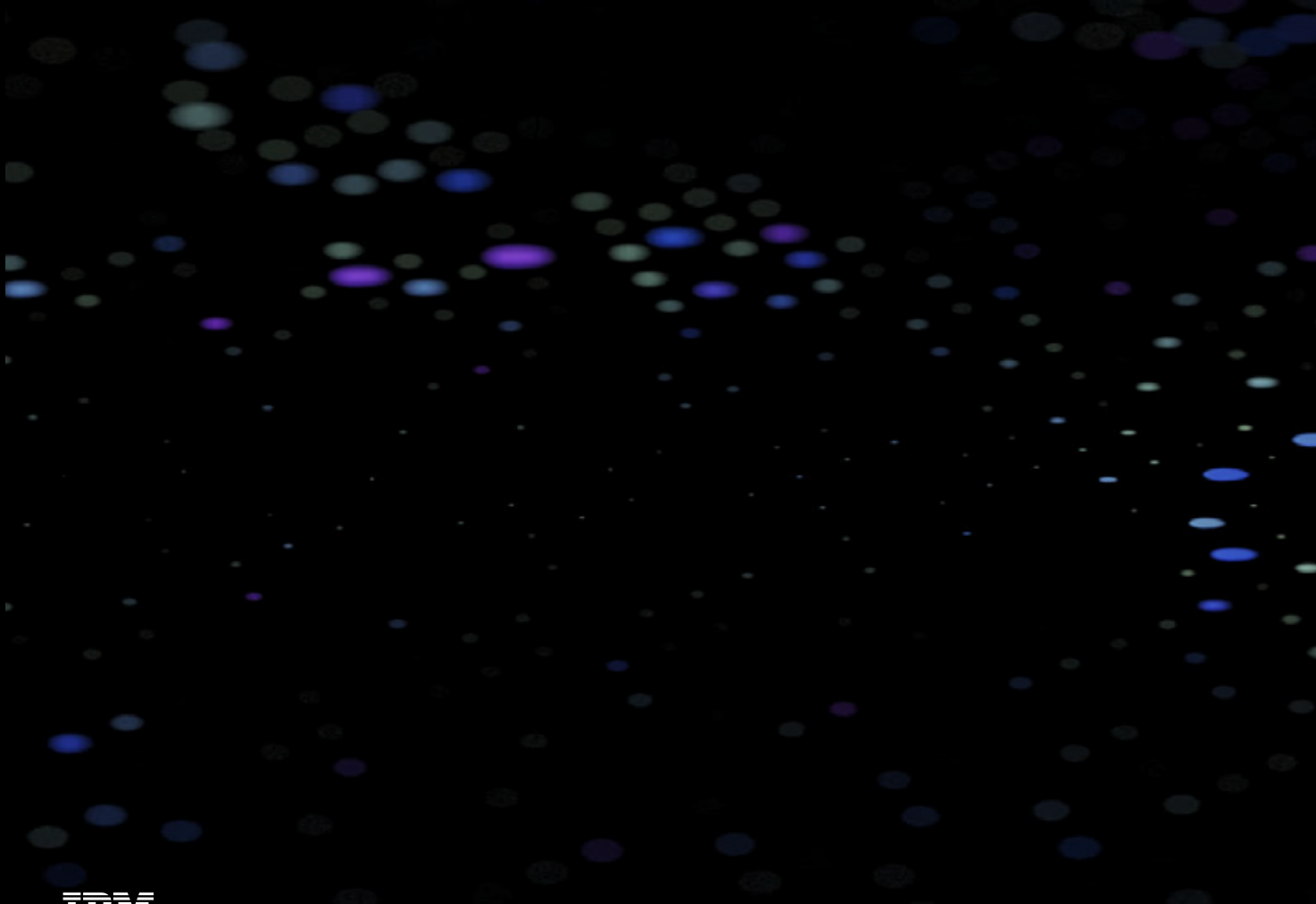
IBM Security

X-Force Threat Intelligence Index 2020



IBM

Creato da IBM X-Force Incident Response and Intelligence Services (IRIS)

Indice dei contenuti

Indice dei contenuti

Riepilogo e principali trend

IBM Security sviluppa soluzioni di sicurezza e servizi aziendali intelligenti che aiutano le aziende a creare una maggiore resilienza oggi per le minacce del futuro.

Al fine di tenere i professionisti della sicurezza aggiornati sulle principali minacce, IBM® X-Force® rilascia regolarmente blog, white paper, webinar e podcast sulle minacce emergenti e su tattiche, tecniche e procedure (TTP) utilizzate dagli aggressori.

IBM Security® rilascia annualmente l'IBM X-Force Threat Intelligence Index, che offre un riepilogo dei risultati dell'anno precedente in termini di principali minacce evidenziate dai nostri vari team di ricerca, al fine di fornire ai team operanti nel settore della sicurezza le informazioni necessarie per garantire la sicurezza delle loro organizzazioni.

Dati e informazioni presentati in questo rapporto sono ottenuti dai servizi di sicurezza gestiti, i servizi di risposta agli incidenti, dai test di penetrazione e dai servizi di gestione delle vulnerabilità di IBM Security.

I team di ricerca di IBM X-Force analizzano i dati provenienti da centinaia di migliaia di endpoint e server protetti, unitamente ai dati derivanti dalle risorse di soggetti non clienti, come sensori di spam e honeynet. IBM Security Research esegue anche trappole per lo spam in tutto il mondo, monitorando decine di milioni di attacchi di spam e phishing, analizzando miliardi di pagine web e immagini per identificare campagne di attacchi, attività fraudolente e abusi dei marchi. Tutto ciò al fine di offrire una migliore protezione dei clienti e delle vite connesse che caratterizzano la nostra quotidianità.

X-Force Incident Response and Intelligence Services (IRIS), ha compilato una serie di analisi dei servizi e dei software di IBM Security risalenti allo scorso anno, che indicano come il 2019 sia stato un anno caratterizzato dal riemergere di nuove minacce utilizzate in maniera innovativa.

— Secondo i dati di X-Force, un incremento del 2000 percento degli incidenti mirati a danno delle tecnologie operative (OT) nel 2019 potrebbe indicare un crescente interesse degli attori delle minacce verso i sistemi industriali nell'arco del 2020.

— Nel 2019 sono stati compromessi oltre 8,5 miliardi di registrazioni. Un numero superiore del 200 percento rispetto al numero delle registrazioni perse nel 2018. La responsabilità di tale incremento è in larga parte da addebitare disattenzioni di dipendenti interni. I dati esposti a causa di server non configurati correttamente (incluso lo storage cloud accessibile pubblicamente, database cloud non sicuri, backup rsync non messi in sicurezza correttamente o dispositivi di storage area network su reti internet aperte) costituiscono l'86 percento dei casi di violazioni dei dati registrati nel 2019.

— Il panorama dei malware è mutato nel 2019, con un ritorno dei criminali informatici al ransomware e alla creazione di botnet. Durante il 2019, X-Force IRIS ha risposto a minacce ransomware in 12 paesi differenti sparsi su 5 continenti e 13 settori industriali differenti. Inoltre, le attività malware distruttive mostrano come malware potenzialmente catastrofici continuino a innalzare il livello della minaccia.

— I tre principali vettori di infezioni iniziali osservati nei casi seguiti da X-Force IRIS nel 2019 occupavano posizioni molto vicine tra loro nella graduatoria dei rischi: Phishing (31 percento), scansioni ed exploit (30 percento) e furto di credenziali (29 percento). In particolare, il phishing è passato dal rappresentare circa la metà degli incidenti totali nel 2018 a meno di un terzo nel 2019. In compenso, le minacce associate alla scansione e allo sfruttamento delle vulnerabilità sono cresciute di circa un terzo, passando dall'otto percento del 2018 all'attuale percentuale pari a circa un terzo del totale.

— L'analisi dello spam globale effettuata da X-Force indica che le email di spamming continuano a utilizzare un ridotto subset di vulnerabilità, che si concentra in particolare su due soli CVE: 2017-0199 e 2017-11882. Entrambe queste vulnerabilità sono state corrette e hanno rappresentato circa il 90 delle minacce associate a vulnerabilità che i criminali informatici hanno cercato di sfruttare attraverso campagne di spamming.

— Sebbene il settore dei servizi finanziari abbia mantenuto il ruolo di settore più colpito nel 2019, il focus delle minacce in settori specifici ha evidenziato priorità mutevoli per gli aggressori, con i settori al dettaglio, dei media, dell'educazione e quello governativo che hanno visto una crescita delle minacce su scala globale.

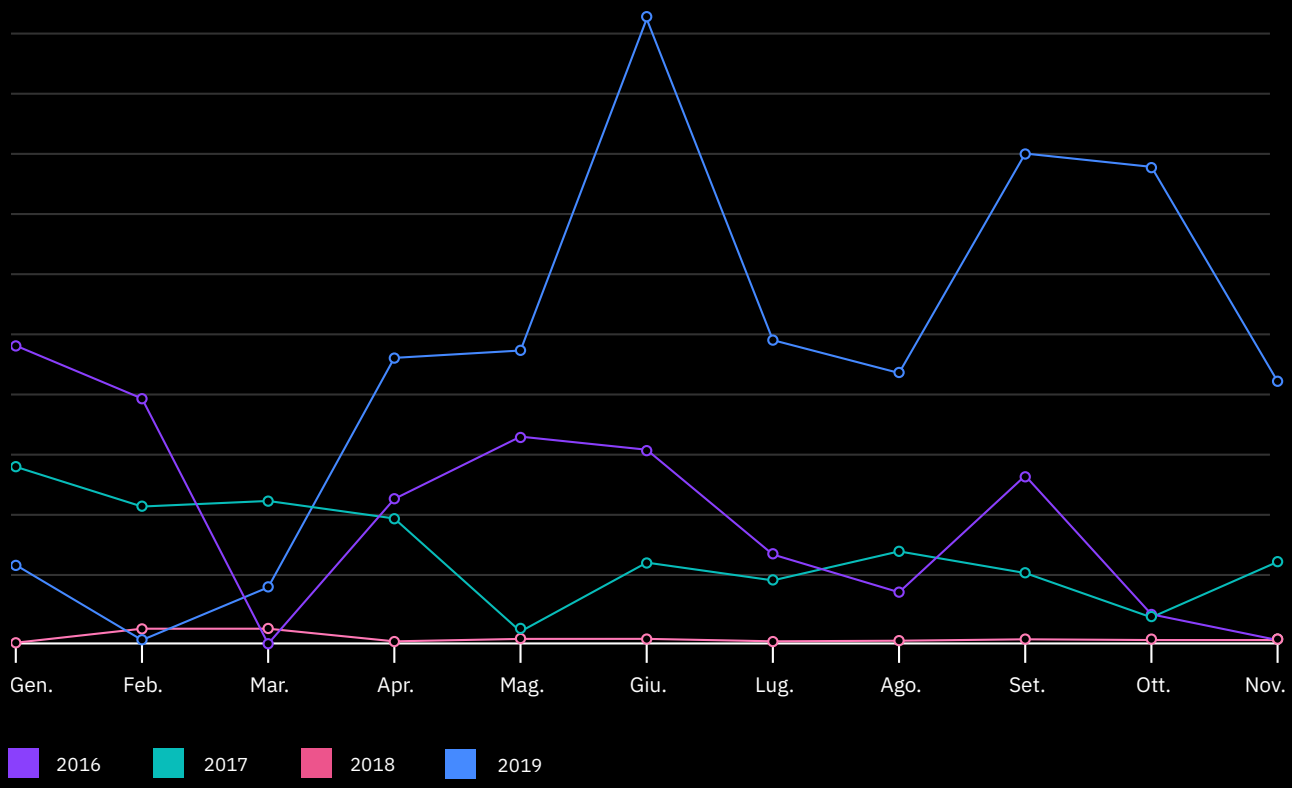
— Una novità introdotta dall'X-Force Threat Intelligence Index quest'anno è costituita dalle informazioni geocentriche, che forniscono dati sui trend osservati attorno al mondo. IBM Security continua a monitorare criminali informatici e minacce multiple in diverse regioni del globo. Questo rapporto evidenzia le principali minacce che caratterizzano ciascuna regione, gli attacchi osservati nel 2019 e le potenziali date di interesse per la sicurezza informatica nel 2020.

Le sezioni seguenti di questo rapporto annuale analizzano i principali trend con approfondimenti relativi alle informazioni che ne hanno caratterizzato la loro natura nel 2019.

Targeting e vettori di infezione iniziali

Figura 1:
Trend degli attacchi alle tecnologie operative (OT)

Volume di attacchi OT mensili; comparativa triennio 2016-2019 (Fonte: IBM X-Force)



Crescita esponenziale di targeting delle infrastrutture delle tecnologie operative (OT)

I dati di IBM X-Force indicano che gli eventi in cui gli attori delle minacce hanno preso di mira sistemi di controllo industriali (ICS) o altre risorse associate alle tecnologie operative (OT), hanno subito una crescita di oltre il 2000 percento dal 2018. In realtà, il numero degli eventi che hanno avuto come obiettivo le risorse OT nel 2019 è stato notevolmente superiore rispetto al volume delle attività osservate nell'arco dei tre anni precedenti.

La maggior parte degli attacchi osservati era focalizzata sull'uso di una combinazione di vulnerabilità note, all'interno di componenti hardware SCADA e ICS, nonché su attacchi diffusi a tappeto sulle password, mediante tattiche di accesso brute force contro obiettivi ICS.

Alcune delle attività registrate, incentrate su attacchi ICS, sono state associate con due attori criminali noti, e hanno coinciso con un picco di attacchi durante il periodo oggetto di analisi da parte dei nostri sistemi telemetrici. Due campagne specifiche sono state compiute dai gruppi Xenotime E IBM Hive0016 (APT33), che hanno espanso i loro attacchi verso gli obiettivi ICS.

La sovrapposizione tra infrastruttura IT e OT, come PLC (Programmable Logic Controller) e ICS, nel 2019 ha continuato a presentare rischi per le organizzazioni che si affidano a tali infrastrutture ibride.

La convergenza di infrastrutture IT/OT consente alle minacce IT di attaccare i dispositivi OT che gestiscono risorse fisiche, con un notevole incremento dei costi di ripristino. Per esempio, a inizio 2019, IBM X-Force IRIS ha collaborato alla formulazione di una risposta a un attacco condotto ai danni di un'azienda manifatturiera mondiale in cui un'infezione ransomware iniziata su un sistema IT si è poi spostata lateralmente sull'infrastruttura OT costringendo l'intero impianto a interrompere le operazioni di produzione. L'attacco ha causato un impatto non solo sui processi della stessa azienda ma ha anche causato un effetto dirompente sui mercati globali.

Le valutazioni di sicurezza di X-Force IRIS fornite ai clienti durante il 2019, hanno sottolineato la vulnerabilità dei sistemi OT che spesso utilizzano software e hardware obsoleti. Mantenere sistemi di produzione le cui vulnerabilità non possono più essere corrette mediante patch ed esposti a vecchie vulnerabilità da tempo di pubblico dominio, espone tali sistemi privi di patch ad attacchi anche quando questi non sono connessi a internet. Nei casi di infiltrazioni laterali delle minacce, dopo che un aggressore è riuscito a penetrare nei sistemi, tali minacce possono essere utilizzate dall'interno delle reti, creando danni notevoli attraverso tecniche di exploit relativamente semplici.

Sebbene il trend degli attacchi alle reti ICS illustrato in figura 1 indichi una flessione a partire da inizio ottobre 2019, X-Force prevede che gli attacchi contro gli obiettivi OT/CS continueranno a crescere nel 2020, mentre numerosi aggressori pianificano e lanciano nuove campagne contro reti industriali in tutto il mondo. Con oltre 200 nuovi CVE associati a sistemi ICS rilasciati nel 2019, il database delle vulnerabilità di IBM X-Force indica che, con tutta probabilità, le minacce ai sistemi ICS continueranno a crescere durante il 2020.

X-Force prevede che gli attacchi contro gli obiettivi OT/CS continueranno a crescere nel 2020, mentre numerosi aggressori pianificano e lanciano nuove campagne contro reti industriali in tutto il mondo.

Notevole crescita delle violazioni dei dati

Il numero delle violazioni dei dati è cresciuto notevolmente nel 2019, con oltre 8,5 miliardi di registrazioni esposte. Un volume tre volte superiore a quello del 2018. La ragione principale di questo notevole incremento risiede nel fatto che le registrazioni esposte a causa di configurazioni errate sono cresciute di oltre dieci volte nell'arco di un anno. Questi casi rappresentano l'86 percento dei casi di dati compromessi nel 2019. Si tratta di un dato notevolmente differente rispetto a quello registrato nel 2018, quando avevamo osservato un decremento del 52 percento rispetto al 2017, in termini di casi di violazioni dei dati a causa di errate configurazioni, con il volume totale che ammontava a meno della metà del totale.

Si noti che in realtà è stato registrato un decremento nel numero degli incidenti causati da configurazioni errate nel 2019, con una variazione del 14 percento rispetto all'anno precedente. Ciò implica che quando si è verificata una violazione dei dati a causa di configurazioni errate, il volume di dati coinvolto era significativamente superiore nel 2019. Circa tre quarti delle violazioni che implicavano la perdita di oltre 100 milioni di dati sono state causate da incidenti dovuti a configurazioni errate. In due di questi incidenti causati da configurazioni errate, verificatisi nel settore dei servizi professionali, il volume di dati violati era nell'ordine dei miliardi, per ciascun incidente.

Tale significativo incremento in termini di dati persi in vari settori sottolinea il crescente rischio di violazioni dei dati, anche nel caso di organizzazioni operanti in settori che non sono tradizionalmente considerati come target prioritari.

