Acronis

Report 2020

Report Acronis sulle minacce digitali 2020

Tendenze della cybersecurity nel 2021, l'anno dell'estorsione

Acronis
Report sulle minacce digitali 2020

Sommario

AUTORI:

Alexander Ivanyuk

Direttore senior, Product and Technology Positioning, Acronis

Candid Wuest

Vice presidente Cyber Protection Research, Acronis

Introduzione e sommario

Acronis è stata la prima azienda a implementare la Cyber Protection integrata e completa per proteggere tutti i dati, le applicazioni e i sistemi. Questo tipo di protezione informatica richiede costanti attività di ricerca e monitoraggio delle minacce, nonché l'adozione dei cinque vettori della Cyber Protection: salvaguardia, accessibilità, privacy, autenticità e sicurezza (noti anche con l'acronimo SAPAS). Nell'ambito della nostra strategia, gestiamo tre centri CPOC (Cyber Protection Operation Center) in diverse zone del mondo per monitorare e indagare le minacce digitali 24 ore su 24.

Abbiamo inoltre rinnovato i nostri prodotti di punta: Acronis Cyber Protect Cloud, parte della piattaforma Acronis Cyber Cloud per service provider, e Acronis Cyber Protect 15, una soluzione on-premise. Già prima di rilasciare questi prodotti Acronis era uno dei leader nel mercato della Cyber Protection grazie alla sua tecnologia anti-ransomware innovativa Acronis Active Protection, che nel corso del tempo si è evoluta consolidando l'esclusiva competenza di Acronis nel bloccare le minacce sferrate contro i dati. È tuttavia importante notare che le tecnologie di rilevamento basate su intelligenza artificiale e analisi comportamentale, sviluppate da Acronis nel 2016, sono state successivamente perfezionate al fine di contrastare tutte le forme di malware e altre potenziali minacce.

Questo report si occupa del panorama delle minacce rilevato dai nostri sensori e analisti nel corso del 2020.

I dati generali sul malware presentati nel report sono stati raccolti da giugno a ottobre 2020, dopo il lancio di Acronis Cyber Protect a maggio 2020, e riflettono le minacce rivolte agli endpoint che abbiamo rilevato durante tale periodo.

Il report illustra un quadro globale ed è basato su oltre 100.000 endpoint singoli distribuiti in tutto il mondo. Abbiamo incluso nel report solo le minacce che prendono di mira i sistemi operativi Windows poiché sono molto più prevalenti di quelle rivolte a macOS. Continueremo a osservare gli sviluppi della situazione e potremmo includere anche i dati sulle minacce a macOS nel report dell'anno prossimo.

I CINQUE NUMERI PRINCIPALI DEL 2020:

- Il **31%** delle aziende globali ha subito attacchi da parte di criminali informatici almeno una volta al giorno
- Il ransomware Maze è responsabile di quasi il **50%** di tutti i casi di ransomware registrati
- Oltre **1.000** aziende hanno subito una perdita di dati dopo un attacco ransomware
- Microsoft ha rilasciato patch per quasi **1.000** vulnerabilità nei propri prodotti in soli nove mesi
- La vita media di un esemplare di malware è di **3,4** giorni

TENDENZE PRINCIPALI DELLA CYBERSECURITY CHE PREVEDIAMO PER IL 2021:

- Gli attacchi ai lavoratori remoti sono destinati ad aumentare
- L'esfiltrazione di dati supererà la crittografia dei dati
- Più attacchi contro MSP, piccole aziende e cloud
- Il ransomware cercherà nuovi target da colpire
- Gli aggressori ricorreranno più spesso all'automazione e la quantità di esemplari di malware in circolazione crescerà

CHE COSA TROVERETE IN QUESTO REPORT:

- Principali tendenze delle minacce e della sicurezza osservate nel 2020
- Statistiche generali sul malware e principali famiglie esaminate
- Statistiche del ransomware con un'analisi approfondita delle minacce più pericolose
- Perché l'esposizione dei dati riservati è la fase due nella maggior parte degli attacchi ransomware riusciti
- Quali vulnerabilità contribuiscono al successo degli attacchi
- Perché gli MSP sono sempre più minacciati
- Le nostre previsioni sulla sicurezza e raccomandazioni per il 2021

Parte 1

Principali minacce informatiche e trend del 2020

1. Exploit a tema COVID-19
2. Lavoratori remoti sotto attacco
3. MSP nel mirino dei criminali informatici
4. Il ransomware è ancora la minaccia numero uno
5. Backup e sicurezza di base non bastano più

La pandemia di COVID-19, iniziata alla fine del 2019, ha avuto conseguenze drammatiche sulla vita dell'intera popolazione mondiale, ma oltre agli evidenti pericoli per la salute umana e l'enorme impatto economico, ha trasformato il mondo digitale, il modo in cui lavoriamo e come passiamo il nostro tempo libero online.

A seguito del blocco degli spostamenti, la maggior parte delle aziende e dei servizi ha dovuto trasferire online la propria attività. Chi già operava online ha dovuto espandersi, mentre altri hanno introdotto processi completamente nuovi. Organizzazioni pubbliche, mediche e di servizi hanno dovuto adottare nuovi strumenti per gestire le loro esigenze operative quotidiane.

Le riunioni di lavoro sono state trasferite su app di telecomunicazioni come Zoom, Webex e Microsoft Teams, che sono diventate il nuovo standard di riferimento. Gli impiegati degli uffici sono stati mandati a casa, spesso in modo frettoloso e senza supporto adeguato, e sono dovuti ricorrere ai dispositivi personali per svolgere il proprio lavoro.

Purtroppo, in queste circostanze complicate, i criminali informatici non sono rimasti a guardare e hanno attivamente e spietatamente intensificato i propri attacchi.

1. Exploit a tema COVID-19

Come previsto, tantissime persone si sono rivolte subito al web per cercare informazioni su argomenti associati alla nuova pandemia: modi per proteggersi, ultime notizie, forme di assistenza disponibili e così via. Questo interesse ha generato un'enorme quantità di truffe e altri tipi di exploit.

I criminali informatici continuano a utilizzare i vecchi trucchi per sfruttare l'argomento COVID-19 nei loro attacchi, inducendo le vittime a inserire le loro credenziali o informazioni personali in una pagina web di phishing oppure caricando payload dannosi in documenti che fingono di contenere informazioni essenziali relative alla pandemia. Ricorrono anche ad altri metodi degni di nota, come quelli indicati di seguito che abbiamo incontrato durante l'osservazione delle truffe a tema COVID-19.

Falso test Covid gratuito

L'ultima versione del malware Trickbot/Qakbot/Qbot è stata diffusa attraverso molte e-mail di phishing che offrivano test COVID-19 gratuiti. Alle vittime veniva chiesto di compilare un modulo allegato che altro non era che un documento falso nel quale era incorporato uno script dannoso. Per evitare di rivelare il payload nelle sandbox malware, lo script iniziava a scaricare il payload solo dopo un certo intervallo di tempo.

Il documento "esca" utilizzava uno dei soliti stratagemmi per indurre gli utenti a cliccare su un pulsante "Attiva contenuto", azione che provocava l'esecuzione dello script VBA dannoso incorporato nel documento.

Sostegno finanziario fasullo

In molti casi gli attacchi digitali sono di tipo locale, a seconda dell'impatto dell'epidemia di COVID-19 su un particolare paese. Ad esempio, lo stato del Nord Reno-Westfalia in Germania è stato vittima di una campagna di phishing. Gli hacker hanno creato copie fasulle del sito web del Ministero degli Affari Economici dello stato, nelle quali era possibile fare richiesta di aiuti finanziari per l'emergenza COVID-19. I truffatori raccoglievano i dati personali inviati dalle vittime, quindi

presentavano le proprie richieste al sito web legittimo utilizzando le informazioni delle vittime e associandovi i propri dati bancari. Gli uffici statali hanno dichiarato di aver autorizzato fino a 4.000 richieste fraudolente, per un totale di 109 milioni di dollari accreditati ai criminali.

Truffe associate alla didattica a distanza

I criminali hanno anche preso di mira le attività didattiche remote. Una nuova e-mail di phishing con oggetto riguardante la pandemia recapitava un trojan Formbook incorporato in una finta richiesta di valutazione per gli insegnanti. Formbook è un malware di tipo “infostealer”, in grado di rubare credenziali di login dai browser Internet. Viene promosso sui forum di hacker da febbraio 2016.

È interessante notare come gli hacker abbiano impiegato varie tecniche anti-analisi e anti-rilevamento, come il rilevamento delle sandbox e delle virtual machine, la steganografia e la crittografia XOR per nascondere il payload, riuscendo a evitare di essere intercettati da Windows Defender.

I criminali dietro le campagne Formbook sono anche noti per gli attacchi ad aziende biomediche finalizzati a sottrarre risorse finanziarie, dati personali riservati e proprietà intellettuale.

Falsi documenti di congedo per motivi medici

Anche la campagna Trickbot ha sfruttato le paure legate alla pandemia di COVID-19 per diffondere un documento dannoso dal titolo “Family and Medical Leave of Act 22.04.doc” (SHA256: 875d0b66ab7252cf8fe6ab23e31926 b43c1af6dfad6d196f311e64ed65e7c0ce).

Il documento Family Medical Leave Act (FMLA) riconosce ai dipendenti il diritto di prendere un congedo retribuito per motivi medici. Ma non appena l'utente attiva la macro contenuta nei documenti falsi, uno script dannoso inizia a scaricare un malware nel computer.

Un nuovo tipo di estorsione a sfondo sessuale

Abbiamo scoperto una nuova variante di truffa del tipo "sextortion". Anche in questo caso i criminali informatici usano una password precedentemente rubata come elemento per convincere l'utente, ma invece di minacciare di divulgare un video registrato, prendono di mira direttamente la vita dell'utente, dichiarando di conoscere esattamente l'indirizzo dell'abitazione e le abitudini quotidiane della vittima e spingendosi a minacciarla di "contagiare la sua famiglia con il coronavirus". Per evitare le queste conseguenze, la vittima deve versare 4.000 dollari in bitcoin.

Non è la prima volta che i criminali informatici minacciano la vita degli utenti. In passato abbiamo assistito a casi in cui minacciavano di inviare dei teppisti per picchiare le vittime, ma la minaccia di contagio da coronavirus rappresenta una notevole escalation.

Nella maggior parte dei casi le e-mail sono inviate da indirizzi falsificati, oppure anche da account e-mail reali. Ovviamente, il messaggio stesso si presenta come fraudolento e può essere semplicemente cancellato.

A caccia di segreti governativi e aziendali relativi al COVID-19

Certi dati di valore relativi alla pandemia di COVID-19, che alcuni analisti sospettano essere stati tenuti segreti dal governo cinese, stanno attirando l'interesse degli hacker a livello globale. Ad esempio, il gruppo di hacker vietnamita APT32 (noto anche con il nome OceanLotus), sponsorizzato dallo stato, avrebbe attaccato le organizzazioni statali cinesi con l'intento di sottrarre misure di controllo del virus, ricerche mediche e statistiche sui contagi che si sospetta non siano state divulgate dalla Cina. Il Vietnam confina con la Cina e il suo interesse sarebbe motivato dal desiderio di controllare la diffusione della pandemia nella regione.

