THE RANSOMWARE GUIDE

2022

ALESSANDRO VANNINI

CEH MASTER - MODERATORE ETHICAL HACKER ITALIANI

RANSOMWARE DAGLI ALBORI AD OGGI (2022)

I primi ransomware iniziano ad arrivare alla volta del 2012-2013. Il primo ransomware lato cliente che ho visto era una semplice schermata della Polizia di Stato che partiva all'avvio del desktop bloccando il profilo utente e non permetteva di fare nient'altro. C'era scritto che avevi vistato siti illegali e dovevi pagare per evitare che la Polizia ti facesse una denuncia e soprattutto per poter riutilizzare il pc. Sulla destra in basso (perché la cifra è sempre in basso a destra), c'era l'importo di 200 e di inserire gli estremi della carta di credito. Il discorso carta di credito è durato come la neve al sole. Hanno capito che era una cosa tracciabile ed hanno iniziato ad usare criptomoneta. Ricordo di aver pagato 200€ in UKASH (reperiti tramite un sito sloveno) per un poveraccio che non sapeva che fare. Giravano 2 tipi di ransomware: quello che realmente criptava il disco, quello che invece era solo una schermata per allocchi e si rimuoveva facilmente ed era il 90%, ma la gente pagava ugualmente.

Gli Ukash sono durati poco, ha vinto il Bitcoin. Il primo server criptato è stato un 2003 STD. Era Agosto 2013, ultima settimana. Ero in ferie. Chiama il cliente che non accede ai dati. Lo passo ai colleghi ed intervengono. Il cliente aveva naturalmente una porta Terminal Server aperta con utenti con password pippo\pippo o ancora peggio. Per quanto tu ti impegni a fare sicurezza, ci sarà sempre qualcuno che te la bypassa perché tanto non succede nulla. Lì abbiamo visto il primo cryptolocker. Bloccava tutti i file office. Word, Excel, Access. Il cliente aveva un backup su una share condivisa (il cliente non era mio..lo sottolineo) ma 10 anni fa la security era comunque meno "strong" di ora. Criptato anche il backup. C'era allegata una mail che diceva, per sbloccare paga qui 5 BTC (allora valeva 300€ cad). In quel caso non abbiamo pagato. Sono tornato dalle ferie il lunedì successivo e stavamo ancora cercando di capire cosa fosse quel "virus" che si era fumato quel server. Mi è venuta un'idea. Il cliente aveva un raid 1 sul nas. Sono andato a smontare uno dei due dischi ed ho ripescato con un tool di recovery che leggeva l'ext4 come filesystem, un'immagine Acronis cancellata di una settimana prima dal set di backup. Era integra. L'ho ripristinata ed ha funzionato. Il cliente mi ha elevato alla stregua di Dio dell'Olimpo Informatico e si è sparsa la voce che la IT4YOU faceva miracoli. In realtà, per quanto fosse stata un'idea fantastica, avevo avuto la fortuna che il NAS non era pieno e che l'immagine era coerente, però il mio pensiero "non puoi criptare quello che non c'è" era corretto. Dio salvi lo spazio vuoto e soprattutto la non sovrascrittura dei settori.

Il ransomware ha iniziato prendere piede in tutte le sue forme. La criptatura da 128 bit era passata in poco tempo a 256. Oggi è a 1024 o 2048 addirittura.

C’erano società in Russia che calcolavano con le loro reti di calcolatori le chiavi private per sbloccare i file ed in 2-3 giorni con cifre comunque importanti ma ti salvavano se i server bloccati erano più di uno. Da parte nostra avevano già messo in sicurezza tutte le porte terminal obbligando i clienti a comprare questo benedetto firewall (perché anche alcuni dei nostri non erano esenti).

I pirati allora cambiarono linea. Invece di bucare il TS ed entrare e piazzare l’eseguibile, iniziarono a camuffarlo ed inviarlo via mail. Prima con comunicazioni tipo bollette di rimboso, corrieri espressi (UPS ha avuto i magazzini intasati per 2 mesi perché la gente non ritirava più la merce per paura di aprire le mail) poi con documenti ufficiali di enti tipo Agenzia delle Entrate, Poste italiane ecc.

Gli antivirus e le aziende di firewalling reagirono cassando la possibilità di aprire eseguibili di tutti i tipi.

I black hat cambiarono ancora metodo. Crearono applet java, macro per word ed excel. Altra reazione di Microsoft e compagnia bella: macro disabilitate di default, java considerato nocivo e scansionato come se non ci fosse un domani.

