KASPERSKY lab

Kaspersky Security Bulletin 2016

NOVITÀ DELL'ANNO: LA RIVOLUZIONE DEL RANSOMWARE

GREAT

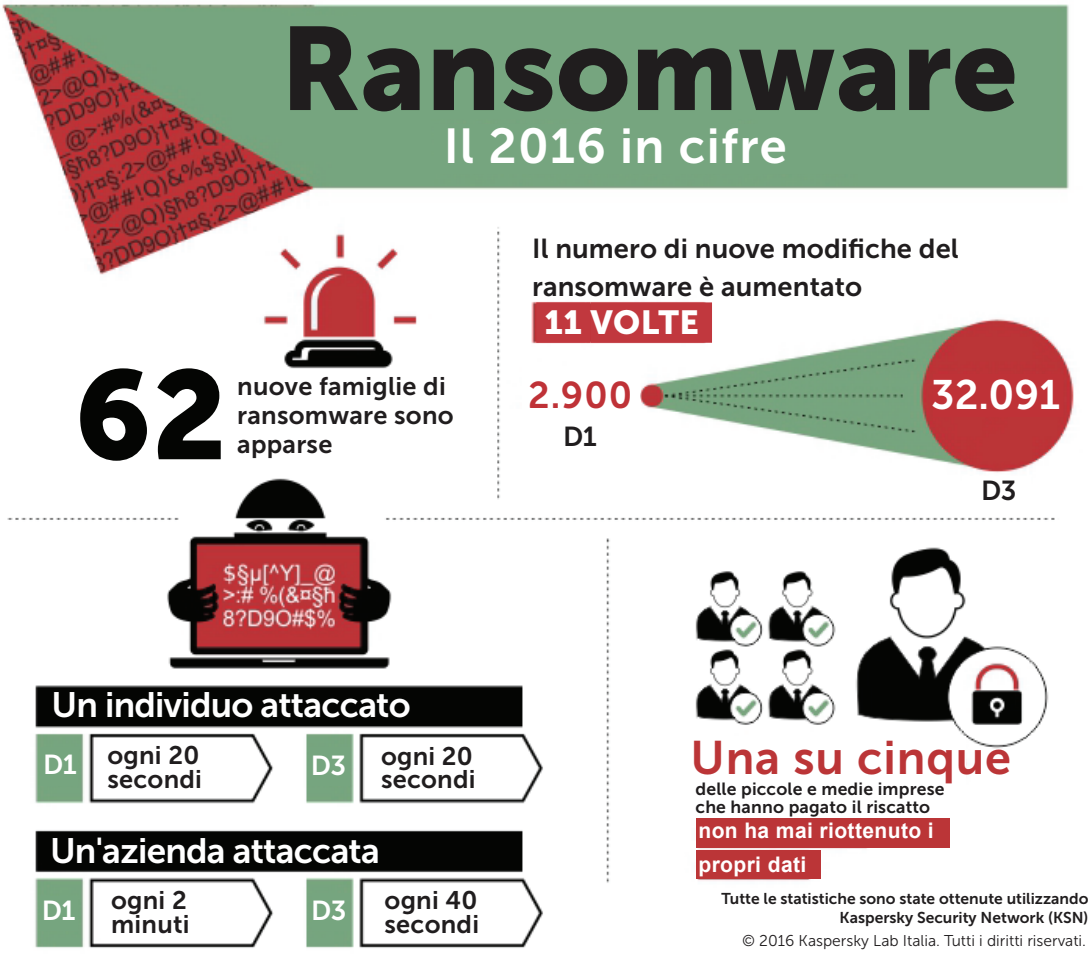
SOMMARIO

INTRODUZIONE

Nel 2016 il ransomware ha continuato la scalata in tutto il mondo, stringendo la morsa su dati, dispositivi, aziende e singoli utenti.