Violazioni di dati registrate nel 2019

8,5 miliardi

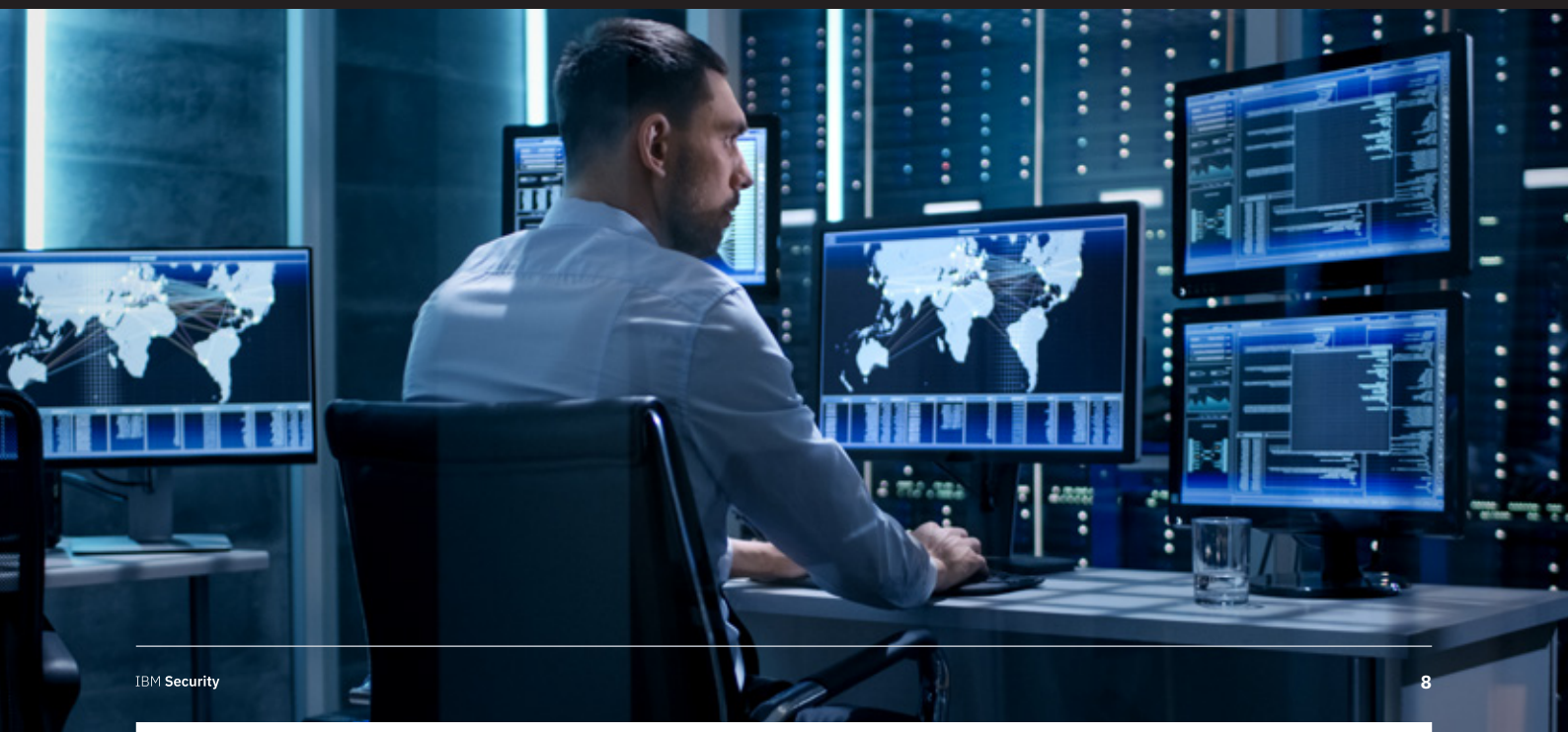
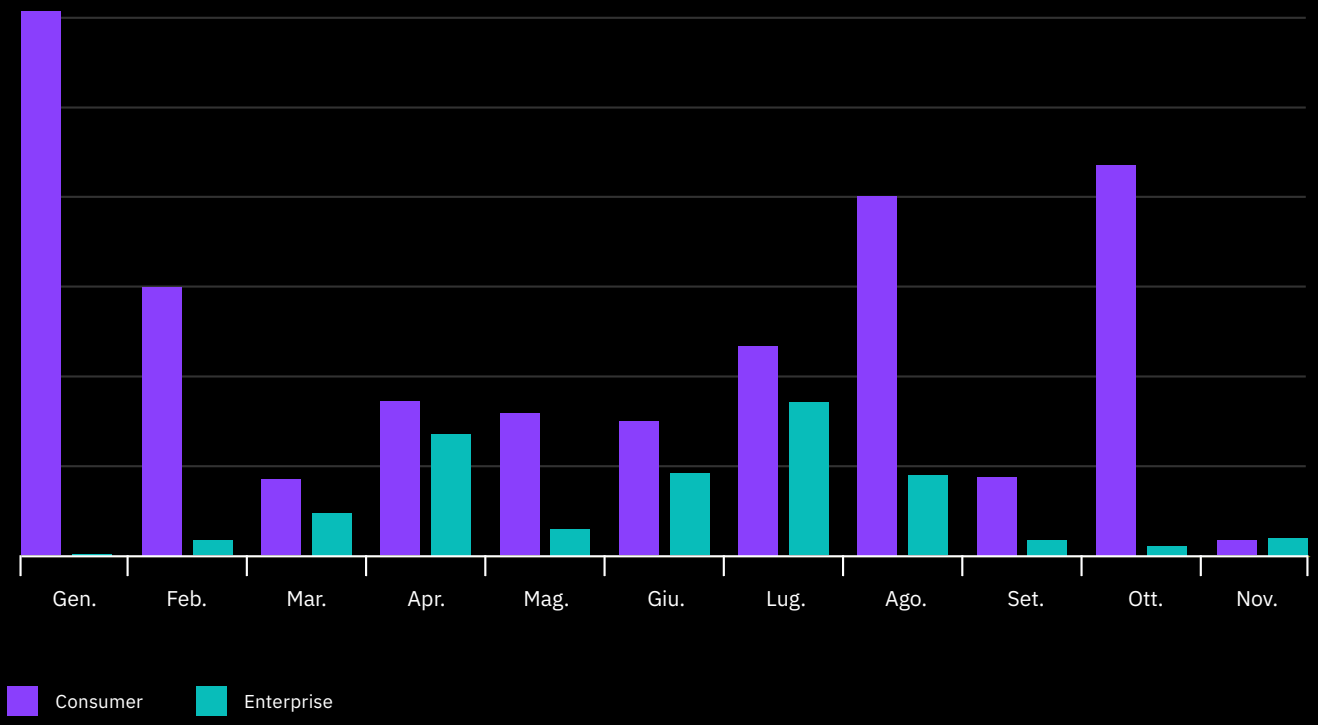


Figura 2:

Attacchi IoT nel settore consumer e in quello IoT a confronto

Volume mensile di attacchi IoT nel settore consumer e in quello aziendale nel 2019 (fonte: IBM X-Force)



Targeting di dispositivi IoT che include anche le aziende

con oltre 38 miliardi dispositivi connessi a internet nel 2020, il panorama delle minacce associate all'Internet delle cose (IoT) è gradualmente divenuto un crescente vettore di minacce in grado di danneggiare le attività di consumatori e aziende, attraverso attacchi malware relativamente semplici e automatizzati, spesso basati su script.

Nell'ambito dei codici maligni utilizzati per infettare i dispositivi IoT, i ricercatori di IBM X-Force hanno rilevato molteplici campagne di malware Mirai nel 2019, espandendo l'ambito degli obiettivi dall'elettronica di consumo anche a quella dell'hardware di livello aziendale. Un trend emerso fin dal 2018. I dispositivi compromessi e dotati di un accesso alla rete possono successivamente essere utilizzati dagli attaccanti come vettore di attacco per potenziali tentativi di accedere ai sistemi aziendali.

Mirai è un malware IoT molto prolifico che è stato utilizzato da numerosi attaccanti dal 2016, causando gravi interruzioni e infettando grandi quantità di dispositivi IoT, che venivano poi utilizzati in attacchi di tipo distributed denial of service (DDoS). Nella nostra analisi delle campagne condotte nel 2019, abbiamo rilevato che i TTP delle vittime del malware Mirai sono notevolmente cambiati dal 2018, e nel 2019 gli attacchi si sono concentrati verso gli hardware aziendali, oltre che verso l'elettronica di consumo.

Da un'analisi degli attacchi che hanno colpito i dispositivi IoT nel 2019, abbiamo osservato un diffuso utilizzo degli attacchi basati sull'iniezione di codice (CMDi), contenenti istruzioni per il download di payload maligni finalizzati a colpire vari tipi di dispositivi IoT. La maggior parte di questi attacchi con iniezione di codice sono automatizzati mediante script che effettuano la scansione e cercano di infettare gruppi di dispositivi in blocco. Se il dispositivo IoT attaccato è suscettibile a questi attacchi di iniezione codice, il payload viene scaricato ed eseguito, inserendo il dispositivo in un'ampia botnet IoT. Uno dei principali veicoli per questi attacchi è rappresentato dai dispositivi IoT con password deboli o difettose, che possono essere scoperte mediante un semplice attacco basato su un dizionario.

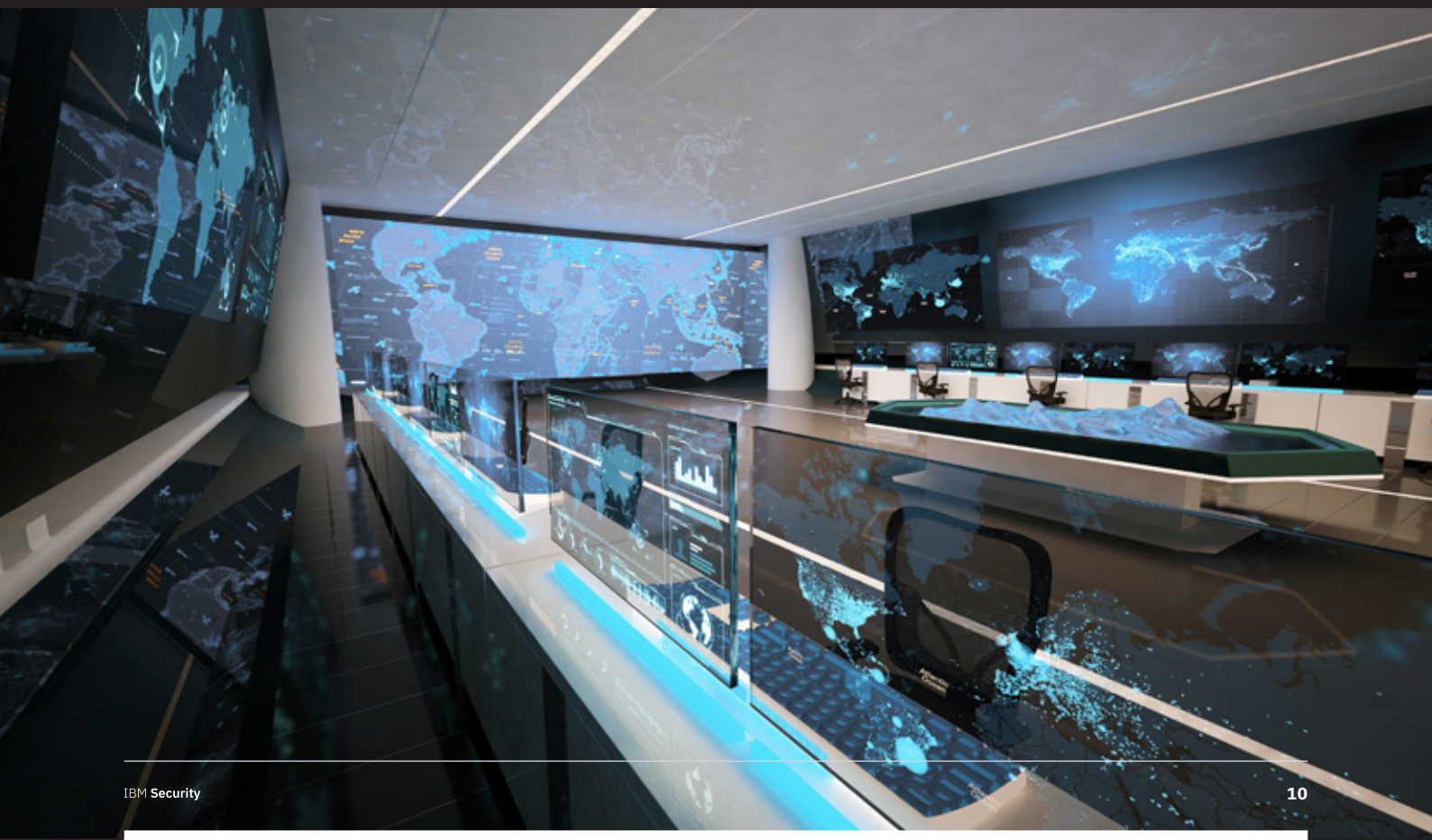
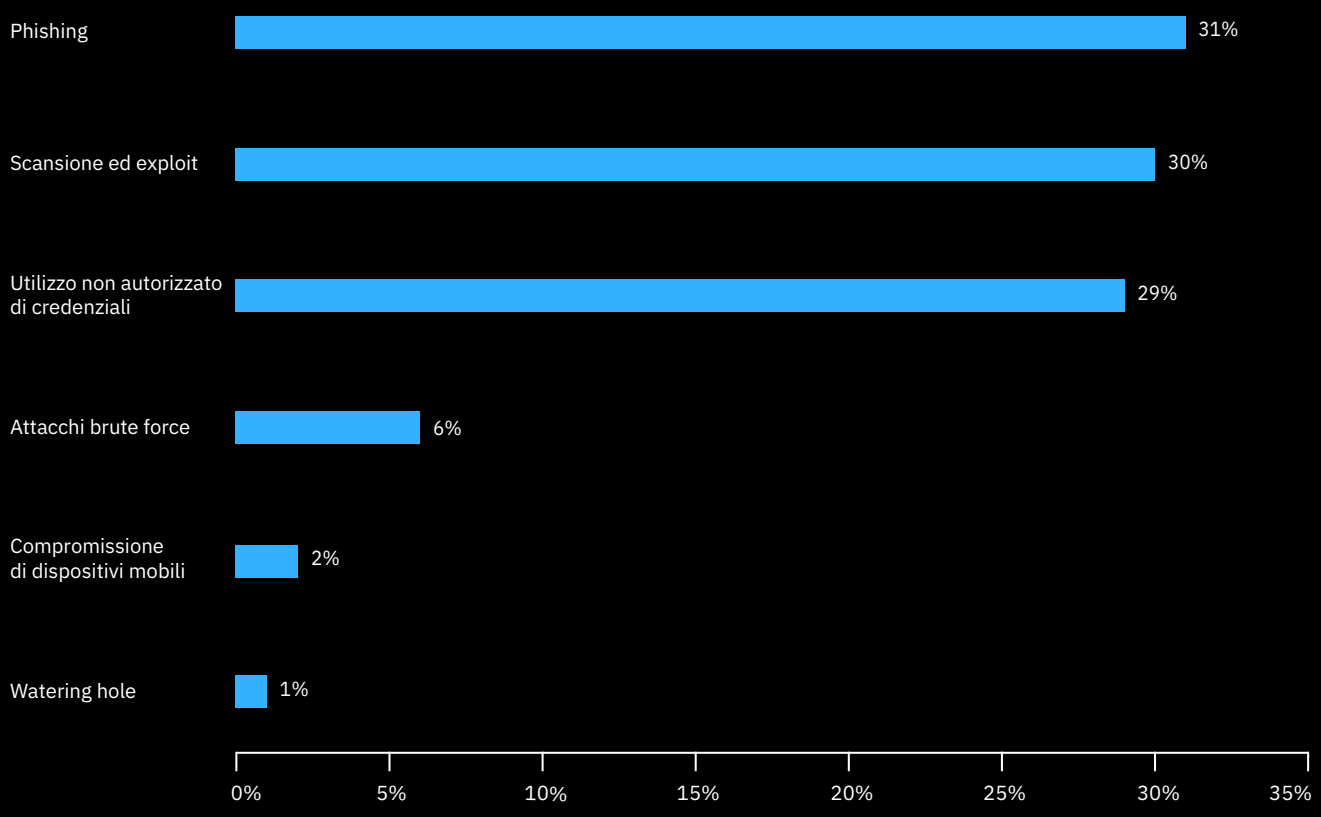


Figura 3:

Principali vettori di accesso iniziale

Descrizione dettagliata dei 6 principali vettori di attacco iniziale nel 2019, sottoforma di percentuale per tutti e sei i tipi di vettori di accesso mostrati (fonte IBM X-Force)

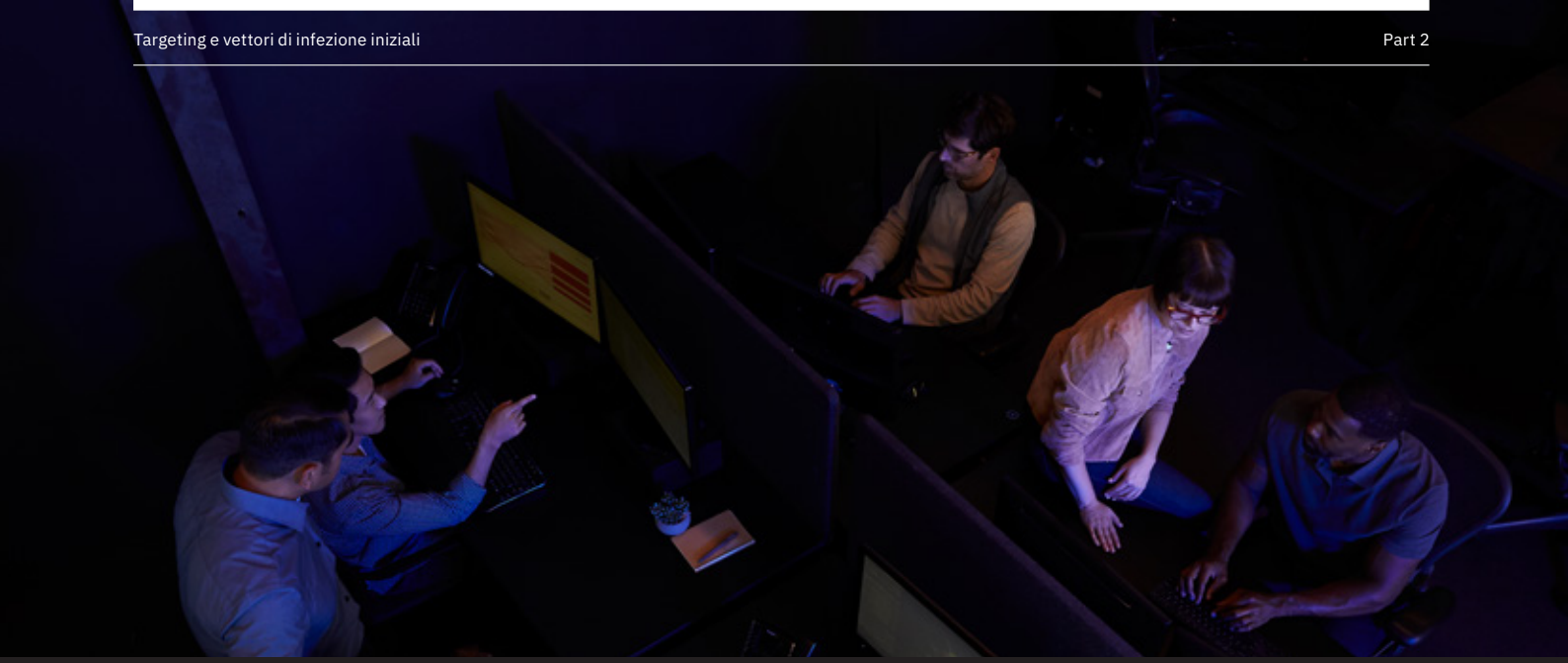


Il phishing svetta tra i vettori di accesso iniziali negli attacchi condotti nel 2019

Le ampie capacità di risposta di IBM X-Force IRIS, offrono estese funzionalità di reazione, fornendo preziose informazioni su metodi e motivazioni degli attacchi e degli aggressori.

Nel 31 percento dei casi, il phishing è stato il metodo più utilizzato per l'accesso iniziale nel 2019; tale percentuale ha subito una riduzione rispetto al dato del 2018, anno in cui tale tipologia di attacco rappresentava circa la metà del totale.

1 L'edizione 2019 dell'X-Force Threat Intelligence Index riporta che circa un terzo, ossia il 29 percento, degli attacchi analizzati da X-Force IRIS, includeva casi di dispositivi compromessi a causa di mail di phishing. Tale percentuale è stata corretta in modo da includere anche le prove aggiuntive emerse dopo la pubblicazione, integrando il dato originale con i numerosi incidenti che hanno portato tale percentuale al 44 percento nel 2018.



In particolare, nel 2019, gli aggressori si sono dedicati alla ricerca di vulnerabilità da sfruttare negli ambienti prescelti, con il personale addetto al contrasto delle minacce che ha indicato che tale metodo è stato utilizzato nel 30 percento degli incidenti, con un incremento dell'8 percento sul totale rispetto all'anno precedente.

Gli aggressori hanno un'ampia varietà di scelta in termini di dispositivi da scansionare e sfruttare. IBM X-Force ha identificato oltre 150.000 vulnerabilità che sono state rivelate pubblicamente. Mentre gli avversari più sofisticati sono in grado di sviluppare exploit di tipo zero-day, l'impiego di exploit già noti è più frequente, in quanto tali exploit consentono agli avversari di disporre di un punto di accesso iniziale senza dover sostenere i costi associati alla necessità di realizzare nuovi TTP, e risparmiando le migliori armi per le reti maggiormente protette. Inoltre, gli aggressori fanno affidamento sul fatto che molte organizzazioni non aggiornano le applicazioni con le patch più recenti, anche nel caso di vulnerabilità per le quali tali patch sono disponibili da tempo. Per esempio, in alcuni casi di infezioni con WannaCry, è possibile osservare che tali infezioni continuano da oltre due anni dopo l'infezione iniziale e che le patch (MS17-010), nonostante l'ampia diffusione delle patch.