Poi arrivarono i rootkit. Aprivi un sito per una ricerca o semplicemente aprivi una mail che ti mandava ad un sito fake, ti veniva scaricato il trojan ed a quel punto l’hacker aveva un canale diretto e ti buttava dentro quel che voleva. Il venerdì sera di solito lanciava l’infezione, arrivati il lunedi mattina e la rete era KO. E chiedevano 2 bitcoin che nel mentre era andato a 5000€.

Qualcuno si inventò i “decrypter” tipo Photorec o Kaspersky, ma la gente pensava di aver trovato la panacea, mentre funzionavano una volta su 20. Li lanciava senza sapere che tipo di ransomware si era presa e cancellava i file originali senza possibilità di recupero. Altri pagavano e si tenevano le macchine comunque bucate mai coi files ripristinati. Sto parlando di professionisti IT, non di persone normali. C’era una gran confusione, molti davano le loro idee (sbagliate) altri le mettevano nero su bianco. Ricordo ancora di aver letto un comunicato della Postale (non me ne voglia) che spiegava come operava e cosa fare in caso di Ransomware che era una serie di inesattezze e fantasia da fare paura. Noi siamo arrivati a 80 aziende tirate fuori dal Ransomware. Ci telefonavano da tutte le parti. Alcune soluzioni che abbiamo tirato fuori sono state davvero mirabolanti, ma in ogni caso erano possibili solo per esperienza, non perché eravamo dei maghi, è che ne avevamo visti talmente tanti che sapevamo come gestirli. Su 80 aziende, 77 le abbiamo tirate fuori dai guai senza pagare. 3 hanno pagato e le abbiamo assistite nel pagamento. Tratterò però il discorso alla fine perché voglio adesso passare alla parte prevenzione, cosa fare se vi prendere un ransomware, cosa fare se non esiste alternativa.

Gli ultimi ransomware non colpiscono più nemmeno i server. Un mese fa abbiamo passato 15 giorni dentro una multinazionale perché ci è stato chiesto aiuto perché hanno criptato 100 macchine Windows 10. La nuova frontiera del ransomware è: prendere credenziali di

tutti i tipi. Criptano la macchina, intanto esfiltrano cookies, password salvate ecc e poi ti chiedono il riscatto ma intanto hanno in mano anche il resto. I server non li hanno nemmeno toccati, ma ora devi cambiare TUTTE le password dell'azienda ed il danno è doppio.

STEP DI PREVENZIONE

Sappiamo che non si può prevenire un ransomware al 100%. Ma si può comunque fare in modo che, se ce lo prendiamo, ci facciamo due risate e ripartiamo in poco tempo. Questi sono gli step che secondo me vanno fatti per salvaguardarsi.

- Niente porte critiche aperte verso l'interno dell'azienda. 3389 (RDP) 80 (WEB) 21 (FTP) devono stare chiuse. La RDP prima di tutto. Per la 80 e la 21 se proprio una DMZ. Ho visto aziende con la 53 e la SQL aperta. Va chiuso tutto. Al massimo una 443. Il resto VPN client to site. Occhio alle VOIP 5060-5061-5059 ecc..il voip se le dovete tenere aperte lo tenete lontano dalla subnet dei client\server. In rete separata
- Firewall\UTM con IPS attivo SEMPRE. Pagatelo sto servizio. Vi salva la vita. VPN client to site per connettersi da fuori. "Eh ma è scomoda" non mi interessa. Se avete un Exchange od un server interno con mx, assolutamente Antivirus\Antispam come servizio del firewall o macchina in DMZ tipo GFI Mail Essentials o similari. Dovete fare inspection di quel che viene dentro via mail.
- Antivirus sugli endpoint e sui file server con Anticrypto attivo, analisi del comportamento ed attacchi di rete. Ormai ce l'hanno tutti quelli blasonati. Pagate 'sto antivirus. Vi salva la vita
- Sistemi operativi patchati (con la dovuta conoscenza di cosa fanno gli update…non updates selvaggi).
- Sistemi operativi SUPPORTATI. Date una scarpata a Windows 7, 2008, 2003 ecc. È arrivato il momento. Non si può sentire ancora gente che ha XP o 2003 in azienda. Poi finite a gambe all'aria.
  Costa? Certo. Costa di più se vi bucano un 2003 e poi vi passa su tutta la rete. Fidatevi.
- Usate delle VM. Non dovrebbe esserci bisogno di dirlo. Basta coi sistemi fisici. Ne vedo ancora. Ci mettete 3 giorni a ripristinarlo.
- Usate un sistema di backup che abbia un fast recovery, quindi cambi solo i blocchi modificati dall'ultima macchina "valida". Veeam, Acronis, Arcserver, quel che vi pare, la cartella di backup deve essere con accesso limitato al solo utente di backup, non usate l'admin del NAS