I numeri parlano da soli:

- 62 nuove famiglie di ransomware hanno fatto il debutto.
- Il numero delle modifiche del ransomware è aumentato di 11 volte: da 2.900 nuove modifiche a gennaio/marzo fino a 32.091 a luglio/settembre.
- Gli attacchi alle aziende sono aumentati di tre volte tra gennaio e la fine di settembre: la differenza tra un attacco ogni 2 minuti e uno ogni 40 secondi.
- Per gli individui, il tasso di aumento è passato da ogni 20 secondi a ogni 10.
- Una su cinque delle piccole e medie imprese che hanno pagato il riscatto non ha mai riottenuto i propri dati.



Il 2016 ha anche assistito alla crescita del ransomware dal punto di vista della sofisticazione e della diversità, ad esempio: modifica dell'approccio se incontra software finanziari scritti in linguaggi di scripting, sfruttamento di nuovi percorsi infettivi, maggiore precisione e offerta di soluzioni Ransomware-as-a-Service preconfigurate a coloro con meno competenze, risorse o tempo, il tutto attraverso un ecosistema "underground" in crescita e maggiormente efficiente.

Contemporaneamente, nel 2016 il mondo si è unito per iniziare a combatterlo:

Il progetto No More Ransom è stato avviato a luglio con la collaborazione tra Dutch National Police, Europol, Intel Security e Kaspersky Lab. A ottobre si sono aggiunte altre 13 organizzazioni. Tra gli altri elementi, la collaborazione ha avuto come risultato diversi strumenti di decrittografia online gratuiti che fino ad ora hanno aiutato migliaia di vittime del ransomware a recuperare i propri dati.

Questa è solo la punta dell'iceberg: c'è ancora molto da fare. Insieme possiamo ottenere molto di più di quanto non potrebbe uno di noi da solo.

Cos'è il ransomware?

Il ransomware può avere due forme. La forma di ransomware più comune è il cryptor. Questi programmi eseguono la crittografia dei dati sul dispositivo della vittima e chiedono denaro in cambio della promessa di ripristinarli. I blocker, al contrario, non influiscono sui dati archiviati sul dispositivo, ma impediscono alla vittima di accedere al dispositivo. La richiesta di riscatto, visualizzata sullo schermo, appare solitamente come un messaggio dalle forze dell'ordine che riferisce che la vittima ha effettuato l'accesso a contenuto Web illegale e deve pagare una multa. È possibile trovare una panoramica di entrambe le forme di ransomware qui.

RANSOMWARE: LE PRINCIPALI TENDENZE E SCOPERTE DEL 2016

"Molti ransomware prosperano su una improbabile relazione di fiducia tra la vittima e il criminale: che, una volta ricevuto il riscatto, i file sequestrati saranno restituiti. I cybercriminali hanno mostrato una sorprendente traccia di professionalità nel mantenere questa promessa."

GReAT, previsioni delle minacce per il 2017

New entry e addii

New entry: nel 2016 il mondo ha assistito all'arrivo di Cerber, Locky e CryptXXX, oltre a 44.287 nuove modifiche del ransomware

Fino ad ora, il ransomware è stato diffuso in

114

paesi

Cerber e Locky sono arrivati a inizio primavera. Entrambi sono specie di ransomware nocive e aggressive che si sono ampiamente propagate, principalmente attraverso allegati spam e kit di exploit. Si sono velocemente affermati come "protagonisti principali", colpendo individui e aziende. Poco dopo è arrivato CryptXXX. Tutte e tre le famiglie continuano a evolversi e a tenere il mondo in ostaggio insieme ai ben consolidati CTB-Locker, CryptoWall e Shade.