L'impiego di credenziali rubate possedute dagli aggressori e utilizzate per accedere alle organizzazioni occupa il secondo posto, con il 29 percento. Spesso, tali credenziali sono rubate presso siti di terzi, oppure ottenute mediante tentativi di phishing ai danni dell'organizzazione target. Gli aggressori possono utilizzare credenziali rubate per confondersi con il traffico legittimo, rendendo il rilevamento ancora più difficoltoso.

Gli attacchi di tipo brute force hanno subito un calo rispetto all'anno precedente, passando al quarto posto, con 6 percento del totale. Tale percentuale è seguita dagli attacchi ai dispositivi BYOD, con una percentuale del 2 percento sul totale degli attacchi di accesso iniziale condotti ai danni delle organizzazioni target.

I ricercatori di X-Force hanno osservato un notevole incremento di attività maligne nel periodo compreso tra giugno e luglio 2019, con il numero di eventi registrati in tale periodo che ha eclissato i totali registrati durante gli altri periodi dell'anno. Sebbene la ragione per tale incremento di attività non sia noto, i mesi estivi appaiono essere quelli più attivi anche in termini di spam, con volumi di spam record registrati nell'agosto del 2019. È anche possibile che gli aggressori rilevati durante tale periodo abbiano agito in maniera meno discreta e pertanto siano stati rilevati con maggiore facilità, oppure che un cambiamento nelle tattiche degli attori o degli strumenti utilizzati abbia causato un picco significativo di attività. I picchi di attività a breve termine raramente derivano dall'ingresso di nuovi aggressori sul mercato, in quanto se così fosse, l'arrivo di nuovi aggressori causerebbe un incremento duraturo delle attività, anziché un picco temporaneo.

Trend del malware

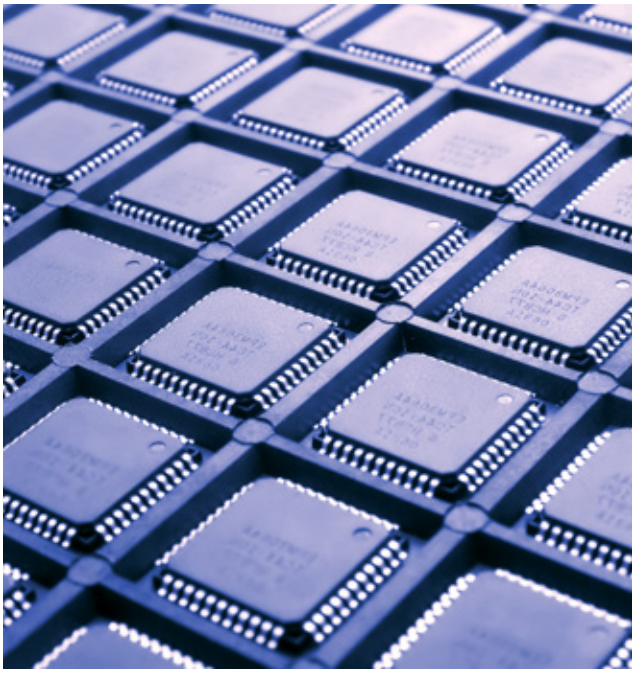
Straordinario incremento degli attacchi di malware con effetti distruttivi

Le indagini condotte da IBM X-Force IRIS indicano che nel 2019 gli attacchi mediante malware distruttivi sono diventati più frequenti in termini di estensione geografica e intensità.

Utilizzati da criminali informatici e da governi, i malware distruttivi sono software maligni che hanno la capacità di rendere i sistemi colpiti inutilizzabili e complicare il ripristino delle attività. Le varianti malware più distruttive sono in grado di causare danni notevoli attraverso l'eliminazione o la sovrascrittura di file critici per il funzionamento dei sistemi operativi. In alcuni casi, i malware distruttivi possono inviare messaggi personalizzati per sistemi industriali, causandone il malfunzionamento. Le nostre definizioni di malware distruttivo includono il tipo di ransomware in grado di eliminare completamente i dati dai sistemi colpiti, oppure crittografare irreversibilmente i dati in essi contenuti.

Tra la seconda metà del 2018 e la seconda metà del 2019, X-Force IRIS ha risposto al medesimo numero di attacchi, evidenziando come questi malware potenzialmente catastrofici continuino a mettere a rischio le organizzazioni.

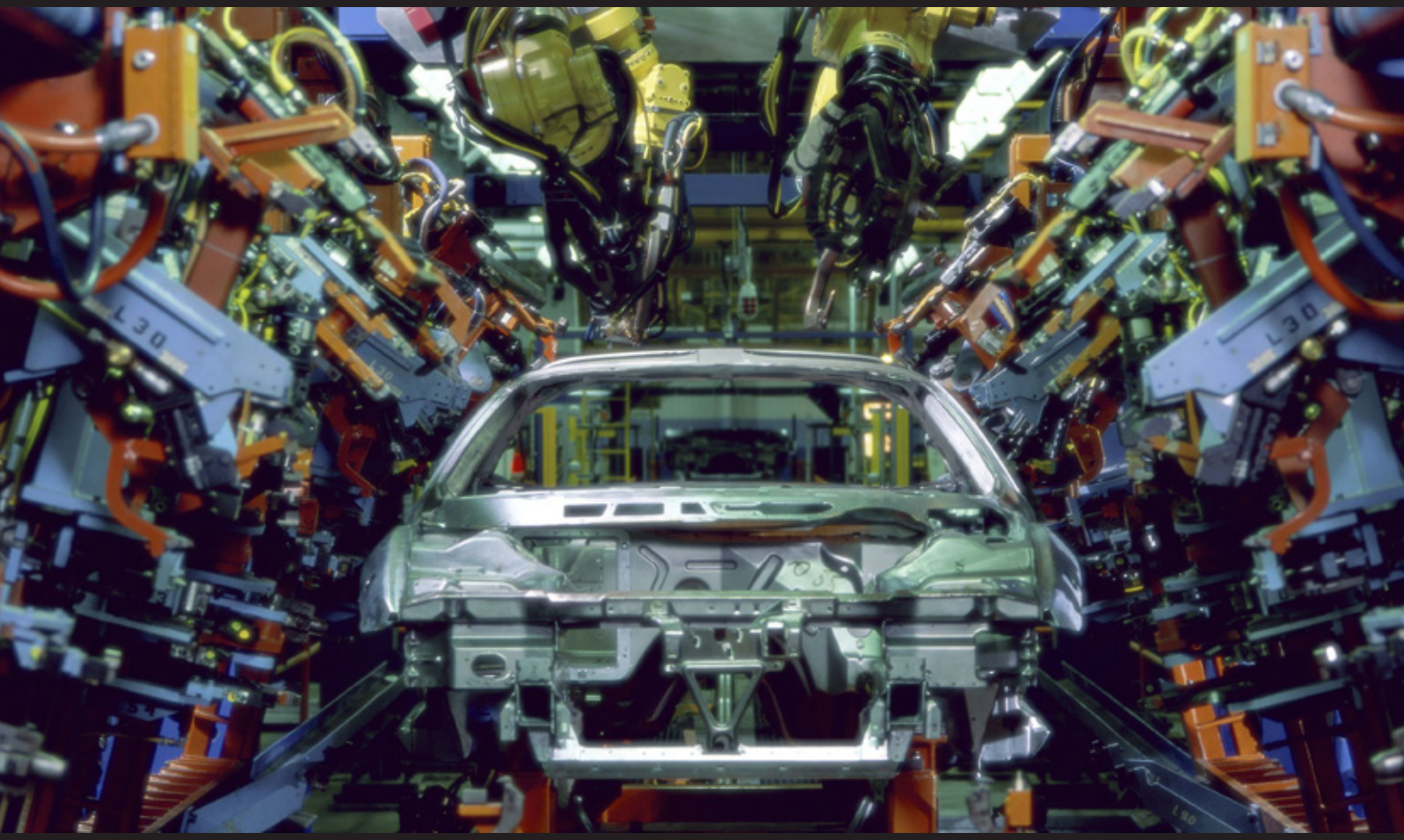
Storicamente, gli attacchi distruttivi normalmente sono stati generati da stati nazione avversari. Tuttavia, abbiamo anche osservato un trend in cui un maggior numero di ransomware orientati verso motivazioni finanziarie integrano componenti distruttivi come parte dell'attacco, con varianti come LockerGoga e MegaCortex che hanno effettuato il loro debutto tra la fine del 2018 e i primi mesi del 2019.



Le stime indicano che gli attacchi distruttivi causano costi pari a 239 milioni di dollari, un valore oltre 60 volte superiore ai costi di una violazione dei dati.

Alla fine del 2019, X-Force IRIS ha messo in evidenza la scoperta di un nuovo malware denominato ZeroCleare. Questo malware di tipo wiper, era indirizzato specificamente al settore energetico, e IBM lo ha associato a un gruppo APT di matrice iraniana denominato ITG13 2, noto anche come APT34/OilRig.

Le stime di X-Force IRIS indicano che i costi di un attacco malware distruttivo diretto verso le aziende può essere notevolmente elevato, con un numerose aziende multinazionali che hanno dovuto sostenere un costo medio per incidente pari a 239 milioni di dollari. Tale stima dei costi è 60 volte superiore rispetto alla media dei costi del 2019, in riferimento alle violazioni dei dati calcolate dal Ponemon Institute. A differenza delle semplici violazioni dei dati, che causano il furto o espongono i dati, gli attacchi distruttivi normalmente possono causare la distruzione di fino a tre quarti dei dispositivi dell'organizzazione oggetto degli attacchi.



2 L'acronimo ITG indica l'IBM Threat Group, un termine che sarà discusso in maniera più approfondita nella sezione dedicata ai settori industriali più colpiti. X-Force utilizza i nomi ITG e altri nomi alternativi indicati tra parentesi dopo l'acronimo ITG.

L’aggressività dei ransomware e dei cryptominer nel 2019

Il numero di varianti di malware e attacchi che utilizzano malware ha subito variazioni notevoli verso l’alto e verso il basso durante l'arco dell'anno. Tuttavia, i dati ottenuti su queste minacce consentono di prioritizzare le tipologie di minacce, aiutando le aziende a gestire i rischi in maniera più ottimale.

Durante la prima metà del 2019, circa il 19 percento degli attacchi osservati erano correlati ad incidenti ransomware. Un sostanziale incremento rispetto alla percentuale del 10 percento registrata nel 2018. Durante il quarto trimestre del 2019 è stato rilevato un incremento del 67 percento degli attacchi ransomware, rispetto al quarto trimestre dell’anno precedente. Durante il 2019, X-Force IRIS ha risposto a minacce ransomware in 12 paesi differenti sparsi su 5 continenti e 13 settori industriali differenti.

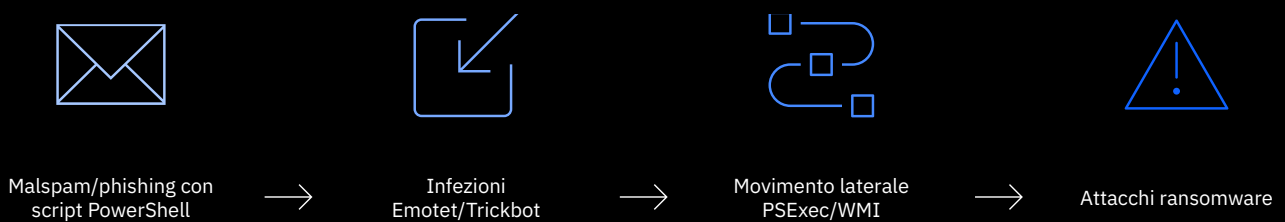
Tale incremento può essere attribuito al crescente numero di aggressori e delle campagne lanciate contro numerose organizzazioni nel 2019. Un settore particolarmente interessato da tali attacchi ransomware è stato quello delle istituzioni pubbliche e comunali, unitamente alle agenzie governative locali e ai provider del settore sanitario. Tali attacchi, hanno spesso colto le organizzazioni di tali settori impreparate e incapaci di rispondere, costringendole quindi a pagare un riscatto e, in alcuni casi, a incorrere in notevoli difficoltà a riprendere le attività dopo gli attacchi, a causa dei rischi per la sicurezza pubblica e la salute umana.

I dati di X-Force indicano che in alcuni casi di attacchi ransomware, i principali vettori di attacco nel 2019 sono stati rappresentati da tentativi di exploit contro le vulnerabilità dei protocolli Windows Server Message Block (SMB), che ne ha consentito la propagazione attraverso le reti. Questa tattica è stata utilizzata in precedenza negli attacchi WannaCry, che hanno costituito oltre l’80 percento dei tentativi di attacco osservati.

Durante il quarto trimestre del 2018 è stato rilevato un incremento del 67 percento degli attacchi ransomware, rispetto al quarto trimestre dell’anno precedente.

Figura 4:
Infezioni ransomware in fasi multiple

Attacchi ransomware mediante routine a fasi multiple (Fonte: IBM X-Force)



Gli attacchi contro le versioni vulnerabili del protocollo SMB possono essere automatizzati; un'alternativa a basso costo e semplice da scalare per gli aggressori, con la possibilità di danneggiare elevate quantità di sistemi con un singolo attacco.

Gli autori degli attacchi hanno anche utilizzato downloader di comodo, come Emotet e TrickBot, per eseguire i ransomware sui sistemi bersaglio. Questa tecnica, spesso ha fatto uso di PowerShell per scaricare il malware e diffonderlo utilizzando funzioni native come PSExec o Windows Management Instrumentation (WMI), che può essere più difficile da rilevare.

Anziché condurre l'attacco in un solo colpo, gli aggressori utilizzano fasi multiple per infettare gli utenti; ciò offre un migliore controllo dell'attacco, consentendo di evadere i controlli e di essere scoperti, ponendo le basi per un attacco ransomware che coinvolgerà un numero di dispositivi sufficiente a spingere le vittime a pagare. La redditività del capitale investito in termini di pazienza e pianificazione è spesso elevata; entro cinque mesi, gli attacchi condotti da Ryuk hanno consentito al gruppo criminale di accumulare oltre 3,7 milioni di dollari. In un altro caso, un attacco a una serie di cliniche private negli Stati Uniti ha consentito agli operatori di Ryuk di guadagnare un riscatto di 14 milioni di dollari.

Ma il ransomware non è stato il solo tipo di malware a registrare picchi importanti durante il 2019. Un'altra tipologia di malware divenuta estremamente popolare nel 2019 è stata quella dei codici per il mining delle criptovalute.

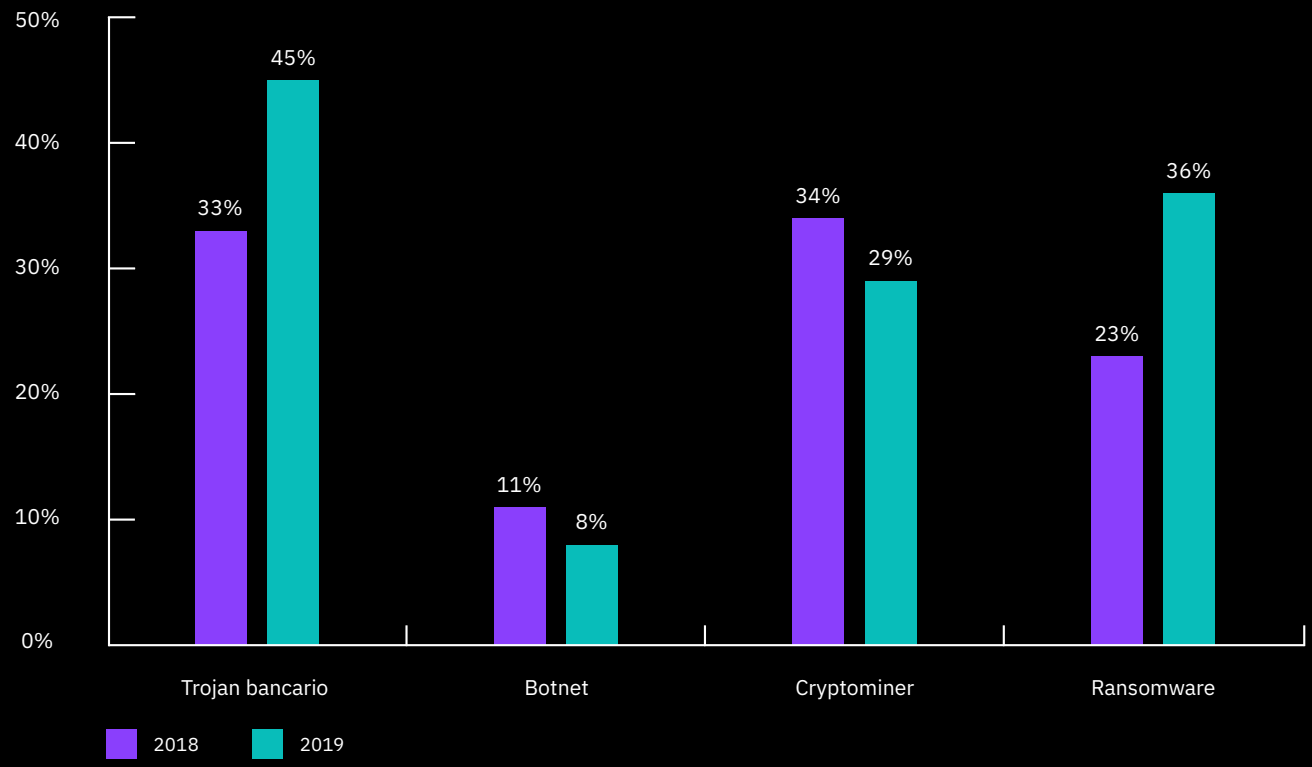
Secondo i dati telemetrici di X-Force, le attività di cryptomining hanno subito un picco senza precedenti a metà 2019, con un incremento di volume che a giugno ha superato tutte le altre attività di cryptomining registrate durante il resto dell'anno.

Sebbene i trend nel settore del malware tendano a variare in base a motivazioni e risorse disponibili per gli operatori delle botnet, questo picco specifico potrebbe essere correlato alla triplicazione del valore del Monero, una criptovaluta spesso utilizzata dai malware miner.

Figura 5:

Livello di innovazione del codice genetico del malware

Percentuale di nuovo codice (non osservato in precedenza), per categoria, 2018-2019 (fonte: Intezer)



I principali innovatori del 2019 nel settore dell'evoluzione del codice malware

Ispirandosi alle precedenti collaborazioni con X-Force nell'ambito del rilevamento delle nuove varianti di malware, Intezer ha utilizzato la sua tecnologia di analisi genetica del malware rivelando le origini genetiche di tutto il codice software per identificare le similarità di codice e il riutilizzo di codice per misurare il livello di "innovazione" nella creazione di nuovi malware. Questa misura di innovazione è rappresentata dall'entità degli investimenti che gli aggressori hanno effettuato nello sviluppo di nuovo codice. Un dato che indica che gli avversari stanno tentando di espandere le loro capacità di attacco e sfuggire all'identificazione.

I dati di Intezer indicano che nel 2019 gli aggressori si sono concentrati prevalentemente sullo sviluppo e l'evoluzione del codice di base per i cavalli di Troia e il ransomware per i servizi di banking, mantenendo un elevato livello di impegno verso la modifica e la creazione di differenti ceppi di malware per il cryptomining.

Questa sezione del rapporto è stata scritta in collaborazione con i ricercatori IBM X-Force e Intezer. Intezer effettua l'analisi genetica del codice binario del malware.