L'azienda cinese Huiying Medical, che sostiene di aver sviluppato intelligenza artificiale in grado di diagnosticare il COVID-19 con un'affidabilità del 96% in base alle immagini di una tomografia computerizzata (TC), avrebbe subito un'incursione di hacker. Secondo l'azienda di cybersecurity Cyble, un hacker con il nome di battaglia "THE0TIME" ha messo in vendita sul Dark Web dati di Huiying Medical che potrebbero contenere informazioni di utenti, codice sorgente e relazioni su esperimenti, al prezzo di quattro bitcoin (circa 30.000 dollari al momento).

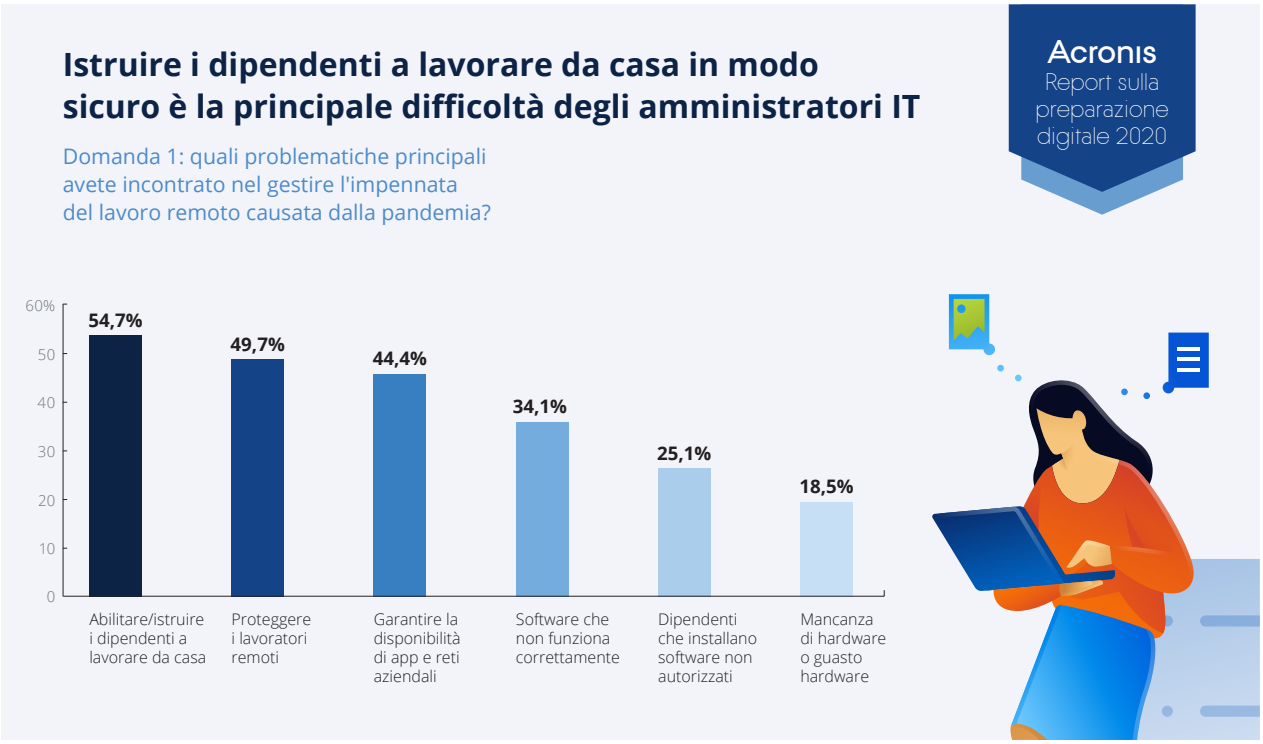
Altri gruppi ATP hanno preso di mira aziende farmaceutiche e laboratori vaccinali con l'intento di rubare altri dati preziosi.

2. Lavoratori remoti sotto attacco

La pandemia di COVID-19 ha trasformato sensibilmente il panorama delle minacce, evidenziando vari rischi per la sicurezza e la privacy associati a diversi aspetti del lavoro a distanza, come l'accesso remoto ai server aziendali, le videoconferenze e la formazione in materia di sicurezza per i dipendenti.

Per valutare l'efficacia con cui i team IT hanno affrontato questa esperienza, ovvero se sono stati in grado di predisporre e proteggere con successo gli ambienti remoti, oppure se vi è un evidente margine di miglioramento, abbiamo stilato il nostro primo Report Acronis sulla preparazione digitale. Per farlo, abbiamo sondato 3.400 aziende e lavoratori remoti a livello internazionale nei mesi di giugno e luglio 2020, raccogliendo le loro esperienze su minacce, problematiche e tendenze che hanno osservato da quando sono passati al lavoro a distanza. I risultati sono allarmanti:

- Quasi la metà di tutti i responsabili IT ha avuto difficoltà a formare e proteggere i lavoratori remoti.
- Il 31% delle aziende globali ha subito attacchi da parte di criminali informatici almeno una volta al giorno. I tipi di attacchi più comuni sono stati tentativi di phishing, attacchi DDoS e attacchi ai servizi di videoconferenza.
- Il 92% delle organizzazioni mondiali ha dovuto adottare nuove tecnologie per completare la transizione al lavoro a distanza. Di conseguenza, il 72% di esse ha visto aumentare i costi dell'IT nel corso della pandemia.
- Gli attacchi riusciti rimangono frequenti nonostante la maggiore spesa tecnologica, perché le organizzazioni non danno la giusta priorità alle capacità di difesa.
- Il 39% delle aziende ha registrato attacchi alle videoconferenze durante la pandemia.



Zoom sotto attacco durante la pandemia

Fin dall'inizio della pandemia di COVID-19, la piattaforma di videoconferenza Zoom ha attirato l'attenzione dei criminali informatici. Con l'allargarsi della base di utenti, sempre più persone hanno iniziato ad analizzare il codice di Zoom alla ricerca di vulnerabilità, sollevando dubbi sulla privacy della piattaforma.

Ad esempio, Vice.com ha segnalato che due vulnerabilità zero-day (falle nella sicurezza ignote ai produttori del software e per le quali quindi non esistevano patch) erano disponibili sul mercato del Dark Web: una per Windows e un'altra per macOS. L'exploit RCE (Remote Code Execution) di Zoom per Windows era in vendita a 500.000 dollari.

Zoom è stato il bersaglio anche di una campagna di phishing finalizzata a rubare credenziali di servizio. Le e-mail di phishing sono state recapitate a più di 50.000 mailbox, prendendo di mira utenti Microsoft 365 con un invito e-mail fasullo per un'imminente chiamata Zoom con il reparto risorse umane relativamente alla valutazione del rendimento (un argomento pensato per indurre ansia nella vittima e aggirare la normale cautela nel cliccare sui link contenuti nelle e-mail). A seguito di questi attacchi di phishing, combinati agli attacchi di "credential stuffing" in cui gli hacker controllano se l'utente ha usato la stessa password su più servizi, oltre 500.000 credenziali di utenti Zoom sono state esposte sui forum clandestini.

Anche il fatto che molte videoconferenze Zoom fossero prive di password ha attirato i criminali informatici, che hanno iniziato a provare tutti i possibili ID riunione finché non trovavano una riunione in corso. A quel punto entravano nella videoconferenza e disturbavano i partecipanti riproducendo video o musica a tutto volume, o altri contenuti inappropriati. Questi attacchi di "Zoom-bombing" hanno costretto molte scuole a interrompere i loro programmi di didattica a distanza.

Non solo Zoom: anche gli utenti di Microsoft 365 sono vittime di attacchi

Ovviamente Zoom non è stato l'unico strumento di collaborazione a finire nel mirino degli hacker. Attacchi analoghi sono stati sferrati contro Microsoft Teams e Webex. Ad esempio, fino a 50.000 utenti di Microsoft 365 sono stati attaccati nel giro di una settimana con e-mail di phishing contenenti false notifiche di Microsoft Teams che reindirizzavano le vittime a una finta pagina di login di Microsoft 365.

I servizi Microsoft di condivisione file come Sway, SharePoint e OneNote sono stati attaccati da varie mini-campagne di phishing che prendevano di mira società di servizi finanziari, studi legali e gruppi immobiliari. Un particolare attacco, denominato PerSwaysion perché aveva come bersaglio i servizi Sway, veniva eseguito in tre fasi. Inizialmente inviava e-mail di phishing contenenti un allegato PDF dannoso, che si presentavano come notifiche di condivisione file di Microsoft 365 con un link "Leggi ora". Con un clic sul link si apriva un altro documento a scopo diversivo nei servizi di condivisione file Microsoft (Sway, per l'appunto) con un altro link "Leggi ora" che indirizzava la vittima a una pagina di login Microsoft fasulla dove le sue credenziali venivano rubate.

Mancanza di sicurezza per il personale che lavora da casa

Ora che molte persone devono lavorare da casa con il proprio computer, le minacce alla sicurezza sono al livello di massima allerta. Non solo i computer domestici sono spesso privi di una protezione informatica efficace, ma molti utenti non applicano regolarmente le più recenti patch di sicurezza per il sistema operativo e i software più comuni, lasciando il computer vulnerabile a eventuali attacchi. Molti di questi computer personali non sono gestiti dal reparto IT dell'azienda e pertanto non sono conformi alle policy aziendali.

La risoluzione di questi problemi di vulnerabilità e patch management sul perimetro della rete è diventata un vero grattacapo per amministratori e tecnici che forniscono alle piccole aziende il supporto IT vitale per sopravvivere durante l'attuale emergenza.

Inoltre, le reti domestiche sono spesso esposte ad altri dispositivi non protetti, ad esempio appartenenti a bambini o ad altri membri della famiglia. Quando poi il router della banda larga è obsoleto, gli hacker sono in grado di assumerne il controllo e di reindirizzare il traffico in modo specifico.

3. MSP nel mirino dei criminali informatici

Poiché molte piccole e medie imprese sono servite da Managed Service Provider (MSP), numerosi MSP sono diventati vittime di attacchi informatici. La logica è semplice: anziché compromettere 100 aziende diverse, per i criminali è sufficiente violare i sistemi di un unico MSP tramite i quali accedere a 100 clienti. Gli attacchi registrati nel 2020 indicano che è possibile penetrare nei sistemi degli MSP mediante varie tecniche e che i software di accesso remoto non configurati correttamente sono i vettori di attacco preferiti. I criminali hanno sfruttato le vulnerabilità, l'assenza dell'autenticazione a due fattori (2FA) e il phishing per accedere agli strumenti di gestione degli MSP e, quindi, ai sistemi dei loro clienti.

DXC Technology, provider internazionale di servizi e soluzioni IT, ha denunciato ad esempio un attacco ransomware subito dai propri sistemi presso la filiale Xchanging. Tra i clienti di Xchanging figurano principalmente aziende che operano nel settore assicurativo, ma anche società di altri settori: servizi finanziari, industria aerospaziale, difesa, automotive, istruzione, prodotti di consumo, sanità e settore manifatturiero. Un altro esempio è quello di Canadian MSP Pivot Technology Solutions, che ha registrato un attacco informatico alla propria infrastruttura IT. L'azienda ha subito una violazione dei dati a seguito di un attacco ransomware, con il rischio di esporre le informazioni personali dei clienti. Si tratta di uno scenario tipico del 2020 e prevediamo che altri casi analoghi siano destinati ad emergere.

