gli attacchi alle reti domestiche mirano ad abusare non solo dei dispositivi tradizionali come i computer, ma anche dei telefoni cellulari e dell'Internet of Things (IoT). Una quantità significativa di traffico degli attacchi può essere correlata ai malware mobili e alle botnet IoT.

Durante la nostra analisi dei dati DNS, abbiamo individuato una rapida diffusione di malware FluBot in Europa, Medio Oriente e Africa (EMEA); America Latina (LATAM); e Asia-Pacifico e Giappone (APJ). Le tattiche di social engineering del malware e il suo utilizzo di più lingue dell'Unione europea (UE) potrebbero essere alcuni dei fattori che contribuiscono all'aumento dell'infezione.



Terminologia dell'analisi del traffico DNS di Akamai

L'Edge DNS e l'infrastruttura DNS di Akamai osservano fino a 7 mila miliardi di richieste DNS al giorno. Per proteggere gli utenti e le aziende, Akamai blocca le richieste che indirizzano a domini che distribuiscono malware o a siti che potrebbero rubare le vostre informazioni. L'esame di queste transazioni DNS dannose ci consente inoltre di classificare questi domini in tre categorie (malware, siti di phishing e C2) e condurre un'analisi approfondita per comprendere le maggiori minacce odierne per le aziende e gli utenti domestici.

Da un attento campionamento dei dati del traffico DNS dannoso, possiamo trarre conclusioni significative sulle minacce più diffuse. Il nostro sistema di protezione copre due segmenti demografici: un segmento demografico è quello delle imprese in cui Akamai protegge le reti aziendali, mentre l'altro segmento demografico è quello degli utenti domestici che accedono a Internet tramite le loro reti personali e sono esposti a minacce quali le botnet che mirano a controllare i loro dispositivi per scopi nefasti come il guadagno finanziario tramite il cryptomining.

Innanzitutto, definiamo i termini *siti di phishing*, *malware* e *C2* e spieghiamo come li utilizziamo in questo rapporto.

I **siti di phishing** sono domini legati a kit di phishing che imitano e clonano l'aspetto di aziende retail, banche, società high-tech e altri al fine di indurre gli utenti a divulgare informazioni come credenziali e informazioni di identificazione personale (PII). Akamai osserva questo traffico tramite DNS per proteggere gli utenti aziendali e privati dal furto di identità e dalla perdita di informazioni.

Per **malware** si intende uno o più domini dannosi che distribuiscono o contengono file dannosi. Questa categoria contiene anche siti che ospitano JavaScript dannoso e siti web compromessi che pubblicano annunci indesiderati o reindirizzano gli utenti a una pagina contenente tali annunci. Molti attacchi moderni richiedono il download di un file dannoso su un dispositivo da una fonte esterna per il payload iniziale o per scaricare la fase successiva di un attacco in corso. Osservare e bloccare questo traffico può aiutare a proteggere un'organizzazione da un'infezione iniziale o da un attacco in corso.

C2, nel contesto della nostra analisi del traffico DNS, è un dominio utilizzato per comunicare con i dispositivi infetti per inviare comandi e quindi controllare il dispositivo. Dopo la compromissione iniziale, gli autori di attacchi stabiliscono comunicazioni C2 tra il sistema infetto e un server controllato dagli autori di attacchi per inviare comandi aggiuntivi, come il download e la diffusione di altro malware, l'esfiltrazione di dati e l'arresto e il riavvio del sistema, tra gli altri, per compromettere ulteriormente la sicurezza del sistema o della rete. Il rilevamento del traffico C2 è fondamentale in quanto segnala un attacco in corso che potrebbe ancora essere mitigato. Inoltre, il blocco dei domini associati ai server C2 evita che vengano stabilite comunicazioni C2 e impedisce al malware di scaricare ulteriori istruzioni o comandi, riducendo le possibilità che gli autori di attacchi eseguano attività dannose nella rete.

Pericolo futuro: la diffusione del traffico dannoso nelle organizzazioni

In base all'analisi del traffico DNS di Akamai, possiamo osservare che il 13% dei dispositivi ha tentato di raggiungere almeno una volta i domini associati al malware nel quarto trimestre del 2022 (Figura 1). Inoltre, il 6% ha comunicato con domini relativi al phishing. Nell'area C2, su cui ci concentreremo notevolmente in questo rapporto, abbiamo osservato una tendenza all'aumento durante tutto l'anno con un leggerissimo calo nel quarto trimestre.

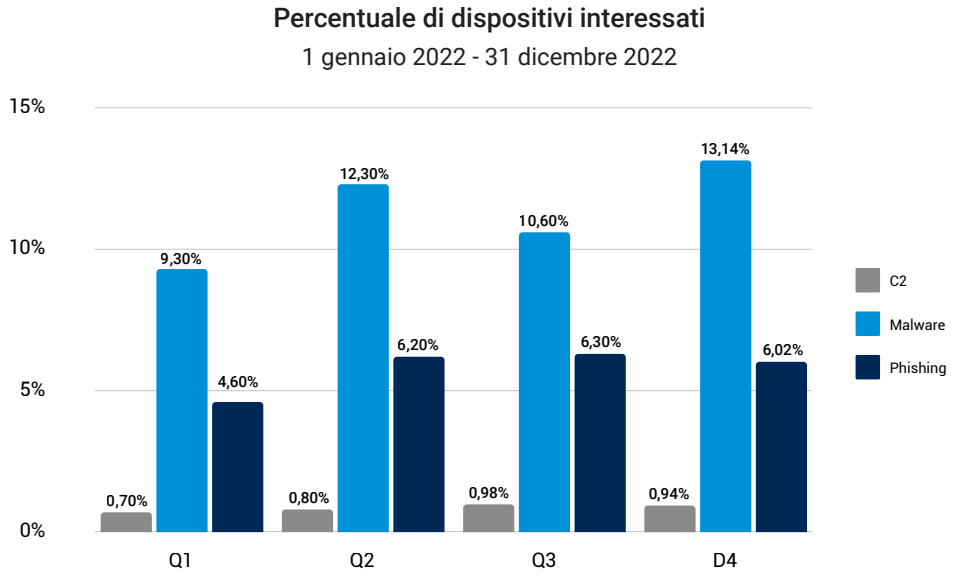


Figura 1: Osserviamo una tendenza crescente nei dispositivi protetti che raggiungono destinazioni dannose

La Figura 1 si riferisce solo ai singoli dispositivi che hanno tentato di comunicare con domini dannosi. È importante sottolineare la disparità tra i dispositivi che raggiungono le destinazioni del malware (che possono essere utilizzati dagli autori di attacchi per scaricare malware) e i dispositivi che raggiungono i domini C2 (tipicamente utilizzati durante un attacco in corso per facilitare la comunicazione tra l'autore di attacchi e il malware e possibilmente usati per scaricare malware aggiuntivo per proseguire un ciclo di attacco). Questa disparità può essere indicativa delle differenze tra tentativi di infiltrazione nella rete, che possono essere bloccati al primo tentativo di scaricare malware su un computer, e infiltrazioni riuscite (che, nei nostri dati, potrebbero non essere passate tramite il DNS) o attacchi in corso, che possono raggiungere un dominio C2 per eseguire l'attacco.

Questo rapporto si concentrerà principalmente sul traffico C2 come potenziale indicatore di un'istanza in cui un autore di attacchi è riuscito ad accedere a un dispositivo. Per poter comprendere la prevalenza di tali attacchi, dobbiamo esaminare i dati attraverso una lente diversa. Piuttosto che esaminare i singoli dispositivi, possiamo aggregare i dati per organizzazione per esaminare la frequenza con cui un attacco in corso (indicato dall'esistenza di traffico C2) appare all'interno del set di dati.

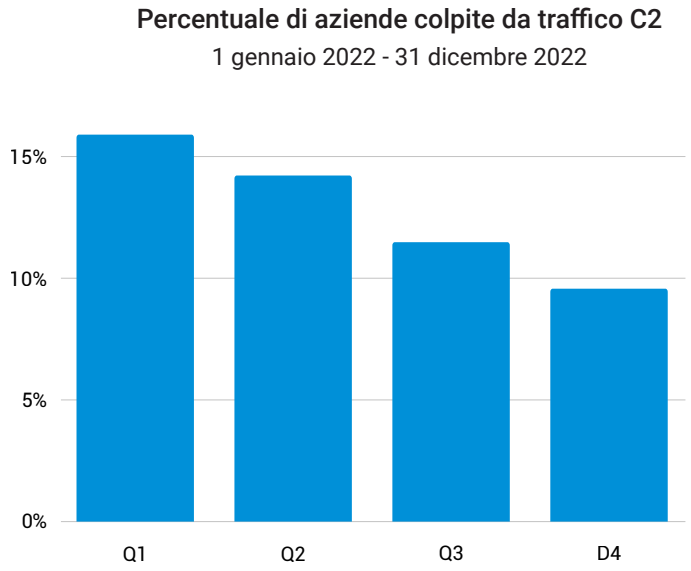


Figura 2: Un'analisi del traffico C2 dannoso mostra la percentuale di organizzazioni in cui almeno un dispositivo ha raggiunto un dominio C2 in un anno

> **Secondo i nostri dati DNS, tra il 10 e il 16% delle organizzazioni ha riscontrato almeno un caso di uscita di traffico C2 dalla propria rete in un dato trimestre.**

Secondo i nostri dati DNS, tra il 10% e il 16% delle organizzazioni ha riscontrato almeno un caso di uscita di traffico C2 dalla propria rete in un dato trimestre (Figura 2). Ciò può indicare un malware che tentava di comunicare con un operatore ed essere il segnale di una potenziale violazione. Questo traffico C2 è stato bloccato dalla nostra soluzione e non ha raggiunto la destinazione ma, in caso di successo, avrebbe provocato esfiltrazione di dati, attacchi ransomware e molto altro. Nella prima metà del 2022 sono stati rilevati 2,3 miliardi di ceppi di malware, con una media di 1.501 al giorno. La nostra ricerca evidenzia l'efficacia dell'utilizzo del DNS per impedire ai malware di penetrare in una rete e provocare danni.

Gli IAB (Initial Access Broker) rappresentano una minaccia prevalente per le organizzazioni

Gli attacchi multifase sono diventati un caposaldo del moderno panorama degli attacchi (Figura 3). Gli autori di attacchi hanno scoperto di avere maggiore successo se lavorano insieme (o si ingaggiano tra loro) oppure se sono in grado di combinare vari strumenti in un singolo attacco. Le funzionalità C2 sono cruciali per il successo di questi attacchi. Possono essere usate non solo per la comunicazione, ma anche per facilitare il download di un payload e del malware nelle fasi successive dell'attacco, per far penetrare l'attacco. Ciò è meglio esemplificato dalla catena di attacchi ransomware Emotet/TrickBot/Ryuk osservata negli ultimi anni. Emotet si infiltra prima nella rete della vittima e, una volta effettuato l'accesso iniziale, raggiunge un dominio per scaricare il payload di TrickBot per ottenere dati personali, credenziali e altro. Se la vittima è considerata un obiettivo di alto valore per gli autori di attacchi, il malware raggiunge quindi i suoi server C2 e scarica il payload finale: ransomware Ryuk.

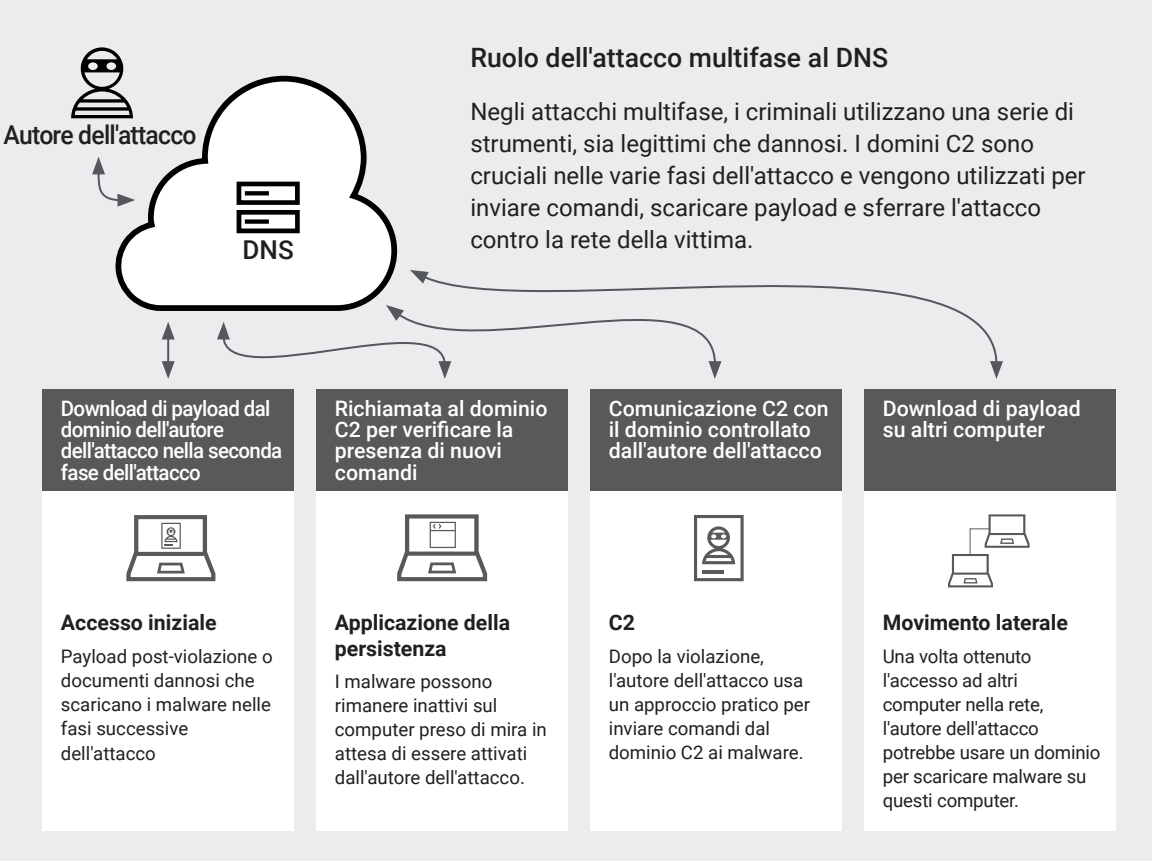


Figura 3: Il ruolo di C2 in ogni fase dell'attacco

Questa catena di eventi è importante da considerare quando si valutano le informazioni contenute in questo rapporto. La comunicazione C2 può avvenire in varie fasi dell'attacco. La nostra recente analisi della metodologia dei moderni gruppi di ransomware, come il gruppo Conti, ha mostrato che criminali sofisticati spesso assegnano a operatori il lavoro di tipo "mani sulla tastiera" per portare avanti un attacco in modo rapido ed efficiente. La capacità di visualizzare e bloccare il traffico C2 può essere fondamentale per fermare un attacco in corso.