Nel 2019, i cavalli di Troia dedicati al banking hanno fatto registrare il maggiore incremento di nuovo codice (45 percento), seguiti dal ransomware (36 percento). Storicamente, IBM vede questo interesse e gli investimenti in queste tipologie di malware come strumenti efficaci contro gli utenti aziendali. Ciò suggerisce che queste famiglie di malware potrebbero attaccare le aziende nel 2020. Se non evolvono costantemente, gli aggressori che utilizzano cavalli di Troia e ransomware per il banking rischiano l'estinzione, in quanto i malware generati vengono rilevati e neutralizzati rapidamente; una prassi che riduce la redditività del capitale investito nell'arco del tempo.

Nel 2019, i criminali informatici si sono concentrati sullo sviluppo e l'evoluzione del codice di base per cavalli di Troia e ransomware per il banking.

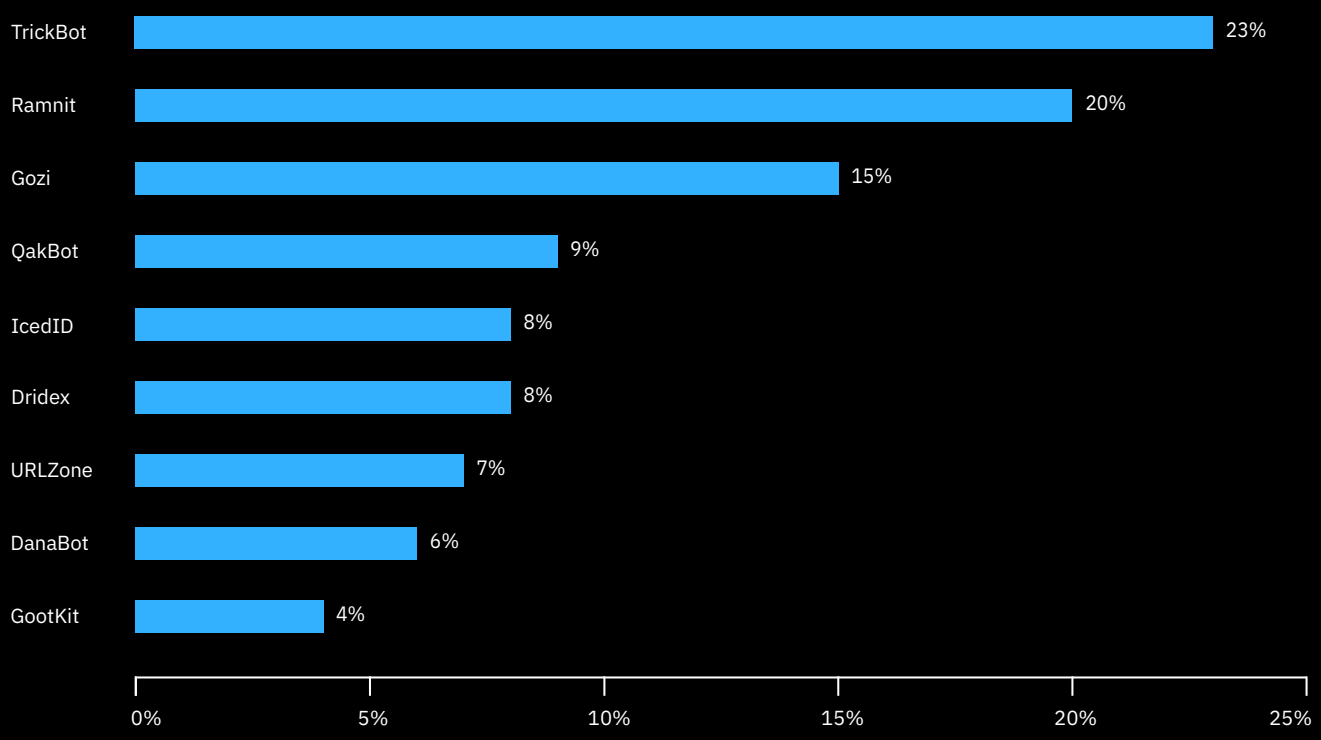
Nel 2019, i cryptominer hanno evidenziato un calo dell'innovazione nel 2019, ma il volume delle attività di mining era ancora elevato. Ciò suggerisce che i criminali informatici continuano a sviluppare nuove versioni di cryptominer che però si affidano in larga parte a codice già esistente. In base all'esperienza di IBM, questi codici semplici codici malware spesso fanno affidamento su antenati non progettati con scopi maligni, come XMRig per esempio, poi modificati per il mining illegale di criptomoneta. I nuovi miner sono anche scritti per scopi differenti, come la raccolta di criptomoneta su dispositivi IoT, oppure, in altri casi, per l'uso su server infetti, in cui la potenza della CPU è superiore rispetto ai dispositivi mobili e ai PC individuali.

Per converso, il malware generico per botnet (11 percento), conteneva meno innovazione del codice rispetto all'anno precedente, e ciò indica una quantità di investimenti inferiore per la modifica delle capacità di tali tipologie di minacce. IBM ha osservato come queste tipologie di codice siano inviate agli utenti vittima attraverso spam o malvertising. Il ruolo principale del malware per botnet generiche è quello di conquistare una testa di ponte su un dispositivo infetto. Ma le funzionalità di tale malware restano minime, e ciò spiega perché tali tipologie di minacce non sono soggette a grandi investimenti in termini di evoluzione del codice.

Traslando i trend di innovazione del codice nel contesto di settore per il 2020, tali tendenze possono essere indice di tipologie di malware che richiederà un maggiore sforzo per l'identificazione e il contenimento a causa degli investimenti richiesti per aggiornare costantemente il codice.

Figura 6:
Principali famiglie di cavalli di Troia

Riepilogo dettagliato delle principali famiglie di cavalli di Troia nel 2019, sottoforma di percentuali delle nove famiglie di cavalli di Troia indicate (fonte: IBM X-Force)



Trojan e ransomware dedicati al banking – Una combinazione malefica che peggiora con l'andare del tempo

Il settore del malware finanziario è divenuto un problema comune da circa un decennio. Ciò a causa dell'incremento di malware come Zeus Trojan, che all'epoca era il primo cavallo di Troia dedicato al banking commerciale disponibile nel settore del crimine informatico globale. Un'analisi del panorama delle minacce per il settore finanziario nel 2019 indica un chiaro trend in ascesa per i gruppi operanti nel settore dei cavalli di Troia per il banking. Queste botnet malware sono sempre più utilizzate come strumento per stabilire una testa di ponte che consente di effettuare attacchi ransomware di alto livello.

Una tabella delle famiglie di cavalli di Troia più diffuse in questa categoria di minacce per il 2019, appare piuttosto simile a quella ottenuta nel rapporto riepilogativo annuale del 2018. TrickBot, Gozi, e Ramnit restano in vertice alla classifica, occupando le prime tre posizioni. Questi cavalli di Troia sono utilizzati da gruppi organizzati che offrono svariati modelli aziendali per altri tipi di criminali informatici, come programmi botnet-as-service e distribuzione di contenuti attraverso risorse compromesse.

La gang che utilizza TrickBot è stata, finora, di gran lunga quella più attiva tra i gruppi operanti nel settore della pirateria informativa nel 2019. Queste attività si manifestano in vari modi:

— Frequenza degli aggiornamenti e delle correzioni del codice (codice, versione ed evoluzione delle funzionalità)

— Frequenza e scala delle campagne di infezione

— Frequenza e volume delle attività di attacco

Le gang che hanno occupato i titoli dei giornali grazie a una serie di importanti attacchi di ransomware nel 2019 sono le stesse che si sono rese protagoniste di attacchi informatici di alto profilo nel 2015. In un certo senso, la strategia di base è la stessa; solo le tattiche cambiano nel tempo, con le aziende come obiettivo primario per estorcere profitti maggiori.

I principali esempi di cavali di Troia tramutati in ransomware per il banking includono:

Dridex
In precedenza dedicato alla diffusione del bot LokiBot sui dispositivi degli utenti, è ora utilizzato per diffondere le minacce BitPaymer/DopplePaymer sulle reti aziendali.

GootKit
Sospetto vettore di infezione del payload LockerGoga su reti aziendali. LockerGoga è apparso all'inizio del 2019 e da allora ha costituito un elemento fondamentale di importanti attacchi aziendali.

QakBot
Diffonde il payload MegaCortex sulle reti aziendali.

TrickBot
Diffonde il payload Ryuk sulle reti aziendali.

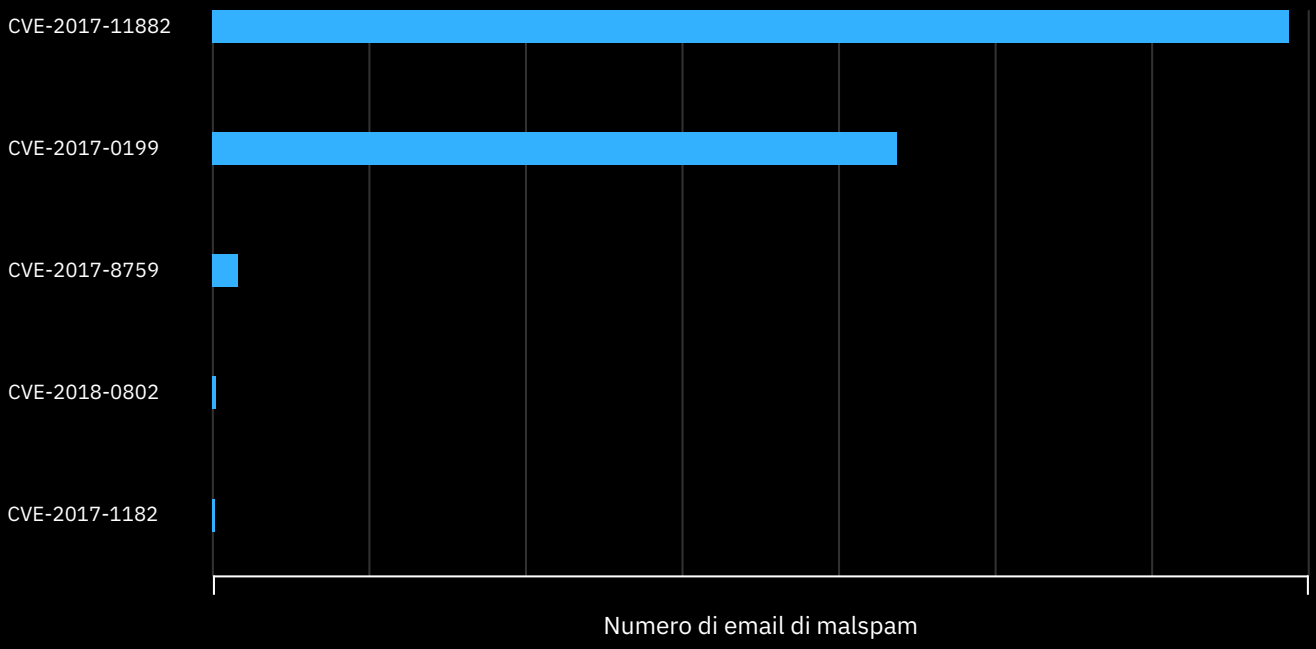
Inoltre, i rapporti redatti alla fine del 2019 indicano che ITG08, (FIN6), un gruppo storicamente dedito al furto su larga scala di dati di carte di credito, ha iniziato anch'esso a diversificare le sue attività. Tali attività ora includono anche l'implementazione di ransomware e reti aziendali. L'accumulo e la vendita o l'uso dei dati delle carte di credito rubate, può richiedere tempo e notevole impegno per monetizzare i dati acquisiti, mentre un attacco ransomware è potenzialmente in grado di raccogliere milioni di dollari in un singolo colpo. Ciò ha convinto sempre più gruppi a dedicarsi a tipologie di attacchi basati su ransomware e estorsione informatica.

Trend nel settore dello spam e del phishing

Figura 7:

Principali vulnerabilità utilizzate nello malspam

Riepilogo dettagliato delle principali vulnerabilità negli allegati di malspam nel 2019, per volume (fonte: IBM X-Force)



Le vulnerabilità del 2017 nell'ambito dello spam continuano a costituire una priorità anche nel 2019

IBM X-Force utilizza spam trap in tutto il mondo, monitorando decine di milioni di messaggi di spam e phishing ogni giorno. I nostri team e le nostre tecnologie analizzano milioni di pagine e immagini web, per rilevare attività fraudolente e abusi di marchi.

L'analisi dello spam globale effettuata da X-Force indica che le email di spamming continuano a utilizzare un ridotto subset di vulnerabilità, che si concentra in particolare su due soli CVE: 2017-0199 e 2017-11882. Entrambe queste vulnerabilità sono state corrette e hanno rappresentato circa il 90 delle minacce associate a vulnerabilità che i criminali informatici hanno cercato di sfruttare attraverso campagne di spamming. Entrambi questi CVE colpiscono Microsoft Word e non richiedono alcuna interazione da parte dell'utente a parte l'apertura di un documento contenente la minaccia.

I nostri dati degli eventi indicano che la frequenza di utilizzo di queste due vulnerabilità da parte degli aggressori nel 2019 è stato superiore a qualunque altra vulnerabilità associata all'esecuzione di codice per Microsoft Word, con un rapporto di 5 a 1.

Sebbene tali due vulnerabilità siano presenti in un cospicuo numero di email, non vi è alcuna indicazione del livello di successo conseguito negli attacchi verso gli utenti. Detto ciò, lo spam è spesso una questione di numeri; con un volume adeguato, spesso anche una ridotta percentuale di successo è sufficiente per generare valore per i criminali. Dato che numerosi utenti e anche organizzazioni possono trascurare l'installazione delle patch per risolvere determinate vulnerabilità, è ancora possibile rilevare dispositivi compromessi da vecchi bug.

Ci sono molte spiegazioni per la popolarità di utilizzo di vecchie vulnerabilità, inclusa la semplicità di integrazione e disponibilità di generatori di documenti gratuiti, la loro continua efficacia, oppure la loro versatilità nell'iniettare un'ampia varietà di payload maligni.

Il costante utilizzo delle vecchie vulnerabilità mette in evidenza la lunga scia di attività maligne e in che modo significative vulnerabilità possono ancora essere utilizzate contro gli utenti anche dopo anni dalla loro scoperta e dal rilascio delle relative patch correttive.

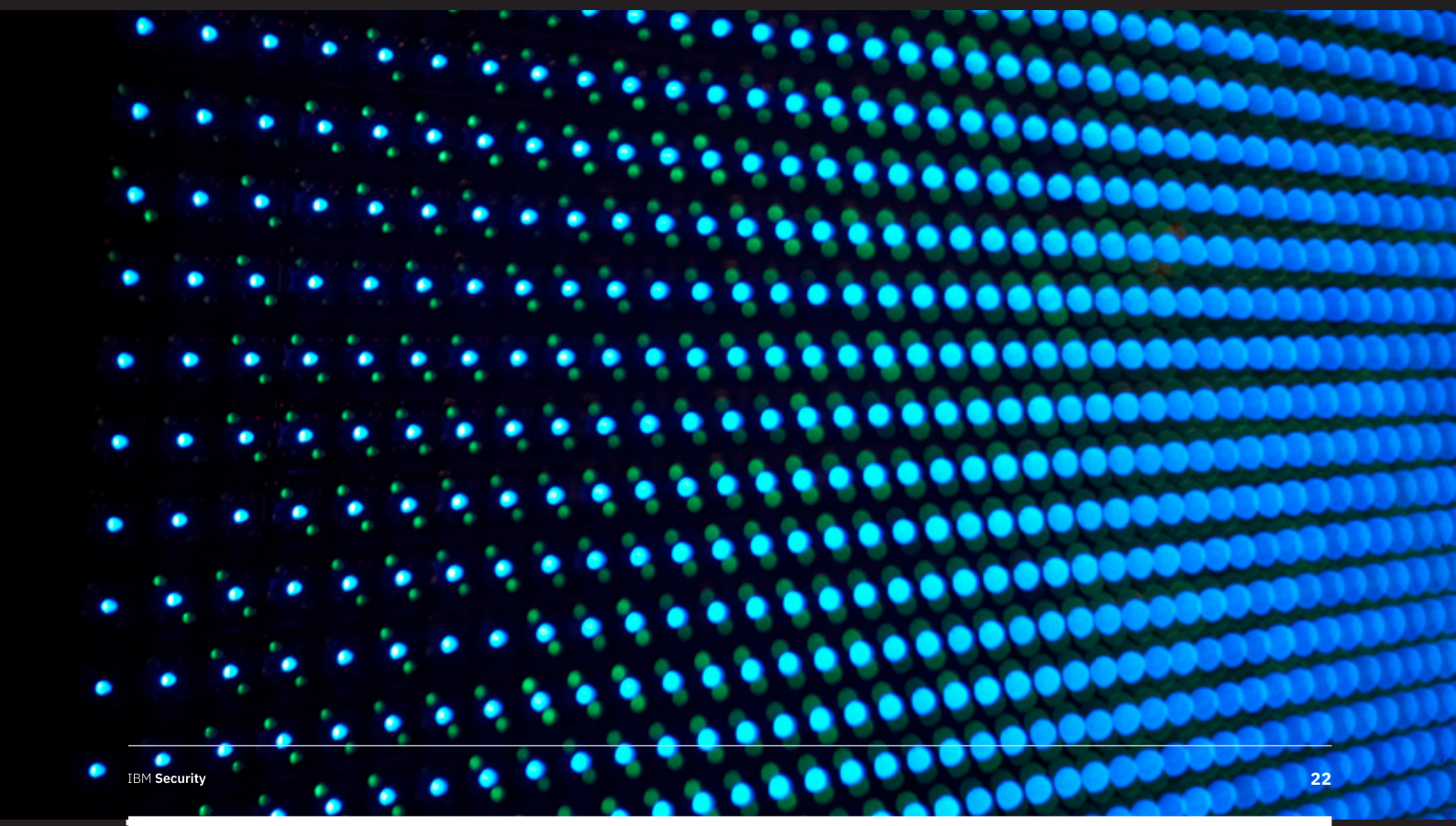
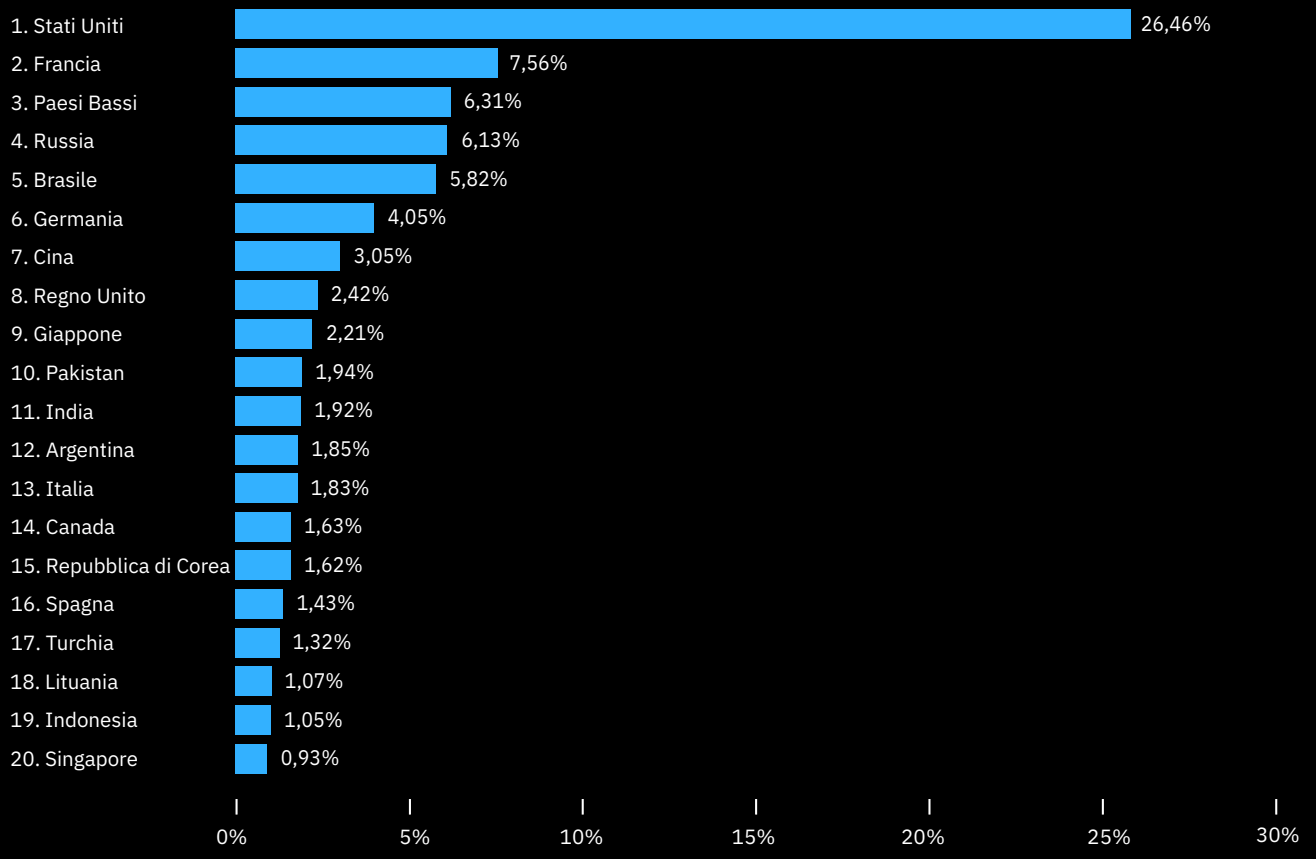