4. Il ransomware è ancora la minaccia numero uno

Il 2020 è stato chiaramente un anno all'insegna del ransomware, con più attacchi, perdite più ingenti e nuove tecniche di estorsione messe in atto dai criminali informatici. Praticamente ogni settimana sono registrati nuovi casi eclatanti. Secondo un report pubblicato da Coalition, uno dei principali fornitori di servizi di "assicurazione digitale" del Nord America, i casi di ransomware hanno rappresentato il 41% delle denunce di sinistro di natura digitale presentate nella prima metà del 2020. "Il ransomware non distingue tra un settore e l'altro. Abbiamo registrato un aumento degli attacchi ransomware in quasi tutti i settori che serviamo", afferma Coalition. Acronis può confermare questa circostanza.

Qui delineiamo le preoccupanti tendenze a livello generale, mentre nelle sezioni successive del report potete consultare le statistiche dettagliate dei nostri Cyber Protection Operation Center.

Bersagli grossi per riscatti sostanziosi

Il 18 luglio, il principale fornitore di servizi di telecomunicazioni argentino è stato colpito da un attacco ransomware – probabilmente sferrato dal gruppo Sodinokibi – con una richiesta di riscatto di 7,5 milioni di dollari. Come spesso accade in questi casi, per costringere la vittima a una decisione rapida i criminali hanno fissato un ultimatum di 48 ore, allo scadere del quale l'importo del riscatto sarebbe raddoppiato. Il ransomware avrebbe infettato più di 18.000 workstation, compresi terminali con dati altamente sensibili.

Garmin, uno dei più importanti produttori di dispositivi indossabili, ha confermato che l'importante guasto avvenuto il 24 luglio è stato causato da un attacco ransomware WastedLocker, che ha costretto l'azienda a bloccare le attività del call center, Garmin Connect e anche le linee di produzione a Taiwan. Con un fatturato annuale stimato di 4 miliardi di dollari, Garmin è decisamente un target di alto profilo. Si ritiene che sia stato richiesto un riscatto di 10 milioni di dollari. In altri attacchi WastedLocker recenti sono state avanzate richieste di importi variabili da 500.000 dollari a svariati milioni.

La lista delle vittime di alto profilo continua ad allungarsi. In febbraio, l'FBI ha pubblicato le stime dei proventi di alcuni gruppi di ransomware. Dai dati emergeva che gruppi come Ryuk hanno rastrellato circa 3 milioni di dollari al mese nel 2019. Con profitti del genere, è improbabile che questo tipo di minaccia possa indebolirsi nel breve periodo.

Inoltre, le famiglie di ransomware moderne non si limitano a pretendere un riscatto per decifrare i dati ma anche per non divulgare al pubblico informazioni riservate, il che non fa che aumentare le chance di successo.

Richiesta di riscatto per evitare la divulgazione

Il gruppo ransomware REvil/Sodinokibi ha annunciato il 14 agosto di aver compromesso l'azienda del Kentucky Brown-Forman, che possiede marchi di whisky come Jack Daniels, Old Forester, The Glendronach e vari altri vini e liquori. Con un rendiconto annuale 2020 che registra profitti lordi superiori a 2 miliardi di dollari e un utile netto di 872 milioni, Brown-Forman è innegabilmente un bersaglio di alto profilo per gli autori di attacchi ransomware.

Il gruppo REvil sostiene di aver sottratto 1 TB di dati, tra cui informazioni personali dei dipendenti, dati finanziari, comunicazioni interne e contratti aziendali. Le immagini pubblicate nel sito di divulgazione del gruppo indicano che i dati in suo possesso risalgono fino al 2009.

Canon, l'azienda multinazionale specializzata nei prodotti ottici e di imaging, è stata vittima di un attacco ransomware Maze che ha colpito il sistema e-mail, Microsoft Teams, il sito USA dell'azienda e altre applicazioni interne. I criminali dietro il ransomware Maze hanno dichiarato di aver rubato oltre 10 TB di dati da Canon, compresi database privati. Canon ha ammesso l'attacco in un messaggio interno inviato al personale.

CWT, una delle principali aziende di organizzazione viaggi ed eventi al mondo, è stata compromessa dal ransomware Ragnar Locker. Gli aggressori avrebbero sottratto 2 TB di dati aziendali sensibili e sostengono di aver compromesso oltre 30.000 sistemi. Nonostante la richiesta iniziale dei criminali fosse di 10 milioni di dollari per ottenere la restituzione dei dati rubati, CWT ha avviato una trattativa ed è riuscita a concordare il pagamento di un riscatto di 414 bitcoin, pari a più di 4 milioni di dollari al tasso attuale.

Conti, un nuovo ransomware as a service (RaaS) evoluzione della famigerata variante Ryuk, ha rilasciato un sito web di divulgazione di dati per rafforzare la propria strategia di estorsione e costringere le vittime a pagare un riscatto.

Anche se Conti è attivo da vari mesi, solo recentemente i criminali informatici hanno rilasciato un sito di divulgazione di dati nel quale minacciano di pubblicare i dati rubati alle vittime in caso di mancato pagamento del riscatto. "Conti.News" ha fatto finora 112 vittime, tra cui alcune note aziende di grandi dimensioni.

In totale, circa 20 gruppi di ransomware diversi hanno creato pagine dedicate per divulgare i dati rubati, ospitate sulla rete clandestina Tor. Oltre 700 aziende hanno visto i propri dati pubblicati; nel 37% dei casi la fuoriuscita di dati era la conseguenza di infezioni del ransomware Maze, seguito da Conti (15%) e da Sodinokibi (12%).

Queste violazioni di dati possono causare danni alla reputazione, attacchi di follow-up e varie multe. Inoltre, la perdita dei dati dei clienti potrebbe essere sanzionabile ai sensi delle normative sulla privacy quali GDPR o CCPA, e il pagamento del riscatto potrebbe configurare un reato ai sensi del regolamento OFAC degli Stati Uniti.

5. Backup e sicurezza di base non bastano più

Dal 2016 abbiamo segnalato che il ransomware avrebbe attaccato le soluzioni di backup. La nostra previsione si basava sul fatto che iniziative come No More Ransom, di cui Acronis fa orgogliosamente parte dal 2017, incoraggiano persone e aziende a non pagare i riscatti e, al contrario, a proteggere adeguatamente i sistemi dal ransomware. Se avete un backup, non dovete pagare nessun riscatto perché potete semplicemente ripristinare i vostri dati. L'idea di base era questa, ma i criminali informatici si sono presto dati da fare per aggirare l'ostacolo. Dal 2017 praticamente ogni ceppo di ransomware ha iniziato a cancellare o disabilitare le copie shadow del volume di Windows e a tentare di disabilitare le soluzioni di backup tradizionali. Non è stato difficile, poiché queste soluzioni prevedono in genere meccanismi di protezione molto semplici o non li prevedono affatto. Il test condotto dal laboratorio NioGuard, membro AMTSO, riflette chiaramente questa situazione preoccupante.

Diamo un'occhiata ad alcuni esemplari di ransomware recenti.

RANSOMWARE CONTI:

- La richiesta di riscatto media di questo ransomware è di meno di 100.000 dollari
- Usa Windows Restart Manager per chiudere i file aperti o non salvati prima di applicare la crittografia
- Contiene più di 250 routine di decrittografia di stringhe e circa 150 servizi da bloccare
- Esegue la crittografia rapida dei file in 32 thread simultanei utilizzando le porte di completamento I/O di Windows
- Segue la tendenza e recentemente ha lanciato il sito di divulgazione dati 'Conti.News'

Ma non è tutto: il ransomware cancella le copie shadow dei file e ridimensiona gli storage shadow per i dischi da C: a H:, potenzialmente eliminando altre copie shadow. Inoltre, arresta i servizi appartenenti a soluzioni SQL, antivirus, di cybersecurity e di backup BackupExec e Veeam, e tenta di bloccare anche la soluzione di Acronis Cyber Protect, ma fallisce nell'intento grazie alla nostra funzionalità di auto-protezione. L'elenco contiene circa 150 servizi, tra cui:

Acronis VSS Provider	BackupExecRPCService	VeeamDeploySvc
Veeam Backup Catalog Data Service	BackupExecVSSProvider	VeeamEnterpriseManagerSvc
AcronisAgent	EPSecurityService	VeeamMountSvc
AcrSch2Svc	EPUpdateService	VeeamNFSSvc
Scansione	mozyprobackup	VeeamRESTSvc
BackupExecAgentAccelerator	VeeamBackupSvc	VeeamTransportSvc
BackupExecAgentBrowser	VeeamBrokerSvc	VeeamHvIntegrationSvc
BackupExecDeviceMediaService	VeeamCatalogSvc	Zoolz 2 Service
BackupExecJobEngine	VeeamCloudSvc	AVP
BackupExecManagementService	VeeamDeploymentService	

RANSOMWARE NETWALKER:

Un altro esempio è quello del ransomware Netwalker, scoperto in circolazione nell'agosto 2019, che implementa il modello RaaS e prende di mira sia organizzazioni che singoli utenti. Da marzo 2020, gli autori di questo ransomware sono riusciti a estorcere circa 25 milioni di dollari. Il tratto distintivo della versione più recente di Netwalker è l'impiego del loader PowerShell pesantemente offuscato per avviare il ransomware su un sistema infetto. L'uso dello script PowerShell, o in generale l'abuso di tool preinstallati mediante la tattica LotL (Living off the Land), rimane molto diffuso tra i criminali informatici.