- Ogni tanto controllate che non ci siano vulnerabilità sui FW dei Nas. Capita che vi vanno direttamente sui backup perché il QNAP magari ha un bug. Dopo siete a piedi.
- Usate un backup OFFLINE almeno una volta a settimana. Disco da portare via, NAS secondario che si accende solo per quel task, backup in cloud criptato, quel che vi pare. Se siete fregati su tutto almeno avete un salvagente.
- Di un backup avete sempre bisogno. Se lavorate con grandi quantità di dati e fate lavori particolari a casa, o avete il backup oppure staccate dalla rete il pc\client. Altrimenti, vi vengono dentro senza che ve ne accorgiate e dopo non avete soluzione se non pagare.
- Formate i dipendenti e voi stessi a pensare prima di cliccare. Guardare cosa leggete, non andate in automatico. La formazione abbassa del 50% il rischio. Se implementate tutto questo sopra ed avete formazione ed attenzione un ransomware da voi avrà vita davvero corta. Guardatevi i porno da una VM a parte o da un pc a parte, scusate, dovevo dirlo, ma il 50% dei ransomware lo vedo perché la gente va a cercare roba nel darkweb od in siti strani dal pc principale. Fate sesso sicuro, almeno dal lato sistema. 😉
- Attenzione se usate 365. Le mail NON sono salvate. Le mail sono sempre disponibili. Sento spesso “ma tanto ho office 365” si ok. Dovete spendere per un programma di backup che ve le salvi. Microsoft offre la continuità, non il backup nella sottoscrizione. Questo più che per il ransomware è una prassi anche in caso di cancellazione massiva di mail.
- Con l’avvento dello smart working e delle vpn, state molto attenti quando permettete lo split tunnel ai vostri collaboratori: poter navigare con la propria connessione mentre si è connessi alla rete aziendale è un rischio altissimo. Fate passare tutti dal proxy in azienda e dal firewall aziendale. Se qualcuno si lamenta perché è lento, pazienza, ma non si prenderà una schifezza mentre sta aprendo i documenti riservati perché sta guardando qualcosa in streaming su un sito dubbio e facendo passare il tutto sulla VPN verso l’azienda.

HO PRESO UN CRYPTO..AIUTO

Qui ci sono due diverse considerazioni da fare prima, anche se il risultato è lo stesso: vi siete beccati un crypto.

1) Se ve lo siete presi perché avete uno zero day, qualcuno della vostra organizzazione ha cliccato 2 volte su un pdf nocivo e voi siete l'IT, avevate un buco che non sapevate o qualcuno vi ha attaccato ed ora siete nei guai: AVETE IL MIO APPOGGIO.
2) Se ve lo siete presi perché ignorate tutto quello detto sopra, non vi curate di quel che cliccate, l'antivirus a pagamento non volete comprarlo, il vostro capo vi ha imposto misure minime e voi gli avete dato retta lo stesso, sapendo che questo giorno sarebbe arrivato o ancora peggio sapevate delle problematiche ma per non far spendere il cliente o la vostra aziende le avete ignorate: NON AVETE IL MIO APPOGGIO, ANZI.

Nel secondo caso, professionalmente, bacchetto e rilascio palle di fuoco come se fossi un mago del 36esimo livello di AD & D. Perché non esiste alcun motivo se non quello di NON SAPERE per rischiare un crypto. Perché prima o poi la pagate. Non siete fighi, siete solo fortunati, ma la fortuna finisce. Sono veramente stando di leggere di professionisti piangenti che hanno tutto fermo perché il loro capo non gli ha dato gli strumenti ed ora se l'è presa con loro. Se dovete fare gli IT e poi non rispettare nessuna procedura, anche se imposto, non va la pena fare gli IT. Scusate la durezza, ma il Sysadmin non è il servo della gleba. Il Sysadmin decide cosa fare. Non può? Bene, fate una bella manleva, nero su bianco, che se l'azienda si blocca, il problema non è vostro e la sottoponete al proprietario. Vedrete che arriveranno i fondi, perché alla fine, nessuno vuole prendersi quella responsabilità. Fidatevi.

La mancata conoscenza non è colpa vostra. Ma sono passati ormai 10 anni. È ora di svegliarsi. Questo per i professionisti. Per il privato non posso dire nulla, ma un privato, di solito, non investe nel recupero, non paga, non ha soldi, è solo fregato e basta perché il 99% delle volte ha un backup su un disco esterno usb e lo fa una volta ogni 2 anni. Ora che avete questo documento. Anche se siete privati. Scuse non ne avete più. Backup, sempre e potete prendervi un crypto al giorno. Ci sono programmi gratis di backup, non vi serve spendere miliardi. Via la pigrizia e Backup della vostra vita. Non avete il backup? Perché? E allora sono affari vostri…e non ve lo dico più.