Figura 8:

Primi 20 paesi in cui sono ospitati server C2 di spamming

Riepilogo dettagliato, sottoforma di percentuale, dei primi 20 paesi in cui sono basate le architetture di comando e controllo dello spamming, per il 2019 (proporzione di server C2 totali nei principali 20 paesi = 80,6%) (fonte: IBM X-Force)



Le botnet di spamming situate in occidente hanno un impatto globale

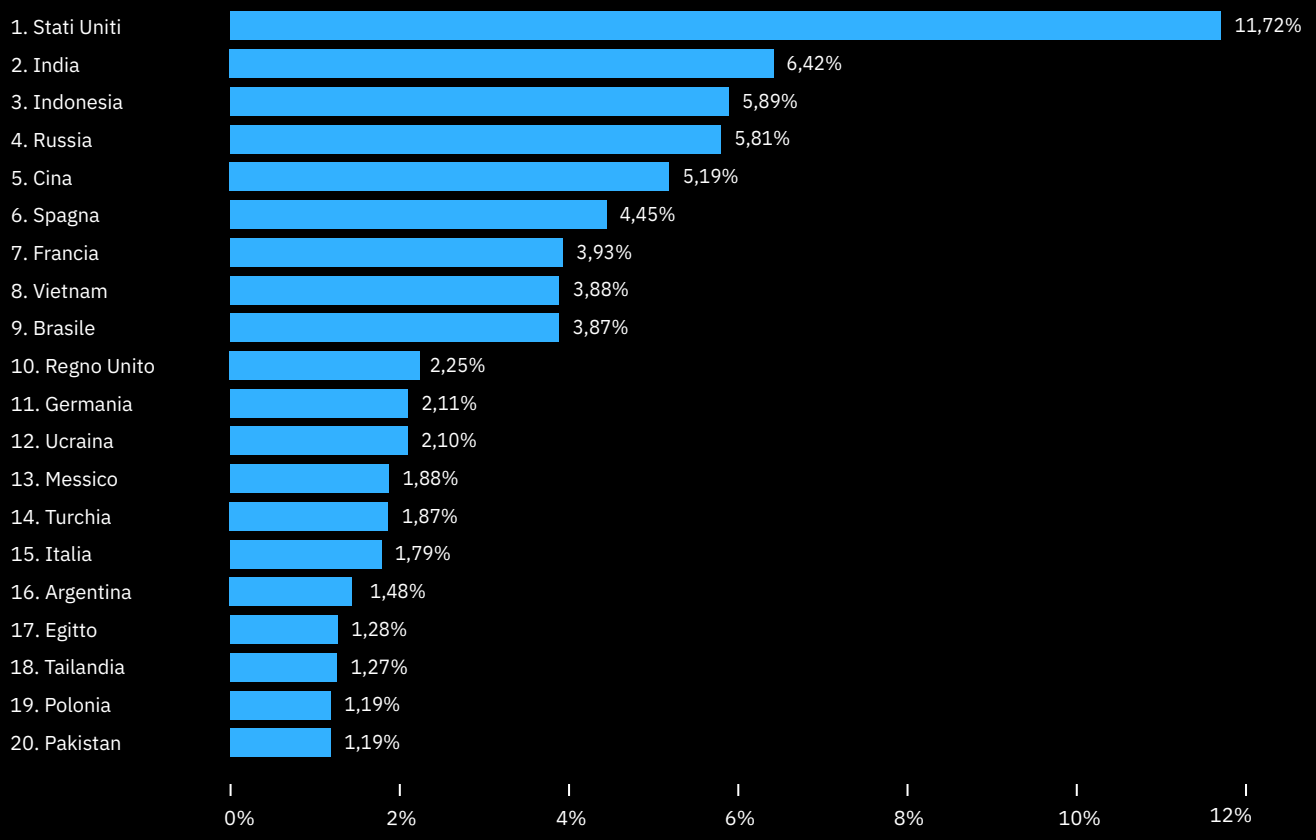
La ricerca di IBM X-Force nel settore delle botnet di spamming analizza un'ampia gamma di punti dati geo-specifici associati alle infrastrutture di comando e controllo (C2) per le botnet di spamming. Uno dei parametri che abbiamo misurato è la posizione geografica in cui sono ospitate le botnet C2. Nel 2019 abbiamo rilevato che le infrastrutture C2 erano ospitate prevalentemente in Nord America e Europa occidentale, con oltre la metà dei casi di CS osservati nel 2019. Gli altri casi di hosting C2 erano suddivisi in un ampio spettro di regioni in aree diverse del globo.

In molti casi, l'infrastruttura C2 della botnet è ospitata su server compromessi, e l'impiego di server Nordamericani ed Europei è in linea con il fatto noto che questi paesi in genere hanno tempi di attività dei server generalmente più elevati. Inoltre, i criminali informatici preferiscono basare i loro attacchi sulle risorse locali, in quanto tali attacchi hanno meno probabilità di essere scoperti quando il traffico di questi server opera con dispositivi e reti associate alla stessa area geografica.

Figura 9:

Primi 20 paesi in termini di vittime delle botnet di spamming

Riepilogo dettagliato dei primi 20 paesi in cui risiede il totale degli utenti vittime delle botnet, sottoforma di percentuale di utenti totali colpiti dalle botnet nei primi 20 paesi indicati per l'anno 2019 (proporzione totale di client botned nei 20 principali paesi = 69,6%) (fonte: IBM X-Force)



Vittime dello spam per area geografica

Nel 2019 le vittime delle botnet di spamming interessano l'intero globo, con gli Stati Uniti che occupano il primo posto in termini di vittime, seguiti da India, Indonesia, Russia e Cina. Questa distribuzione degli obiettivi degli attacchi è in linea con le motivazioni degli spammer, il cui obiettivo è quello di raggiungere il maggior numero di destinatari possibile, attraverso campagne di spamming caratterizzate da elevati volumi di mail. Naturalmente, i paesi con popolazioni di grandi dimensioni sono oggetto di un maggior numero di email di spamming.

I domini maligni bloccati evidenziano una prevalenza di servizi di anonimizzazione

Quando si tratta di mantenere le reti al sicuro dalle minacce online, uno dei metodi più diffusi consiste nell'impedire a utenti e risorse di comunicare con domini potenzialmente o notoriamente maligni. Al fine di minimizzare tale rischio, molte organizzazioni utilizzano le blocking list per effettuare il blacklisting degli indirizzi IP sospetti. Utilizzando lo stesso presupposto su scala globale, Quad9, un servizio DNS (Domain Name Server)[3], blocca in media 10 milioni di richieste DNS maligne al giorno.

Quad9 secondo un campione di dati di Quad9 correlato a una ricerca di intelligence delle minacce condotta da IBM Security, gli URL associati alle email di spamming costituivano la maggioranza delle richieste DNS sospette, con una percentuale pari al 69 percento del totale nel 2019. Sebbene tale percentuale indichi un calo rispetto al 77 percento del 2018, la categoria degli URL di spamming rappresenta ancora la principale origine di domini maligni rispetto al totale. Il calo di 8 punti percentuali potrebbe essere attribuibile alla categoria di anonimizzazione dei servizi, che costituisce il 24 percentuale delle richieste DNS.

Lo spam email resta uno dei metodi più efficaci per raggiungere il maggior numero di potenziali vittime. Ciò grazie alle vaste botnet di spamming, come Necurs botnet, che inviano quotidianamente milioni di messaggi di spamming. I domini maligni spesso diffondono malware al fine di distribuire ransomware, script finalizzati al furto di credenziali o link che reindirizzano gli utenti vero ulteriori frodi. Questi sistemi sono progettati per ingannare gli utenti, presentandosi come messaggi legittimi o simulando una comunicazione inviata da un marchio noto agli utenti.

Il collegamento agli URL maligni nei messaggi di spamming è anche il metodo preferito per la stragrande maggioranza di attori guidati da motivazioni finanziarie, in quanto ciò consente loro di gettare un'ampia rete con il minimo sforzo, oppure optare per target specifici in base all'area geografica, limitando in tal modo la visibilità delle loro iniziative di scamming.

La tabella in figura 10 mostra la distribuzione delle tipologie di domini maligni registrati da IBM Security nel 2019.

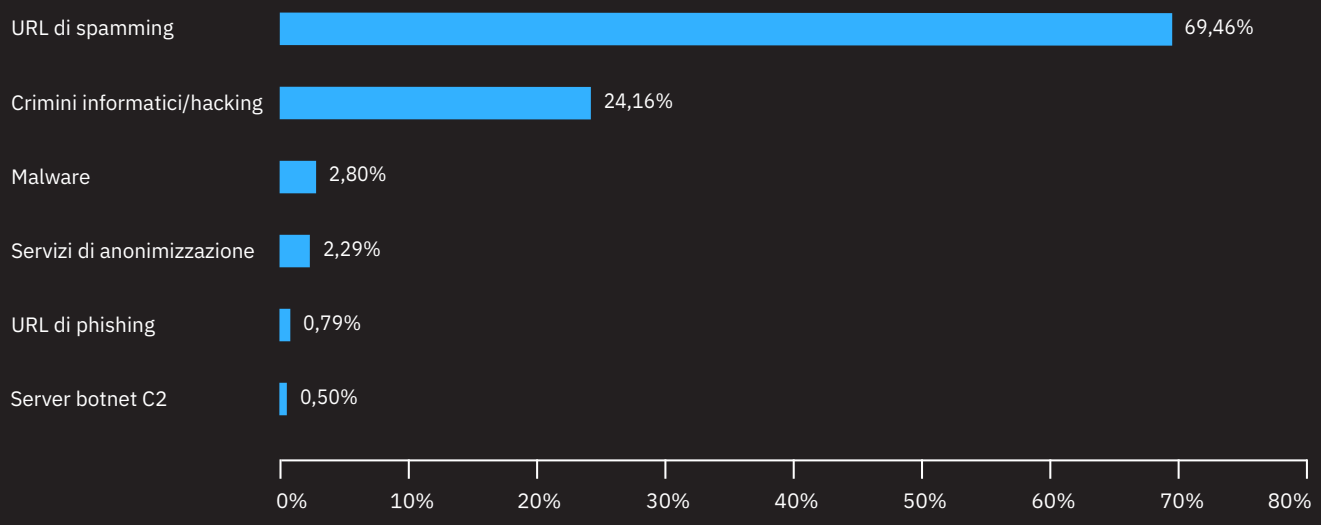
Lo spamming via email resta uno dei metodi più efficaci per raggiungere il più ampio numero di potenziali vittime.

3 Quad9 è stato creato e sponsorizzato attraverso una collaborazione tra IBM, Packet Clearing House (PCH) e Global Cyber Alliance (GCA).

Figura 10:

Principali minacce utilizzate dai domini maligni

Riepilogo dettagliato dei principali domini con contenuti maligni e minacce, espresso in forma di percentuale suddivisa in sei categorie per l'anno 2019 (fonte: IBM X-Force e Quad9)



URL di spamming:
Domini collegati a siti affiliati con campagne di spamming. Spesso fastidiosi ma non associati ad altre attività criminali

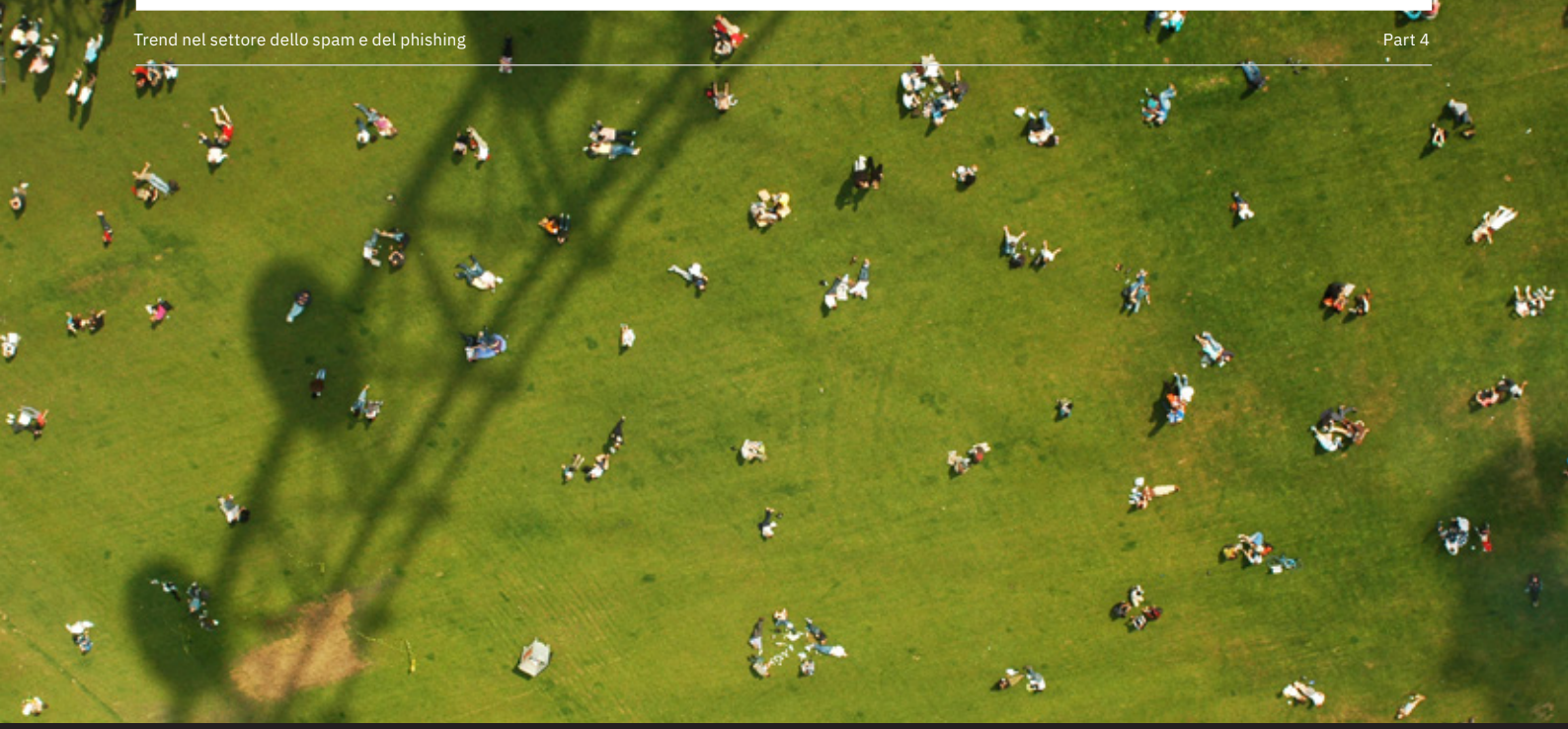
Servizi di anonimizzazione:
Domini collegati a provider di anonimizzazione che nascondono il traffico prevenendone l'identificazione

Crimini informatici/hacking:
Domini specificamente associati ad attività criminali, come siti che ospitano script che sfruttano le vulnerabilità dei browser web

URL di phishing:
Falsi domini che impersonano altri domini legittimi, normalmente al fine di ottenere le credenziali degli utenti o altre informazioni sensibili

Sistemi di comando e controllo delle botnet:
Domini collegati alle attività botnet e visitatori a rischio di infezione

Malware:
Domini che ospitano malware noto



I provider di servizi di anonimizzazione, come Tor, per esempio, consentono agli utenti di anonimizzare l'origine del traffico internet, facendolo passare attraverso nodi gestiti da altri attori. Sebbene i servizi di anonimizzazione: possano, e spesso svolgano di fatto un ruolo legittimo, garantendo agli utenti una maggiore privacy durante la navigazione web, il loro utilizzo può anche rendere più difficile o impossibile monitorare e bloccare le attività maligne.

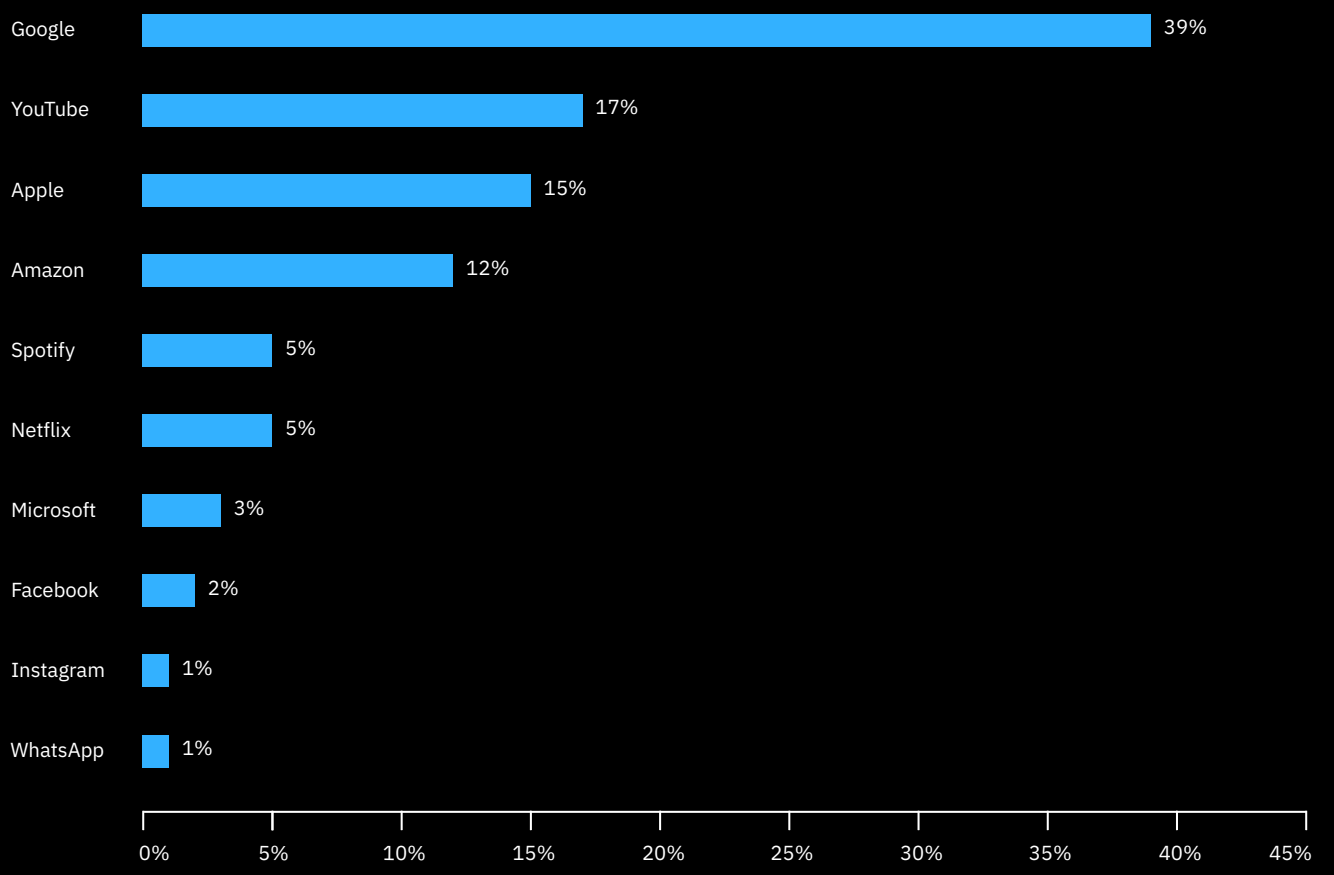
L'anonimizzazione è una pratica comune utilizzata dai criminali informatici per cercare di eliminare le tracce delle loro attività, in quanto tale pratica consente di offuscare i link maligni, estrarre dati senza attivare le regole DLP (Data Loss Prevention), oppure di iniettare ulteriori payload maligni prima che un determinato IP server venga bloccato.