Analogamente ad altri ceppi di ransomware, Netwalker cancella le copie shadow dei file di Windows.

```
Get-Wmiobject Win32_Shadowcopy | ForEach-Object {$_.Delete();} | Out-Null
```

Inoltre, Netwalker tenta di bloccare i servizi di backup che iniziano con le stringhe seguenti, per impedire il ripristino:

veeam*	ShadowProtectSvc	StorageCraft ImageManager
backup*	AcronisAgent	acrsch2svc*
backup	AcrSch2Svc	

Parte 2

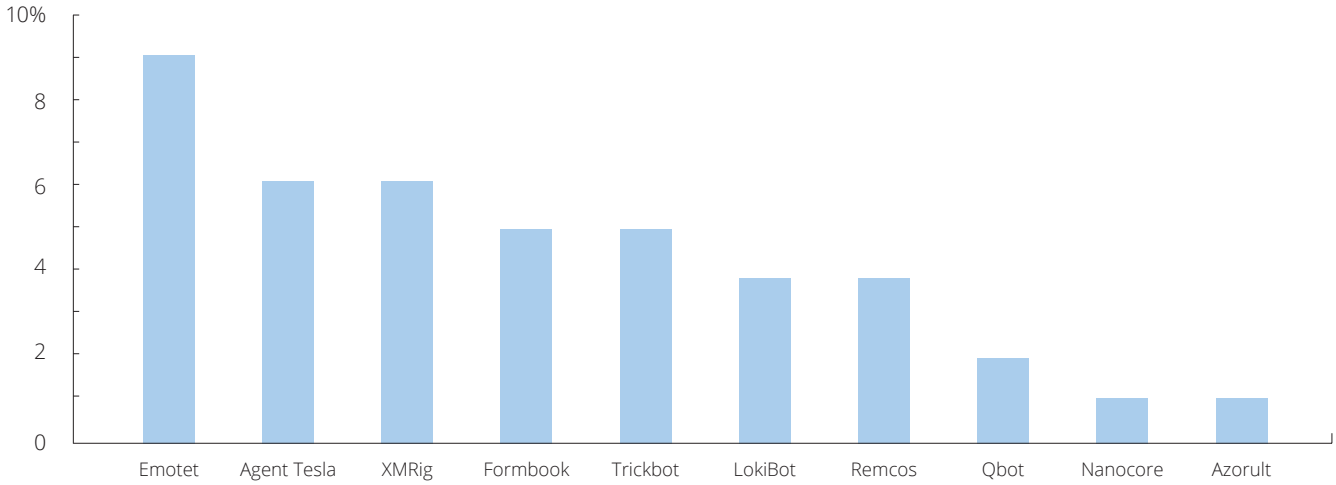
La minaccia generale del malware

Nel terzo trimestre del 2020, in media l'11% dei nostri clienti ha bloccato con successo almeno un attacco malware. Dall'inizio della pandemia, i numeri sono scesi leggermente per tornare a livelli normali. A luglio, la percentuale era ancora dal 14,7%, quindi è passata al 10,1% ad agosto, 8,9% a settembre e 6,7% a ottobre.

Il paese con il maggior numero di clienti che hanno rilevato attacchi malware nel terzo trimestre 2020 sono stati gli Stati Uniti con il 27,9%, seguiti dalla Germania con il 16,7% e dal Regno Unito con il 6,1%.

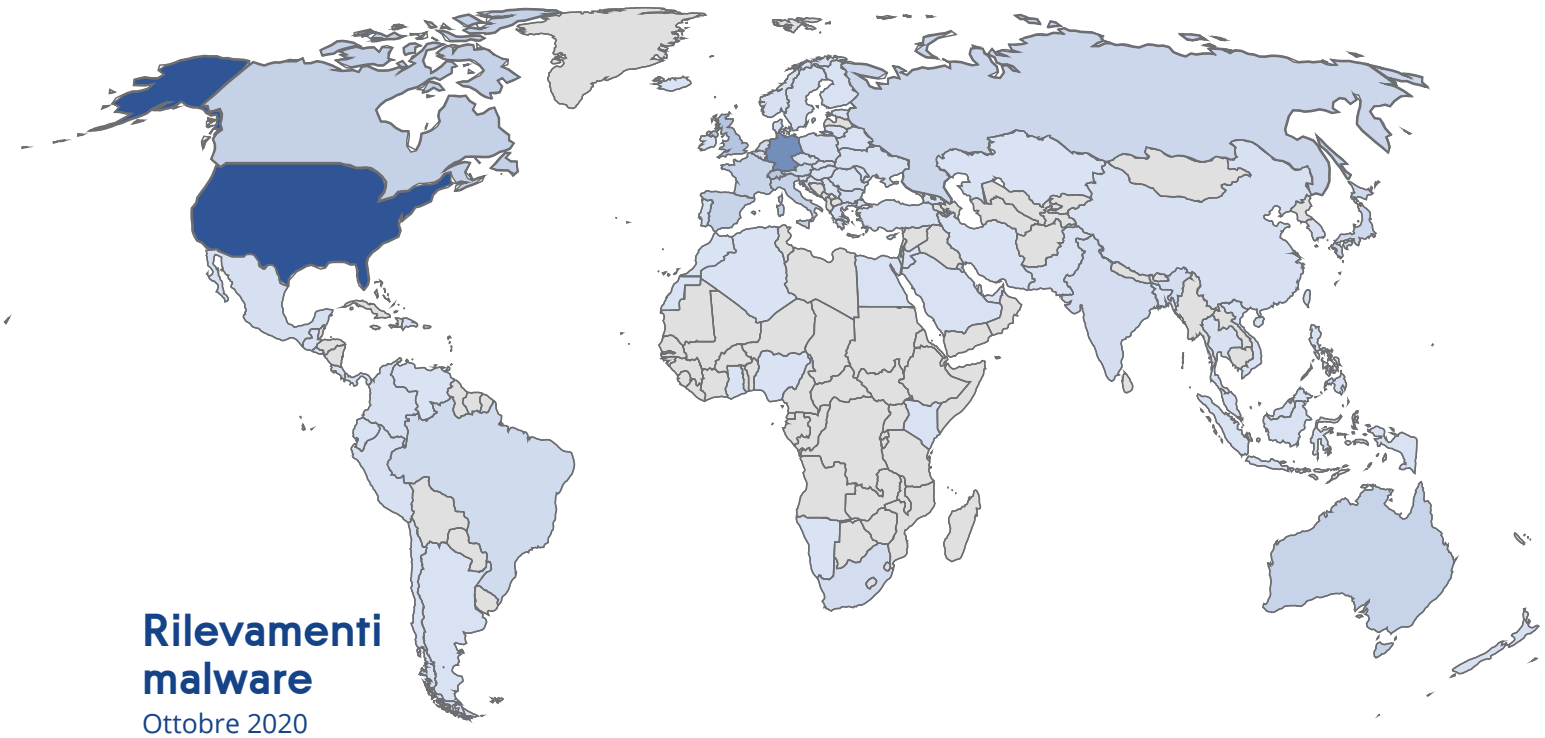
Il laboratorio indipendente di test sul malware AV-Test ha registrato 400.000 nuovi esemplari di malware al giorno nel 3° trimestre del 2020, una chiara indicazione del fatto che i criminali informatici stanno automatizzando i loro processi e generando un'ondata di nuove minacce malware. Tuttavia, la maggior parte di queste minacce viene utilizzata solo per una manciata di attacchi concentrati in un breve periodo. Degli esemplari incontrati, il 19% è stato osservato una sola volta. La vita media di un esemplare dannoso è stata di 3,4 giorni, prima di scomparire definitivamente.

Queste sono le principali 10 famiglie di malware osservate e monitorate nel 2020:



Percentuale mensile di rilevamenti per paese

PAESE	OTTOBRE 2020	SETTEMBRE 2020	AGOSTO 2020	LUGLIO 2020
Stati Uniti	27,5%	27,9%	29,3%	16,4%
Germania	18,4%	16,7%	16,8%	4,3%
Svizzera	7,2%	5,4%	3,6%	3,2%
Regno Unito	5,9%	6,1%	6,4%	4,5%
Canada	3,0%	3,6%	3,6%	1,5%
Francia	3,0%	2,9%	3,3%	2,3%
Italia	3,0%	3,2%	3,3%	1,7%
Australia	3,0%	3,3%	3,1%	2,0%
Spagna	2,6%	3,0%	2,8%	4,2%
Giappone	2,0%	2,3%	3,2%	15,7%



Rilevamenti malware

Ottobre 2020

Percentuale

0% 0,27%

Se normalizziamo il numero di rilevamenti per cliente attivo per paese, otteniamo una distribuzione leggermente diversa. La tabella seguente mostra il numero di rilevamenti riscontrati per 1.000 clienti per paese. Si evince chiaramente che le minacce digitali sono un fenomeno globale.

POSIZIONE	PAESE	RILEVAMENTO MALWARE per 1.000 clienti osservato in agosto
1	Stati Uniti	2.059
2	Giappone	1.571
3	India	1.168
4	Colombia	1.123
5	Brasile	994
6	Thailandia	856
7	Irlanda	729
8	Spagna	634
9	Repubblica Ceca	611
10	Germania	601
11	Italia	589

POSIZIONE	PAESE	RILEVAMENTO MALWARE per 1.000 clienti osservato in agosto
12	Hong Kong	518
13	Taiwan	480
14	Nuova Zelanda	462
15	Polonia	453
16	Francia	444
17	Grecia	437
18	Danimarca	375
19	Australia	361
20	Belgio	358
21	Sudafrica	351
22	Bulgaria	351
23	Canada	347
24	Regno Unito	329
25	Svizzera	311

Numero normalizzato di rilevamenti

ad agosto 2020

Numero di rilevamenti per 1.000 clienti

131 2.059

Minaccia ransomware

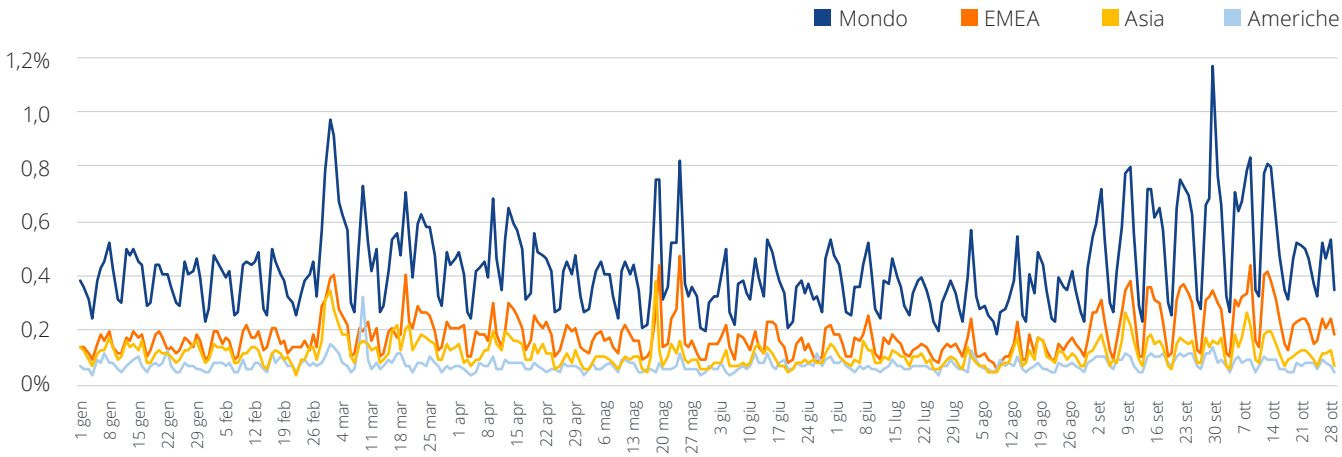
Come abbiamo già segnalato nella sezione sulle tendenze principali, il ransomware è ancora la minaccia informatica numero uno per le aziende. Sebbene osserviamo il ransomware dal 2017, anno in cui abbiamo sviluppato Acronis Active Protection, in questa sezione ci concentriamo sui dati dal 1° gennaio al 31 ottobre 2020.

Queste sono le principali 10 famiglie di ransomware osservate e monitorate nel 2020. Tenete presente che alcuni gruppi tentano di infettare il maggior numero possibile di utenti finali, adottando un approccio ad ampio spettro, mentre altri prendono di mira bersagli di alto profilo, concentrandosi su un numero limitato di infezioni con un maggior potenziale di guadagno. Di conseguenza, il volume delle minacce rilevate non è da solo un'indicazione valida del livello di pericolosità di una minaccia.