Se la vostra macchina è compromessa questi sono gli step.

1) Se vi accorgete di aver cliccato su qualcosa di errato e l'antivirus non è entrato in funzione ed è un antivirus a pagamento di quelli seri magari non preoccupatevi più di tanto, ma una scansioncina offline ed un Malwarebytes lo farei lo stesso.
2) Se vi accorgete di aver cliccato su qualcosa, che i file stanno cambiando, che il pc va in affanno dopo il click o ancora peggio che dopo il click non succede nulla, prima di tutto non cliccateci di nuovo, non girate l'allegato al vostro collega\amico per vedere se a lui si apre. Staccate il cavo di rete del pc, spegnete e chiamate il vostro IT. Siete un privato? Staccate il cavo di rete del pc e chiamate un Sysadmin o vostro cugino che sicuramente ne sa a pacchi. Non avete cugini? Staccate il cavo di rete, spegnete il pc e chiedete un consiglio a noi. Tutti i ransomware lavorano su rete sia con rootkit che con trojan, reverse shell ecc. Se gli togliete l'aria (rete) finito l'ossigeno muoiono. Il pc è il loro ossigeno. La vostra macchina "untore" è comunque compromessa quindi va da sé che lì site fregati. Format c:\. Coi nuovi dischi SSD o M.2 vi cripta tutto il disco in 10 minuti. Ma almeno non va sul resto della rete. E adesso? Vi server il backup..se non l'avete..beh…andate alla sezione "pagamenti". Perché le shadow non vi salvano, se avete 7 forse recuperate qualcosa, ma il ransomware fatto bene stoppa lo shadow service. Game Over. Da 8.1-10 ecc comunque non ci sono più.
3) Se siete su una rete aziendale il discorso è più complesso. Molti ransomware hanno delle timebomb che partono il venerdi sera, quindi magari l'avete dentro ma non lo sapete. Antivirus con anti ransomware vi salvano i server, se non li avete, il lunedì mattina avrete mal di testa. Se invece vi chiamano in tempo. Staccate l'untore. Da indentificare a volte non è facile. Oggi le nuove generazioni criptano PRIMA la rete poi il pc infetto. A quel punto dovete iniziare a spegnere tutto ed a segmentare. Un bagno di sangue. Se siete voi invece i "cliccatori" per favore, chiamate il vostro IT, non mandate in vacca l'azienda. Un'azione tempestiva salva tutto. Avete sbagliato, succede, non fate finta di niente perché poi si risale al problema alla fine. Staccate comunque il pc.
4) Fate lavorare gli IT, se non ce la fate da soli non andate ad usare robaccia, chiamate professionisti che conoscono i ransomware, altrimenti rischiate di cancellare tutto.

LEGGENDE METROPOLITANE POST ATTACCO RANSOMWARE

Una raccolta di leggende. Le definirei “fregnacce” ma sono gentile. Le sento spesso e non hanno niente a che fare con la realtà se non quanto possedere un minipony rosa che corre sull’arcobaleno (io ce l’ho. Sta pascolando al momento).

1) Avevo tutto chiuso ma sono entrati lo stesso e nessuno ha clicca nulla! ERRATO, se era tutto chiuso non passava nulla. Controlla pure, vedrai che il buco lo trovi.
2) Mi sono entrati su un pc client e mi hanno bloccato le shadow copies sul server. ERRATO, le shadow lavorano con un servizio che gira system sul server di destinazione. Se tu via rete potessi stopparlo allora ogni 3x2 avresti le shadow sempre in down. Se ti hanno cancellato le shadow ti sono entrati sul server ed hai probabilmente il domain admin compromesso da un priviledge escalation ma non hai preso un crypto, ti hanno fatto un attacco bello e buono, è un livello totalmente diverso.
3) Mi hanno criptato la cartella dei backup, ERRATO, la cartella te l’hanno criptata perché era guest come accesso, oppure perché c’era la share salvata da qualche parte ed hanno preso le credenziali. Mi è capitato solo un caso in cui hanno bucato la macchina VEEAM ed hanno eliminato i backup. Ma la macchina VEEAM non dovrebbe stare sotto AD, dovrebbe essere magari in una diversa VLAN ed avere accessi a sé giusto? Quindi…l’errore è comunque di chi la implementa.
4) Uso un decrypter od una società che decripta. OK. Usali. I decrypter il 50% delle volte ti segano i file originali, le società di decrypt ci sono, funzionano, ma a volte costano di più del riscatto, mica lavorano gratis. Vedi tu. Tanto comunque devi rifare i server in ogni caso. La società di “decrypting” il 50% delle volte usa delle stringhe pubbliche già emesse per decriptare il tuo tipo di ransomware (controlla prima di chiamarle) l’altro 50% dei casi, paga l’hacker e poi ti rivende la key a prezzo maggiorato. (sì ho visto anche questo da quelli che dicono che “sbloccano in poche ore”) quindi occhio che non esiste modo di decriptare una chiave a 256bit senza la chiave privata. Chi ti dice che c’è..ti racconta una bufala.
5) Una volta decriptato mi tengo il server così com’è: ERRATO. Se hai la fortuna di decriptare qualcosa, estrai i dati, pialli la macchina e la rifai più strong di prima e glieli ripiazzi dentro. Serve tempo? Chi se ne frega.
6) Ora che ho rifatto la struttura ho risolto. ERRATO, ora devi capire dove hai fallito ed andare a fare hardening della struttura, se no domani entrano nello stesso modo. Il post remediation ha un valore immenso. Non hai tempo per farlo? Ha dei costi? Preparati a finirci sotto un’altra volta.