I domini C2 che abbiamo osservato possono essere suddivisi in domini con o senza attribuzione a una famiglia di minacce o un gruppo di criminali specifici. In questa sezione, esamineremo in modo approfondito i domini C2 associati a un tipo di minaccia e aiuteremo i lettori a valutare il livello di rischio in base alle funzionalità e alle metodologie di ciascun gruppo. Tenete presente che alcune di queste famiglie di malware possono adattarsi a più casi di utilizzo, a seconda di come gli autori di attacchi le utilizzano durante un attacco.

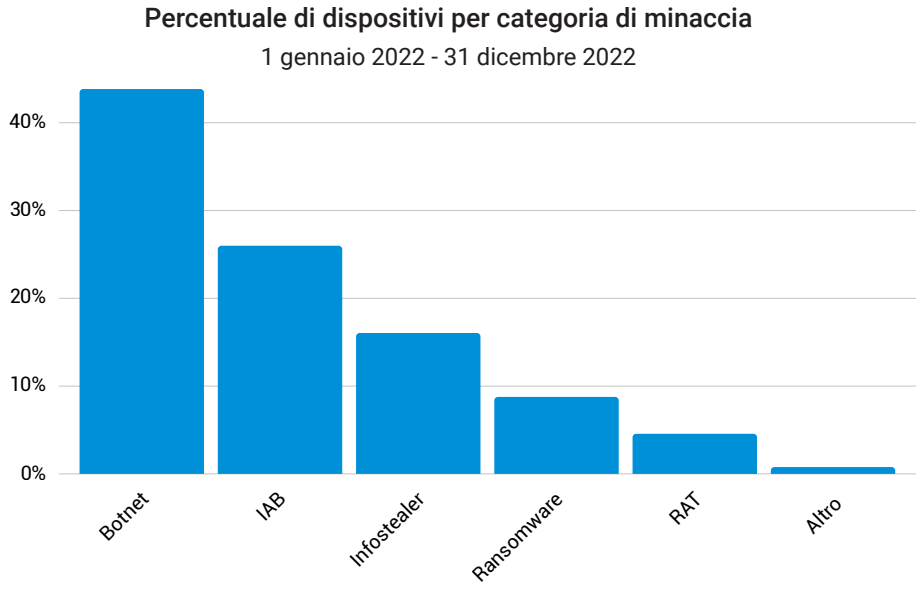


Figura 4: Le aziende sono prevalentemente prese di mira dalle botnet, seguite da IAB e infostealer

Nella Figura 4, i gruppi di autori di attacchi sono classificati in gruppi RaaS, IAB e botnet. I risultati dei nostri dati rivelano che gli IAB rappresentano una delle principali minacce per le reti aziendali, come le botnet che puntano all'esfiltrazione dei dati.

IAB (Initial Access Broker)
Gli IAB si concentrano principalmente sulla fornitura di un punto di accesso iniziale per altri criminali informatici, compresi i gruppi di ransomware, per prendere piede nelle reti delle organizzazioni. persistenza, esecuzione remota del payload dopo l'intrusione ed esfiltrazione di dati.

Gruppi RaaS (Ransomware as a Service)
Si tratta di gruppi che consentono ad altri autori di attacchi (anche quelli senza competenze tecniche) di diventare affiliati e utilizzare il loro software ransomware a pagamento.

Botnet
Gli autori di attacchi possono utilizzare le botnet per una miriade di scopi: dagli attacchi di cryptomining e DDoS all'esfiltrazione di dati, alla distribuzione di malware e al movimento laterale.

Ladri di informazioni
Gli infostealer raccolgono vari tipi di dati come nomi utente, password, informazioni di sistema, credenziali bancarie, cookie e così via.

Inoltre, stiamo registrando anche la presenza di ransomware, RAT (Remote Access Tool) e infostealer, che ricoprono tutti un ruolo importante nelle varie fasi di un attacco. Con un numero così elevato di strumenti disponibili illegalmente per i cybercriminali nuovi e esperti, con cui è possibile ottenere l'accesso iniziale, restare nascosti nella rete e proseguire l'attacco, le organizzazioni sono più suscettibili che mai al crimine informatico. Proseguendo con questi raggruppamenti, stabiliremo anche le intersezioni sulle quali operano e le implicazioni e gli impatti potenziali per le organizzazioni.

Gruppi di IAB (Initial Access Broker)

Soprannominato "IAB" (Initial Access Broker), questo specifico gruppo di criminali informatici si concentra principalmente sulla fornitura di un punto di accesso iniziale per altri criminali informatici e autori di attacchi per prendere piede nelle reti delle organizzazioni. Sebbene diversi gruppi di criminali informatici abbiano metodologie di violazione simili, come lo sfruttamento delle vulnerabilità relative a RDP e VPN, l'utilizzo di attacchi di forza bruta, la raccolta di credenziali violate e l'invio di e-mail di phishing contenenti malware, gli IAB sono specializzati nell'ottenere l'accesso a questi sistemi infetti e nella vendita di tale accesso ad altri gruppi di criminali, piuttosto che portare a termine l'intero attacco. Secondo quanto riferito, i gruppi di ransomware dietro LockBit, DarkSide, Conti e BlackByte, tra gli altri, hanno sfruttato gli IAB per svolgere le loro operazioni. Uno studio di ricerca del 2023 ha rilevato che il prezzo medio di vendita per l'accesso iniziale è di circa 2.800 dollari USA.

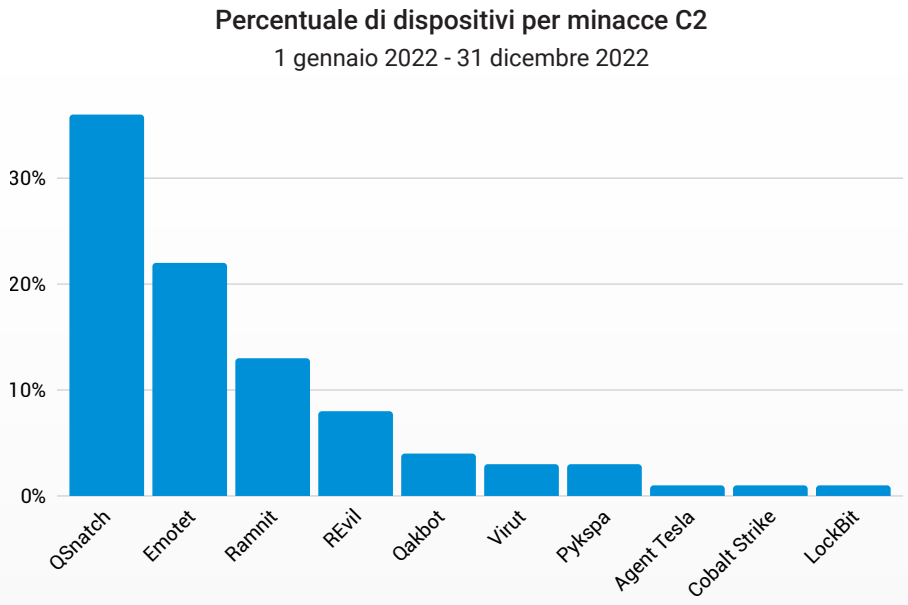
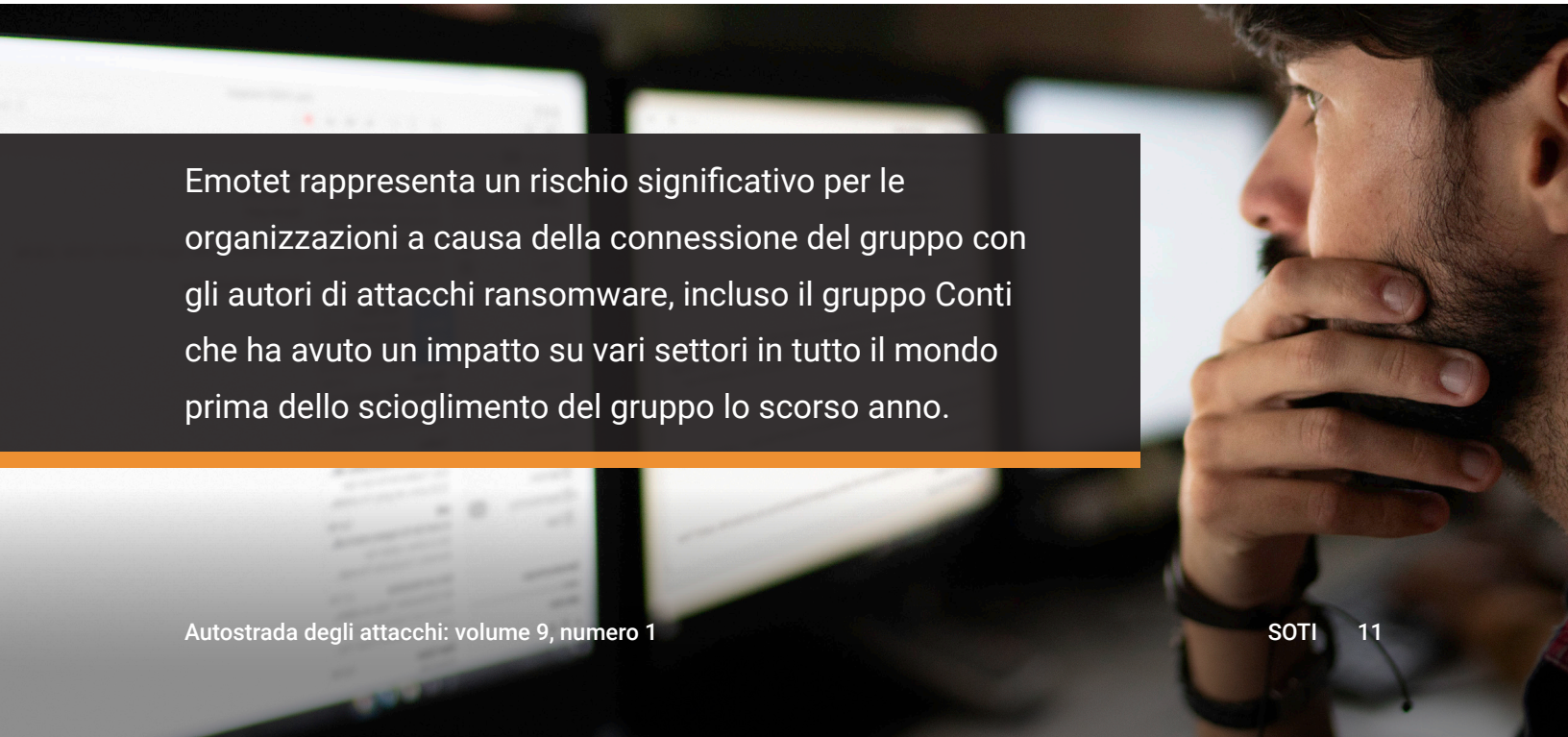


Figura 5: QSnatch, Emotet e Ramnit sono le principali famiglie C2 osservate nel traffico di rete aziendale

In base ai nostri dati sul DNS (Figura 5), il 26% dei dispositivi infetti ha raggiunto domini correlati a IAB come Qakbot (4% dei dispositivi infetti) ed Emotet (22% dei dispositivi infetti). Gli IAB svolgono un ruolo importante nel modello aziendale RaaS e nel panorama del crimine informatico. Gli autori di attacchi ransomware e i criminali informatici necessitano dell'accesso remoto e delle credenziali non solo per infiltrarsi nelle reti delle proprie vittime, ma anche per spostarsi lateralmente, stabilire la persistenza e ottenere privilegi di accesso, tra le altre attività. Gli autori di attacchi sfruttano gli IAB per svolgere attività dispendiose in termini di tempo, quali ricognizione, esame del potenziale bersaglio e infezione iniziale. L'accesso immediatamente disponibile venduto clandestinamente elimina quel passaggio e abbassa il livello di competenza o il tempo necessario agli autori di attacchi per sferrare un attacco. Pertanto, introduce una moltitudine di potenziali attacchi contro le organizzazioni bersaglio previste, con conseguenti ransomware, furto di informazioni riservate e sensibili, spionaggio e violazioni dei dati.