Negli ultimi nove mesi abbiamo assistito alla comparsa di circa 50 nuove famiglie di ransomware. In alcuni casi si tratta di piccoli gruppi che prendono di mira i consumatori, ma la tendenza dei nuovi gruppi come Avaddon, Mount Locker e Suncrypt è quella di attaccare le grandi aziende per realizzare profitti più elevati. Un numero crescente di questi gruppi è attivo nel business del ransomware-as-a-service e opera redistribuendo minacce ransomware già note e collaudate, la cui diffusione quindi aumenta ancora di più.

Rilevamenti ransomware quotidiani

Quest'anno abbiamo osservato un'evidente impennata globale all'inizio del lockdown di marzo legato alla pandemia di COVID-19. Da allora, l'attività del ransomware è rimasta a livelli più alti del normale. Relativamente ai settori e alle regioni geografiche che hanno subito attacchi, non abbiamo registrato eccezioni: tutti i settori sono stati presi di mira. A settembre abbiamo iniziato a osservare una nuova ondata di attacchi ransomware, specialmente rivolti contro istituti scolastici e aziende manifatturiere nel Nord America.



Primi 10 paesi: rilevamenti di ransomware per regione

Asia:

PAESE	Percentuali di ransomware rilevati per regione nel 3° trimestre 2020
Giappone	17,7%
Filippine	13,3%
Taiwan	9,6%
Cina	8,6%
India	7,8%
Turchia	5,4%
Iran	5,3%
Corea del Sud	3,9%
Indonesia	3,7%
Thailandia	3,6%

EMEA:

PAESE	Percentuali di ransomware rilevati per regione nel 3° trimestre 2020
Germania	17,7%
Francia	13,3%
Italia	9,6%
Regno Unito	8,6%
Svizzera	7,8%
Spagna	5,4%
Austria	5,3%
Paesi Bassi	3,9%
Belgio	3,7%
Repubblica Ceca	3,6%

Americhe:

PAESE	Percentuali di ransomware rilevati per regione nel 3° trimestre 2020
Stati Uniti	67,3%
Canada	15,9%
Cile	4,7%
Brasile	3,0%
Messico	2,7%
Colombia	1,7%
Perù	1,0%
Argentina	0,8%
Bolivia	0,4%
Ecuador	0,3%

Gruppi di ransomware in evidenza

Maze è un ransomware furtivo che crittografa e sottrae TB di dati privati tramite attacchi mirati

Il ransomware Maze è stato osservato in attacchi mirati fin da maggio 2019 e si ritiene che sia responsabile dell'attacco più recente subito da Canon il 30 luglio 2020, che ha causato il blocco del servizio di cloud storage image.canon. Inoltre, gli autori del ransomware Maze sostengono di aver sottratto 10 TB di dati privati nel corso della loro incursione nei sistemi Canon. Hanno anche già pubblicato i dati di Xerox e LG che hanno rubato durante l'attacco di giugno 2020, poiché le aziende si sono rifiutate di pagare un riscatto.

- **Non si limita a crittografare i dati ma li trafuga, per pubblicarli successivamente in caso di mancato pagamento del riscatto**
- **Canon, Xerox e LG sono tra le vittime più illustri di Maze**
- **Impiega tecniche anti-disassemblaggio e anti-debug**
- **Non applica la crittografia ai sistemi con impostazioni regionali predefinite russe**
- **La chiamata wmic.exe per cancellare le copie shadow è offuscata**
- **Invia una richiesta di check-in HTTP al server server C&C ubicato nella rete "91.218.114.0" di Mosca in Russia**
- **Usa i tool di hacking Mimikatz, ProcDump e Cobalt Strike per la proliferazione**

Il ransomware Maze viene solitamente inoculato a seguito di un attacco mirato contro un'organizzazione, che esordisce con un'e-mail di spear-phishing per ottenere accesso a una connessione RDP o VDI compromessa (le cui credenziali vengono in genere acquistate sul Dark Web) e sfruttare le vulnerabilità delle VPN.

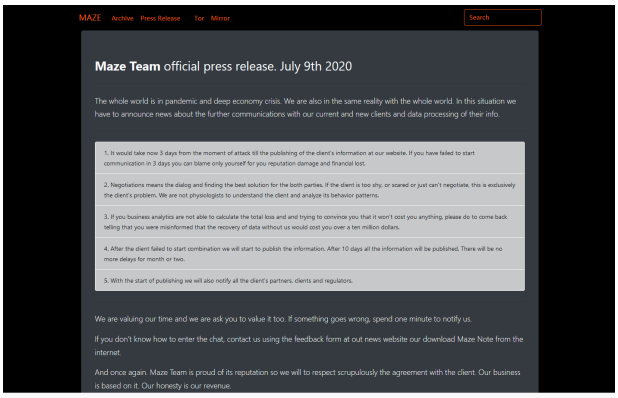
Una volta che l'operatore Maze è riuscito ad accedere alla rete interna dell'organizzazione, esegue Mimikatz e ProcDump per rastrellare le password memorizzate nella memoria e avviare la ricognizione utilizzando il tool di red-teaming Cobalt Strike.

Maze impiega tecniche anti-disassemblaggio per impedire l'analisi del codice in un disassembler.

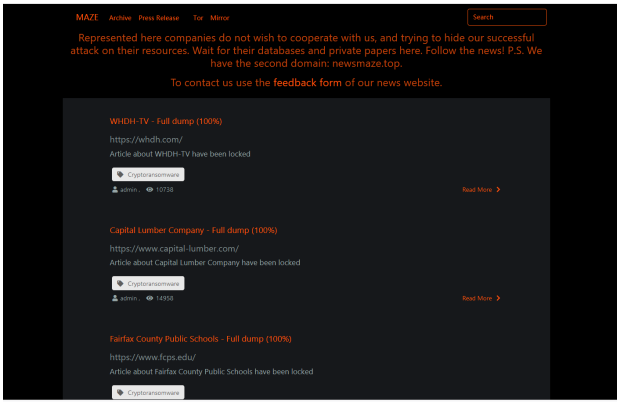
Le tecniche di offuscamento includono:

1. **Salti condizionali che reindirizzano alla stessa posizione, in sostituzione dei salti assoluti**
2. **Chiamate seguite dalla trasmissione dell'indirizzo di risposta allo stack e dal salto all'indirizzo del chiamante**

Maze è anche in grado di rilevare se il codice viene sottoposto a debug. Controlla il flag "BeingDebugged" nella struttura PEB per verificare se il processo viene eseguito in un debugger. In caso affermativo, il codice entra in una ripetizione ciclica infinita e non esegue la crittografia. Inoltre, Maze arresta i processi dei tool di analisi del malware e dei programmi per ufficio in base agli hash dei rispettivi nomi.



Maze è simile ad altri ceppi di ransomware recenti come WastedLocker, Netwalker e REvil per il fatto che non si limita a crittografare i dati, ma li trafuga.



Usa l'utilità 7zip per comprimere i dati raccolti ed esfiltrare gli archivi nel server FTP dell'aggressore mediante il client WinSCP. In alcuni incidenti è stato osservato che i dati esfiltrati sono anche stati codificati in Base64.

Nel complesso, tutto questo rende la famiglia di ransomware Maze una delle più pericolose tra quelle emerse nel 2020.

Il ransomware DarkSide non attacca ospedali, scuole e governi

DarkSide è un nuovo ceppo di ransomware. Gli attacchi sono cominciati all'inizio di agosto 2020, apparentemente condotti da criminali affiliati a precedenti campagne ransomware che, dopo aver fatto soldi nel business delle estorsioni, hanno deciso di sviluppare un codice in proprio. In base agli incidenti noti, l'ammontare del riscatto è compreso tra 200.000 e 2 milioni di dollari. Come altri ransomware utilizzati in attacchi mirati, DarkSide non solo crittografa i dati ma li esfiltra dai server compromessi.

A differenza di Maze, che ha attaccato con successo il distretto scolastico Newhall e le scuole della Contea di Fairfax, DarkSide osserva un codice di condotta che proibisce di attaccare ospedali, scuole e organizzazioni governative.

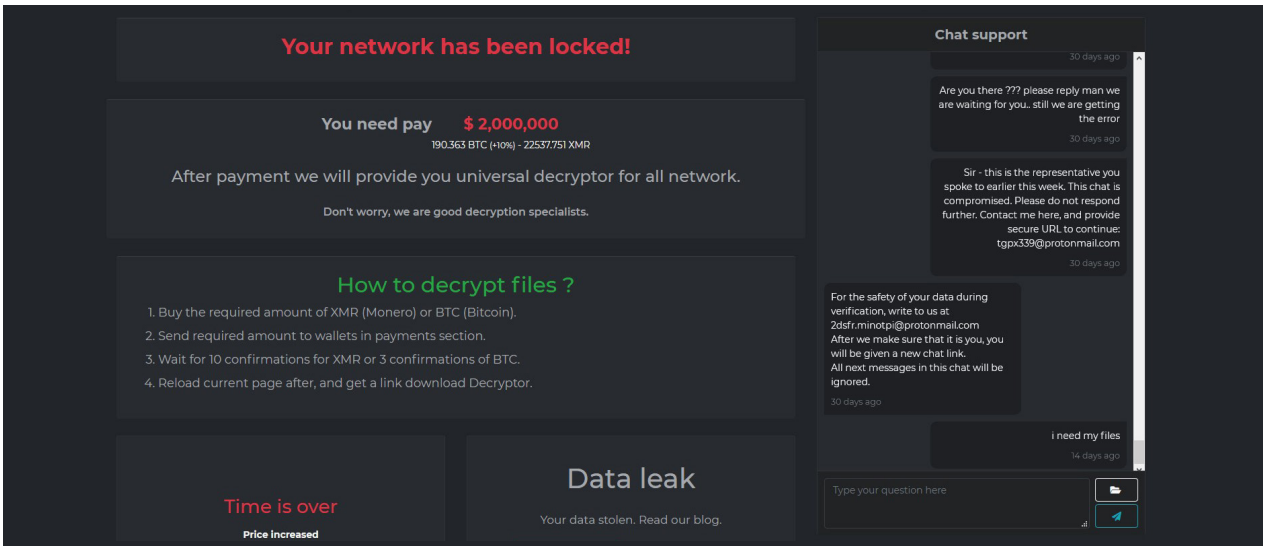
- **Scoperto ad agosto 2020**
- **Prende di mira solo paesi di lingua inglese, evitando quelli dell'ex Unione Sovietica**
- **Non attacca ospedali, case di riposo, scuole, università, organizzazioni no-profit e il settore pubblico**
- **Usa Salsa20 con la matrice personalizzata e gli algoritmi di crittografia RSA-1024**
- **Le richieste di riscatto variano da 200.000 a 2.000.000 $**

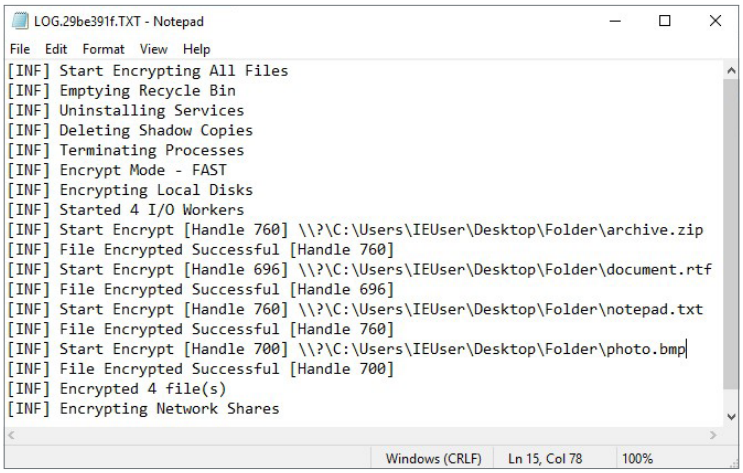
Il ransomware svuota il Cestino del sistema senza usare la funzione SHEmptyRecycleBinA() per risultare più furtivo e cancella invece uno alla volta i file e le cartelle presenti nel Cestino.