A ottobre 2016, le principali famiglie di ransomware rilevate dai prodotti Kaspersky Lab hanno questo aspetto:

	Nome	Risultati*	Percentuale di utenti**
1	CTB-Locker	Trojan-Ransom.Win32.Onion/ Trojan-Ransom.NSIS.Onion	25,32
2	Locky	Trojan-Ransom.Win32.Locky/ Trojan-Dropper.JS.Locky	7,07
3	TeslaCrypt (attivo fino a maggio 2016)	Trojan-Ransom.Win32.Bitman	6,54
4	Scatter	Trojan-Ransom.Win32.Scatter/ Trojan-Ransom.BAT.Scatter/ Trojan-Downloader.JS.Scatter/ Trojan-Dropper.JS.Scatter	2,85
5	Cryakl	Trojan-Ransom.Win32.Cryakl	2,79
6	CryptoWall	Trojan-Ransom.Win32.Cryptodef	2,36
7	Shade	Trojan-Ransom.Win32.Shade	1,73
8	(Risultato generico)	Trojan-Ransom.Win32.Snocry	1,26
9	Crysis	Trojan-Ransom.Win32.Crusis	1,15
10	Cryrar/ACCDFISA	Trojan-Ransom.Win32.Cryrar	0,90

* Queste statistiche si basano sui risultati di rilevamento dei prodotti Kaspersky Lab, ricevuti dagli utenti dei prodotti Kaspersky Lab che hanno acconsentito a fornire i propri dati statistici.

** Percentuale di utenti colpiti da una determinata famiglia di crypto-ransomware in relazione a tutti gli utenti colpiti da crypto-ransomware.

Addii: arrivederci a TeslaCrypt, Chimera e Wildfire - o così sembrava...

Probabilmente la sorpresa più grande del 2016 è stata la sconfitta di TeslaCrypt e il conseguente rilascio della chiave master, apparentemente dagli stessi autori del malware.

TeslaCrypt "ha commesso suicidio" mentre la polizia arrestava l'attività di Encryptor RaaS e Wildfire

Encryptor RaaS, uno dei primi Trojan a offrire un modello Ransomware-as-a-Service ad altri criminali, ha chiuso bottega dopo che parte della sua botnet è stata presa di mira dalla polizia.

Successivamente, a luglio, circa 3.500 chiavi per il ransomware Chimera sono state rilasciate pubblicamente da qualcuno che sosteneva di essere dietro al ransomware Petya/Mischa. Comunque, dato che Petya utilizzava parte del codice sorgente Chimera per il proprio ransomware, poteva effettivamente appartenere allo stesso gruppo, aggiornando semplicemente la propria suite di prodotti e causando danni.

Analogamente, Wildfire, i cui server sono stati colpiti e per il quale è stata sviluppata una chiave di decrittografia grazie a uno sforzo congiunto di Kaspersky Lab, Intel Security ed Europol, ora sembra essere tornato come Hades.

Abuso del ransomware "formativo"

Ricercatori con buone intenzioni hanno sviluppato il ransomware "formativo" per offrire agli amministratori di sistema uno strumento per simulare un attacco ransomware e testare le proprie difese. I criminali hanno fatto in fretta a sfruttare questi strumenti per i propri scopi dannosi.

Il ransomware sviluppato per motivi "formativi" ha portato alla nascita di Ded Cryptor e Fantom, ma non solo

Lo sviluppatore del ransomware formativo Hidden Tear & EDA2 ha generosamente pubblicato il codice sorgente su GitHub. Inevitabilmente, il 2016 ha visto la comparsa di numerosi Trojan nocivi basati su questo codice. Tra questi c'era Ded Cryptor, che cambiava lo sfondo sul computer della vittima con un'immagine di un Babbo Natale dall'aspetto malvagio e chiedeva un riscatto di due Bitcoin (circa $ 1.300). Un altro programma simile era Fantom, che simulava una vera schermata di aggiornamento di Windows.

Approcci non convenzionali

I criminali ora stanno prendendo di mira i dati di backup, i dischi rigidi e il forzamento brutale delle password

- Perché preoccuparsi di un file quando si può avere il disco?