Emotet emerge come uno degli IAB più importanti nei nostri dati. Emotet rappresenta un rischio significativo per le organizzazioni a causa della connessione del gruppo con gli autori di attacchi ransomware, incluso il gruppo Conti che ha avuto un impatto su vari settori in tutto il mondo prima di sciogliersi lo scorso anno. Nel corso degli anni, Emotet ha aggiunto altri moduli, come DDoS (Distributed Denial of Service) e funzionalità di furto di e-mail, e ha ampliato i suoi obiettivi prefissati. Da un trojan bancario/botnet con una moltitudine di funzionalità, Emotet si è trasformato in un MaaS (Malware as a Service), distribuendo minacce come il trojan bancario IcedID, TrickBot e il ransomware UmbreCrypt. È stato anche osservato che il gruppo TrickBot utilizza Emotet per distribuire diversi attacchi ransomware, tra cui Ryuk, ProLock e Conti, tra gli altri. Una visione più dettagliata delle tecniche utilizzate da Emotet è disponibile nel framework MITRE ATT&CK sull'argomento.



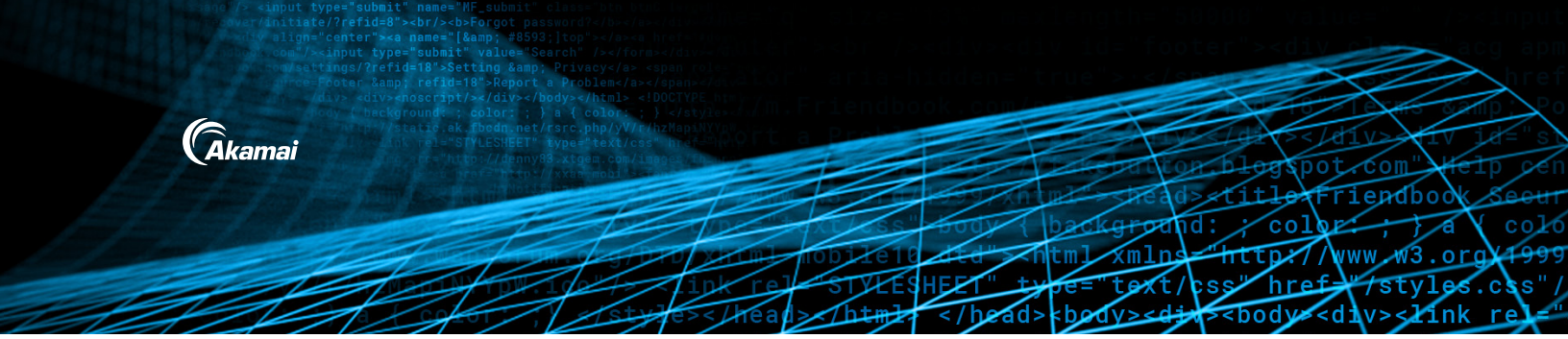
Emotet rappresenta un rischio significativo per le organizzazioni a causa della connessione del gruppo con gli autori di attacchi ransomware, incluso il gruppo Conti che ha avuto un impatto su vari settori in tutto il mondo prima dello scioglimento del gruppo lo scorso anno.

Il secondo IAB più importante nei dati è Qakbot. Questo gruppo è noto per aver collaborato con il gruppo ransomware Black Basta che, secondo quanto riferito, ha avuto un impatto su almeno 50 organizzazioni di varie parti del mondo. Il team di Qakbot è noto per le sue funzionalità di furto di informazioni e per la distribuzione di malware di seconda fase per compromettere ulteriormente la sicurezza del sistema. Secondo la ricerca, Qakbot sfrutta Cobalt Strike, uno strumento per test di penetrazione legittimo utilizzato dai red team e abusato dai criminali, per eseguire una serie di attività dannose post-intrusione e per facilitare una backdoor nell'ambiente di una vittima. Questa è una tecnica sempre più utilizzata dagli IAB negli ultimi anni. Il framework MITRE ATT&CK può fornire informazioni aggiuntive relative alle tecniche sfruttate da Qakbot durante il suo attacco.

Gruppi botnet

Nella nostra analisi, le botnet costituiscono il maggiore raggruppamento di tipi di minaccia con il 44% del traffico C2 analizzato. In questo raggruppamento è rappresentata un'ampia gamma di autori di attacchi ed è essenziale ricordare che non tutte le botnet sono uguali. Le varianti più benigne potrebbero installare cryptominer o sfruttare il computer della vittima per sferrare attacchi DDoS. Sebbene questi rappresentino di per sé un costo, le botnet che abbiamo individuato nelle aziende possono essere utilizzate per l'esfiltrazione di dati e attacchi multifase, che possono rappresentare un rischio più significativo. Le botnet possono diffondersi lateralmente nella rete ed essere utilizzate per distribuire ransomware, come nel caso di TrickBot oppure possono concentrarsi specificamente sul furto di informazioni e sulla raccolta di credenziali.

Abbiamo scoperto che QSnatch, la maggiore botnet presente negli ambienti aziendali, fa esattamente questo: l'esfiltrazione di dati da dispositivi collegati alla rete. Secondo i nostri dati, il 36% dei dispositivi sono stati infettati da QSnatch. Questo malware prende di mira specificamente QNAP, un tipo di dispositivo NAS utilizzato per i backup o l'archiviazione dei file dalle aziende. Sebbene il metodo di infezione sia ancora sconosciuto, i ricercatori ipotizzano che QSnatch potrebbe infettare sfruttando le vulnerabilità del firmware o attacchi di forza bruta su dispositivi con un nome utente/password predefiniti. Si consiglia vivamente alle aziende che utilizzano QNAP di mantenere aggiornato il proprio firmware (dopo l'infezione, QSnatch impedisce l'installazione di patch e disabilita i prodotti di sicurezza) e di modificare immediatamente le password predefinite. QSnatch viene utilizzato dagli autori di attacchi per eseguire lo scraping delle credenziali, la registrazione delle password, l'accesso remoto e l'esfiltrazione dei dati, solo per citare alcuni esempi. Gli autori di attacchi potrebbero prendere di mira i dispositivi di archiviazione poiché contengono informazioni preziose e la compromissione di questi dispositivi lascia le aziende senza backup in caso di attacchi ransomware. I dettagli su tattiche e contromisure sono evidenziati in questo avviso CISA.



Gruppo RaaS (Ransomware as a Service)

Nella nostra analisi del traffico DNS, il 9% dei dispositivi infetti che hanno raggiunto le famiglie C2 ha avuto accesso ai domini associati ai gruppi RaaS. Questo tipo di gruppo di criminali informatici consente ad altri autori di attacchi (anche senza le competenze tecniche) di diventare un loro affiliato e utilizzare il loro software ransomware a pagamento. Le organizzazioni colpite dal ransomware affrontano una moltitudine di conseguenze che non si limitano alla perdita di dati aziendali riservati. Le aziende potrebbero potenzialmente affrontare costi di risoluzione e ripristino, spese legali, sanzioni, downtime con conseguente perdita di produttività e danni al brand e alla reputazione. Cybersecurity Ventures ha affermato che il costo degli attacchi ransomware potrebbe ammontare a circa 265 miliardi di dollari all'anno entro il 2031. Il rapporto sul ransomware globale di Akamai evidenzia anche gli impatti paralizzanti del ransomware che vanno oltre le perdite finanziarie, come l'interruzione della supply chain e, in alcuni casi, il ransomware potrebbe essere una questione di vita o di morte.

Un prolifico gruppo RaaS è il gruppo REvil, diventato famoso per aver preso di mira un fornitore di soluzioni per la gestione IT in un attacco alla supply chain che ha colpito più di 1.500 fornitori di servizi gestiti. Le loro operazioni sono cessate con l'arresto di diversi membri da parte del governo russo. Tuttavia, pochi mesi dopo lo scioglimento, i ricercatori di sicurezza hanno osservato che il sito delle fughe di notizie di REvil era di nuovo attivo con le informazioni delle sue ultime vittime, comprese alcune università negli Stati Uniti. I ricercatori hanno ipotizzato che potrebbe non essere lo stesso gruppo REvil a condurre questa campagna e hanno messo in guardia contro gli stati nazione che affermano di essere il gruppo REvil per nascondere le proprie tracce. In termini di tattiche, REvil è noto per personalizzare, il proprio flusso di attacco in base alle vittime, il che esemplifica il livello di conoscenza che il gruppo ha dei propri obiettivi. Per saperne di più sulle tattiche, tecniche e procedure relative a REvil, leggete il post di MITRE.

> **Gli autori di attacchi potrebbero prendere di mira i dispositivi di archiviazione poiché contengono informazioni preziose e la compromissione di questi dispositivi lascia le aziende senza backup in caso di attacchi ransomware.**

Un altro gruppo RaaS che abbiamo individuato nel nostro esame del traffico DNS è LockBit. Dopo la "scomparsa" di Conti, il gruppo LockBit è diventato uno dei provider RaaS più attivi. In precedenza (da novembre 2019 a marzo 2022), secondo questo rapporto, era il RaaS che ha colpito il maggior numero di organizzazioni dopo Conti.

Il gruppo LockBit è orgoglioso di disporre di un meccanismo di crittografia più veloce rispetto ad altri gruppi RaaS e ha affermato di aver colpito più di 12.000 aziende con il suo LockBit 2.0. Nel giugno 2022, il gruppo ha rilasciato LockBit 3.0, con funzionalità aggiuntive, incluso il programma Bug Bounty. Inoltre, secondo quanto riferito, sta sfruttando la vulnerabilità Log4j per ottenere l'accesso iniziale ai propri obiettivi, sottolineando l'importanza delle patch. Le organizzazioni che non hanno affrontato tali falle di sicurezza potrebbero essere maggiormente a rischio di essere infettate da LockBit. LockBit continua a reinventarsi: un'aggiunta recente è la tattica di tripla estorsione in cui crittografano i file, li pubblicano in siti di fughe di notizie e sferrano attacchi DDoS se le vittime si rifiutano di pagare il riscatto.

Strumenti del mestiere

Gli strumenti identificati in questa sezione possono svolgere un ruolo specifico in un attacco, sia tramite la violazione del sistema, ottenendo informazioni che mediante l'escalation dei privilegi. L'arsenale di vari gruppi di autori di attacchi che abbiamo osservato richiede spesso la comunicazione per operare come ladri di informazioni e RAT. La comprensione di questi strumenti, insieme alle tattiche utilizzate dai gruppi di autori di attacchi, può aiutare i professionisti della sicurezza a comprendere come avvengono gli attacchi e a pianificare di conseguenza.

Infostealer

Progettati per ottenere vari tipi di dati come nomi utente, password, informazioni di sistema, credenziali bancarie e cookie, tra gli altri, gli infostealer rimangono una delle offerte MaaS frequentemente utilizzate negli attacchi. Gli autori di attacchi che potrebbero non avere le conoscenze e/o le competenze tecniche potrebbero semplicemente acquisire infostealer a un costo relativamente basso e sferrare i propri attacchi.

Nell'elenco delle famiglie di malware C2, abbiamo osservato che il 16% dei dispositivi che hanno avuto accesso all'attribuzione C2 nota tramite gli infostealer. Ramnit (13% dei dispositivi infetti) non è un ladro di informazioni qualunque. La sua potenza risiede in un'elevata modularità, che consente agli autori di attacchi di sfruttare le sue varie funzionalità, come il furto di altri dati sensibili e il download/la distribuzione di altro malware per raggiungere l'obiettivo finale o favorire l'attacco. Nel 2021, Ramnit era considerato il principale trojan bancario, con notizie recenti che citavano come un altro malware condividesse un codice simile con Ramnit.

La presenza di infostealer nella vostra rete è un segnale rivelatore che le credenziali utente potrebbero essere a rischio. Le informazioni rubate raccolte potrebbero essere vendute nei mercati clandestini e utilizzate per ottenere l'accesso iniziale da parte di altri criminali. I gruppi di ransomware potrebbero distribuire un infostealer tramite phishing o botnet per ottenere credenziali valide, noleggiare una licenza di accesso a un infostealer in un forum clandestino che offre MaaS o acquistare l'accesso alla rete tramite IAB. In alcuni casi, gli operatori infostealer potrebbero diventare IAB e vendere credenziali di alto valore raccolte (come l'accesso VPN o RDP) ai migliori offerenti o ad altri autori di attacchi che potrebbero sferrare un attacco molto più sofisticato.

Strumenti per l'accesso remoto

Cobalt Strike è stato abusato da diversi gruppi di autori di attacchi nell'ambito delle loro operazioni. Esistono vari mezzi in cui questo potente RAT viene utilizzato dagli autori di attacchi, tra cui ricognizione, escalation dei privilegi, movimento laterale sulla rete, applicazione della persistenza, esecuzione remota del payload dopo l'intrusione (come il ransomware) ed esfiltrazione di dati. Sebbene lo strumento venga utilizzato principalmente dopo la violazione per il movimento laterale e l'esfiltrazione, è anche in grado di essere il vettore di accesso iniziale, in quanto dispone di un modulo di spear phishing. I gruppi noti per utilizzare questo strumento sono Conti, Qakbot, TrickBot ed Emotet, solo per citarne alcuni. Per facilitare il rilevamento di Cobalt Strike in un ambiente, è stato creato questo set di regole YARA per determinare l'uso dannoso dello strumento.

I nostri dati mostrano anche la presenza di traffico C2 di Agent Tesla. Questo RAT viene venduto nel mercato clandestino e il suo prezzo accessibile e la facilità d'uso rendono questo strumento attraente per i criminali informatici. Gli autori di attacchi potrebbero utilizzare questo strumento per raccogliere credenziali da vari browser, acquisire sequenze di tasti premuti e screenshot e registrare i tasti digitati. Una delle sue tattiche degne di nota è il form grabbing (acquisizione di moduli), che consente agli autori di attacchi di raccogliere PII e altre informazioni sensibili. Tali informazioni rubate potrebbero essere utilizzate per furti di identità o frode. PCrisk ha pubblicato maggiori dettagli sulle tecniche di Agent Tesla e il suo impatto sugli utenti colpiti.