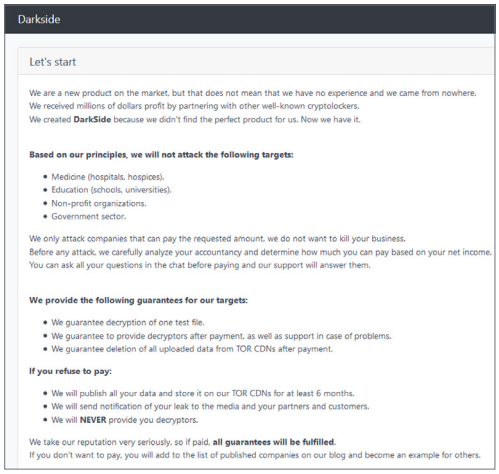
DarkSide disinstalla i seguenti servizi relativi alle soluzioni di sicurezza e backup:

Dopo aver disinstallato Servizio Copia Shadow del volume (VSS), il ransomware cancella le copie shadow lanciando uno script PowerShell offuscato. DarkSide specifica anche una chiave, che deve essere inserita nel primo sito. La chiave non è univoca per ciascun utente, ma sembra essere univoca per ogni esemplare, poiché il valore è hardcoded e crittografato nell'eseguibile.

La conclusione qui è la stessa: le nuove famiglie di ransomware, anche quelle non particolarmente complicate, attaccano di default i backup. Purtroppo questo approccio è diventato la norma.







Siti web pericolosi

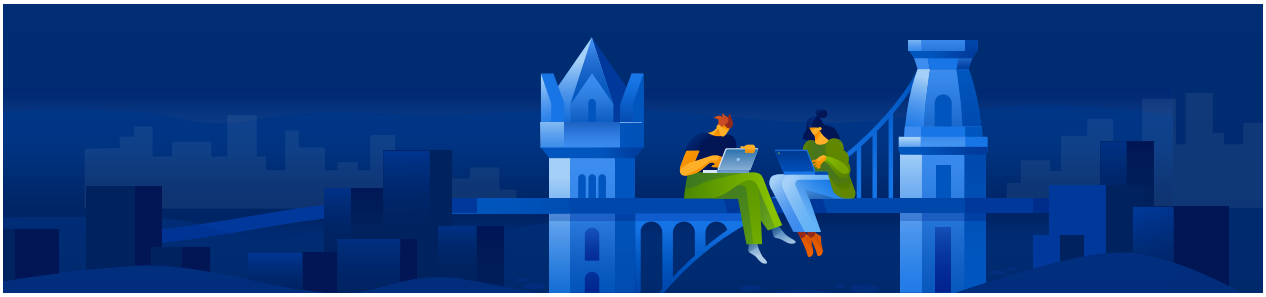
Durante la pandemia abbiamo assistito a un aumento degli attacchi di phishing, specialmente contro strumenti per la collaborazione e servizi di condivisione file che hanno visto crescere la loro diffusione grazie al lavoro da casa. Dopo il picco iniziale a marzo, abbiamo osservato una normalizzazione degli attacchi di phishing. Alcuni dei gruppi criminali informatici sembrano essere tornati alla tattica degli allegati dannosi. Anche il famigerato gruppo Emotet vi ha fatto ritorno a luglio, dopo un'assenza di cinque mesi, ricominciando a inviare documenti Office dannosi.

MESE	PERCENTUALE DI UTENTI che hanno cliccato su URL pericolosi
Giugno	5,5%
Luglio	5,1%
Agosto	2,3%
Settembre	2,7%
Ottobre	3,4%

La percentuale più elevata di URL pericolosi bloccati nel 3° trimestre 2020 è stata registrata negli Stati Uniti (16,4%), seguiti dalla Germania con il 14,1% e dalla Repubblica Ceca con il 10,4%. Tuttavia, nel 51% dei casi gli URL bloccati erano HTTPS crittografati e quindi più difficili da filtrare sulla rete. Abbiamo osservato anche altri gruppi dediti al phishing di token 2FA, che vengono quindi utilizzati immediatamente con uno script per effettuare il login. Per renderle più difficili da rilevare, le pagine di phishing sono spesso ospitate in domini di provider di servizi cloud attendibili, come Azure o Google. Alcuni hacker aggiungono anche una pagina CAPTCHA che l'utente deve risolvere per raggiungere la pagina di phishing finale – una tattica che consente di evitare che le soluzioni di scansione automatica analizzino e blocchino il sito web di phishing.

Primi 20 paesi per URL bloccati nel 3° trimestre

POSIZIONE	PAESE	PERCENTUALE DI URL BLOCCATI NEL 3° TRIM. 2020
1	Stati Uniti	16,4%
2	Germania	14,1%
3	Repubblica Ceca	10,4%
4	Spagna	8,3%
5	Regno Unito	6,7%
6	Cina	5,8%
7	Sudafrica	5,2%
8	Hong Kong	3,6%
9	Italia	3,4%
10	Australia	2,4%
11	Francia	2,1%
12	Canada	2,0%
13	Perù	1,9%
14	Norvegia	1,9%
15	Paesi Bassi	1,8%
16	Giappone	1,6%
17	Svizzera	1,6%
18	Bulgaria	0,9%
19	Singapore	0,8%
20	Austria	0,7%



Parte 3

Vulnerabilità nel sistema operativo e nel software Windows

1. Anche le app di terze parti sono vulnerabili e vengono sfruttate dai criminali
2. Le applicazioni più sfruttate dai criminali a livello mondiale

Il numero di vulnerabilità scoperte e di patch rilasciate è aumentato vertiginosamente nel 2020. Il team VulnDB di Risk Based Security ha raccolto 11.121 vulnerabilità divulgate durante la prima metà del 2020.

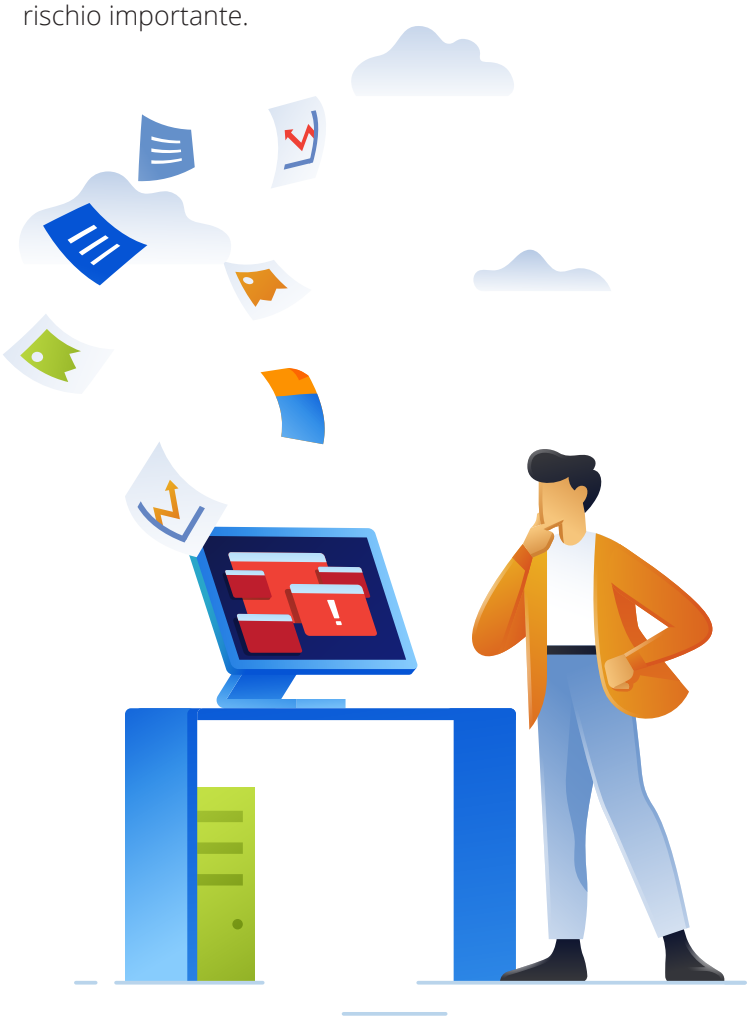
Nell'ultima patch Microsoft di settembre, l'azienda ha segnalato 129 vulnerabilità risolte, 23 delle quali potevano essere sfruttate dai malware per assumere il controllo completo di computer Windows con poco o nessun aiuto da parte degli utenti. Si tratta del settimo mese di fila in cui Microsoft ha fornito soluzioni per oltre 100 falle nella sicurezza dei suoi prodotti, e il quarto mese consecutivo in cui ne sono state risolte più di 120.

Il problema non è nuovo: anche se un produttore è veloce nel rilasciare una patch, ciò non significa che la patch sia stata applicata ovunque. Ad esempio, la vulnerabilità CVE-2020-0796, più nota oggi con il nome SMBGhost, era ritenuta così pericolosa in caso di exploit che ha ottenuto il punteggio più raro nel sistema di valutazione delle vulnerabilità comuni (CVSS): un 10 "perfetto". Nonostante Microsoft abbia rilasciato una correzione di emergenza non programmata nel giro di pochi giorni, società di cybersecurity di tutto il mondo, compresa Acronis, hanno continuato ha osservare casi in cui la vulnerabilità veniva sfruttata.

Analogamente, le vulnerabilità catalogate come CVE-2020-1425 e CVE-2020-1457, del tipo RCE (Remote-Code Execution), sono state classificate rispettivamente di gravità "critica" e "importante". Sono entrambe relative alla libreria dei codec di Microsoft Windows, che gestisce gli oggetti in memoria. Secondo Microsoft, un hacker in grado di sfruttare la vulnerabilità CVE-2020-1425 "potrebbe ottenere informazioni utilizzabili per compromettere ulteriormente il sistema dell'utente", mentre nel caso della seconda falla gli aggressori potrebbero eseguire un codice arbitrario sul sistema colpito. A entrambe le falle è stata assegnata la classificazione "exploit meno probabile" nel Microsoft Exploitability Index.