  Nuovi approcci agli attacchi ransomware apparsi per la prima volta nel 2016 comprendono la crittografia del disco, con la quale i criminali bloccano l'accesso o eseguono la crittografia di tutti i file in una sola volta. Petya ne è un esempio, codificando l'indice master del disco rigido di un utente e rendendo impossibile il riavvio. Un altro Trojan, Dcryptor, anche conosciuto come Mamba, ha compiuto un ulteriore passo in avanti, bloccando l'intero disco rigido. Questo ransomware è particolarmente sgradevole, perché codifica ogni settore del disco tra cui sistema operativo, app, file condivisi e tutti i dati personali, utilizzando una copia del software open source DiskCryptor.

- La tecnica di infezione "manuale"

  L'infezione di Dcrypter avviene manualmente: i criminali forzano brutalmente le password per accedere da remoto alla macchina della vittima. Sebbene non sia nuovo, questo approccio è diventato molto più rilevante nel 2016, spesso come modo per colpire i server e ottenere l'accesso in un sistema aziendale.

  Se l'attacco ha successo, il Trojan installa ed esegue la crittografia dei file sul server e, possibilmente, su tutte le porzioni di rete da lì accessibili. Abbiamo scoperto che TeamXRat ha utilizzato questo approccio per diffondere il suo ransomware sui server brasiliani.

Shade scarica spyware se trova software finanziari

- Infezione due in uno

  Ad agosto abbiamo scoperto un modello di Shade con una funzionalità inattesa: se un computer si rivelava appartenere a servizi finanziari, scaricava e installava una parte di spyware con l'obiettivo a lungo termine di rubare denaro.

Ransomware in linguaggi di scripting

Un'altra tendenza che ha attirato la nostra attenzione nel 2016 è stato il numero crescente di cryptor scritti in linguaggi di scripting. Soltanto nel terzo trimestre ci siamo imbattuti in numerose nuove famiglie scritte in Python, tra cui HolyCrypt e CryPy, oltre a Stampado scritto in AutoIt, il linguaggio di automazione.

Una lunga serie di principianti e imitatori

Il ransomware di bassa qualità aumenta la probabilità di perdere per sempre i dati

Molti dei nuovi Trojan ransomware rilevati nel 2016 erano in realtà di bassa qualità, poco sofisticati, con vulnerabilità del software ed errori grossolani nelle note di riscatto.

Questo fatto è stato accompagnato da un aumento di ransomware di imitazione. Tra gli altri elementi, abbiamo rilevato che:

- Bart copia la nota di riscatto e la pagina di pagamento di Locky.
- Un'imitazione basata su Autoit di Locky (detta AutoLocky) utilizza la stessa estensione ".locky".
- Crusis (anche noto come Crysis) copia l'estensione ".xtbl" utilizzata originariamente da Shade.
- Xorist copia l'intero schema di nomenclatura dei file crittati da Crusis.

Probabilmente, l'imitazione più evidente che abbiamo scoperto quest'anno è stata Polyglot (anche conosciuto come MarsJoke). Imita completamente l'aspetto e l'approccio di elaborazione dei file di CTB-Locker.

Ci si aspetta un aumento di queste tendenze nel 2017.

"Con il continuo aumento di popolarità e un grado inferiore di criminali che decidono di invadere lo spazio, è probabile che incontreremo sempre più un "ransomware" che manca di standard qualitativi o di capacità generali di programmazione per mantenere realmente questa promessa. Ci aspettiamo che il ransomware "skiddie" blocchi i file o l'accesso al sistema o cancelli semplicemente i file, convinca la vittima a pagare il riscatto e non restituisca niente."