7) Avevo il terminal server aperto ma le password erano strong. Questa non la commento neanche..e la sento spesso..andate su Shodan…e guardate.
8) Il ransomware non passa sulle VPN site to site. ERRATO visto personalmente. Azienda criptata a Milano, unità mappate a Ferrara, criptate anche quelle. Ed era un tunnel site to site.
9) Ho letto degli articoli che…Lasciate stare. Per favore. Chiedete a gente che ha a che fare con questa roba. Non andate a leggere laqualunque cosa. Ci sono articoli validi ed altri no, un approccio diretto con un professionista PARLANDO con lui, vi fa capire realmente intanto se questo parla con cognizione di causa, secondo se vi può aiutare. La consulenza di solito non si fa pagare. Se trovate uno a cui chiedete un consiglio e vi spara una cifra è un ladro a prescindere.
10) Ah ma io faccio da solo. Niente di più sbagliato. Magari a volte c'è un modo per uscirne, ma se è il vostro primo ransomware siete talmente coinvolti emotivamente che difficilmente siete lucidi. Un consiglio è sempre meglio averlo. NON chiedete una soluzione al telefono. Nessun professionista ve la darà, ma vi dirà fin dove si può arrivare poi in qualsiasi modo dovrete pagare il vostro sbaglio. Inevitabile. Accettatelo e vedete cosa vi costa meno.
11) Se paghi non ti danno il decrypter e perdi i soldi e fai pure la figura del pirla. Per questo leggetevi la fine della storia qui sotto.

L'ULTIMA SPIAGGA: PAGARE

Ora questo ultimo punto mi ha fatto litigare in almeno 5 o 6 casi con colleghi integerrimi, che però non si sono mai trovati con i LORO dati bloccati senza via d'uscita. Qui ci starebbe una battuta volgare, ma se vi trovaste voi in una situazione in cui la vostra azienda è inevitabilmente bloccata, non avete alternativa e l'unica alternativa è chiudere baracca non sareste disposti a rischiare? Io sì.

Qui non si sta fomentando il crimine. Ma siccome nel mondo vengono pagati continuamente riscatti per salvare persone anche se non si dovrebbe, la stessa cosa è con i dati. Ransomware vuol dire "ti blocco, mi paghi, ti sblocco e la prossima volta stai attento a non farti fregare". Ransomware non è sintomo di "ti frego i soldi e scappo" perché il mercato finirebbe in un attimo. Se uno sa che pagando non ottiene niente, correrebbero tutti a fare backup e gli hackers black hat sarebbero a spasso. Invece è il mercato più fiorente degli ultimi anni. Come dicevo, in tre casi ho seguito i clienti che hanno pagato. Non avevano alternativa. Hanno voluto rischiare. Tanto il risultato era che avrebbero perso comunque tutto. In tutti e tre i casi sono stati sbloccati. Voglio che capiate che quel che scrivo qui sotto non lo condivido. Anche io sono per non pagare, ma se fossi io il diretto

interessato, pagherei, non mi vergogno. Solo un bugiardo direbbe il contrario anche perché la Polizia Postale non vi risolve il problema dei dati, al massimo arresta il pirata, ma voi restate criptati, loro sono il pronto intervento. Al massimo vi fermano l'attacco, ma poi sono affari vostri. Quindi, se decidete di pagare lo fate a vostro rischio.