Il panorama delle attività mostra sporadiche campagne di malware nel corso dell'anno

Nel corso di un anno, abbiamo osservato fluttuazioni nelle attività del malware C2 (Figura 6). Un esempio: Emotet è stato particolarmente attivo nei mesi di gennaio e febbraio 2022, dopo il suo ritorno nel novembre 2021. Questo aumento dell'attività dimostra una formidabile campagna per aiutarlo a riconquistare il suo status dopo mesi di inattività. Nei mesi successivi al suo ritorno, Emotet ha migliorato le sue tattiche includendo modi per aggirare l'azione di Microsoft per disabilitare le macro di Visual Basic, Applications Edition. Alcuni rapporti indicano che Emotet era diventato nuovamente inattivo tra luglio e novembre del 2022; dai dati osservati risulta un calo del traffico C2 a luglio, confermato dalla minore percentuale di dispositivi infetti che hanno raggiunto i domini Emotet. Ciò potrebbe indicare che il gruppo è rimasto attivo per tutto l'anno o potrebbe trattarsi di un caso di malware installato che sta ancora comunicando con un'infrastruttura obsoleta. Le osservazioni nel 2023 potrebbero aiutarci a determinare se il gruppo Emotet sia effettivamente inattivo.

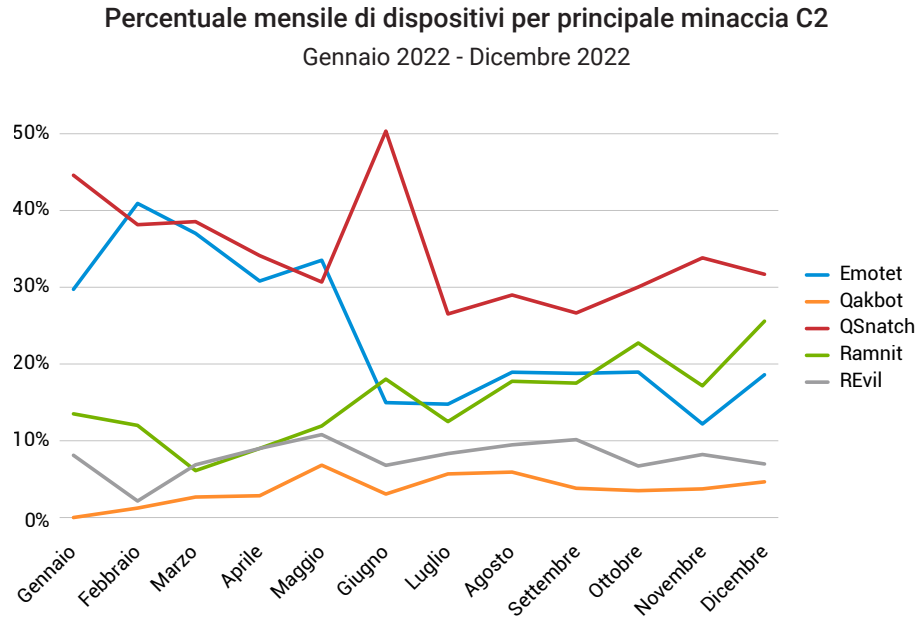


Figura 6: Il grafico delle tendenze mensili mostra che QSnatch è stato costantemente attivo per tutto il 2022

> **Emotet è stato particolarmente attivo nel periodo tra gennaio e febbraio 2022, dopo il suo ritorno nel novembre 2021. Questo aumento dell'attività dimostra una formidabile campagna per aiutarlo a riconquistare il suo status dopo mesi di inattività.**

QSnatch è risultato costantemente attivo tutto l'anno, con un picco intorno a giugno, a dimostrazione di quanto sia diventata diffusa questa minaccia. I server NAS sono obiettivi possibili per gli autori di attacchi per diversi motivi: in primo luogo, contengono dati sensibili; secondo, le probabilità che ai server NAS vengano applicate patch sono inferiori; e, in terzo luogo, questi dispositivi sono potenzialmente più accessibili nella rete dell'organizzazione e potrebbero fungere da hub per il movimento laterale. Nonostante negli ultimi anni vi siano stati alcuni cambiamenti, come l'aggiunta di soluzioni per la sicurezza integrate, i criminali informatici li hanno aggirati disabilitando i prodotti di sicurezza installati e/o impedendo l'aggiornamento dei dispositivi con nuove correzioni. Pertanto, questi dispositivi rimangono vulnerabili contro questi nuovi malware.

Abbiamo osservato anche una crescente presenza di Ramnit nelle reti aziendali da agosto a dicembre. Ciò è preoccupante in quanto questo malware potrebbe sottrarre un'ampia gamma di informazioni sensibili che gli autori di attacchi potrebbero successivamente vendere ad altri criminali per attacchi futuri.

QSnatch ed Emotet: minacce comuni in tutte le regioni

Per determinare le minacce prevalenti per ciascuna regione, abbiamo esaminato la percentuale di dispositivi della singola regione che raggiungono i domini C2 (Figura 7). Ogni percentuale è relativa al numero di dispositivi interessati per regione, anch'esso diverso a seconda della regione. È interessante notare che stiamo assistendo a tendenze di attacco simili in tutte le regioni, anche se con pochissimi valori anomali. Raccomandiamo pertanto che ogni regione segua le raccomandazioni fornite nella sezione "Conclusioni e raccomandazioni" o quelle relative a ciascun gruppo di malware nelle sezioni precedenti.

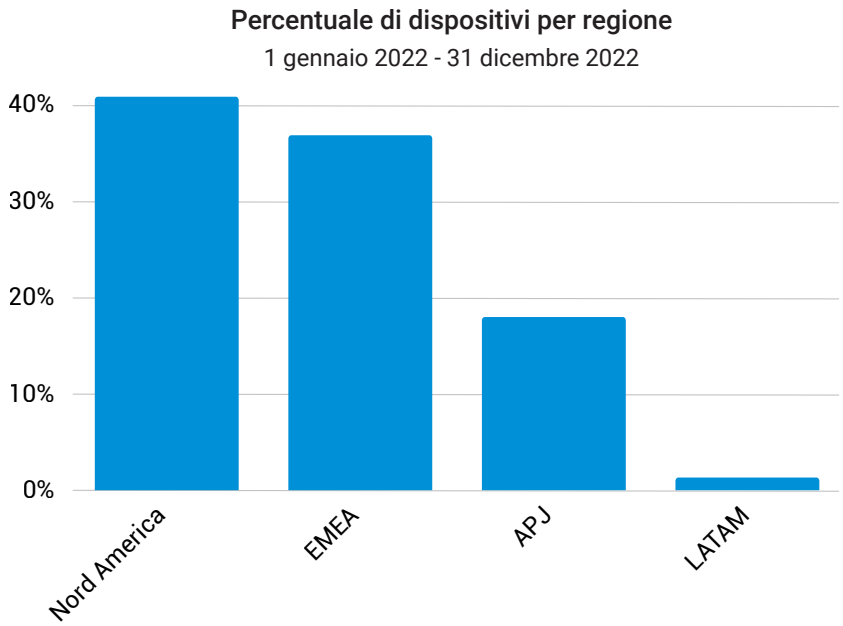


Figura 7: Il Nord America è in testa con il 41%, seguito dall'area EMEA (37%) e dall'area APJ (18%), per quanto riguarda il numero di dispositivi colpiti per regione

Nord America

La maggior parte delle organizzazioni a livello globale ha subito queste due maggiori minacce: QSnatch e Emotet. In Nord America, circa il 29% dei dispositivi colpiti all'interno della regione è stato attaccato da Emotet, mentre il 33% è stato vittima di QSnatch (Figura 8). Secondo un rapporto di Dark Reading, una ricerca di Shodan ha mostrato che ci sono 300.000 dispositivi QNAP connessi a Internet, il che li rende un obiettivo interessante. Inoltre, i dispositivi NAS come QNAP possono essere utilizzati come backup e fungere da media o file server.

Altre minacce degne di nota in Nord America includono Ramnit, Qakbot e REvil. Ciò è un fatto interessante, dato che gli IAB come Emotet hanno spianato la strada ad altre infezioni, incluso (a titolo di esempio) il ransomware.

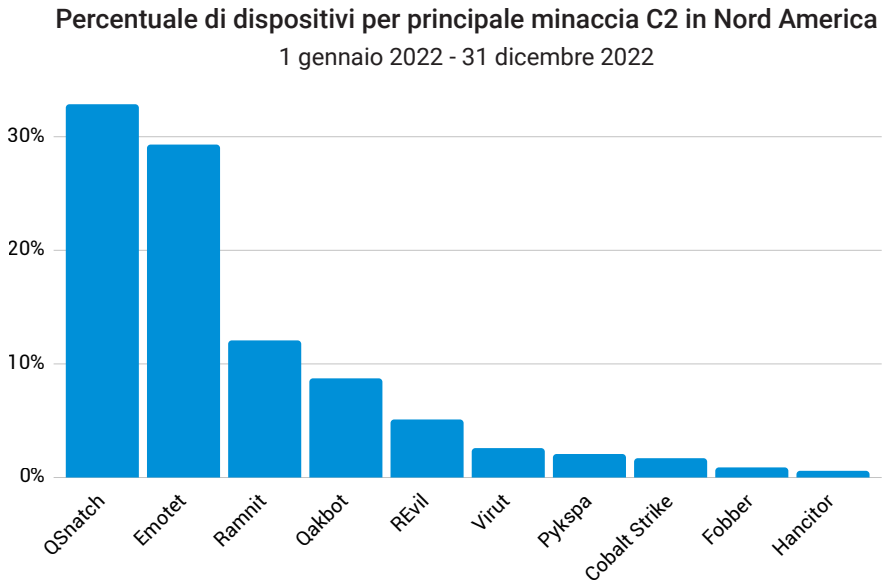


Figura 8: La maggior parte dei dispositivi colpiti nelle organizzazioni nordamericane ha avuto accesso a domini relativi a QSnatch, Emotet e Ramnit almeno una volta

Europa, Medio Oriente e Africa

L'area EMEA presenta la più alta percentuale di dispositivi colpiti insieme al Nord America. Le principali minacce che abbiamo rilevato nella regione (Figura 9) includevano QSnatch (28%) e Ramnit (21%). Non sorprende vedere l'ascesa di Ramnit nella regione, poiché in passato i suoi operatori hanno preso di mira istituzioni bancarie/finanziarie in Italia, Regno Unito e Francia. In una delle sue iterazioni, la configurazione di Ramnit includeva i paesi dell'UE come obiettivi principali. Infatti, se si confronta il numero di dispositivi colpiti da Ramnit a livello globale, l'area EMEA ha registrato il maggior numero di infezioni da Ramnit. Inoltre, anche i dispositivi con infezione da Emotet erano numerosi nella regione, pari al 19%.

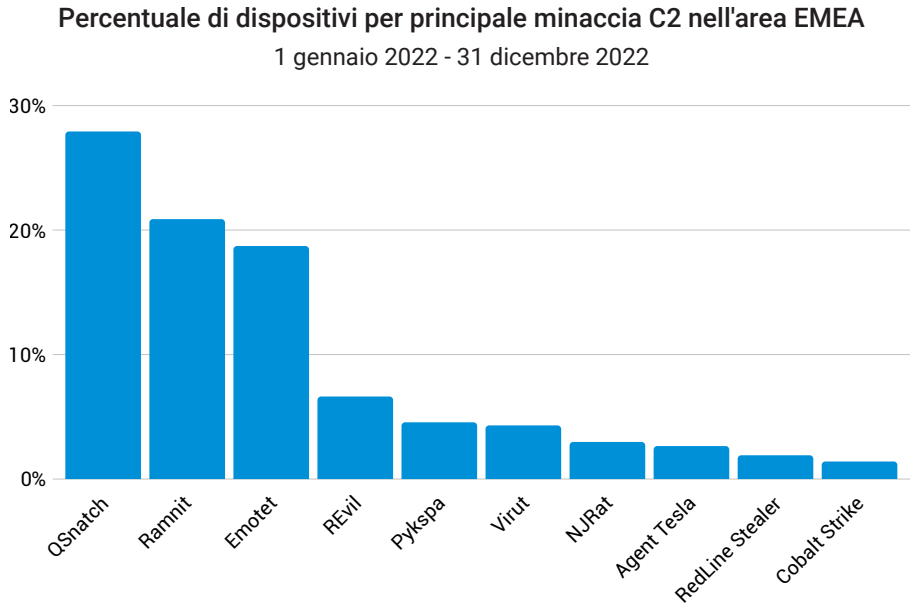
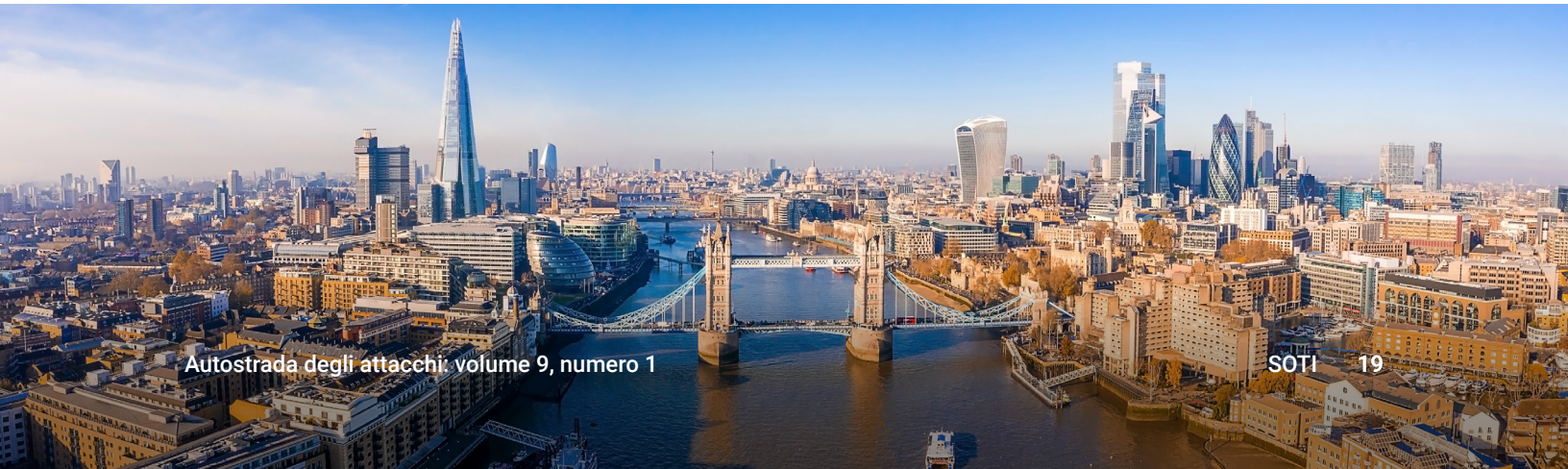