GReAT, previsioni delle minacce per il 2017

LA PROSPEROSA ECONOMIA DEL RANSOMWARE

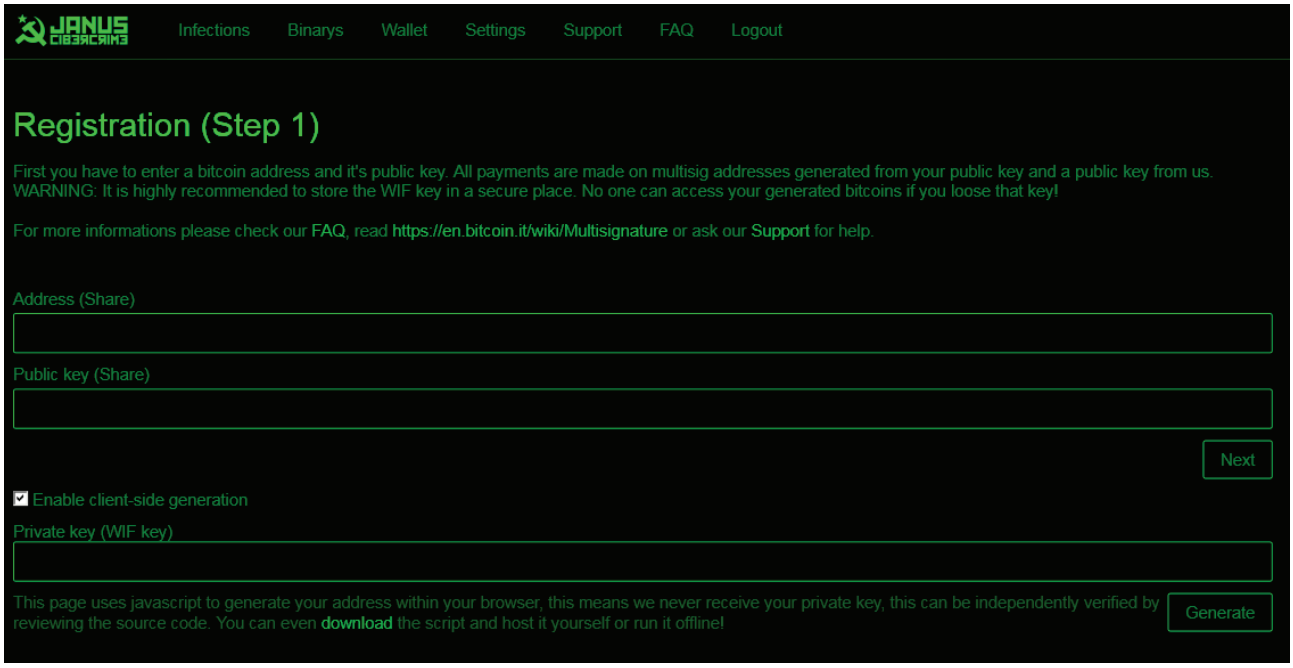
Il ransomware è sempre più disponibile per il noleggio nella realtà criminale

La diffusione di RaaS

Nonostante Ransomware-as-a-Service non sia una nuova tendenza, nel 2016 questo modello di propagazione ha continuato a svilupparsi, con sempre più creatori di ransomware che offrono i propri prodotti nocivi "su richiesta". Questo approccio è particolarmente interessante per i criminali che mancano di competenze, risorse o inclinazione per lo sviluppo del proprio prodotto.

Esempi rilevanti di ransomware apparsi nel 2016 che utilizzano questo modello sono Petya/Mischa e Shark, il cui marchio è stato successivamente rimodellato sul nome Atom.

Questo modello di attività è sempre più sofisticato:



Il sito partner del ransomware Petya

Il partner spesso sottoscrive un accordo tradizionale basato su commissione. Ad esempio, la "tabella di pagamento" per il ransomware Petya mostra che se un partner realizza 125 Bitcoin alla settimana, dopo la commissione si porterà a casa 106,25 Bitcoin.

Volume/Week	Share
<5 BTC	25%
<25 BTC	50%
<125 BTC	75%
>=125 BTC	85%

Tabella di pagamento di Petya

C'è anche una tassa iniziale di utilizzo. Un criminale che desidera utilizzare il ransomware Stompado, ad esempio, deve mettere insieme solo $ 39.