Non è IL METODO DEFINITIVO, ma se dall'altra parte c'è un pirata "etico" passatemi il termine, perché anche loro hanno la loro etica, vi invierà il decrypter.

- Usate una mail che non sia gmail\outlook ecc per le comunicazioni, vi serve qualcosa in cui possiate tirare giù l'antispam del tutto. Questo perché di solito il decrypter è un exe rinominato. Se viene cassato dall'antispam non avrete una seconda chance, lo mandano una volta solo.
- Non tentate di parlare col black hat come fosse un vostro amico. Inviate una mail di contatto, eventualmente trattate sul prezzo e fine, niente offese, allusioni ecc.
- Inviate sempre un file criptato e richiedete una prova di sblocco. NON inviate file di progetti o roba simile, devono pensare che siete un poveraccio che non ha soldi, in alcuni casi hanno inviato progetti e quando hanno visto cosa faceva la società gli hanno triplicato il prezzo. Usate il più sfigato file di word che trovate con la lista della spesa. Loro non sanno cosa hanno criptato nel 90% dei casi, non usate chiaramente mail aziendali. Se invece è un attacco mirato a voi allora dovete essere molto grossi, lì sono dolori, ma lì si gioca in serie A del cybercrime. Entrano in gioco tanti altri fattori e giocatori.
- Se pagate createvi un wallet apposito, prendete bitcoin su piattaforme conosciute tipo Coinbase. Non vi fate fregare anche da quel lato.
- Una volta pagato, incrociate le dita. Spesso sono su fusi orari diversi, nella mia esperienza passano anche 24 ore per avere il decrypter, le più brutte della vostra vita, ve lo assicuro. Tenendo presente che la cifra deve avere un senso. Se è troppo lasciate perdere.
- In tutto questo date comunque poche speranze a voi stessi ed al cliente e siate consapevoli che, può sempre capitare che vi facciano su i soldi, anche se, ripeto, non mi è mai successo finora ma deve essere imperativo che voi non siete né assicuratori, né avete certezze. Si chiama "ultima spiaggia" perché dopo c'è l'oceano. Buona Fortuna.

Alla luce degli ultimi due anni di ransomware, molti dei colleghi che fomentavano il "non pago nemmeno morto" si sono ricreduti perché "piccole" società come Garmin, sono state bloccate da ransomware ed hanno pagato 10 Milioni di dollari per farsi sbloccare, perché non c'era modo per farlo diversamente. Sono stati pagati 5 Milioni di dollari per sbloccare un oleodotto negli USA. Ora, ad un attacco del genere, mettetevela via, non riuscite a contrastarlo, sono professionisti atti a fare quello ed al 99% dei casi, hanno un basista