Alcune di queste vulnerabilità vengono sfruttate attivamente, come registriamo nei nostri dati: CVE-2020-1020 e CVE-2020-0938. Come abbiamo segnalato il 23 marzo, Microsoft ha confermato che queste vulnerabilità di Windows prive di soluzione sono sfruttate attivamente dagli hacker. Gli utenti di Windows 10 che non applicano le patch quando vengono rilasciate da Microsoft corrono il rischio che un hacker riesca a installare dei programmi, visualizzare e modificare dati o creare nuovi account.

La vulnerabilità di spoofing di Windows CVE-2020-1464 è un altro bersaglio di numerosi attacchi. La falla si crea quando Windows convalida erroneamente le firme dei file. Un hacker capace di sfruttare con successo questa opportunità potrebbe utilizzare una firma contraffatta associata a un eseguibile dannoso per caricare qualsiasi file, che verrebbe considerato legittimo dal sistema operativo. Questa vulnerabilità è presente in tutte le versioni supportate di Windows e, se la patch non è stata ancora applicata, rappresenta un rischio importante.



Anche le app di terze parti sono vulnerabili e vengono sfruttate dai criminali

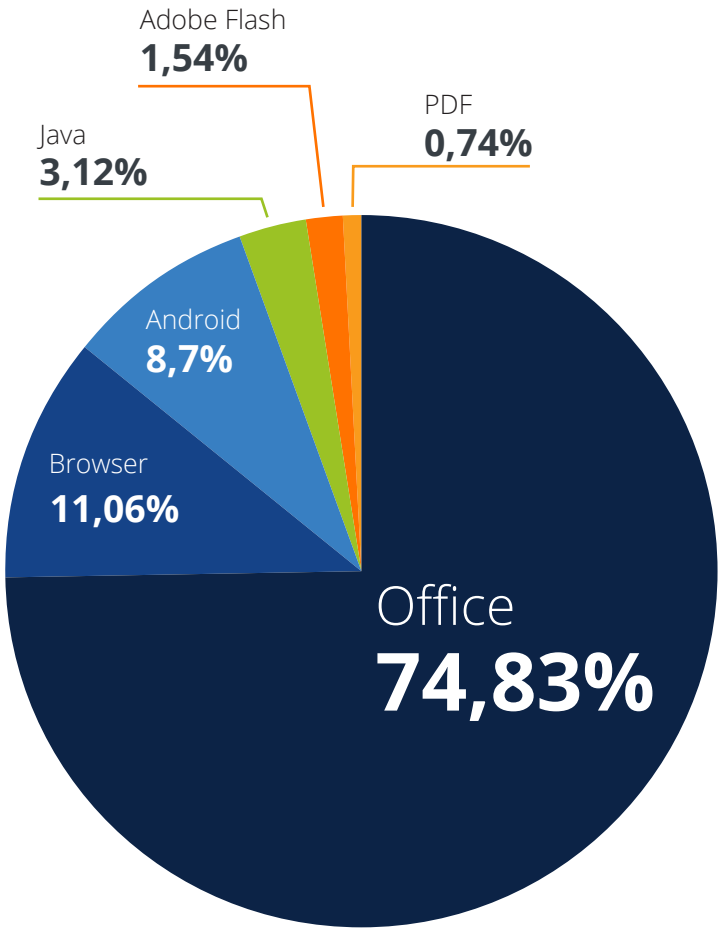
Naturalmente Microsoft non è l'unica azienda il cui software presenta delle vulnerabilità. Ecco alcune altre vulnerabilità che abbiamo visto attaccare nel 2020.

Adobe ha rilasciato periodicamente patch di sicurezza per i propri prodotti, con un aggiornamento di emergenza non programmato per Photoshop, Prelude e Bridge pubblicato a luglio. Una settimana dopo il rilascio del suo aggiornamento mensile della sicurezza, Adobe ha pubblicato degli avvisi di sicurezza che segnalavano 13 nuove vulnerabilità, 12 delle quali considerate critiche. Se sfruttate, possono consentire l'esecuzione di codice arbitrario.

Ad agosto, Adobe ha rilasciato patch per 26 vulnerabilità riscontrate in Adobe Acrobat e Adobe Reader, tra qui 11 falle di sicurezza classificate come critiche. Queste ultime potrebbero essere sfruttate per bypassare i controlli di sicurezza e, in nove casi, per l'esecuzione remota di codice arbitrario.

Il software per Windows non ha l'esclusiva delle vulnerabilità. I criminali informatici prendono di mira sempre più spesso le vulnerabilità prive di patch delle reti VPN. Ad esempio, sono stati rilevati in circolazione exploit programmati per colpire una vulnerabilità delle appliance VPN di Citrix, nota come CVE-2019-19781, che consente l'esecuzione di codice arbitrario. Una vulnerabilità di lettura file arbitraria dei server VPN di Pulse Secure, nota come CVE-2019-11510, continua ad attirare l'interesse di hacker malintenzionati.

Le applicazioni più sfruttate dai criminali a livello mondiale



Parte 4

Previsioni per il 2021

I consigli di Acronis per rimanere protetti nel panorama attuale e futuro delle minacce

Gli attacchi ai lavoratori remoti sono destinati ad aumentare

Con i numeri dei contagi da COVID-19 in rapida crescita, è difficile immaginare che la pandemia possa concludersi quest'anno. Più probabilmente, bisognerà aspettare per tutto il 2021 e forse anche il 2022 affinché i vaccini vengano distribuiti a livello globale. Dobbiamo quindi abituarci al lavoro remoto e al livello inadeguato di protezione ad esso associato. Nel 2020 i criminali informatici hanno compreso che il phishing funziona ancora molto bene e che i dipendenti sono la porta di accesso ai dati aziendali. Ci aspettiamo una crescita in numero e sofisticazione degli attacchi ai lavoratori remoti, dal momento che sempre più criminali prenderanno di mira i dati aziendali e i sistemi ubicati negli uffici deserti o nei data center.

L'esfiltrazione di dati supererà la crittografia dei dati

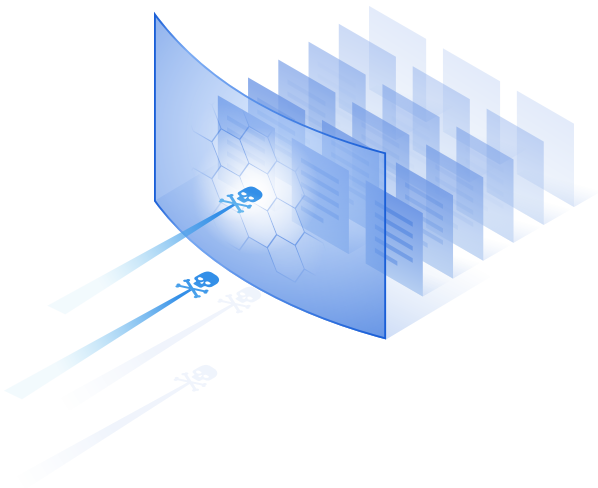
I casi di ransomware più recenti indicano che gli hacker vogliono monetizzare ogni singolo attacco. Di più, si stanno accorgendo che le estorsioni basate su dati riservati rubati funzionano molto bene, forse anche meglio di quando si limitano a crittografare quegli stessi dati, e per questo prevediamo che l'obiettivo principale di ogni attacco ransomware sarà l'esfiltrazione dei dati. Le soluzioni di protezione dei dati e prevenzione della perdite e fughe di informazioni rivestiranno un ruolo molto importante quest'anno, perché anche se la quantità di famiglie di ransomware si sta riducendo, quelle attive faranno danni enormi e saranno molto efficaci. Tutto questo significa che, secondo le nostre previsioni, il ransomware rimarrà la minaccia informatica numero uno per le aziende anche l'anno prossimo.

Più attacchi contro MSP e piccole aziende

Alla luce del numero crescente di piccole e medie imprese che si rivolgono a servizi cloud MS(S)P, sempre più criminali informatici sono invogliati ad attaccarle. Nel 2019-2020, i "cattivi" hanno capito che attaccare gli MSP è molto efficiente, specialmente quelli più piccoli che potrebbero non essere adeguatamente preparati. Attaccando gli MSP, riescono a colpire le decine di aziende loro clienti e accumulare un bottino più ricco mediante infezioni ransomware o trojan bancari. Inoltre, gli hacker possono fare ricorso ad altri strumenti ampiamente collaudati, come l'accesso remoto e i tool di distribuzione del software. Gli attacchi di questo tipo sono destinati a crescere di numero e in termini di portata geografica, poiché né le piccole imprese né gli MSP sono attrezzati per far fronte ad attacchi seri e potrebbero essere inclini a pagare un riscatto di entità moderata.

Il cloud sotto attacco

Durante il lockdown, molte aziende hanno trasferito i propri servizi nel cloud. Purtroppo, in molti casi, la configurazione è stata eseguita di fretta e non è quindi sicura; applicazioni e servizi dati su cloud sono potenzialmente accessibili a tutti via Internet. Questo scenario offre ai criminali l'opportunità di accedere ai dati ed esfiltrarli, come abbiamo già visto durante le violazioni di dati che hanno colpito i data bucket S3 e i database di ricerca elastici. Inoltre, la gestione delle identità e degli accessi viene ancora spesso trascurata, benché le identità stiano diventando il nuovo perimetro. Questa situazione porterà a un aumento del monitoraggio comportamentale delle entità utente e a controlli degli accessi dinamici.



Il ransomware cerca nuovi target da colpire

Gli attacchi ransomware stanno ampliando il raggio d'azione oltre i sistemi desktop Windows e Mac. Gli hacker stanno tentando di imporsi nell'ambiente cloud perché i database e i container cloud sono un obiettivo redditizio. All'interno delle organizzazioni, i sistemi di controllo industriale (ICS) del lato OT sono sempre più esposti e rappresentano un altro bersaglio interessante per i tentativi di estorsione. Per gli utenti domestici, la crescente adozione dell'Internet of Things (IoT), specialmente in abbinamento al 5G, può aprire il varco a nuove infezioni, anche solo per generare attacchi DDoS al fine di convincere le vittime a pagare un riscatto.

Gli aggressori ricorrono più spesso all'automazione e la quantità di esemplari di malware in circolazione è in crescita

I criminali informatici stanno tentando di automatizzare il più possibile i loro processi. Avvalendosi di strumenti di analisi dei Big Data e di tool di machine learning, riescono a trovare nuove vittime e a generare messaggi di spam personalizzati. Il modello "crimeware as a service" e i programmi di affiliazione accelerano ancora di più la tendenza. Tuttavia, dopo l'accesso iniziale e la fase di esecuzione, la maggior parte dei gruppi ricorre ancora a metodi manuali per diffondere il malware nelle reti aziendali. Ciononostante, osserveremo con maggiore frequenza metodi di attacco già noti, con livelli variabili di personalizzazione.