Con altri criminali che offrono i propri servizi per la distribuzione di spam, note ransomware, ecc., non è difficile per un aspirante criminale iniziare la propria attività.

Da reti basate su commissione ad assistenza ai clienti e branding

I criminali offrono assistenza ai clienti per assicurarsi che più vittime paghino

I criminali più "professionali" hanno offerto alle proprie vittime un helpdesk e assistenza tecnica, guidandoli attraverso il processo di acquisto di Bitcoin per pagare il riscatto e, a volte, aprendosi anche a trattative. Ogni passo in avanti ha incoraggiato le vittime a pagare.

Inoltre, gli esperti di Kaspersky Lab che studiano i ransomware in Brasile hanno notato che per molti criminali il dare un marchio al ransomware è stato una faccenda con una certa importanza. Coloro alla ricerca di attenzione mediatica e paura del cliente opterebbero per un alto profilo, un tema celebre o uno stratagemma, mentre coloro che puntano a passare inosservati abbandonerebbero la tentazione della fama e si limiterebbero a lasciare alle proprie vittime solo un'e-mail per contattare i ragazzi cattivi e un indirizzo Bitcoin per effettuare il pagamento.

È ancora tutta una questione di Bitcoin

Nel 2016 le famiglie di ransomware più popolari hanno ancora preferito i pagamenti in Bitcoin. Le richieste della maggior parte dei ransomware non sono state eccessive, con una media di circa $ 300, nonostante alcune abbiano preteso un importo assai maggiore.

Altre, soprattutto operazioni artigianali e regionali, hanno preferito opzioni di pagamento locali, sebbene questo comporti l'impossibilità di nascondersi ulteriormente e mescolarsi con il resto dei ransomware.

IL RANSOMWARE HA PUNTATO LE PROPRIE ARMI CONTRO LE AZIENDE

Un'azienda viene attaccata dal ransomware ogni 40 secondi

Nei primi tre mesi del 2016, il 17% degli attacchi ransomware è stato rivolto alle aziende: questo corrisponde a un attacco a un'azienda in qualche parte del mondo ogni due minuti*. Entro la fine del terzo trimestre questi attacchi hanno raggiunto il 23,9%: un attacco ogni 40 secondi.

Secondo la ricerca di Kaspersky Lab, nel 2016 un'azienda su cinque in tutto il mondo ha subito un incidente di sicurezza IT come conseguenza di un attacco ransomware.

- Il 42% delle piccole e medie imprese è stato colpito dal ransomware nel corso degli ultimi 12 mesi.
- Il 32% delle aziende ha pagato il riscatto.
- Una su cinque non ha mai riottenuto i propri file, anche dopo aver pagato.
- Il 67% di quelle colpite dal ransomware ha perso parte o tutti i dati aziendali, mentre un'azienda su quattro ha impiegato molte settimane nel tentativo di ripristinare l'accesso.

* Stime basate su: il 17% di 372.602 utenti unici con attacchi ransomware bloccati dai prodotti di Kaspersky Lab nel primo trimestre 2016 e il 23,9% di 821.865 utenti unici con attacchi ransomware bloccati dai prodotti di Kaspersky Lab nel terzo trimestre 2016.

Una su cinque piccole e medie imprese non riottiene mai i propri dati, anche dopo aver pagato

Non esiste più un settore a basso rischio

Il social engineering e l'errore umano rimangono i fattori chiave nella vulnerabilità aziendale. Uno su cinque dei casi che hanno implicato la perdita significativa di dati si è verificato per disattenzione o mancanza di comprensione del dipendente.

Alcuni settori industriali sono più difficili da colpire rispetto ad altri, ma la nostra ricerca mostra che tutti sono a rischio.