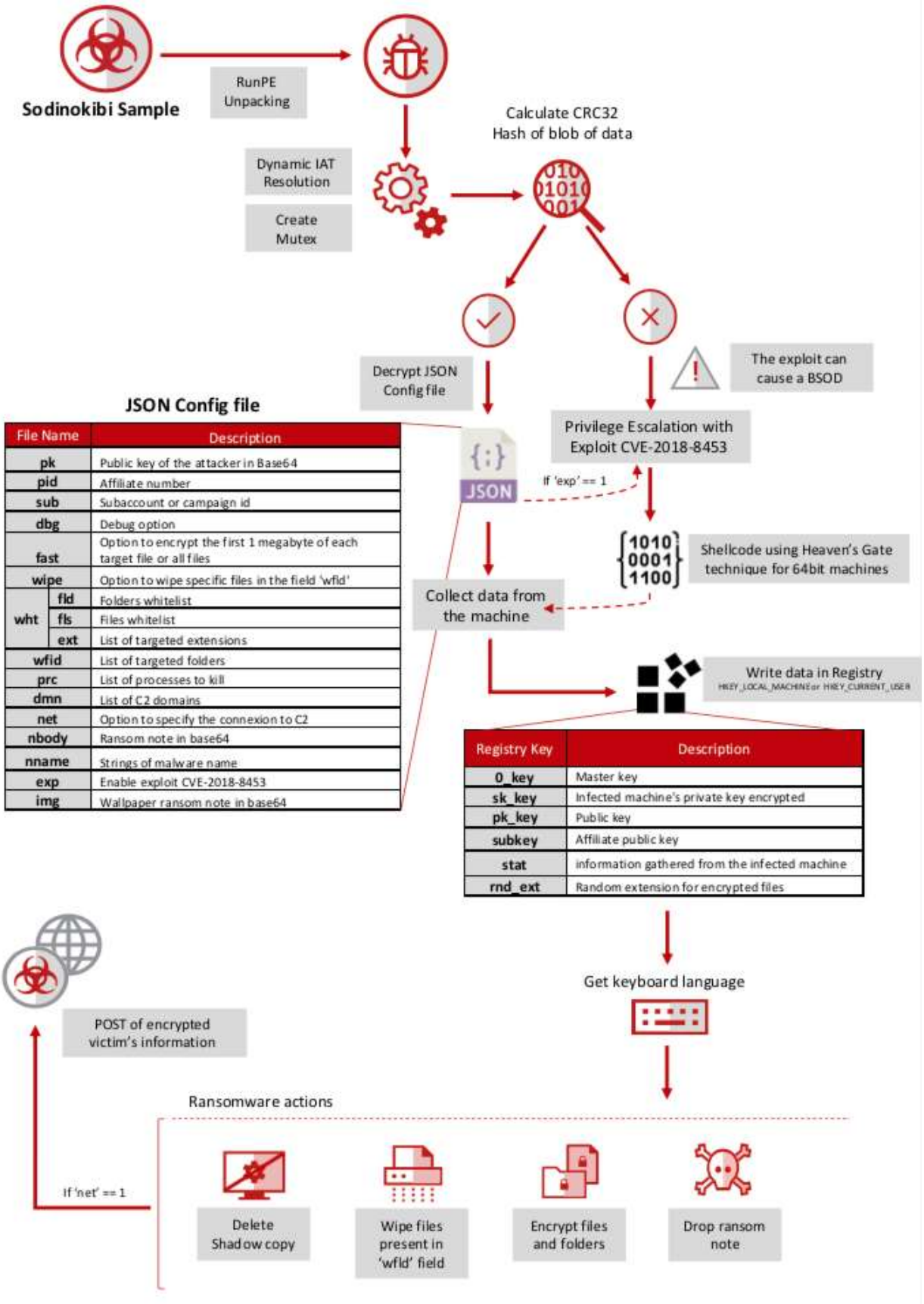
all’interno che gli “attacca una chiavetta”, ma voi, nel vostro piccolo, potete provare a proteggervi con quello che avete. Sicuramente non spenderete 5 Milioni di dollari.

COME OPERA UN RANSOMWARE: SODINOKIBI

Il Sodinokibi, by Revil è una delle “bestie” da giardino più rognose del mondo dei ransomware. Nel corso degli anni l’anno perfezionato ed evoluto al punto che non si muove più semplicemente criptando un pc e chiedendo un riscatto, ma, partendo da una mail di phishing a cui voi date l’ok, aprendo il file, accettando la macro o cliccando sull’exe contenuto nello zip, il malware una volta instaurato, si muove lateralmente andando a sfruttare vulnerabilità della vostra rete. Lancia comandi powershell ed attacca le connessioni RDP che trova sulla rete. Sega tutte le shadow copies andando a modificare il vvsadmin.exe (lo stoppa) ed usano il seriale del vostro HD e il CPUID va a creare l’URL e le chiavi publiche e private che serviranno ai vostri amici pirati per poi darvi il decrypter.

Qui sotto come si muove il giocattolino, se vi sembra una cosa “semplice”.

Sodinokibi Ransomware Functionalities



File Name		Description
pk		Public key of the attacker in Base64
pid		Affiliate number
sub		Subaccount or campaign id
dbg		Debug option
fast		Option to encrypt the first 1 megabyte of each target file or all files
wipe		Option to wipe specific files in the field 'wfld'
wht	fld	Folders whitelist
	fls	Files whitelist
	ext	List of targeted extensions
wfld		List of targeted folders
prc		List of processes to kill
dmn		List of C2 domains
net		Option to specify the connexion to C2
nbody		Ransom note in base64
nname		Strings of malware name
exp		Enable exploit CVE-2018-8453
img		Wallpaper ransom note in base64

Registry Key	Description
0_key	Master key
sk_key	Infected machine's private key encrypted
pk_key	Public key
subkey	Affiliate public key
stat	information gathered from the infected machine
rnd_ext	Random extension for encrypted files

LA REMEDIATION E LA GESTIONE DELLO STRESS DA INCIDENT

Negli ultimi due anni, anche grazie a questa piccola guida che se n'è andata in giro per il paese, sono diventato una specie di "punto di riferimento" per quel che riguarda la remediation e la gestione degli incidents. Mi sono quindi mosso su aziende di calibro nazionale con fatturati anche da 500 milioni di euro l'anno a coordinare delle task force e dei pool di persone che hanno subito un attacco.