Figura 9: Abbiamo osservato più dispositivi raggiungere Ramnit C2 in EMEA che in altre regioni, aumentando significativamente il rischio delle loro organizzazioni



Asia Pacifico e Giappone

Nell'area APJ, abbiamo osservato che le infezioni da QSnatch hanno avuto un impatto significativo sulla regione (Figura 10). Se confrontiamo i numeri di ogni regione, l'area APJ è al secondo posto dopo il Nord America in termini di dispositivi con infezioni QSnatch. D'altra parte, l'area APJ dovrebbe anche prestare attenzione agli attacchi ransomware di tipo REvil e LockBit poiché si sono attestati tra le prime cinque minacce rilevate nei dispositivi interessati nella regione. Anche se i membri del gruppo REvil sono stati arrestati lo scorso anno, questo malware è stato rivisto in circolazione diversi mesi dopo. È possibile che i vecchi membri che hanno accesso al codice abbiano tentato di riutilizzare REvil. Non sorprende osservare minacce ransomware (che presentano largamente motivazioni finanziarie) come LockBit e REvil. E poiché gli operatori RaaS continuano a sfruttare IAB come Emotet, il ransomware rimarrebbe una sfida di sicurezza critica per le aziende di tutti i settori e le regioni.

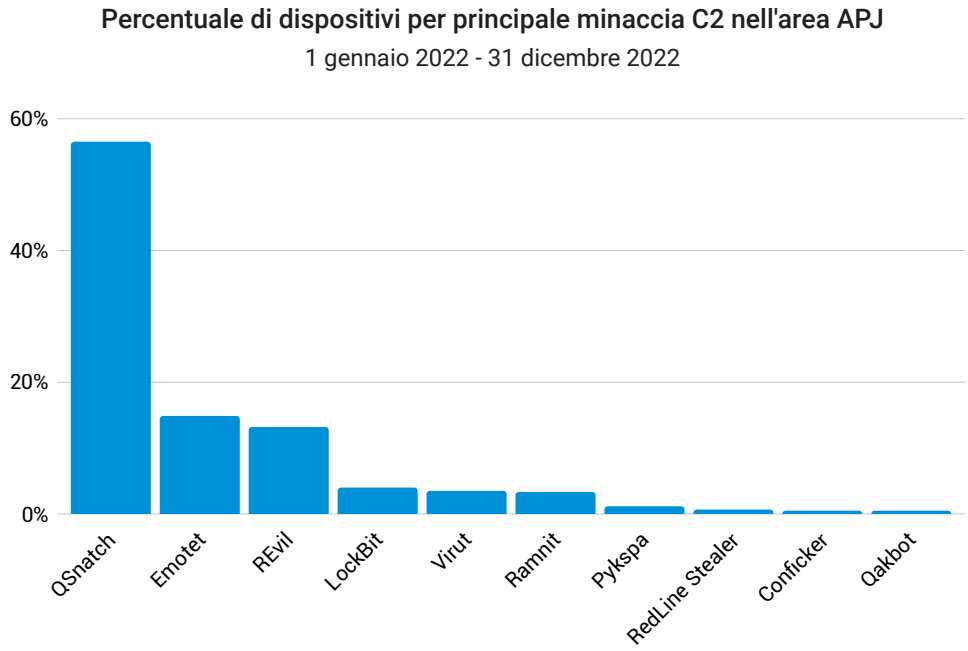


Figura 10: Akamai ha osservato un numero significativo di infezioni da QSnatch nella regione

America Latina

Esaminiamo ora le tendenze nell'area LATAM. Sebbene questa regione presenti il minor numero di dispositivi colpiti, ciò non significa necessariamente che sia meno presa di mira o soggetta ad impatti negativi. Analogamente alle tendenze globali, questa regione è stata influenzata da QSnatch ed Emotet (Figura 11). Un semplice esame di questa singola regione rivela che Agent Tesla, Virut e Ramnit sono prominenti.

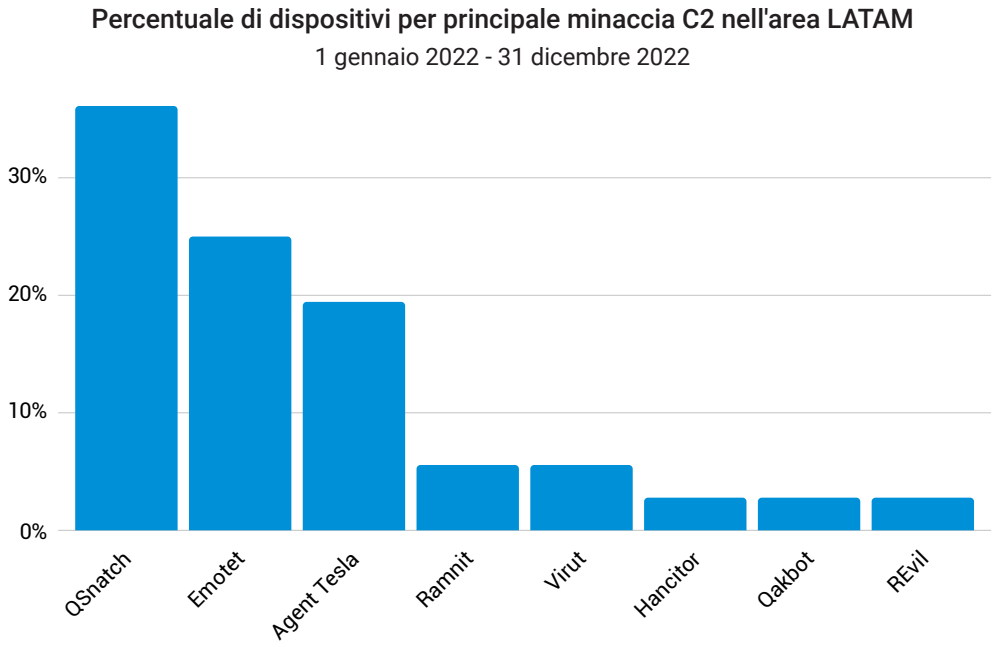
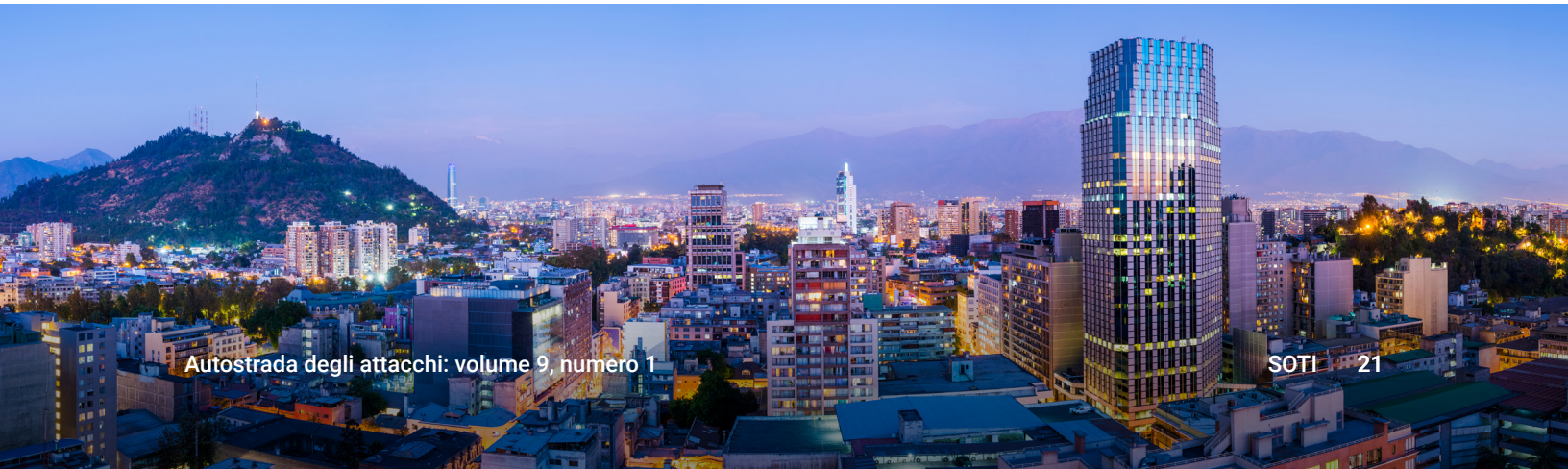


Figura 11: Le tendenze globali sono rispecchiate anche nel panorama delle minacce dell'area LATAM

Le suddivisioni regionali sono importanti non solo per notare le similarità, ma anche per identificare quali minacce specifiche sono esclusive per ciascuna regione. Sebbene QSnatch sia sempre la principale famiglia di minacce, le successive quattro principali minacce variano da regione a regione con una combinazione di Emotet, REvil, Ramnit e Agent Tesla. Le minacce regionali sono molto utili per decidere su cosa dovrebbero concentrarsi i vostri team di gestione delle vulnerabilità e dei test di penetrazione.



Tendenze del settore e dei segmenti verticali: settore manifatturiero fortemente colpito da IAB e botnet

Un'analisi delle tendenze del settore ci consente di osservare il livello di rischio di ogni singolo segmento verticale e come se la cava rispetto ad altri settori. Invece di esaminare il numero di dispositivi colpiti, abbiamo aggregato i dispositivi in base ai clienti per stabilire quante aziende sono soggette a impatti negativi per segmento verticale (Figura 12). In base ai nostri dati DNS, abbiamo osservato che oltre il 30% delle organizzazioni analizzate con traffico C2 dannoso si trova nel settore manifatturiero. Inoltre, sono state colpite le aziende nei settori dei servizi alle imprese (15%), dell'high-tech (14%) e del commercio (12%). I primi due segmenti verticali nei nostri dati DNS (settore manifatturiero e dei servizi aziendali) sono anche i principali settori colpiti dal ransomware Conti, che abbiamo affrontato nel nostro rapporto sul ransomware globale. In tale rapporto, abbiamo esaminato nei dettagli le vittime del ransomware Conti e le abbiamo profilate in base a segmento verticale, ricavi e regione, illustrando le tendenze di attacco di questa prolifica minaccia.

> **In base ai nostri dati DNS, abbiamo osservato che oltre il 30% delle organizzazioni analizzate con traffico C2 dannoso si trova nel settore manifatturiero. Inoltre, sono state colpite in modo simile le aziende nei settori dei servizi alle imprese (15%), dell'high-tech (14%) e del commercio (12%).**

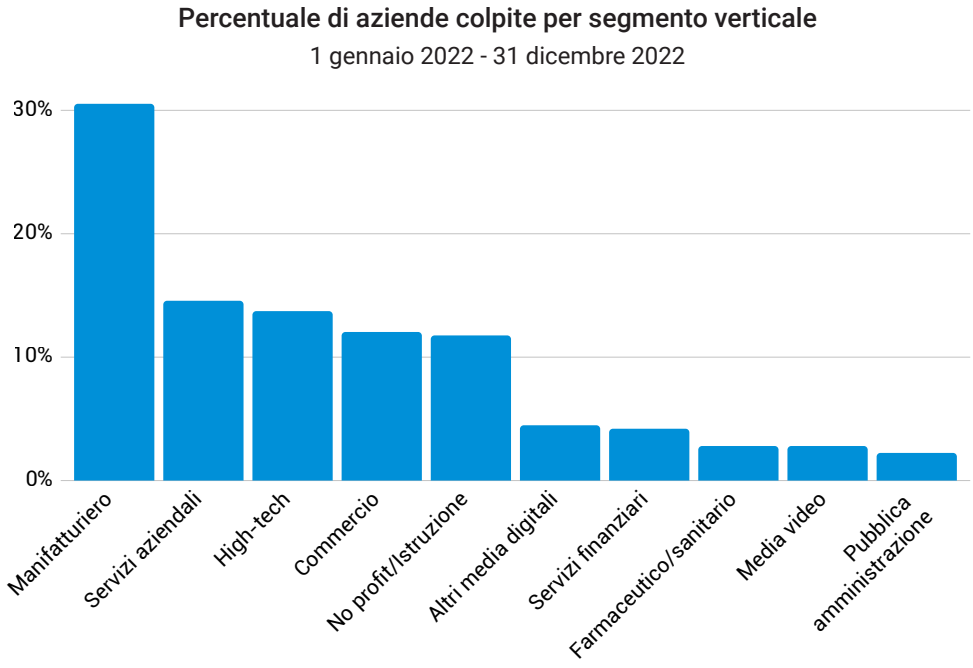


Figura 12: I settori manifatturiero, dei servizi alle imprese e high-tech sono i più colpiti dalle infezioni da C2

Il fatto che stiamo osservando che il settore manifatturiero sia pesantemente colpito da vari attacchi C2 è preoccupante poiché è considerato un'infrastruttura critica e gli attacchi riusciti a questo settore potrebbero potenzialmente causare effetti concreti, come interruzioni della supply chain. I dati non dimostrano ragioni specifiche per cui il settore manifatturiero sia il segmento verticale più colpito, ma un'indagine più approfondita sui tipi di minaccia in questo settore potrebbe fornire alcune informazioni.