	Settore industriale	% di attacchi con ransomware
1	Istruzione	23
2	IT/Telecomunicazioni	22
3	Intrattenimento/Media	21
4	Servizi finanziari	21
5	Edilizia	19
6	Governo/settore pubblico/difesa	18
7	Produzione	18
8	Trasporti	17
9	Servizi sanitari	16
10	Vendita al dettaglio/commercio all'ingrosso/ tempo libero	16

"Stiamo assistendo a ransomware più mirati, dove i gruppi di criminali scelgono accuratamente ed effettuano spear-pishing dei propri bersagli per i dati in loro possesso e/o per il loro affidamento sulla disponibilità di questi dati preziosi."

John Fokker, coordinatore del team digitale presso la Dutch National High Tech Crime unit

Attacchi ransomware che hanno fatto notizia

- **Gli ospedali sono diventati un bersaglio primario**, con un impatto potenzialmente devastante come l'annullamento di operazioni, pazienti dirottati verso altri ospedali e altro ancora.
  - L'esempio più noto di un attacco ransomware è avvenuto a marzo, quando i criminali hanno bloccato i computer dell'Hollywood Presbyterian Medical Center a Los Angeles finché l'ospedale non ha pagato $ 17.000.
  - Nel corso delle settimane sono stati colpiti anche numerosi ospedali in Germania.
  - Nel Regno Unito, 28 fondi del servizio sanitario nazionale ammettono di essere stati attaccati nel 2016.
- **Il fornitore di servizi cloud e desktop ospitati** VESK ha pagato quasi $ 23.000 di riscatto per ripristinare l'accesso a uno dei suoi sistemi in seguito a un attacco avvenuto a settembre.
- **I media leader del settore**, tra cui New York Times, BBC e AOL, sono stati colpiti da malware contenenti ransomware a marzo 2016.
- **L'Università di Calgary in Canada**, un importante centro di ricerca, ha ammesso di aver pagato circa $ 16.000 per ripristinare e-mail che sono state crittografate per una settimana.
- **Una piccola stazione di polizia** nel Massachusetts ha dovuto pagare un riscatto di $ 500 (tramite Bitcoin) per recuperare dati fondamentali relativi a casi, dopo che un agente aveva aperto un allegato e-mail infetto.
- **Anche il mondo delle corse automobilistiche è stato colpito:** una importante squadra corse NASCAR ha perso dati che valevano milioni in un attacco TeslaCrypt ad aprile.

REAZIONE

Attraverso la tecnologia

Le versioni più recenti dei prodotti Kaspersky Lab per le piccole aziende sono stati migliorati con la funzionalità anti-cryptomalware. Inoltre, un nuovo e gratuito strumento anti-ransomware è stato messo a disposizione di tutte le aziende per il download e l'utilizzo, indipendentemente dalla soluzione di sicurezza in uso.

È disponibile un nuovo strumento anti-ransomware gratuito e indipendente da AV

Lo strumento anti-ransomware per aziende di Kaspersky Lab è una soluzione "leggera" che può funzionare in parallelo con altri software antivirus. Lo strumento utilizza due componenti necessari per il rilevamento anticipato dei Trojan: Kaspersky Security Network distribuito e System Watcher, che monitora l'attività delle applicazioni.

Kaspersky Security Network verifica velocemente la reputazione di file e URL di siti Web servendosi del cloud, mentre System Watcher monitora il comportamento dei programmi e fornisce protezione proattiva dalle versioni di Trojan ancora sconosciute. Ancora più importante, lo strumento può eseguire il backup dei file aperti da applicazioni sospette ed eseguire il rollback delle modifiche se le azioni intraprese dai programmi si rivelano essere dannose.

Attraverso la collaborazione: L'iniziativa No More Ransom

No More Ransom ha consentito fino ad ora a 4.400 persone di recuperare i propri dati e ha sottratto ai criminali $ 1,5 milioni in riscatto

Il 25 luglio 2016 Dutch National Police, Europol, Intel Security e Kaspersky Lab hanno annunciato l'avvio del progetto No More Ransom: un'iniziativa non commerciale che unisce organizzazioni pubbliche e private con l'obiettivo di informare le persone dei pericoli del ransomware ad aiutarle nel recupero dei propri dati.