Il quattro percento delle richieste DNS maligne rientravano nella categoria dei crimini informatici o in quello dell'hacking di pagine web da parte di gruppi blackhat, in cui alcuni criminali tentano di violare i browser web, distribuire informazioni su frodi o attuare altre attività criminali online. Questo numero relativamente ridotto è probabilmente dovuto al fatto che questi link sono spesso instradati attraverso nodi di anonimizzazione, oppure rilevati e bloccati attraverso proxy e firewall aziendali, e successivamente disattivati.

Figura 11:

La top 10 dei marchi oggetto di imitazione

Riepilogo dettagliato dei primi 10 marchi oggetto di spoofing nel 2019, sottoforma di percentuali per i 10 marchi mostrati (fonte: IBM X-Force)



Il phishing ha impersonato aziende tecnologiche e social media

Il phishing ha continuato a rappresentare una minaccia chiave nel 2019. I dati di X-Force indicano che i marchi più esposti allo spoofing nelle campagne di phishing sono stati quelli del settore tecnologico e le piattaforme social media. I domini oggetto di spoofing possono essere difficili da identificare visivamente per gli utenti. Spesso, tali siti sono una copia identica dei domini utilizzati dall'azienda reale. Un sito falso ma dall'aspetto realistico può convincere gli utenti a divulgare dati personali su un sito maligno.

Tali dati sono stati ottenuti attraverso l'analisi dei domini maligni bloccati da Quad9 nel 2019 e basati sui rilevamenti di domain-squatting effettuati da IBM X-Force.

Prendere di mira social media o siti dedicati allo streaming di contenuti, come Instagram o Spotify, potrebbe non consentire agli aggressori di monetizzare i dati con sufficiente rapidità, come invece accade nel caso del furto di credenziali degli account Google o Amazon. Tuttavia, gli aggressori potrebbero confidare nella possibilità che gli utenti riutilizzino la stessa password con account e servizi differenti, al fine di utilizzare le credenziali raccolte per cercare di accedere ad account di maggior valore dello stesso utente.

Settori maggiormente interessati dagli attacchi

Nell’attuale panorama delle minacce, la specificità di alcune tipologie di attacchi, sulla base delle motivazioni degli aggressori, fa si che la gestione dei rischi informatici assuma sfumature notevolmente differenti tra un settore e l’altro.

Al fine di ottenere una panoramica dei settori industriali più colpiti, ogni anno i ricercatori di X-Force classificano il volume degli attacchi osservati per ciascun settore. I settori industriali presi di mira con maggior frequenza sono stati determinati in base ai dati su attacchi e incidenti ricavati dalle reti gestite di X-Force, nonché dai dati e dalle informazioni ottenute dai nostri servizi di reazione agli incidenti e dagli incidenti divenuti di pubblico dominio.

Figura 12:

10 principali settori industriali oggetto di attacchi

I primi 10 settori industriali classificati per volume di attacchi, 2018 e 2019 a confronto (fonte: IBM X-Force)

Settore	Classifica 2019	Classifica 2018	Cambiamento
Servizi finanziari	1	1	–
Retail	2	4	2
Settore dei trasporti	3	2	-1
Media	4	6	2
Servizi professionali	5	3	-2
Settore governativo	6	7	1
Formazione	7	9	2
Produzione industriale	8	5	-3
Settore energetico	9	10	1
Settore sanitario	10	8	-2

La figura 12 illustra una tabella comparativa raffigurante il settore più colpiti nel 2019 e la differenza con i dati del 2018.

È semplice osservare come, sebbene non ci fosse alcuna sorpresa sul fronte dei servizi finanziari, il settore al dettaglio ha fatto registrare un crescente interesse da parte degli aggressori. Lo stesso è accaduto anche per i settori dei media e dell’intrattenimento, dell'educazione e per le agenzie governative.

Le seguenti sezioni offrono una descrizione approfondita della frequenza relativa dei bersagli, ottenute sulla base di differenti sorgenti dati e in base alle nostre ricerche effettuate in ciascuno di tali settori nel 2019. Le descrizioni di alcuni settori indicano come gli aggressori siano stati particolarmente attivi nel prendere di mira settori specifici negli anni recenti. Tuttavia, tale lista non è esaustiva e include dati precedenti al 2019. X-Force IRIS monitora e profila dozzine di gruppi di criminali informatici e sponsorizzati dai governi. Le attività riconducibili a sorgenti e campagne non identificabili scoperte, vengono monitorate sottoforma di attività “HIVE”. Una volta che l’attività risulta conforme ai rigidi standard di analisi, viene trasferita a un IBM Threat Group (ITG), il cui ruolo è quello di effettuare la raccolta di TPP, infrastrutture target e strumenti.

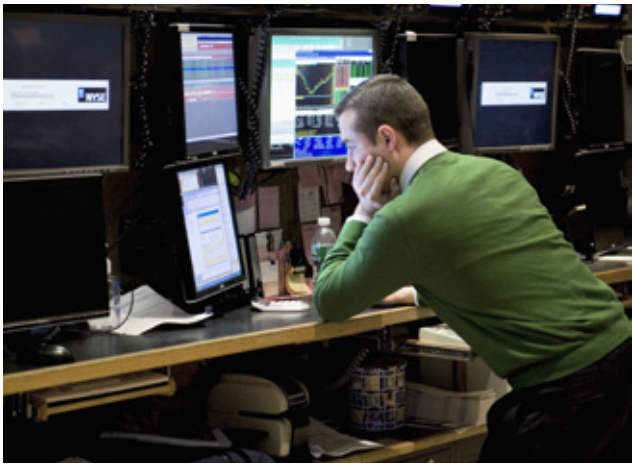
Finanza e assicurazioni

Da quattro anni consecutivi il settore finanziario e assicurativo rappresenta quello maggiormente interessato dagli attacchi. Il 2019 conferma questo trend. Gli attacchi in questo settore hanno costituito il 17 percento del totale, nella top 10 dei settori più colpiti.

Con tutta probabilità, i criminali informatici guidati da motivazioni finanziarie rappresentano la maggioranza degli attori criminali operanti in questo settore. L'attrattività delle aziende del settore finanziario per i criminali informatici è chiara, con la potenziale prospettiva di profitti notevoli e rapidi, che possono ammontare a milioni di Euro quando gli attacchi vanno a buon fine.

I dati relativi alle risposte agli incidenti registrati da X-Force indicano che i settori finanziario e assicurativo erano i primi tra quelli colpiti, nonostante l'esiguo numero di violazioni rivelate pubblicamente

Ciò suggerisce che le aziende finanziare e assicurative tendono a essere soggette a un maggior volume di attacchi relativi ad altri settori, ma proprio per questo motivo, esse tendono anche a disporre di migliori strumenti e processi per l'identificazione e il contenimento delle minacce prima che queste si tramutino in incidenti gravi. Le aziende del settore finanziario sono anche quelle più inclini a mettere alla prova i loro piani di reazione, e costituiscono un'importante fetta delle aziende che utilizzano i servizi degli IBM Security Command Center per le attività di preparazione e contrasto contro le minacce informatiche. I test estesi di piani di reazione e team contro le minacce in scenari realistici, si sono rivelati efficaci per mitigare i danni finanziari derivanti da violazioni dei dati, secondo un rapporto denominato "2019 Cost of Data Breach Report"[4], condotto dal Ponemon Institute e sponsorizzato da IBM Security.Per esempio, le organizzazioni oggetto di violazioni i cui piani di reazione erano stati sottoposti a test estensivi in un ambiente che simulava una serie di minacce informatiche, in media hanno perso 320.000 dollari in meno in termini di costi, nel caso di violazioni dei dati che hanno causato una perdita totale di 3,92 milioni.



I principali gruppi di aggressori dedicati al settore finanziario nel 2019 sono stati ITG03 (Lazarus), ITG14 (FIN7) e varie fazioni di Magecart. I cavalli di Troia dedicati al banking, come TrickBot, Ursnif e URLZone hanno costituito le principali minacce per il settore bancario nel 2019, spesso riuscendo a carpire le informazioni e sfruttando gli account degli utenti per portare a termine numerose frodi.

4 Il rapporto annuale "Cost of a Data Breach Report" è condotto dal Ponemon Institute e sponsorizzato da IBM.

Dettaglio

Secondo i dati ricavati da X-Force nel 2019, il settore al dettaglio occupa il secondo posto tra i settori più attaccati. Tra i principali 10 settori, questo settore specifico è stato colpito dal 16 percento degli attacchi totali; un notevole incremento rispetto al quarto posto e all'11 percento degli attacchi registrati nel 2018. Questo settore ha fatto registrare il secondo maggior numero di attacchi alle reti nel 2019.

Nel 2019, il settore al dettaglio occupava il secondo posto, in base ai dati ottenuti da X-Force IRIS e dalle informazioni pubbliche diffuse in materia di violazioni dei dati. La tipologia di aggressore più comune per le aziende del settore del commercio al dettaglio è quella dei criminali informatici guidati da motivazioni finanziarie, che attaccano le aziende del settore al fine di ottenere informazioni personali che identificano gli utenti (PII), dati delle carte di pagamento, dati finanziari, cronologie degli acquisti e informazioni sui programmi fedeltà. I criminali informatici tipicamente utilizzano questi dati per penetrare negli account degli utenti, frodare gli utenti e riutilizzare i dati per svariate tipologie di furti.

Una tecnica di attacco diffusa tra i criminali informatici nel 2019 è consistita nel prendere di mira i punti vendita al dettaglio. In particolare, le tecniche utilizzate includevano malware per i punti vendita (POS) e lo skimming delle carte di credito nel settore dell'e-commerce, ciascuno dei quali ha lo scopo di carpire i dati delle carte di pagamento durante le transazioni effettuate mediante terminali di pagamento fisici o online, rispettivamente.

In particolare, un gruppo di fazioni di criminali informatici, denominate Magecart, ha preso di mira le piattaforme di pagamento di provider terzi e note catene al dettaglio online, attraverso l'iniezione diretta di codice JavaScript maligno nelle pagine web contenenti i dati delle carte di pagamento. Il codice viene eseguito come parte del processo di checkout, allo scopo di trasmettere i dati delle carte di pagamento della vittima ai criminali informatici, mentre questi transitano verso la piattaforma del venditore legittimo.

I rispondenti agli incidenti del team di X-Force IRIS hanno notato come questi tipi di attacchi abbiano causato molteplici violazioni nel 2019, sottolineando che, sebbene le porzioni di codice maligno siano essenzialmente molto elementari, la compromissione delle piattaforme di backend sottostanti sia stata in grado di causare un danno aggregato elevato, consentendo ai criminali di colpire migliaia di punti vendita mediante la stessa tecnica.

Principali gruppi di criminali informatici che hanno preso di mira il settore della vendita al dettaglio includono:

ITG14 (FIN7)	Hive0061 (Magecart 10)
HIVE0065 (TA505)	Hive0062 (Magecart 11)
ITG08 (FIN6)	Hive0066 (Magecart 12)
Hive0038 (FIN6)	Hive0067 (FakeCDN)
Hive0040 (Cobalt Gang)	Hive0068 (GetBilling)
Hive0053 (Magecart 2)	Hive0069 (Illum Group)
Hive0054 (Magecart 3)	Hive0070 (PostEval)
Hive0055 (Magecart 4)	Hive0071 (PreMage)
Hive0056 (Magecart 5)	Hive0072 (Qoogle)
Hive0057 (Magecart 6)	Hive0073 (ReactGet)
Hive0058 (Magecart 7)	Hive0083 (Inter Skimmer)
Hive0059 (Magecart 8)	Hive0084 (MirrorThief)
Hive0060 (Magecart 9)	Hive0085 (TA561)

Oltre agli skimmer per il commercio online, i malware per punti vendita continuano a rappresentare una tecnica diffusa tra i criminali informatici per gli attacchi nel settore al dettaglio e ai punti vendita fisici. Tali attacchi hanno come obiettivo quello di intercettare i dati delle carte di pagamento utilizzate presso i punti vendita e nei server di backend durante le transazioni o mentre i dati della carta vengono trasferiti in memoria.

Settore dei trasporti

Il settore dei trasporti è considerato parte dell'infrastruttura critica di un dato paese. Le aziende di questo settore mobilizzano l'economia attraverso tre principali tipologie di trasporti, inclusi i trasporti via terra, via mare e via aria, sia nel settore industriale che in quello dei servizi ai consumatori. Questo settore occupa il terzo posto tra quelli maggiormente soggetti ad attacchi nel 2019, con una riduzione che va dal 13 percento del 2018 al 10 percento nel 2019.

Il terzo posto del settore dei trasporti, dietro al settore finanziario e di quello al dettaglio, sottolinea la crescente attenzione dei criminali verso i dati e le infrastrutture gestite dalle aziende di trasporti. Queste risorse attirano i criminali informatici e gruppi governativi. Le informazioni in possesso delle aziende di trasporto costituiscono un bersaglio interessante per i criminali informatici, in quanto esse possono contenere PII, dati biografici, numeri di passaporto, informazioni sui programmi fedeltà, dati sulle carte di pagamento e itinerari di viaggio.

In questo settore, e in particolare in quello aeronautico e aeroportuale, si nota un crescente numero di attacchi perpetrati da criminali informatici e governi, finalizzati a monitorare i movimenti di specifici viaggiatori o alla monetizzazione dei dati personali dei passeggeri, rivendendoli sul dark web.

Le minacce informatiche per il settore dei trasporti comportano rischi aggiuntivi rispetto ad altri settori. Ciò a causa dei potenziali effetti cinetici causati da un potenziale attacco, che può mettere a rischio vite umane, con impatti negativi anche su altri settori che fanno affidamento sui servizi di trasporto per condurre le loro attività.

I gruppi di criminali informatici che hanno preso di mira il settore dei trasporti sono stati vari durante il 2019, includendo sia gruppi di criminali informatici indipendenti che gruppi operanti per conto di entità governative. In entrambi i casi, tali gruppi hanno lanciato attacchi contro organizzazioni sparse in tutto il mondo.

Principali gruppi di criminali informatici che hanno preso di mira il settore della dei trasporti includono:

ITG07 (Chafer)	ITG17 (Muddywater)
ITG09 (APT40)	Hive0016 (APT33)
ITG11 (APT29)	Hive0044 (APT15)
ITG15 (Energetic Bear)	Hive0047 (Patchwork)

Media e intrattenimento

Il quarto settore maggiormente esposto ad attacchi incluso nella classifica di X-Force nel 2019 è stato quello dei media e dell'intrattenimento, con una percentuale del 10 percento tra i primi 10 settori colpiti. Tale dato registra un incremento rispetto all'8 percento del 2018, proiettando questo settore dalla sesta alla quarta posizione.

Il settore dei media include sotto settori ad alto profilo, come quello delle telecomunicazioni, nonché numerose aziende che producono, elaborano e distribuiscono notizie e programmi di intrattenimento. Il settore dei media e dell'intrattenimento costituisce un bersaglio ad alto valore aggiunto per i criminali informatici alla ricerca di metodi per influenzare l'opinione pubblica e controllare i flussi di informazione al fine di tutelare la reputazione delle loro organizzazioni o del loro paese. In particolare, i gruppi operanti per conto di agenzie governative possono considerare i contenuti mediatici come una significativa minaccia per la sicurezza nazionale, mentre i criminali informatici tradizionali considerano gli attacchi in questo settore particolarmente redditizi in quanto consentono di rubare programmi non ancora distribuiti per poi chiedere un riscatto.

In generale, nel 2019, questo settore è stato oggetto di attacchi da parte di criminali informatici e gruppi affiliati a entità governative.

Principali gruppi di criminali informatici che hanno preso di mira il settore dei media e dell'intrattenimento includono:

ITG03 (Lazarus)

Hive0003 (Newscaster)

Hive0047 (Patchwork)

Servizi professionali

Il settore dei servizi professionali è composto da varie aziende che offrono servizi di consulenza specialistici ad altri settori. Alcuni esempi includono aziende che offrono servizi legali, contabilità, risorse umane e supporto clienti specializzato, tanto per citarne alcuni. Secondo i dati raccolti da X-Force, nel 2019 questo settore è stato oggetto del 10 percento di tutti gli attacchi perpetrati ai danni dei 10 principali settori, con un calo rispetto al 12 percento registrato nel 2018.

La pubblica diffusione delle informazioni ottenute mediante violazioni dei dati indicano anche che il settore dei servizi professionali è stato anche quello con il maggior numero di registrazioni violate rispetto a tutti gli altri settori della nostra classifica. Molte di queste aziende acquisiscono dati altamente sensibili dai loro clienti. Tali dati includono informazioni associate a procedure legali, dati contabili e fiscali; tutte informazioni che possono diventare un obiettivo redditizio per aggressori alla ricerca di un guadagno monetario o di informazioni riservate.

Inoltre, questo settore include aziende tecnologiche, sempre più oggetto di attacchi causati dal fatto che tali aziende possiedono enormi quantità di dati di soggetti terzi, utilizzabili dagli aggressori per tentare di violare organizzazioni di maggiori dimensioni e caratterizzate da misure di sicurezza più elevate per le quali tali utenti lavorano.

Inoltre, il flusso di lavoro quotidiano delle aziende del settore dei servizi professionali, tende a creare vettori di attacco naturali per i criminali, attraverso email di phishing e macro maligne. Numerosi servizi professionali fanno affidamento su file di produttività, come gli allegati Word e Excel, per la scrittura di contratti, le comunicazioni con i clienti e per il completamento delle attività quotidiane. L'uso delle macro è uno dei metodi più noti e utilizzati, attraverso il quale, i criminali informatici iniettano script maligni in quei formati di file che nessuna azienda si può permettere di bloccare completamente.

Quelli seguenti, sono i principali gruppi che hanno preso di mira il settore dei servizi professionali nel 2019: ITG01 (APT10, Stone Panda), un gruppo operante per conto di enti governativi che sembra essere originato in Cina.