Abbiamo osservato che alcuni paesi utilizzano le normative per rafforzare la sicurezza in settori critici come quello manifatturiero. La normativa europea denominata NIS2 ha rafforzato gli standard di cybersicurezza e i requisiti di sicurezza, come l'analisi dei rischi e le policy di sicurezza dei sistemi informatici, la sicurezza della supply chain e la gestione degli incidenti per entità essenziali (ad esempio, energia, trasporti, banche, sanità, ecc.). Ha anche ampliato l'ambito dei settori verticali interessati.

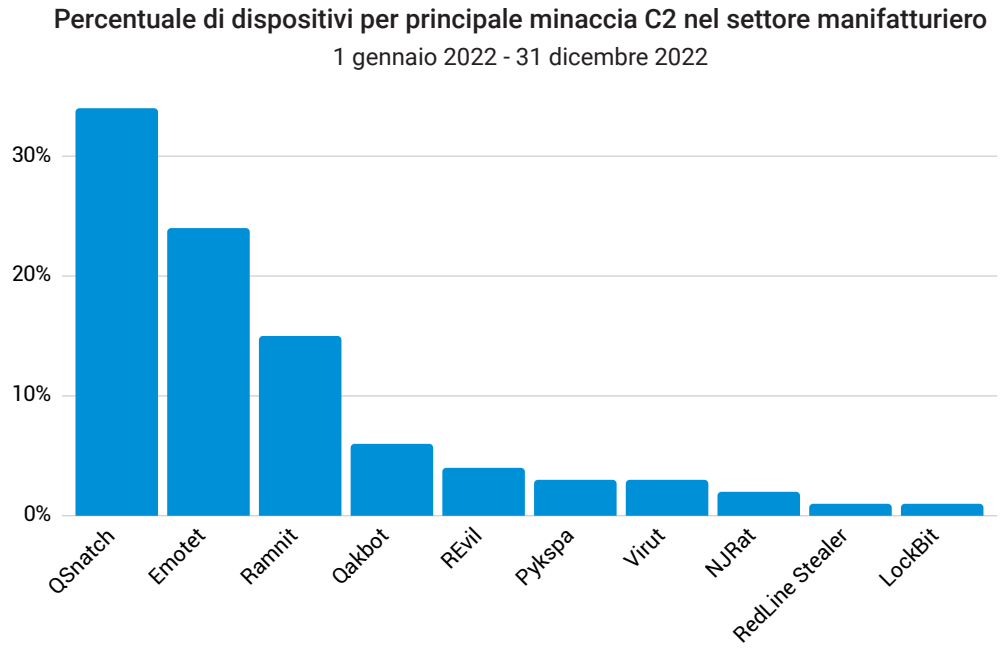


Figura 13: Le principali famiglie di minacce C2 rilevate nel settore manifatturiero sono QSnatch, Emotet e Ramnit

Uno sguardo approfondito al settore manifatturiero rivela che QSnatch, IAB e Ramnit sono alcuni dei principali domini correlati a C2 a cui le organizzazioni in questo segmento verticale hanno effettuato l'accesso (Figura 13). La presenza di IAB nella loro rete potrebbe essere indicativa del fatto che gli autori di attacchi stanno raccogliendo informazioni sui loro potenziali obiettivi e, una volta che hanno accesso ai computer compromessi, possono vendere tali dati ad altri criminali informatici come i gruppi RaaS. Inoltre, osserviamo che anche gli infostealer figurano nell'elenco del malware C2 che sta minacciando questo settore. Una minaccia a cui prestare attenzione è RedLine Stealer, che ha la capacità di raccogliere informazioni sul browser, come credenziali e dettagli delle carte di credito, e viene attualmente venduto come MaaS, in forma di abbonamento mensile a 100-150 dollari USA. Secondo una ricerca di Group-IB, questo infostealer ha raccolto circa 35.585.412 log, che potrebbero contenere account Single Sign-On, tra il 2° semestre 2021 e il 1° semestre 2022. Inoltre, i domini C2 relativi a questo infostealer sono aumentati del 409% solo nel terzo trimestre del 2022.

Le tendenze del settore sono sempre interessanti da monitorare. Ciò che sta accadendo in un segmento è spesso solo un punto di partenza mentre i criminali informatici si fanno strada in tutti i segmenti verticali del settore. A volte, osserviamo che gli autori di attacchi si concentrano su una tecnologia importante in un settore. Altre volte, attaccano i settori che offrono una maggiore probabilità di profitto o quelli che consentono di ottenere i maggiori profitti.
Li abbiamo anche visti operare in settori che tradizionalmente non investono tanto nella sicurezza informatica. Il concetto chiave è che se si vede del fumo nella porta accanto, è consigliabile controllare il proprio sistema antincendio.

Utenti domestici sotto attacco

Gli autori di attacchi puntano gli occhi sulle aziende perché, nel caso in cui riescano a violare le loro reti, ottengono un guadagno maggiore. Essi utilizzano un'ampia gamma di strumenti e tattiche per infiltrarsi in un perimetro aziendale, mantenere la persistenza e, in alcuni casi, esfiltrare informazioni riservate. Per tale motivo, osserviamo minacce come infostealer e IAB nelle reti aziendali, come discusso nella sezione precedente. Tuttavia, le reti domestiche rappresentano uno scenario diverso, per quanto riguarda quali minacce vengono impiegate e a quale scopo.

Gli utenti domestici rappresentano un segmento che, spesso, non è sicuro come un ambiente aziendale, ma non ha lo stesso ritorno economico. I criminali lo sanno bene e, pertanto, cercano dei modi per monetizzare la loro capacità di infettare più facilmente i dispositivi domestici, lanciando, ad esempio, campagne su larga scala nell'intento di compromettere quanti più dispositivi possibile con tecniche "spray and pray", mentre gli attacchi alle aziende sono più mirati. Una volta che questi dispositivi domestici diventano parte di un'enorme botnet, gli autori di attacchi potrebbero mobilitare questi dispositivi "zombie" per eseguire una moltitudine di attività di crimine informatico all'insaputa dell'utente, come lo spamming e il lancio di attacchi DDoS contro organizzazioni. E affinché le botnet abbiano successo o i criminali informatici possano noleggiare le loro botnet, devono infettare quanti più dispositivi possibile. Un altro modo per gli autori di attacchi di guadagnare finanziariamente dall'impatto sugli utenti domestici è utilizzare le risorse informatiche dei dispositivi infetti per scopi di cryptomining.

> **Una volta che questi dispositivi diventano parte di un'enorme botnet, gli autori di attacchi potrebbero mobilitare questi dispositivi "zombie" per eseguire una moltitudine di attività di crimine informatico all'insaputa dell'utente, come lo spamming e il lancio di attacchi DDoS contro organizzazioni.**

Le reti domestiche registrano un traffico intenso proveniente dalle botnet

Spostando il nostro interesse sugli utenti domestici, esamineremo il traffico DNS dannoso delle reti domestiche analizzando un campione anonimo delle milioni di query segnalate negli ultimi sei mesi, al fine di dimostrare quali minacce devono preoccupare gli utenti. A prima vista, le principali minacce riguardano le botnet, il che potrebbe spiegare come gli autori di attacchi stiano sfruttando i dispositivi IoT per scopi diversi, di cui parleremo nelle sezioni successive.

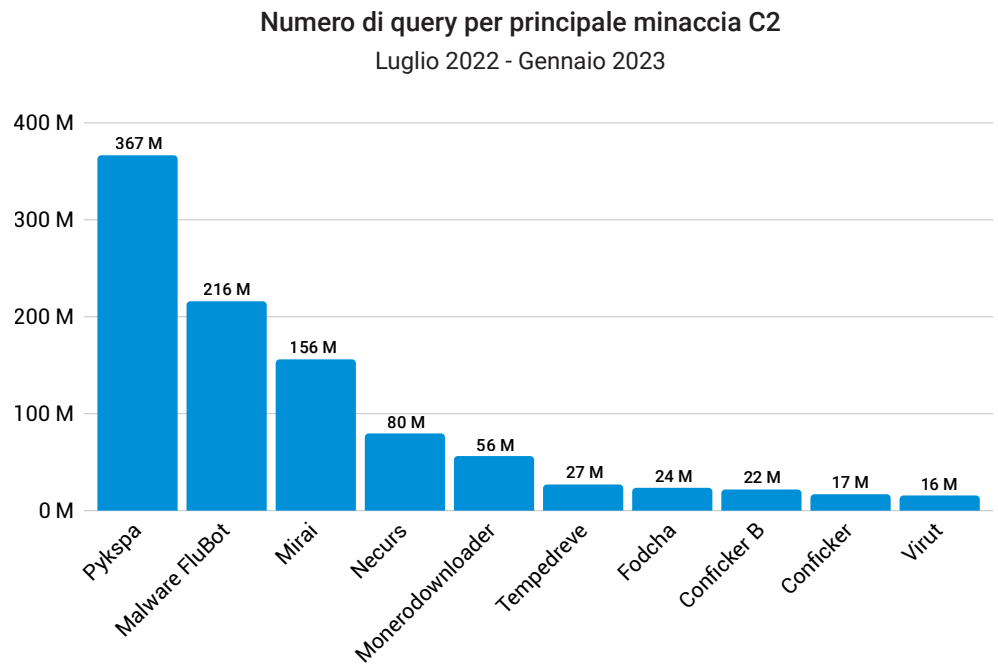


Figura 14: Pykspa, il malware FluBot e Mirai sono le tre principali botnet osservate nel traffico DNS delle reti domestiche

Pykspa: propagazione tramite i social media

Sulla base dei risultati dei nostri dati, Pykspa ha causato 367 milioni di query DNS rilevate a livello globale (Figura 14). Questa minaccia si diffonde tramite Skype inviando link dannosi ai contatti degli utenti colpiti. In alcuni casi, quando Twitter viene aperto nella scheda del browser, creerà anche un tweet con un link per il download del malware. Inoltre, utilizza un algoritmo di generazione del dominio (DGA) per stabilire la comunicazione C2. In passato, la sua v2 utilizzava un sottoinsieme della sua DGA per evitare di essere rilevata e rimanere all'interno della rete per un periodo più lungo.

Le sue funzionalità backdoor consentono a un utente malintenzionato di connettersi a un sistema remoto ed eseguire comandi arbitrari come scaricare file, terminare processi e propagarsi attraverso vari mezzi (ad esempio, unità mappate, condivisioni di rete), tra gli altri. Pykspa invia query anche alla configurazione di Skype per raccogliere dati personali sugli utenti colpiti. Impedisce inoltre agli utenti di accedere a determinati siti web, in particolare se contengono determinate stringhe relative a soluzioni antimalware. In particolare, Pykspa controlla l'interfaccia linguistica della versione Skype dell'utente colpito e, se rientra in una delle tante lingue monitorate, tra cui inglese, tedesco, francese, spagnolo e italiano, il malware modifica di conseguenza il messaggio Skype inviato come spam.

FluBot: botnet malware Android

Il malware FluBot è la principale famiglia di malware C2 dopo Pykspa. Infetta principalmente i telefoni Android tramite messaggi di testo, invitando gli utenti a fare clic su un link dannoso, che successivamente comporta il download del malware. Come parte della sua tattica di propagazione, il malware FluBot carica gli elenchi di contatti degli utenti colpiti sul server C2 e invia anche i contatti delle vittime con la stessa esca di social engineering. Per gli utenti, avere FluBot sul proprio dispositivo mette a rischio le proprie informazioni bancarie e finanziarie poiché questo malware ha la capacità di sovrapporre una pagina fittizia quando gli utenti accedono ad app bancarie legittime. Pertanto, queste credenziali potrebbero essere utilizzate per il furto di identità o per effettuare transazioni fraudolente.

Questo malware utilizza varie esche di social engineering. Ad esempio, potrebbe suggerire agli utenti di fare clic su un link per verificare lo stato della consegna di un pacco; in altre situazioni, può indurre gli utenti a scaricare un'app di messaggi vocali fittizia dicendo loro che è presente un messaggio vocale. Potrebbe anche fingere di essere un aggiornamento della sicurezza e invitare gli utenti a fare clic sul link. Una volta che gli utenti fanno clic sul link, viene chiesto loro di scaricare un'app. Questa app, a sua volta, richiede l'autorizzazione per accedere agli elenchi di contatti ed effettuare telefonate, ecc. Ciò che rende questa minaccia così pericolosa è che richiede anche l'autorizzazione per i servizi di accessibilità che consentono agli autori di attacchi di controllare i tocchi dello schermo, potendo potenzialmente causare l'installazione di più app. Si consiglia agli utenti di ripristinare le impostazioni di fabbrica dei propri dispositivi per rimuovere questo malware.

Mirai: sfruttamento della potenza dell'Internet of Things per causare interruzioni su larga scala

Nella nostra ricerca, Mirai segue da vicino il malware FluBot, con 156 milioni di query DNS rilevate. Conosciuta per aver preso di mira i dispositivi IoT con porte telnet aperte, Mirai è diventata famosa per l'attacco DDoS contro uno dei maggiori provider DNS. Questo worm autopropagante cerca dispositivi vulnerabili che utilizzano combinazioni predefinite di nome utente e password. Ad un certo punto, ha raggruppato oltre 100.000 dispositivi "zombie" che gli autori di attacchi hanno utilizzato negli attacchi DDoS contro obiettivi di alto profilo. In uno dei suoi precedenti attacchi, Mirai ha sfruttato 145.000 dispositivi per attaccare un'azienda tecnologica. Questo è un esempio di come i dispositivi non sicuri potrebbero essere utilizzati come armi per commettere attacchi informatici e causare interruzioni su larga scala contro le aziende.