Non è mai facile arrivare quando il latte è versato e spesso, si viene chiamati in una situazione critica. Nel nostro mondo la chiameresti WIN\WIN perché spesso, difficilmente puoi fare più danno di quello che c'è. In realtà, una cattiva gestione del problema non solo può portare a peggiorare le cose, ma a far aumentare il costo poi di rimessa in opera dell'azienda. Perché il business DEVE ripartire. Parlo di aziende private. Non mi sono mai mosso su una PA. Questo perché non tratto PA per alcuni motivi principali: nessuno si prende mai una responsabilità ed una colpa nella pubblica amministrazione, non saltano teste, non falliscono aziende e le perdite di dati che ci sono state, non sono state pagate da nessuno se non da noi cittadini, questo mi ha fatto sviluppare nel corso del tempo, una vera e propria allergia alle PA e la cosa mi fa un'enorme tristezza, perché dovrebbe essere il posto in cui i nostri dati sono più al sicuro: casa nostra, ma il politico di turno che sfrutta l'attacco e la perdita di dati a suo favore, facendo vedere che "tiene duro" quando la cosa migliore da fare sarebbe dimettersi e licenziare in tronco i responsabili mi fa quantomeno alterare nel profondo.

Detto questo, non posso mettere qui gli step di una remediation. Sono troppi, ci sono troppi fattori in gioco, ma alcune cose le posso scrivere con la massima sicurezza:

1) SE non siete in grado di gestire il problema o il vostro team IT non lo è, CHIAMATE QUALCUNO CHE HA PIU' ESPERIENZA. Non fate da soli. Un piccolo breach può diventare una diga del Vayont. Lasciate perdere orgoglio e immagine e chiedete aiuto.
2) Lo stress da incident, va gestito. È come una maratona. SE non siete abituati a gestire lo stress, come da punto 1, chiamate qualcuno. Una persona esterna avrà la lucidità e la capacità di vedere le cose sotto un'ottica diversa dalla vostra e non avrà la vostra ansia.
3) Chiudete TUTTO. Non mi interessa se dovete lavorare. Avete subito un attacco, difendetevi. Non potete stare chiusi? Non è un problema mio. Sbarrati. Connessione staccata e si riparte SOLO quando siete sicuri di essere salvi. Il 99% dei ransomware se non trova connessione esterna non lavora, il server Command & Control non viene contattato e gli amici hacker non possono vedere nulla. La prima cosa che si fa col nemico è togliergli la vista (Sun Tzu).

4) Preparatevi all'urto economico. Non avete speso prima, avete speso ma sono entrati lo stesso ecc. Ok. Adesso però spenderete tanto. Perché siete obbligati a chiudere e rimediare PER FORZA. Dimenticatevi di andare al risparmio ed investite quel che c'è da investire. Ho visto aziende chiudere per ransomware. Non è una barzelletta, è la realtà.
5) Preparatevi a gestire la perdita di dati. Inevitabile. Non sapete cosa è uscito? Polizia Postale, GDPR ecc..più siete grandi e più fate cose sensibili, più avete un problema che va gestito di Privacy. Potete anche non farlo, ma se domani vi pubblicano su Lockbit e non avete avvertito i vostri clienti ed i vostri legali, chiudete per sempre.
6) Ci sarebbero altri 30 punti. Ma vale sempre il punto 1. C'è chi fa questa cosa di lavoro, c'è chi attacca le strutture e le difende da una vita, se vi hanno bucati, non siete pronti a gestire il "dopo", servitevi di queste persone, non verranno a bacchettarvi, verranno a darvi una mano, l'assegnazione della colpa sarà comunque inevitabile ma nessuno è lì col fucile puntato sul reparto IT. L'imparzialità di queste persone è totale (se sono professionisti) e quello che è il loro interesse primario è salvarvi per quanto possibile.

Spero che questa piccola guida possa fare un po' di chiarezza. Salvate i vostri dati come se non ci fosse un domani, non avrete bisogno di pagare nulla, al massimo avrete un grattacapo od un immenso mal di testa, ma tutto si risolverà. Tutto quello che esula dal backup è vostra responsabilità, il ransomware evidenzia solo un problema che esiste, non forza assolutamente nulla, quindi chiudendo la porta al problema, il mercato prima o poi sparirà. Una piccola postilla. Spesso vengo identificato come l'Ing. Vannini. Non ho una laurea, ho solo un poco di esperienza e qualche pezzo di carta, lavoro sul campo ogni giorno, ed ho una piccola azienda di Cybersec coi miei soci, ma non ve la citerò qui. Siete abbastanza skillati per trovarmi. Qui sono solo Alessandro. Per tutti. Grazie.

Alessandro Vannini – Certified Ethical Hacker Master
EC-Council USA Board Member
8th Microsoft MVP Award
Ethical Hacker Italiani Group Moderator