Settore governativo

Il settore governativo occupa il sesto posto tra quelli più colpiti nella nostra classifica. In totale, questo settore è stato oggetto dell'8 percento degli attacchi nel gruppo dei 10 principali settori colpiti. Una percentuale invariata rispetto allo scorso anno, anche se questo settore ha scalato la classifica complessiva di una posizione, rispetto al settimo posto occupato nel 2018.

Il settore governativo costituisce un obiettivo ad alto valore aggiunto per i criminali informatici che operano per conto di enti governativi che cercano di predominare su avversari reali o percepiti, per hacktivisti che cercano di diffondere informazioni compromettenti o dimostrare le loro abilità tecniche, nonché per criminali informatici alla ricerca di guadagni facili attraverso attività di estorsione e furto di dati.

In particolare, le aziende municipali sono state oggetto di crescenti attacchi negli ultimi anni, con i criminali informatici che cercavano di estorcere denaro dalle sicurezza da queste organizzazioni, tradizionalmente viste come meno orientate alla sicurezza rispetto a quelle del settore privato. Gli enti governativi possiedono risorse di valore che consentono di minacciare altri attori, specialmente mediante informazioni riservate e segreti di stato. Tali dati possono includere anche PII su dipendenti e agenti governativi, informazioni finanziarie, comunicazioni internet e funzionalità delle reti critiche.

Gli stati nazione hanno dimostrato un interesse a lungo termine verso gli attacchi agli enti governativi e la valutazione di X-Force Iris è che gli stati rappresentano gli attori più capaci per conseguire tali obiettivi. Nel 2019, numeri crescenti di gruppi di criminali informatici hanno preso di mira entità governative, tentando di crittografare i dati utilizzati da tali entità a fini di riscatto. In particolare nel caso di enti operanti a livello municipale o provinciale.

Nel 2019, oltre 70 entità governative sono state colpite da ransomware nel periodo compreso tra gennaio e luglio. I criminali informatici hanno rubato dati, inclusi quelli dei siti della difesa, rendendoli poi disponibili sul dark web. Notoriamente, gli attivisti considerano i governi come bersagli di interesse; in particolare laddove vi siano in corso controversie sulle quali tali gruppi desiderano attirare l'attenzione. Spesso, le organizzazioni governative mancano delle risorse finanziarie dedicate alla sicurezza informatica di cui godono le controparti del settore privato, pur con la necessità di mantenere un livello del servizio coerente e uniforme per la clientela. Un aspetto questo che non fa che esacerbare la sfida che tali minacce rappresentano per tali organizzazioni.

Principali gruppi criminali informatici dediti agli attacchi contro agenzie governative del 2019.

Formazione

Il settore dell'educazione è stato oggetto dell'8 percento del volume totale degli attacchi perpetrati ai danni dei 10 principali settori. Una crescita del 6 percento rispetto al 2018, che posiziona questo settore al settimo posto nella nostra classifica.

Il settore dell'educazione include numerose risorse di valore che offrono una valida motivazione per gli attacchi da parte di gruppi motivati da ragioni finanziarie e stati nazione. Dai dati relativi alla proprietà intellettuale (PI) fino ai dati PII, le organizzazioni del settore dell'educazione costituiscono un ottimo bersaglio per differenti tipologie di aggressori.

Caratterizzati da differenti motivazioni, gli aggressori hanno utilizzato svariati metodi di infezione iniziale per accedere alle reti delle istituzioni accademiche. Tuttavia, il metodo più comune resta quello delle email di phishing, che spesso vengono create appositamente per istituzioni o settori di ricerca specifici.

Spesso, le organizzazioni del settore dell'educazione utilizzano infrastrutture IT vaste, con una notevole impronta in termini di servizi digitali. Tali istituzioni utilizzano differenti risorse, che servono un elevato numero di utenti, che includono personale, studenti e appaltatori esterni. Questa ampia area esposta agli attacchi è difficile da mettere in sicurezza e può essere utilizzata dagli aggressori per attuare numerose attività maligne. In base a rapporti pubblicati a ottobre 2019, è emerso che, nello stesso anno, nel solo territorio degli Stati Uniti almeno 500 scuole sono state colpite da attacchi informatici, la maggior parte dei quali di tipo ransomware.

Alcuni notevoli esempi di attacchi sofisticati in questo settore includono le operazioni condotte da alcuni stati nazione al fine di compromettere le reti universitarie, per poi utilizzarle come testa di ponte per infettare organizzazioni operanti nel settore dei media e operatori militari privati. In maniera analoga, gli aggressori che mirano a ottenere dati sulle ricerche finanziate dal governo statunitense, sono alla costante ricerca di accessi che consentano di penetrare all'interno delle reti universitarie al fine di rubare proprietà intellettuali, dal valore spesso inestimabile.

I principali gruppi di criminali informatici che hanno preso di mira il settore dell'educazione includono:

ITG05 (APT28)
ITG12 (Turla Group)
ITG13 (APT34)
ITG15 (Energetic Bear)
ITG17 (Muddywater)
Hive0075 (DarkHydrus)

IBM X-Force IRIS ritiene di poter affermare con un certo livello di certezza che le organizzazioni di questo settore continueranno a essere oggetto di attacchi da parte di gruppi guidati da motivazioni finanziarie e da attori governativi alla ricerca di informazioni di valore.

I principali gruppi criminali informatici operanti in questo settore nel 2019 hanno incluso fazioni di criminali informatici guidate da motivazioni economiche e gruppi sponsorizzati da entità governative cinesi, russe e iraniane.

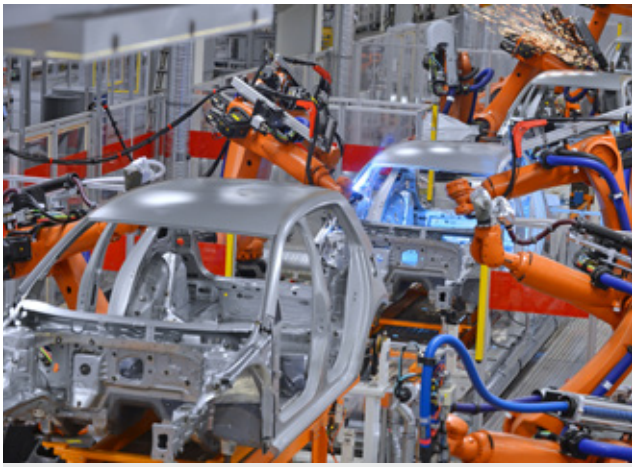
Produzione industriale

Settori manifatturieri trainanti per l'economia, come quello metallurgico, chimico, dei beni strumentali e dell'elettronica, non sono esenti da minacce informatiche e di altro tipo connesse ai sistemi OT operanti in campo. Con l'8 percento del totale, il settore manifatturiero occupa l'ottava posizione nella nostra classifica dei 10 settori più esposti agli attacchi, un calo rispetto al 10 percento fatto registrare nel 2018.

Sebbene questo settore si stato oggetto di un numero inferiore di attacchi rispetto all'anno precedente, tale calo può essere una conseguenza del fatto che, in molti casi, le violazioni dei dati nel settore manifatturiero non includono informazioni necessariamente soggette a diffusione in base a normative e regolamenti. Di conseguenza, non sempre gli attacchi vengono rivelati al pubblico. Per questo motivo, il volume di attacchi registrato potrebbe indicare una frequenza inferiore rispetto al numero reale di attacchi sostenuti.

Inoltre, il settore manifatturiero utilizza ambienti IT e OT. Ciò significa che tale settore è esposto agli stessi rischi e alle stesse minacce che caratterizzano i sistemi ICS e SCADA. Ma sebbene la sicurezza delle informazioni in questo settore sia stata caratterizzata da carenze in passato, il successo conseguito in termini di reazione del pubblico da parte di un produttore norvegese oggetto di un attacco ransomware nel 2019 potrebbe indicare un segnale di cambiamento verso la sicurezza informatica in questo settore.

I criminali informatici o i gruppi sponsorizzati dai governi spinti da motivazioni economiche e dall'interesse verso i dati oggetto di proprietà intellettuale rappresentano il principale rischio informatico per le aziende del settore manifatturiero. Una delle più frequenti tecniche di attacco utilizzate contro il settore manifatturiero nel 2019 è stata quella della frode attraverso la compromissione di email commerciali (BEC); specialmente nel caso di aziende che intrattengono intense relazioni commerciali con fornitori esteri. In tali casi, i server mail o gli account email aziendali sono compromessi dagli aggressori, che si inseriscono nel canale di comunicazione esistente tra le due parti con l'obiettivo di reindirizzare milioni di dollari verso conti controllati dal gruppo degli aggressori.



I principali gruppi che hanno preso di mira il settore manifatturiero includono:

ITG01 (APT10)
ITG09 (APT40)
HIVE0006 (APT27)
Hive0013 (OceanLotus)
Hive0044 (APT15)
Hive0076 (Tick)

I produttori sono anche esposti ad attacchi alle catene di approvvigionamento e possono essere sfruttati da stati nazione come veicoli di infezione per backdoor o malware all'interno dei prodotti assemblati e successivamente spediti verso altri paesi.

Sotto il profilo finanziario, gli aggressori potrebbero essere interessati a un attacco verso i sistemi dei produttori al fine di carpire segreti industriali e proprietà intellettuali. Ricerche che hanno richiesto anni di lavoro e sviluppo da parte delle aziende possono costituire una rapida fonte di profitto per i criminali informatici operanti nel dark web. Oppure tali informazioni potrebbero dare un vantaggio economico o militare al governo di uno stato, quando le violazioni sono a danno di produttori operanti nel settore della difesa e delle attrezzature militari.

Secondo i dati di X-Force, gli attacchi ransomware, phishing e SQLi injection costituiscono un'altra frequente minaccia per il settore manifatturiero.

Settore energetico

Il settore energetico occupa il nono posto della nostra classifica, con una percentuale pari al 6 percento del totale degli attacchi e degli incidenti rilevati nei principali 10 settori nel 2019. La situazione in questo settore resta invariata rispetto al 2018, in cui era stata registrata la stessa percentuale del 6 percento.

Le aziende del settore energetico si sono dimostrate un bersaglio appetibile per gli attacchi informatici; ciò è in parte dovuto alla loro importanza in quando elementi portanti delle infrastrutture critiche di ogni paese. Il settore energetico, in tutte le sue forme, svolge un ruolo essenziale per la sicurezza nazionale, l'economia e per gestione quotidiana di città e industrie.

Gli obiettivi degli attacchi nel settore energetico sono vari. Alcune risorse particolarmente redditizie presenti nelle aziende del settore energetico, come dati dei clienti, materiale finanziario, segreti commerciali e informazioni su tecnologie proprietarie, hanno un valore simile a quello delle aziende di altri settori.

Ciò che differenzia il settore energetico dagli altri settori è la possibilità che tale settore sia soggetto a interruzioni fisiche e distruzione dei sistemi ICS e dei sistemi SCADA preposti alla loro gestione. Questi sistemi costituiscono importanti bersagli per gli avversari che desiderano monitorare o prendere il controllo delle operazioni all'interno di una struttura oggetto di attacco, specialmente quando gli attacchi interessano infrastrutture di cyberwarfare e strutture nucleari in paesi rivali, per esempio. Questo settore è stato anche oggetto di attacchi con malware distruttivi, come ZeroCleare.

Un attacco concluso con successo a un sistema ICS progettato per interrompere le attività di tale sistema, può avere effetti devastanti per i clienti che necessitano di energia, benzina, petrolio o altre risorse generate dal settore energetico. In passato, gli effetti di tali attacchi e i relativi effetti negativi da essi causati sono stati osservati in una serie di incidenti ai danni di centrali energetiche in Ucraina, probabilmente condotti dalla Russia con l'obiettivo di causare danni fisici alle strutture colpite.

I principali gruppi di criminali informatici che hanno preso di mira questo settore includono:

ITG01 (APT10)
ITG09 (APT40)
ITG07 (Chafer)
ITG11 (APT29)
ITG12 (Turla Group)
ITG13 (APT34)
ITG15 (Energetic Bear)
ITG17 (Muddywater)
Hive003 (APT35)
HIVE0006 (APT27)
Hive0016 (APT33)
Hive0044 (APT15)
Hive0045 (Goblin Panda)
Hive0047 (Patchwork)
Hive0076 (Tick)
Hive0078 (Sea Turtle)
Hive0081 (APT34)

Settore sanitario

Il decimo settore più colpito della nostra classifica è quello della sanità, con il 3 percento degli attacchi totali condotti ai danni dei principali 10 settori. Un calo rispetto all'ottava posizione e al 6 percento degli attacchi registrati nel 2018.

La preponderanza di prove indica che i criminali informatici spinti da motivazioni economiche costituiscono il gruppo principale per quanto riguarda gli attacchi alle reti delle organizzazioni sanitarie e ai dispositivi medici. L'obiettivo è quello di carpire e vendere dati medici sul dark web, oppure di crittografare i dati dei dispositivi collegati in rete al fine di generare interruzioni delle attività a fini di riscatto.

Le interruzioni delle reti di ospedali e cliniche sono in grado di spingere le aziende della sanità a pagare per gli attacchi ransomware, al fine di poter ripristinare le loro operazioni e proteggere le vite dei pazienti. In alcuni casi il riscatto è eccessivo, come i 14 milioni di dollari richiesti a seguito di un attacco condotto da Ryuk nel 2019.

Nell'arco del 2020, il settore della sanità continuerà a espandere le misure di sicurezza finalizzate a proteggere i suoi dati. Alla luce dei crescenti attacchi ransomware, gli ospedali devono anche rafforzare le capacità di risposta agli incidenti, per evidenziare gli attacchi emergenti ai danni di dispositivi medici non sicuri, che potrebbero essere utilizzati come veicolo di attacco da parte di gruppi di criminali informatici motivati.

È importante notare come i gruppi di criminali informatici che operano in questo settore includano anche gruppi di criminali informatici guidati da motivazioni finanziarie, come quelli operanti con il ransomware Ryuk. Sebbene gli attacchi ransomware siano il segnale di una potenziale crisi per le strutture sanitarie coinvolte negli attacchi,non è stato rilevato alcun interesse persistente da parte di stati nazione verso questo settore.

Informazioni geocentriche

Nel 2019, i criminali informatici hanno colpito tutte le aree geografiche, con i maggiori livelli di attività osservati in Nordamerica, Asia ed Europa.

Nel 2019, i ricercatori di X-Force hanno scoperto anche attività condotte da criminali informatici in Medio Oriente e Sudamerica, con le minacce indirizzate verso la prima di tali regioni composta prevalentemente attivisti informatici e stati nazione, mentre il Sudamerica è stata la nazione più colpita da crimini a fini finanziari.

Questa sezione è dedicata all'approfondimento degli attacchi condotti in tali regioni, al fine di acquisire una maggiore comprensione della natura degli obiettivi osservati da X-Force, degli attori chiave operanti in ciascuna area e delle date più importanti del 2020 in termini di potenziale incremento delle attività dei criminali informatici. Alcune aree geografiche mettono in evidenza minacce che sono state particolarmente attive nel prendere di mira obiettivi situati in tali regioni. Tuttavia, tale lista non è completa e include dati antecedenti il 2019. Questa sezione utilizza la nomenclatura di IBM Threat Group descritta sopra, con dati ricavati dalla documentazione relativa alle risposte agli incidenti globali di IBM e dai dati pubblici diffusi in materia di violazioni dei dati.

Nord America

Il Nord America occupa la prima posizione in tutte le categorie di minacce, con il 44 percento del totale degli incidenti registrati nel 2019.

Il Nord America contiene numerosi potenziali obiettivi e mantiene un significativo numero di infrastrutture internet. Ciò ne fa un obiettivo importante per i criminali informatici. Nel 2019, in Nord America sono stati compromessi oltre 5 miliardi di dati.

IBM ha reagito a numerosi incidenti occorsi in Nord America nel 2019, molti dei quali hanno fatto uso di codice malware modificato per uso commerciale, acquistabile sul mercato illegale o ottenibile gratuitamente. Spesso è difficile tracciare l'origine dei malware mercificati; tuttavia, tali strumenti possono essere molto efficaci consentire ai criminali informatici di conseguire i loro obiettivi.

Le attività criminali informatiche che hanno preso di mira il Nord America si sono mantenute costanti, nonostante nel 2019 non sia stato registrato alcun incidente di rilievo. Le recenti negoziazioni tra Stati Uniti e Cina potrebbero portare a un incremento degli attacchi verso le organizzazioni che svolgono attività commerciali in entrambe le regioni. Pertanto, tali organizzazioni dovranno mantenersi vigili fintanto che tali negoziazioni non vengono concluse con successo.

Principali eventi dal significato storico sotto il profilo delle minacce informatiche:

13 luglio
(Congresso nazionale del partito democratico, Stati Uniti)

24 agosto
(Congresso nazionale del partito repubblicano, Stati Uniti)

3 novembre
(Elezioni presidenziali degli Stati Uniti)

I principali gruppi di criminali informatici che hanno preso di mira questa regione includono:

ITG05 (APT28)
ITG08 (FIN6)
ITG11 (APT29)
ITG15 (Energetic Bear)
Hive0082 (Cobalt Dickens)
Hive0042 (Kovter)
Hive0016 (APT33)
Hive0013 (OceanLotus)
Hive0006 (APT27)
Hive0003 (APT35)
ITG01 (APT10)
ITG03 (Lazarus)
ITG04 (APT19)
ITG09 (APT40)
ITG07 (Chafer)

Gli attacchi più rilevanti osservati durante le attività di risposta agli incidenti di X-Force nel 2019 hanno incluso:

Compromissione di email aziendali, ransomware, attacchi di gruppi governativi contro il settore finanziario.

Asia

La regione asiatica occupa la seconda posizione della classifica elaborata dall'analisi di X-Force, con il 22 percento degli incidenti registrati e il secondo maggior numero di violazioni pubblicamente dichiarate nel 2019. La regione asiatica ha fatto registrare oltre 2 miliardi di registrazioni nel 2019, un dato inferiore solamente a quello del Nord America.

Un significativo numero di aggressori ha concentrato gli attacchi verso organizzazioni associate all'Asia, con particolare attenzione verso quelle operanti nella penisola coreana, in Giappone e Cina. Numerosi attacchi osservati in questa regione, sono stati condotti da TTP di attori legati a stati nazione. Un esempio è quello del gruppo ITG10, probabilmente composto da attori di origine nordcoreana, che hanno attaccato obiettivi in Sud Corea. Un altro esempio è quello del gruppo ITG01, probabilmente composto da operatori cinesi e avente come obiettivo prevalente il Giappone.

I recenti eventi geopolitici che hanno caratterizzato il≈panorama asiatico, hanno accresciuto la probabilità di attività associate a stati nazione in questa regione. Le proteste per la democrazia a Hong Kong e le misure di contrasto attuate dal governo locale, hanno causato notevole preoccupazione in Cina. Le crescenti tensioni tra la Corea del Nord e i suoi vicini ha spinto il regime a intensificare le sue attività. L'annessione della regione del Kashmir da parte dell'India ha anch'essa portato a un incremento delle tensioni nella regione.

Nel 2020, il monitoraggio di queste situazioni geopolitiche potenzialmente volatili svolge un ruolo cruciale al fine di comprendere i rischi posti dalle organizzazioni operanti in tali regioni.