Nel 2016, il gruppo responsabile di Mirai ha rilasciato il codice sorgente, forse per impedire alle forze dell'ordine di risalire agli autori originali (e quindi evitare l'arresto). Con questo, altri gruppi hanno iniziato a utilizzare il codice di Mirai, modificandolo e potenziandolo con più funzionalità, come la possibilità di infettare i sistemi. Uno degli effetti del rilascio del codice è che abbiamo rilevato nuove varianti, come Okiru, Satori, Masuta e PureMasuta, con lo scopo di lanciare anche attacchi DDoS. Sebbene il riavvio del dispositivo infetto sia utile, poiché il malware esegue costantemente la scansione dei dispositivi, è molto probabile che venga reinfettato a meno che l'utente non modifichi le proprie password.

Necurs: distributore di malware e venditore di accessi

La botnet Necurs, individuata per la prima volta nel 2012, ha causato 80 milioni di query segnalate negli ultimi sei mesi. Rappresenta un serio rischio sia per gli utenti domestici che per le organizzazioni per la sua funzionalità in grado di distribuire altri payload di malware come, ad esempio, Dridex, TrickBot e Locky. Un fattore degno di nota che vale la pena evidenziare è che questa botnet vende anche l'accesso ai computer infetti ad altri gruppi come parte delle sue offerte di botnet a noleggio. Come la maggior parte delle botnet, utilizza un DGA per rendere disponibili più domini per i propri server C2 e per proseguire le sue operazioni nonostante i domini siano bloccati.

Oltre a distribuire ransomware e trojan bancari, Necurs viene utilizzato anche per distribuire vari attacchi di spam, come truffe di siti di incontri russi, truffe farmaceutiche e così via. Durante un'indagine, Microsoft ha monitorato le attività di questa botnet e ha scoperto che in soli 58 giorni ha inviato circa 3,8 milioni di messaggi e-mail di spam. Nel 2020, le operazioni della botnet Necurs sono state interrotte grazie alla collaborazione delle forze dell'ordine e della comunità della sicurezza.

Monerodownloader: botnet di mining

Uno dei molti modi in cui gli autori di attacchi ottengono profitti è utilizzare computer compromessi per il cryptomining. La crescente popolarità della criptovaluta Monero tra i criminali informatici è uno dei motivi per cui osserviamo botnet create appositamente per eseguire il mining. Gli autori di attacchi preferiscono questa criptovaluta poiché la catena non è così esposta e offre anonimato; pertanto, non viene ricondotta a loro. Sebbene si sappia molto poco su Monerodownloader, alcune delle tattiche che esegue includono la raccolta di informazioni e la connessione ai server C2 per il payload effettivo.

Lasciare i sistemi senza patch apre la strada a minacce come i cryptominer Monero. Altri coinminer Monero simili sfruttano le vulnerabilità, si propongono come software gratuito per indurre gli utenti a scaricare il miner e sono in grado di spostarsi lateralmente sulla rete e infettare altri dispositivi per ottenere più guadagni possibili. Sebbene la descrizione del movimento laterale sia più applicabile alle aziende che agli utenti domestici, questo ci dà un'idea di come lavorano i cryptominer per massimizzare l'infezione.

Principali minacce per regione: le botnet continuano a dominare nelle reti domestiche

Diamo un'occhiata più da vicino ai nostri dati regionali per chiarire quali botnet specifiche sono prevalenti per ciascuna regione in base al traffico DNS delle reti domestiche e per esaminare alcuni possibili fattori che contribuiscono a tale tendenza.

Nord America

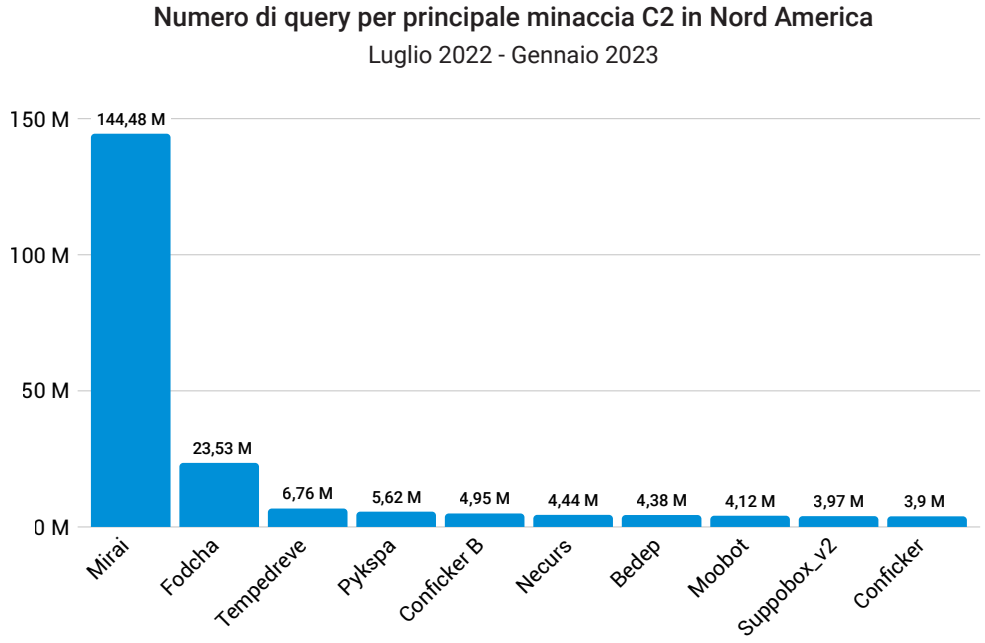


Figura 15: Mirai continua a creare problemi in Nord America potenzialmente a causa di dispositivi IoT non sicuri

In Nord America, nelle reti domestiche sono state rilevate oltre 144 milioni di query associate alla botnet Mirai (Figura 15). Questa botnet prende di mira i dispositivi IoT vulnerabili che utilizzano ancora nomi utente e password predefiniti. L'elevato volume di query provenienti da questa regione potrebbe essere dovuto alla popolarità o all'elevato utilizzo dei dispositivi IoT nelle famiglie. Solo nel 2022, secondo quanto riferito, le famiglie statunitensi avevano una media di 22 dispositivi connessi, che sono leggermente diminuiti rispetto ai 25 dell'anno precedente. E con l'aumento previsto delle connessioni IoT in Nord America (5,4 miliardi entro il 2025), c'è un'alta probabilità che altre minacce come Mirai, o varianti simili, abusino di dispositivi IoT non sicuri.

Per gli utenti domestici, l'impatto di una tale minaccia è che i criminali informatici possono sfruttare i loro dispositivi a loro insaputa per commettere crimini. Ma anche le organizzazioni risentono degli effetti degli attacchi DDoS o persino di campagne di spam dannose lanciati da botnet come Mirai. Come best practice, è consigliabile cambiare il nome utente e la password predefiniti dei vostri dispositivi per proteggerli da Mirai e altri attacchi simili.

Europa, Medio Oriente e Africa

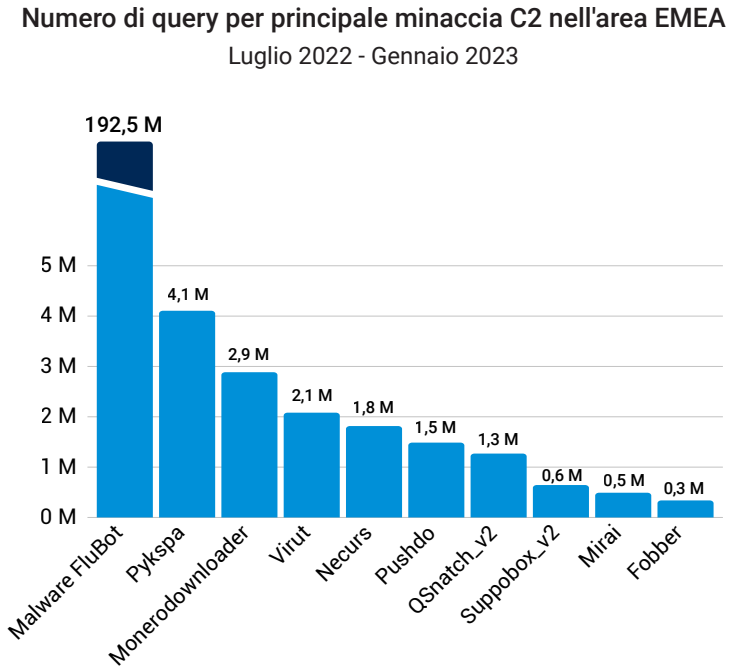


Figura 16: Abbiamo assistito a un attacco di malware FluBot nella regione EMEA, probabilmente a causa della sua tattica di propagazione e dell'uso di diverse lingue europee nella sua esca di social engineering

Dire che il malware FluBot si sta diffondendo a macchia d'olio nell'area EMEA sarebbe un eufemismo. L'enorme volume delle query DNS osservate in questa regione (circa 193 milioni) è notevole. E tramite il nostro esame del traffico DNS, Akamai è stata in grado di rilevare queste infezioni nell'area EMEA (Figura 16). Un fattore che contribuisce è la sua tattica di propagazione dello "smishing", una forma di phishing in cui l'autore di attacchi invia SMS all'elenco dei contatti della vittima. Inoltre, induce gli utenti a scaricare un'app correlata a un'app di consegna pacchi o di messaggi vocali che in realtà è il malware. Oltre a questo, FluBot richiede autorizzazioni aggiuntive e registra segretamente le credenziali bancarie/finanziarie degli utenti a loro insaputa. Secondo quanto riferito, ha preso di mira utenti in Spagna, Germania, Finlandia e Regno Unito, tra gli altri. L'SMS è scritto anche in molte altre lingue dell'UE, come il tedesco e l'ungherese, il che potrebbe essere uno dei tanti fattori per i quali la diffusione di questo malware è aumentata in Europa.

America Latina

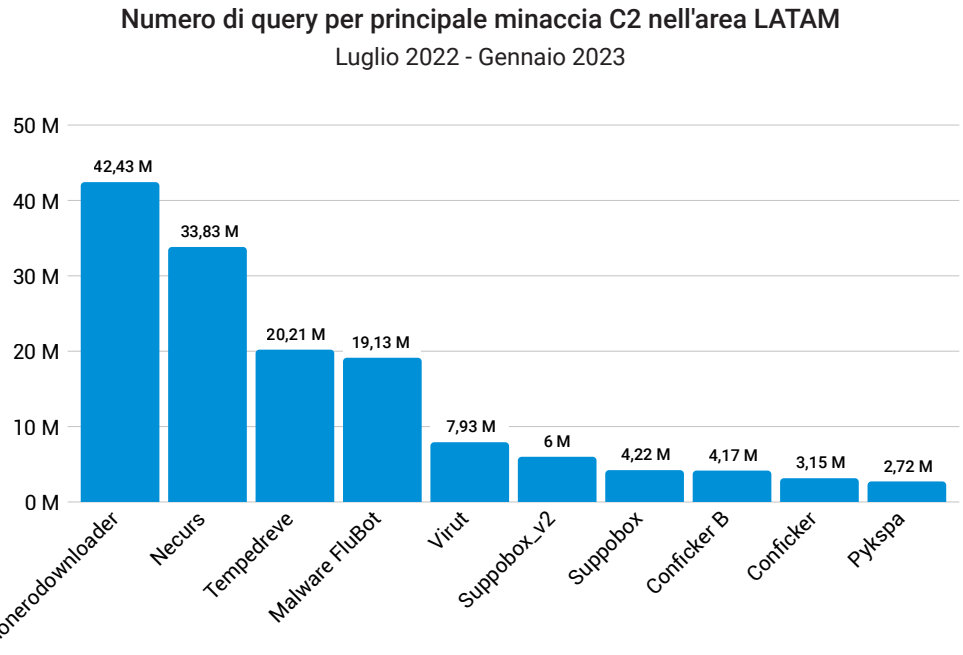


Figura 17: La botnet di cryptomining Monerodownloader è diventata la principale minaccia in America Latina, forse a causa dell'elevato utilizzo di criptovalute nella regione

A differenza del Nord America e dell'area EMEA, l'area LATAM ha mostrato una distribuzione più diversificata delle botnet (Figura 17). Monerodownloader, una botnet di cryptomining, è in testa alla lista dei gruppi di botnet attivi con 42 milioni di query rilevate, seguita da Necurs (34 milioni) e Tempedreve (20 milioni). L'elevato tasso di adozione della criptovaluta nella regione, alimentato dall'elevata inflazione e dalle rimesse, potrebbe spiegare perché botnet come Monerodownloader siano in cima alla lista. All'insaputa dell'utente, i criminali informatici potrebbero utilizzare le risorse dei dispositivi degli utenti per scopi di mining e per il proprio guadagno finanziario. Vale anche la pena notare che FluBot è una delle principali minacce osservate nel traffico DNS, il che dimostra la prevalenza della botnet anche al di fuori della regione EMEA, dove abbiamo registrato un elevato volume di traffico.