Il portale online offre al momento otto strumenti di decrittografia, di cui cinque realizzati da Kaspersky Lab. Questi strumenti possono aiutare a recuperare i file crittografati da oltre 20 tipi di cryptomalware. Ad oggi, oltre 4.400 vittime hanno recuperato i propri dati e sono stati risparmiati oltre $ 1,5 milioni in richieste di riscatto.

A ottobre, forze dell'ordine provenienti da 13 paesi si sono unite al progetto, tra cui: Bosnia ed Erzegovina, Bulgaria, Colombia, Francia, Ungheria, Irlanda, Italia, Lettonia, Lituania, Portogallo, Spagna, Svizzera e Regno Unito.

Anche Eurojust e la Commissione Europea sostengono gli obiettivi del progetto e ci si aspetta di annunciare presto altri partner dal settore privato e delle forze dell'ordine.

"Le partnership pubbliche e private sono l'essenza e la forza dell'iniziativa NMR. Sono fondamentali per affrontare effettivamente ed efficacemente il problema, perché ci consentono di avere capacità e possibilità assai maggiori di quelle che le forze di polizia potrebbero avere da sole."

Steven Wilson, capo dell'EC3 di Europol

Resistere ai ransomware: come difendersi

1. Effettuare regolarmente il backup dei dati.
2. Utilizzare una soluzione di sicurezza affidabile e ricordarsi di tenere abilitate funzionalità chiave come System Watcher.
3. Tenere sempre aggiornati i software su tutti i dispositivi in uso.
4. Trattare con cautela gli allegati e-mail o i messaggi da persone sconosciute. Se in dubbio, non aprirli.
5. Se si è un'azienda, occorrerebbe istruire i propri dipendenti e team IT, tenere separati i dati sensibili, restringere l'accesso ed effettuare sempre il backup, di tutto.
6. Se si è così sfortunati da essere vittima di un attacco, non farsi prendere dal panico. Utilizzare un sistema pulito per controllare il nostro sito No More Ransom: ci potrebbe essere uno strumento di decrittografia utile per recuperare i propri dati.
7. Ultimo, ma non meno importante, ricordarsi che il ransomware è un reato penale. Denunciare l'attacco alle forze dell'ordine locali.

Perché non si deve pagare: consigli dalla Dutch National High Tech Crime Unit

1. Si diventa un bersaglio maggiore.
2. Non ci si può fidare dei criminali: i dati potrebbero non essere mai riottenuti, anche se si paga.
3. Il riscatto successivo sarà più elevato.
4. Si incoraggiano i criminali.

"Abbiamo bisogno che gli attacchi vengano denunciati. Ciascuna vittima detiene un pezzo di prova fondamentale che fornisce informazioni inestimabili. In cambio, noi possiamo tenere la vittima aggiornata e protetta da "offerte" di parti terze sospette per la decrittografia dei dati. Tuttavia, abbiamo bisogno di accertarci che più forze di polizia sappiano come affrontare il crimine digitale."

Ton Maas, coordinatore del team digitale presso la Dutch National High Tech Crime unit

SI POTRÀ MAI VINCERE LA LOTTA CONTRO IL RANSOMWARE?

Crediamo di poterlo fare, ma solo se lavoriamo tutti insieme. Il ransomware è un'azienda criminale di lucro. Per fermarla, il mondo si deve unire per distruggere la catena criminale e rendergli sempre più difficile l'implementazione e lo sfruttamento degli attacchi.

Securelist, la risorsa per le ricerche tecniche, le analisi e le riflessioni degli esperti di Kaspersky Lab.

Seguiteci

Sito Web globale di Kaspersky Lab

Blog Eugene Kaspersky

Blog B2C di Kaspersky Lab

Blog B2B di Kaspersky Lab

Kaspersky Lab security news service

Kaspersky Lab Academy