I consigli di Acronis per rimanere protetti nel panorama attuale e futuro delle minacce

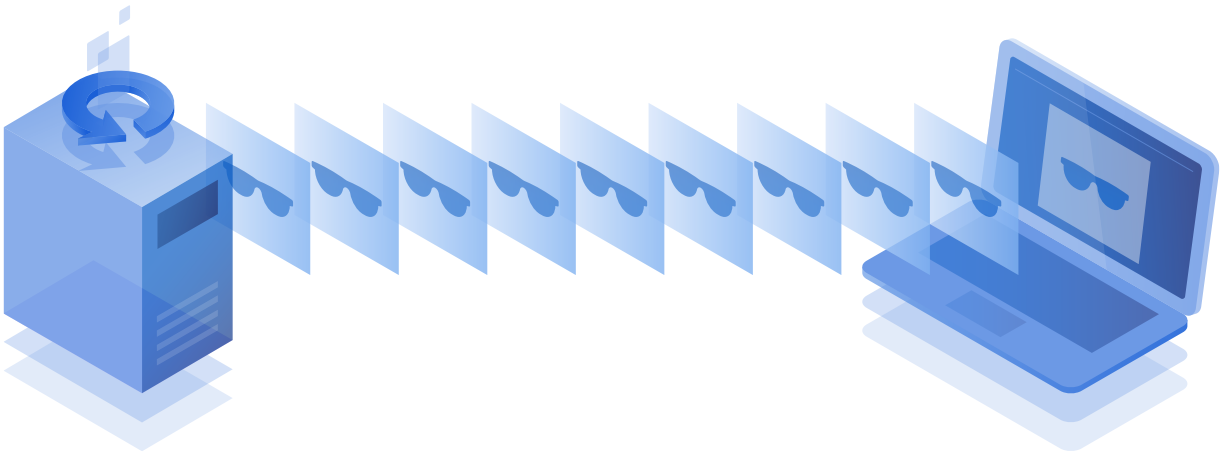
Attacchi informatici moderni, furti di dati e infezioni da ransomware sono tutti sintomi dello stesso problema: la cybersecurity sta fallendo nel suo intento. Questo fallimento è il risultato di tecnologie deboli e di errori umani causati da una sapiente attività di social engineering. Nei casi in cui una soluzione di backup funziona bene e non viene compromessa, ci vogliono solitamente ore e giorni prima di ripristinare l'operatività dei sistemi (con i relativi dati). Il backup è essenziale laddove le soluzioni di cybersecurity falliscono, ma anche le soluzioni di backup possono essere compromesse o disabilitate oppure subire rallentamenti, facendo perdere alle aziende grosse somme di denaro a causa dei fermi operativi che ne conseguono.

Per risolvere questi problemi, consigliamo una soluzione di Cyber Protection integrata come Acronis Cyber Protect, che combina antimalware, valutazione delle vulnerabilità, patch management, RMM e funzionalità di backup in un unico agente eseguito in una famiglia di sistemi operativi Windows. Questa integrazione consente di mantenere prestazioni ottimali, eliminare i problemi di compatibilità e garantire un ripristino rapido. Se una minaccia sfugge al rilevamento oppure viene intercettata mentre i dati stanno già subendo alterazioni, l'agente ripristina immediatamente i dati integri dal backup.

Questo tipo di ripristino automatico non è possibile con un agente antimalware, perché la soluzione antimalware potrebbe sì essere in grado di bloccare la minaccia, ma non di evitare la possibile perdita di dati. Un agente di backup, dal canto suo, non sarebbe in grado di rilevare la minaccia automaticamente e i dati verrebbero ripristinati lentamente – o mai.

Naturalmente, Acronis Cyber Protect Cloud mette in atto tutta una serie di meccanismi di protezione per evitare che sia necessario ripristinare i dati, rilevando ed eliminando le minacce prima che possano danneggiare il vostro ambiente. Questo livello di difesa viene ottenuto grazie alla nostra funzionalità di cybersecurity avanzata multilivello.

Ciò detto, le aziende e gli utenti domestici non devono dimenticarsi di seguire le regole di sicurezza fondamentali anche quando utilizzano soluzioni moderne come Acronis Cyber Protect.



Applicate le patch al sistema operativo e alle app

L'applicazione delle patch è cruciale, poiché molti attacchi hanno successo proprio perché vanno a colpire vulnerabilità non corrette con le rispettive patch. Con una soluzione come Acronis Cyber Protect siete protetti dalle funzionalità integrate di valutazione della vulnerabilità e patch management. Registriamo costantemente tutte le vulnerabilità scoperte e le patch rilasciate, per consentire ad amministratori e tecnici di proteggere facilmente tutti gli endpoint con una configurazione flessibile e report dettagliati. Acronis Cyber Protect supporta non solo tutte le app integrate di Windows ma anche più di 100 app di terze parti tra le più diffuse, tra cui strumenti di telecomunicazione come Zoom e Slack e i client VPN più utilizzati per il lavoro a distanza. Non mancate di applicare le patch per le vulnerabilità ad alto rischio e leggete il report con i risultati per verificare che le patch siano state applicate correttamente.

Se non avete Acronis Cyber Protect e/o non fate uso di un software di patch management, è tutto molto più difficile. Come minimo, dovete accertarvi che Windows riceva tutti gli aggiornamenti di cui ha bisogno e che questi siano installati tempestivamente. Gli utenti tendono a ignorare i messaggi di sistema specialmente quando Windows chiede di riavviare il sistema, ma è un grave errore. Assicuratevi che la funzione di aggiornamento automatico sia attivata nei programmi dei principali produttori di software, come Adobe, e che app come Acrobat Reader siano sempre aggiornate.

Attenzione agli attacchi di phishing, non cliccate su link sospetti

Il COVID-19 è ora ampiamente utilizzato nei tentativi di phishing, ma poiché il volume di queste attività criminali non farà che crescere, è importante che ogni lavoratore remoto sia equipaggiato per difendersi. Ogni giorno compaiono numerosi nuovi siti web di phishing e pericolosi a tema; solitamente vengono intercettati e filtrati a livello di browser, ma con le soluzioni di Cyber Protection come Acronis Cyber Protect potete anche contare sulla funzionalità di filtraggio degli URL dedicato. È la stessa funzionalità disponibile nelle soluzioni di protezione degli endpoint, con la differenza che Acronis Cyber Protect prevede una speciale categoria relativa agli argomenti di salute pubblica, che viene aggiornata con maggiore urgenza. I link pericolosi possono provenire da qualunque fonte, ad esempio e-mail, post di forum e app di messaggistica istantanea. Non cliccate su un link che non vi serve o che non vi aspettavate di ricevere.

Gli allegati di phishing o pericolosi possono arrivare via e-mail, esattamente come i link pericolosi di cui sopra. Nel caso degli allegati, controllate sempre l'effettiva origine e chiedetevi se era un file che stavate aspettando. In ogni caso, prima di aprire un allegato, dovete sempre analizzarlo con la vostra soluzione antimalware.

Usate una VPN quando lavorate con dati aziendali

Se dovete accedere a risorse e servizi remoti della vostra azienda, ma anche se il vostro lavoro non lo richiede e vi limitate a consultare risorse sul web e a utilizzare strumenti di telecomunicazione, usate sempre una rete virtuale privata (VPN). Una VPN applica la crittografia a tutto il traffico, proteggendolo in caso di tentativo da parte di un hacker di catturare i vostri dati in transito. Se la vostra azienda si avvale di una VPN, probabilmente riceverete le istruzioni del caso dal vostro amministratore o dal tecnico dell'MSP. Se invece dovete occuparvi personalmente di proteggere il vostro ambiente di lavoro, utilizzate app e servizi VPN noti e consigliati, che siano ampiamente disponibili nei siti che vendono software o direttamente dal produttore.

Assicuratevi che la vostra soluzione di cybersecurity funzioni correttamente

In Acronis Cyber Protect utilizziamo molte tecnologie di sicurezza ben bilanciate e calibrate di precisione, compresi vari moduli di rilevamento; è un approccio più consigliato rispetto a una soluzione Windows incorporata.

Ma avere una difesa antimalware non è sufficiente, è necessario che sia configurata correttamente. Ciò significa che:

- **È necessario eseguire una scansione completa almeno una volta al giorno**
- **Il prodotto deve essere aggiornato ogni giorno o ogni ora, a seconda della frequenza con cui vengono resi disponibili gli aggiornamenti**
- **Il prodotto deve essere connesso ai propri meccanismi di rilevamento cloud, nel caso di Acronis Cyber Protect, ad Acronis Cloud Brain. La connessione è attivata di default ma è necessario accertarsi che Internet sia disponibile e non bloccato involontariamente da software antimalware**
- **Le scansioni on-demand e all'accesso (in tempo reale) devono essere abilitate e devono attivarsi per ogni nuovo software che viene installato o eseguito**

Inoltre, non ignorate i messaggi visualizzati dalla soluzione antimalware. Leggeteli attentamente e assicuratevi che la licenza sia legittima, se usate una versione a pagamento di un fornitore di soluzioni di sicurezza.

Non condividete con nessuno le vostre password e il vostro spazio di lavoro

Ultimo consiglio per la sicurezza: accertatevi che vostre password quelle e dei vostri dipendenti siano complesse e riservate. Non comunicatele mai a nessuno. Create una password diversa e lunga per ogni servizio che utilizzate. Per aiutarvi a ricordarle, usate un software di gestione delle password. In alternativa, il modo più semplice per generare password sicure è quello di creare una serie di frasi lunghe che siete in grado di tenere a memoria. Al giorno d'oggi, le password di otto caratteri sono più facili da decifrare con attacchi brute force.

In un prodotto sicuro come Acronis Cyber Cloud o Acronis Cyber Backup, non memorizziamo mai le password da nessuna parte, per evitare accessi non autorizzati ai vostri dati.

Infine, non dimenticate di bloccare lo schermo del vostro computer laptop o desktop e di limitare l'accesso al sistema, anche quando lavorate da casa. Non sarebbe la prima volta che una persona riesce a rubare informazioni riservate da uno schermo di PC non bloccato, anche a distanza.

Risorse aggiuntive

Webinar on-demand: Cybersecurity 2021 – Il panorama delle minacce previsto

Whitepaper: Report Acronis sulla preparazione digitale

Tool gratuito: Questionario di valutazione della sicurezza informatica

Acronis

Informazioni su Acronis

Acronis coniuga protezione dati e sicurezza informatica per offrire una Cyber Protection integrata e automatizzata in grado di risolvere i problemi di salvaguardia, accessibilità, privacy, autenticità e sicurezza (SAPAS) del mondo digitale di oggi. Grazie a modelli di deployment flessibili che si adattano alle esigenze dei service provider e dei professionisti IT, Acronis garantisce una Cyber Protection di livello superiore per dati, applicazioni e sistemi con soluzioni innovative di nuova generazione per antivirus, backup, backup, disaster recovery e gestione della protezione degli endpoint. Con le sue pluripremiate tecnologie anti-malware basate su IA e di autenticazione dei dati basate su blockchain, Acronis protegge qualsiasi tipo di ambiente – cloud, ibrido o in sede – a un costo contenuto e senza sorprese.

Fondata a Singapore nel 2003 e costituita in Svizzera nel 2008, Acronis conta oggi più di 1.500 dipendenti in 33 uffici distribuiti in 18 paesi. Alle sue soluzioni si affidano più di 5,5 milioni di utenti privati e più di 500.000 aziende, fra cui la totalità di quelle presenti nella classifica Fortune 1000 e team di sport professionistici ai massimi livelli. I prodotti Acronis sono disponibili presso 50.000 partner e service provider in oltre 150 paesi in più di 40 lingue. Per maggiori informazioni, visitate www.acronis.com