Asia Pacifico e Giappone

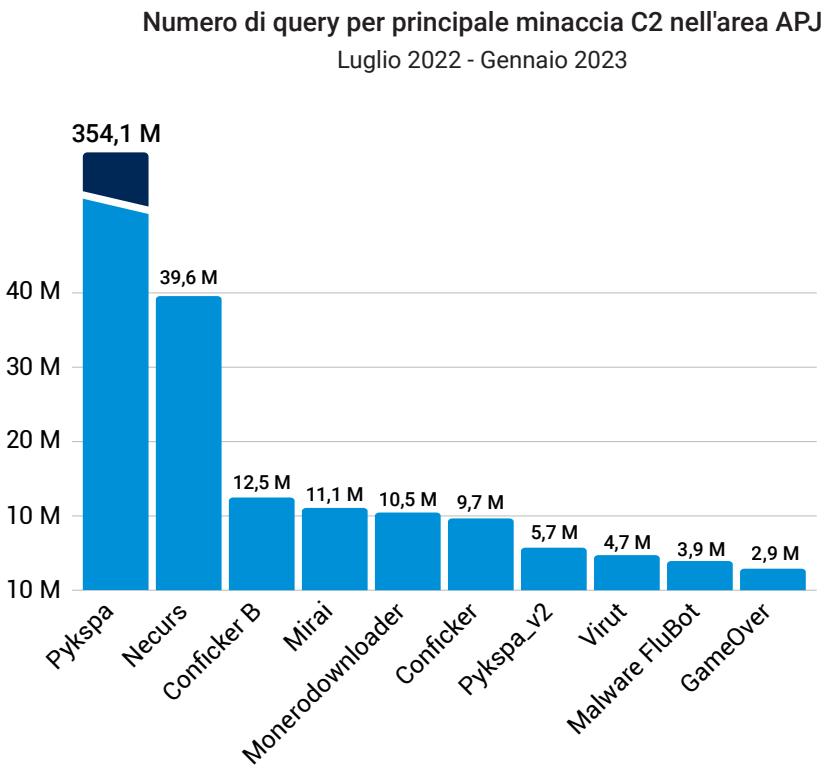


Figura 18: Le minacce dominanti nell'area APJ includono Pykspa e Necurs

Nell'area APJ sono state osservate più di 350 milioni di query relative a Pykspa (Figura 18). In un post sul blog del 2019, abbiamo notato che Pykspa ha utilizzato un meccanismo DGA selettivo per rimanere invisibile per un lungo periodo. I domini evidenziati in quel rapporto si trovavano principalmente nell'Asia orientale. Abbiamo anche osservato query associate a botnet come Necurs, che è un forte indicatore che i sistemi sono infetti da altri malware.

Panoramica sullo scenario degli attacchi di phishing

Nell'ultima parte della nostra analisi del traffico DNS, abbiamo esaminato i kit di phishing e il loro ruolo cruciale nel successo delle campagne di phishing. Il phishing è ancora rilevante, più che mai, a causa delle tattiche in continua evoluzione utilizzate dai criminali e della crescente quantità di informazioni personali disponibili online. I criminali utilizzano il social engineering per far sembrare legittimi i loro tentativi di phishing e le prove indicano che il tasso di successo di questi attacchi rimane elevato. La ricerca di Akamai sulle truffe di phishing durante le festività ha rivelato nuove tecniche e tattiche utilizzate dagli autori di attacchi per continuare a rimanere invisibili. Queste nuove tattiche includono l'utilizzo di false testimonianze di utenti come parte della truffa e la tecnica recentemente scoperta di utilizzare l'ancoraggio HTML per assicurarsi che solo gli utenti validi accedano ai siti web truffa.

Anche l'aumento dello smart working dovuto alla pandemia di COVID-19 ha reso più difficile rilevare e prevenire gli attacchi di phishing, rendendo più importante per gli utenti e le organizzazioni rimanere vigili e adottare misure per proteggersi. Inoltre, l'ascesa dei social media e il crescente numero di dispositivi connessi a Internet hanno creato maggiori opportunità per i criminali.

Campagne di phishing colpiscono i servizi finanziari

Nelle indagini condotte sui brand che vengono violati e imitati da truffe di phishing, sono vari i modi con cui è possibile raccogliere i dati. Abbiamo confrontato il numero totale di campagne con il numero di vittime prese di mira. In tal modo, abbiamo valutato la percentuale di successo di una data campagna e la percentuale di ogni settore preso di mira.

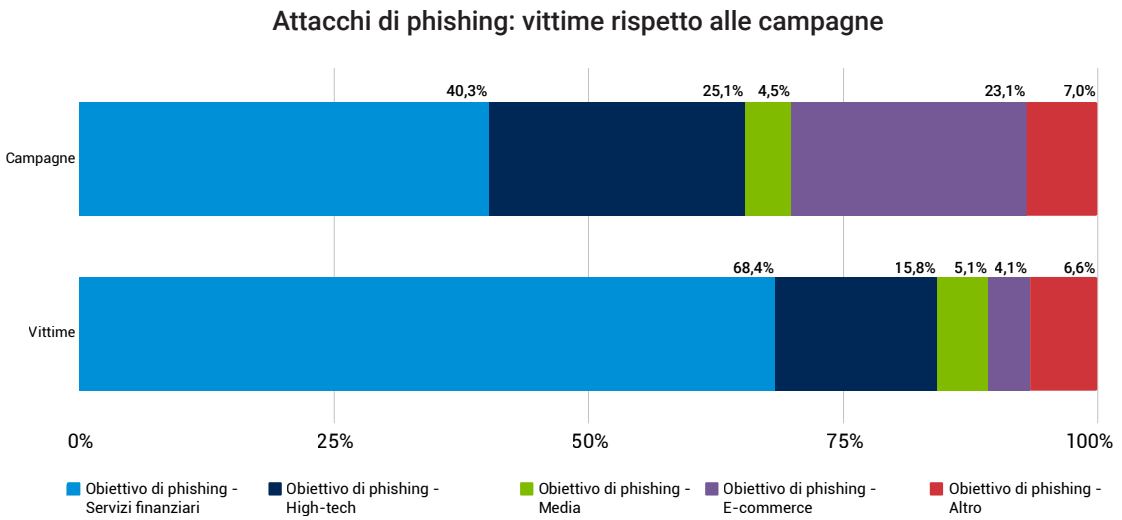


Figura 19: La maggior parte delle campagne di phishing ha preso di mira il settore dei servizi finanziari (4° trimestre 2022)

La nostra ricerca ha rilevato che i brand finanziari e high-tech sono in cima alla lista sia per numero di campagne che per numero di vittime (Figura 19). Abbiamo registrato un 40,3% di campagne sferrate contro i clienti dei servizi finanziari, che hanno determinato un 68,4% di vittime, deducendo che gli attacchi contro i servizi finanziari sono risultati altamente efficaci nel 4° trimestre 2022. Nel nostro rapporto sui servizi finanziari, Il nemico è alle porte: analisi degli attacchi contro i servizi finanziari, abbiamo sottolineato come gli attacchi di phishing abbiano motivazioni finanziarie e prendano di mira principalmente i servizi finanziari e i loro clienti. I potenziali impatti di tali attacchi includono danni al brand e alla reputazione e la perdita della fiducia dei clienti. La soluzione dell'attacco di phishing potrebbe anche richiedere l'utilizzo di risorse dell'organizzazione.

L'e-commerce ha riscontrato il 23% delle campagne di phishing attivate nel 4° trimestre del 2022. Sebbene abbiamo osservato più campagne che vittime effettive, vale anche la pena notare che gli autori di attacchi stanno prendendo di mira questo settore e gli utenti devono rimanere vigili poiché i criminali informatici potrebbero prendere di mira le loro informazioni personali o bancarie.

Toolkit di phishing: fattori che facilitano le truffe di phishing

La straordinaria portata e l'ampiezza degli attacchi di phishing sono favorite dalla presenza di toolkit di phishing, che supportano la distribuzione e la gestione di siti web di phishing consentendo anche a truffatori non dotati di talento tecnico di eseguire truffe di phishing.

Figura 20: Toolkit di phishing classificati per numero di giorni di riutilizzo nel 4° trimestre 2022

Secondo la nostra ricerca che ha rilevato più di 300 diversi toolkit di phishing utilizzati per lanciare nuove campagne di attacchi, nel 4° trimestre 2022, il 2,04% dei kit monitorati è stato riutilizzato in almeno 54 giorni distinti (Figura 20). Inoltre, il 55,5% dei kit è stato riutilizzato per lanciare nuove campagne di attacchi per almeno quattro giorni e, esaminando tutti i kit monitorati, possiamo notare che sono stati tutti riutilizzati per non meno di due giorni distinti sempre nel 4° trimestre 2022.

Conclusioni e raccomandazioni: contrasto degli attacchi moderni con misure proattive

Ora che abbiamo descritto i gruppi di minacce e le metodologie degli autori di attacchi, parliamo di come sfruttare tutte queste informazioni. Inizieremo con come gestire il DNS, internamente o esternalizzato a terzi. Per le organizzazioni più grandi o più complesse, ha senso rivolgersi a un provider specializzato nella gestione del DNS. In ogni caso, assicuratevi di monitorare le performance e i sistemi di protezione per il vostro DNS. Quindi, considerate i diversi controlli di cui avrete bisogno. Protezione DDoS, attacchi malware e scraping, movimento laterale ed esfiltrazione sono le aree chiave da mitigare. Seguire questo percorso di dati e rilevare tutte le vulnerabilità critiche che potete correggere in ogni fase, è un modello di cybersicurezza spesso definito "Cyber Kill Chain".

Valutate la creazione di playbook per le tecniche di attacco descritte in questo rapporto. Verificate se il vostro team di test di penetrazione o red team utilizza gli stessi strumenti e tecniche degli IAB come Qakbot ed Emotet, bot come QSnatch, ransomware come LockBit (in ambiente di laboratorio) e strumenti come Cobalt Strike. È importante assicurarsi che i controlli di sicurezza segnalino e blocchino questi tipi di attacchi in modo efficace e che i team siano formati per affrontarli.

Se nella vostra rete Cobalt Strike viene rilevato, è prudente creare immediatamente un rapporto sull'incidente e indagare. Anche se lo strumento potrebbe essere utilizzato dal vostro red team (nel qual caso, dovrebbe comunque essere indagato e segnalato), la presenza di tale traffico dovrebbe far suonare un allarme in quanto potrebbe indicare l'intrusione di altri gruppi di criminali RaaS o autori di attacchi e segnalare un attacco in corso che potrebbe ancora essere mitigato.

Valutate le modalità in cui opera il vostro centro operativo di sicurezza e determinate il vostro attuale metodo di monitoraggio dei processi (come bit, Wget o cURL) che potrebbero eventualmente indicare la probabilità che una minaccia correlata allo IAB sia presente nella rete che esegue la ricognizione. Le parti critiche sono capire cosa è stato scaricato e bloccarlo se è ancora in esecuzione. Quindi, indagate su cosa abbia attivato lo IAB: è stato un file LNK, una macro o un VScript? Quindi, scoprite come è iniziata la violazione.

Restate aggiornati sulla nostra ultima ricerca consultando il nostro Security Research Hub.

Metodologie

Traffico degli attacchi di comando e controllo

I dati in questo rapporto sono generati dal nostro prodotto Secure Internet Access (SIA) e descrivono il traffico degli attacchi di comando e controllo (C2). SIA è una soluzione SWG basata sul cloud e progettata per consentire agli utenti di connettere facilmente i propri dispositivi a Internet in modo sicuro. I due diversi set di dati utilizzati in questo rapporto riflettono separatamente i dati degli avvisi di sicurezza provenienti da organizzazioni aziendali con grandi quantità di utenti o provider Internet con singoli utenti domestici. Questi dati sono stati misurati rispettivamente in base al numero di dispositivi colpiti e al numero di query. Un dispositivo colpito è stato definito come un dispositivo che ha raggiunto almeno una volta un dominio C2 noto e identificato. Allo stesso modo, una query C2 è stata definita come una query che ha raggiunto un dominio C2 noto e identificato. I nostri team addetti alla sicurezza utilizzano questi dati internamente per effettuare ricerche su attacchi, segnalare comportamenti dannosi per avvisare i clienti e fornire ulteriore intelligence sulle soluzioni per la sicurezza di Akamai.

Riconoscimenti

Editoria e scrittura

Or Katz

Eliad Kimhy

Badette Tribbey

Revisione e contributi di esperti del settore

Tanya Belousov

Shiran Guez

Ophir Harpaz

Stiv Kupchik

Grace Wang

Steve Winterfeld

Analisi dei dati

Ronan Ballantine

Gal Kochner

Chelsea Tuttle

Marketing ed editoria

Georgina Morales Hampe

Shivangi Sahu

Altri rapporti sullo stato di Internet - Security

Leggete le edizioni precedenti e date un'occhiata ai prossimi rapporti sullo stato di Internet - Security: akamai.com/soti

Altre informazioni sulla ricerca delle minacce Akamai

Restate aggiornati con le ultime analisi dell'intelligence sulle minacce, rapporti sulla sicurezza e ricerche sulla cybersicurezza: akamai.com/security-research

Accesso ai dati dal rapporto

Potete visualizzare i grafici e i diagrammi citati in questo rapporto in versioni di alta qualità. L'utilizzo e la consultazione di queste immagini sono forniti a scopo gratuito, purché Akamai venga debitamente citata come fonte e venga conservato il logo dell'azienda: akamai.com/sotidata

Ulteriori informazioni sulle soluzioni Akamai

Per ulteriori informazioni sulle soluzioni Akamai per le minacce che prendono di mira le aziende, visitate la nostra pagina Secure Internet Access Enterprise. I provider di servizi che operano nei mercati dei consumatori e delle PMI possono visitare la pagina Servizi Secure Internet Access per ISP.

A sostegno e protezione della vita online c'è sempre Akamai. Le principali aziende al mondo scelgono Akamai per creare, offrire e proteggere le loro experience digitali, aiutando miliardi di persone a vivere, lavorare e giocare ogni giorno. Akamai Connected Cloud, una piattaforma edge e cloud ampiamente distribuita, avvicina le app e le experience agli utenti e allontana le minacce. Per ulteriori informazioni sulle soluzioni di cloud computing, sicurezza e delivery di contenuti di Akamai, visitate il sito akamai.com e akamai.com/blog o seguite Akamai Technologies su Twitter e LinkedIn. Data di pubblicazione: 03/23