Principali eventi dal significato storico sotto il profilo delle minacce informatiche:

24 luglio
(Giochi olimpici 2020 - Tokyo)

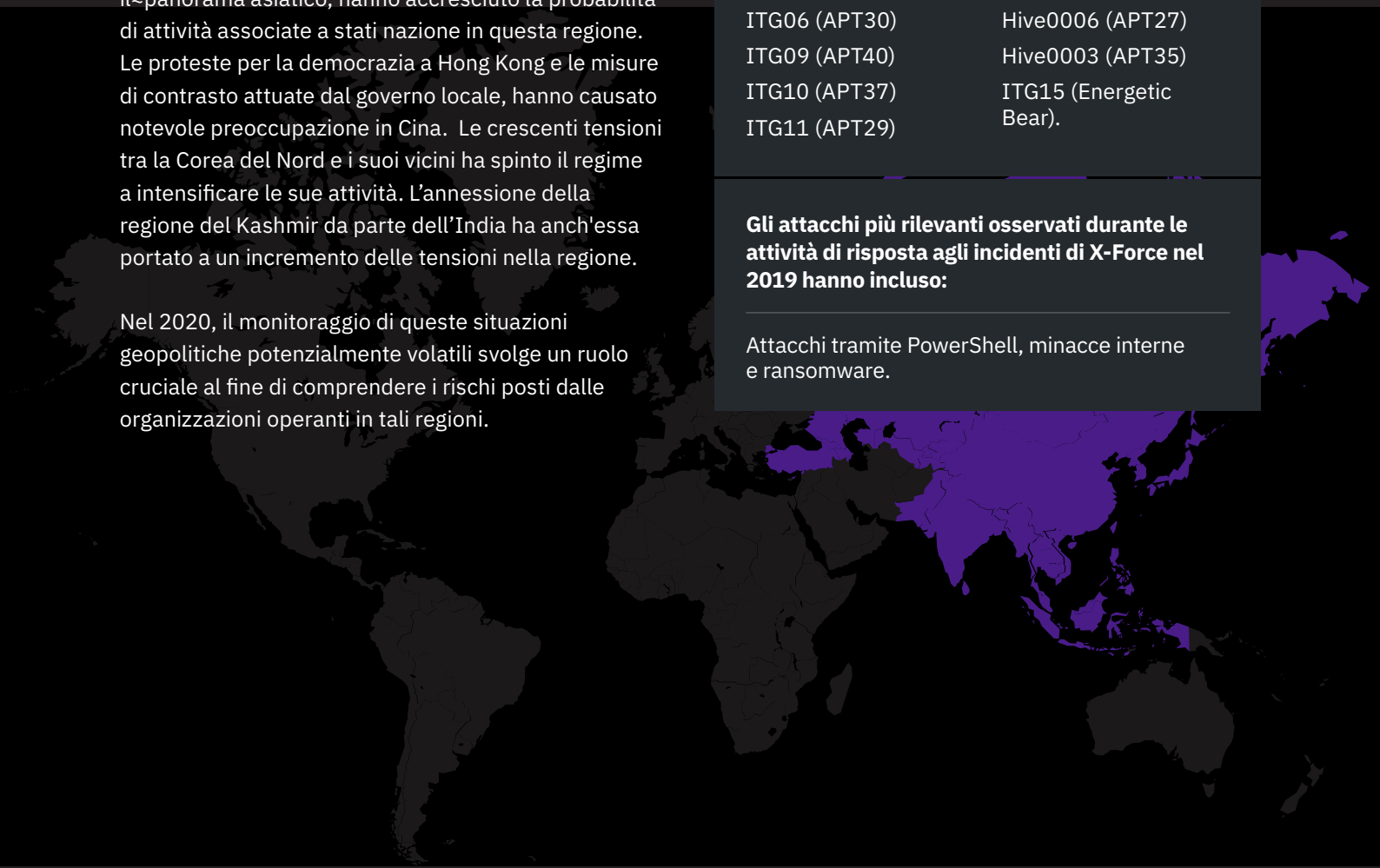
10 ottobre
(Giornata dell'indipendenza a Taiwan).

I principali gruppi di criminali informatici che hanno preso di mira questa regione includono:

Hive0013 (OceanLotus)
Hive0044 (APT15)
Hive0045 (Goblin Panda)
Hive0049 (Samurai Panda)
ITG01 (APT10)
ITG03 (Lazarus)
ITG05 (APT28)
ITG06 (APT30)
ITG09 (APT40)
ITG10 (APT37)
ITG11 (APT29)
ITG16 (Kimsuky)
Hive0016 (APT33)
Hive0040 (Cobalt Gang)
Hive0047 (Patchwork)
Hive0063 (DNSpionage)
Hive0076 (Tick)
Hive0079 (Labryinth Cholima)
Hive0006 (APT27)
Hive0003 (APT35)
ITG15 (Energetic Bear).

Gli attacchi più rilevanti osservati durante le attività di risposta agli incidenti di X-Force nel 2019 hanno incluso:

Attacchi tramite PowerShell, minacce interne e ransomware.



Europa

Anche l'Europa è stata vittima di percentuali simili di attività maligne, con un volume totale degli incidenti pari al 21 percento.

A differenza della regione asiatica, più colpita da attacchi tra stati rivali, l'Europa sembra essere maggiormente colpita da attori gruppi guidati da motivazioni finanziarie. Questa differenza può essere spiegata in ragione della maggiore potenziale probabilità di furto da parte delle aziende europee, in base ai tassi di cambio valutari. In alternativa, le motivazioni dei criminali possono consistere nel perseguimento di proprietà intellettuali, che possono essere vendute alla concorrenza con guadagni notevoli.

Anche l'uscita del Regno Unito dall'Unione Europea (Brexit), potrebbe avere riverberi nei circoli degli attivisti informatici durante il 2020, anche se nel 2019 non è stata osservata alcuna attività in tal senso. Inoltre, l'imminenza di elezioni in alcuni dei principali paesi europei (Germania e Francia), potrebbe potenzialmente rappresentare un obiettivo di interesse per gruppi associati a entità governative interessate a influenzare l'esito delle elezioni in tali paesi.

Principali eventi dal significato storico sotto il profilo delle minacce informatiche:

31 gennaio
(Il Regno Unito esce dall'Unione Europea in conformità all'Articolo 50)

28 giugno
(Giornata della costituzione ucraina/Anniversario di NotPetya).

I principali gruppi di criminali informatici che hanno preso di mira questa regione includono:

ITG05 (APT28)
ITG08 (FIN6)
ITG12 (Turla)
ITG15 (Energetic Bear)
ITG09 (APT40)
ITG07 (Chafer)
ITG11 (APT29)
ITG14 (FIN7)
ITG17 (Muddywater)
Hive0006 (APT27)
Hive0003 (APT35)
Hive0013 (OceanLotus)
Hive0044 (APT15)
Hive0063 (DNSpionage)

Gli attacchi più rilevanti osservati durante le attività di risposta agli incidenti di X-Force nel 2019 hanno incluso:

Compromissione RDP, malware POS, minacce interne.

Medio Oriente

Nel 2019, il team di X-Force IRIS ha osservato numerosi incidenti aventi come protagonisti stati nazione e come vittime numerose organizzazioni con sede in Medio Oriente. Tuttavia, le metriche complessive relative alle attività dei gruppi operanti in tale regione sono state relativamente ridotte nel 2019, con una percentuale pari al 7 percento del totale in questa regione.

Potrebbero esserci svariate spiegazioni per tale riduzione delle attività, come il fatto che altre aree geografiche potrebbero aver offerto una maggiore redditività del capitale investito nel settore dei crimini informatici. Tuttavia, a differenza di altre regioni geografiche, il Medio Oriente ha una percentuale più elevata di attivisti informatici e attività condotte da stati nazione rispetto ad altre parti del mondo.

Le attività condotte da hacker attivisti potrebbero essere correlate all'instabilità politica che ha caratterizzato la regione durante il 2019, con numerosi incidenti aventi l'Iran come protagonista. In maniera analoga, le attività condotte dagli stati nazione, come quelle del gruppo ITG13, operante per conto del governo iraniano, hanno puntato a obiettivi di interesse per tali governi, conducendo attacchi distruttivi nel settore energetico.

L'instabilità politica e il conflitto in Yemen, continuano a generare elevati rischi di attività associate a minacce informatiche, in cui attori operanti per conto di entrambe le parti in conflitto, utilizzano attacchi informatici per diffondere i loro messaggi e generare profitti. Tali rischi continueranno probabilmente a persistere anche durante il 2020, con i vari attori del conflitto che continuano a indirizzarsi minacce a vicenda.

Principali eventi dal significato storico sotto il profilo delle minacce informatiche:

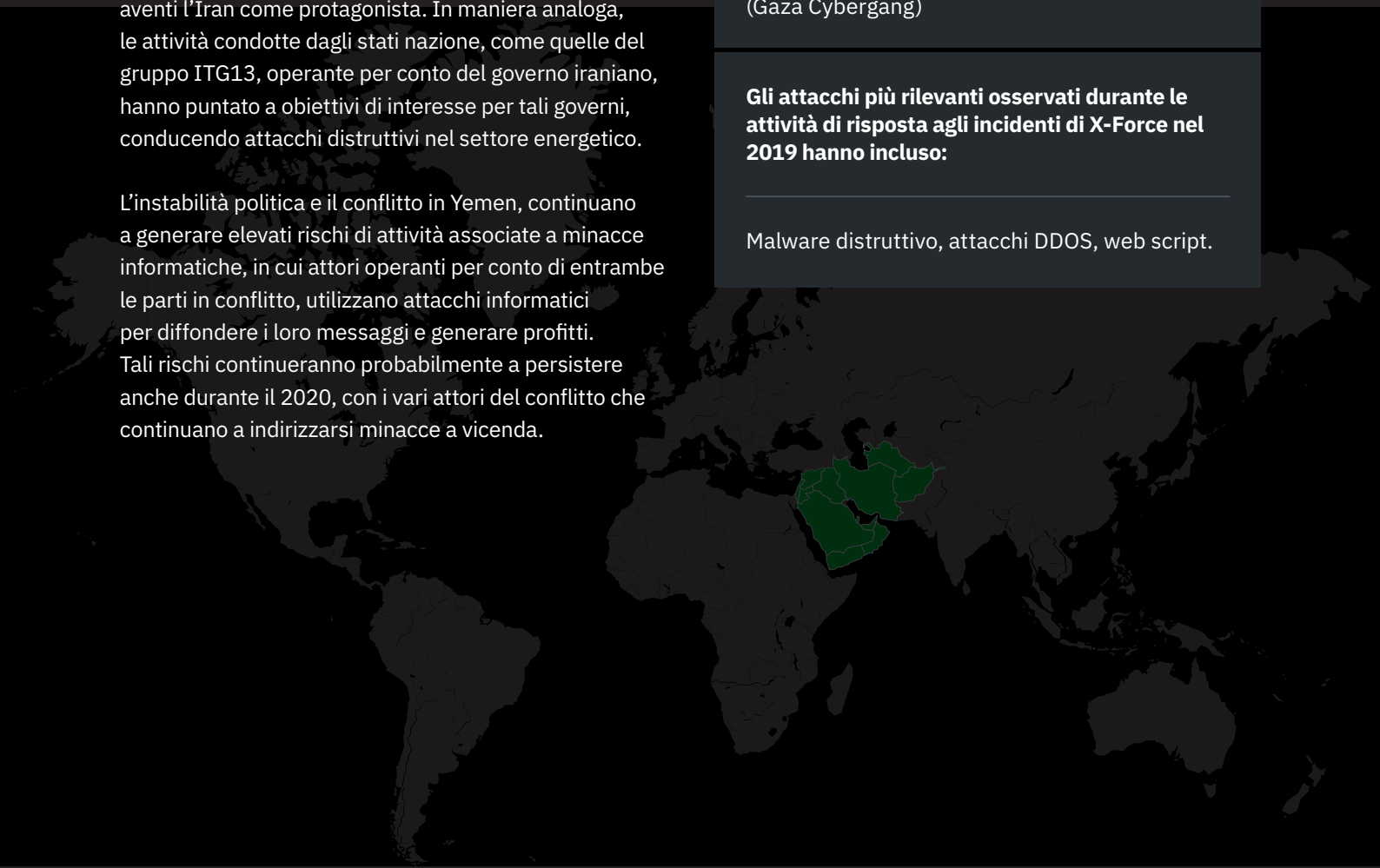
21 Novembre
(Campionato mondiale di calcio 2022 - Qatar)

I principali gruppi di criminali informatici che hanno preso di mira questa regione includono:

Hive0044
ITG07 (Chafer)
ITG13
Hive0081 (APT34
Hive0078 (Sea Turtle)
Hive0075 (DarkHydrus)
Hive0063 (DNSpionage)
Hive0047 (Patchwork)
Hive0022 (Gaza Cybergang)
Hive0016 (APT33)
Hive0006 (APT27)
Hive0003 (APT35)
ITG17 (Muddywater)
ITG12 (Turla)
ITG11 (APT29)
ITG10 (APT37)
ITG09 (APT40)
ITG05 (APT28)
ITG01 (APT10)

Gli attacchi più rilevanti osservati durante le attività di risposta agli incidenti di X-Force nel 2019 hanno incluso:

Malware distruttivo, attacchi DDOS, web script.



Sudamerica

Nel 2019, il Sudamerica ha dovuto fronteggiare un notevole volume di attività informatiche criminali. Tuttavia, la regione non ha ricevuto il livello di attenzione dedicato alle altre tre principali regioni incluse in questa analisi, facendo registrare solamente il 5 percento degli incidenti. Tuttavia, il livello di attività in questa regione continua a crescere, con il team X-Force che ha osservato un notevole incremento in termini di attività di risposta agli incidenti, in particolare nei settori al dettaglio e in quello dei servizi finanziari.

Gli incidenti osservati in questa regione includevano anche a attività ransomware, un tipo di minaccia che ha continuato a crescere in popolarità durante il 2019.

Principali eventi dal significato storico sotto il profilo delle minacce informatiche:

12 Giugno
(Torneo di calcio Coppa America 2020 - Colombia e Argentina).

I principali gruppi di criminali informatici che hanno preso di mira questa regione includono:

Hive0081 (APT34)
Hive0044 (APT15
Hive0016 (APT33)
Hive0013 (OceanLotus)
Hive0003 (APT35)
ITG17 (Muddywater)
ITG12 (Turla)
ITG11 (APT29)
ITG05 (APT28)
ITG03 (Lazarus)
ITG01 (APT10)

Gli attacchi più rilevanti osservati durante le attività di risposta agli incidenti di X-Force nel 2019 hanno incluso:

Compromissione di email aziendali, ransomware, attacchi di gruppi governativi contro il settore finanziario.

Prepararsi per la resilienza nel 2020

Sulla base dei dati emersi da questo rapporto di IBM X-Force, mantenersi al passo in termini di intelligence delle minacce e creare solide capacità di risposta costituiscono metodi efficaci per mitigare le minacce in un panorama in costante evoluzione. Ciò a prescindere dal settore o dal paese in cui si opera.

Il nostro team raccomanda una serie di misure che ciascuna organizzazione può attuare per prepararsi per fronteggiare al meglio le minacce informatiche nel 2020:

- L'impiego di intelligente delle minacce per capire meglio le motivazioni e le tattiche degli aggressori e quindi prioritizzare le risorse nel settore della sicurezza.

- Creare e formare un team di reazione rapida agli incidenti all'interno dell'organizzazione. Qualora ciò non fosse possibile, attuare misure di risposta agli incidenti efficaci, al fine di garantire una pronta risposta in caso di incidenti a impatto elevato. Nel 2019, IBM Security ha osservato come un significativo contenimento dell'impatto consenta di ridurre i costi associati, con il tempestivo intervento del nostro team in un caso di infezione con MegaCortex, che ha consentito di bloccare l'attacco ransomware durante l'esecuzione, evitando in tal modo danni per migliaia di dollari.

- Condurre uno stress test dei piani di risposta agli incidenti della vostra organizzazione, per sviluppare e consolidare solide pratiche di reazione. Gli esercizi pratici e l'acquisizione di esperienze nel settore delle minacce informatiche può fornire ai team le competenze necessarie a migliorare i tempi di reazione, ridurre i tempi di inattività e quindi risparmiare denaro in caso di violazioni.

- L'implementazione dell'autenticazione multifattore (MFA), continua a rappresentare una delle principali priorità per la sicurezza delle aziende. Nel 2019, il furto o il riutilizzo di credenziali ha costituito uno dei metodi di attacco più comunemente utilizzati dagli aggressori. L'adozione dell'MFA è in grado di contrastare efficacemente questi attacchi ancora prima che si verifichino.

- Assicurarsi che l'organizzazione disponga di una soluzione che consenta di identificare e bloccare i domini falsificati, come Quad9, a causa della prevalenza del phishing come vettore di attacco.

- Effettuare backup, backup di test e archiviazione dei backup offline. Non limitarsi a effettuare i backup, ma assicurarsi anche della loro efficacia attraverso test reali in campo, contribuisce a fare la differenza al fine di garantire la sicurezza di una data organizzazione.

Fate un passo avanti con alcune importanti raccomandazioni

Nel 2020, le organizzazioni dovranno preoccuparsi di nuove e vecchie minacce.

- Durante il 2020, la percentuale di rischio continuerà a crescere, con oltre 150.000 vulnerabilità esistenti, e molte nuove vulnerabilità che vengono rilevate costantemente.
- Con un incremento delle violazioni quattro volte superiore nel 2019 rispetto al 2018, si prevede che il 2020 sarà un anno caratterizzato da un numero elevato di violazioni e attacchi.
- Gli aggressori continueranno a modificare le loro tattiche con differenti vettori di attacco, e con una crescente attenzione verso i dispositivi IoT, le tecnologie operative (OT) e verso i sistemi medici e industriali connessi, tra gli altri.
- L'impiego di malware da parte dei criminali informatici continua a fluttuare, con ransomware, cryptominer e botnet che si sono alternate ai vertici della classifica delle minacce più diffuse in differenti periodi del 2019. Riteniamo che questo trend continuerà anche nel 2020. Ciò significa che le aziende dovranno organizzarsi per proteggersi contro varie minacce la cui prevalenza varia nel tempo.
- Gli elevati livelli di innovazione del codice dei ransomware e dei cryptominer, probabilmente implica il fatto che queste minacce continueranno ad evolversi anche nel 2020, richiedendo migliori metodi di rilevamento e capacità di contenimento.
- Le attività di spamming continuano invariate, richiedendo procedure di blacklisting diligenti, patch delle vulnerabilità monitoraggio delle minacce da parte delle aziende.
- La variazione tra un anno e l'altro in termini di obiettivi colpiti in vari settori specifici evidenzia una componente di rischio per tutti i settori interessati, unitamente alla necessità di sviluppare programmi avanzati e maturi di sicurezza informatica a largo spettro.
- Le organizzazioni possono utilizzare la posizione geografica per identificare i probabili aggressori e le motivazioni dell'attacco, al fine di stimare e mitigare alcuni dei principali rischi che si potrebbero presentare.

Informazioni su IBM X-Force

IBM X-Force studia e monitora i trend più recenti, informando i clienti e il pubblico in relazione alle minacce critiche ed emergenti e fornendo contenuti di sicurezza al fine di tutelare i clienti IBM.

Dalla protezione di applicazioni, dati e infrastrutture, fino al cloud e ai servizi di sicurezza gestiti, IBM Security Services dispone di tutta l'esperienza necessaria a garantire la salvaguardia delle risorse critiche. IBM Security protegge alcune delle più sofisticate reti del mondo, utilizzando alcune dei migliori talenti del settore.

Partecipanti

Michelle Alvarez
Dave Bales
Joshua Chung
Scott Craig
Kristin Dahl
Charles DeBeck
Ari Eitan (Intezer)
Brady Faby (Intezer)
Rob Gates
Dirk Harz
Limor Kessem
Chenta Lee
Dave McMillen
Scott Moore
Georgia Prassinos
Camille Singleton
Mark Usher
Ashkan Vila
Hussain Virani
Claire Zaboeva
John Zorabedian

Ulteriori informazioni su IBM Security →

IBM Security
New Orchard Rd
Armonk, NY 10504
Prodotto negli Stati Uniti d'America
Febbraio 2020

Prodotto negli Stati Uniti d'America
Febbraio 2020

IBM **Security**