# INDICAZIONI DI COMPROMISSIONE

Guida all'individuazione e alla prevenzione delle infezioni malware

BERTOLDI
CYBERSECURITY

# SOMMARIO

Difendere le reti dagli attacchi non è un compito facile per i professionisti IT. Gli attacchi si differenziano fra loro per potenzialità e minaccia e una reazione eccessiva o l'implementazione della tecnologia sbagliata può, oltre ad essere costosa, semplificare l'accesso ai criminali.

Questo e-Book descrive le tipologie di attacco che affrontano una rete tipica e presenta alcune strategie di successo per la loro mitigazione che professionisti IT hanno implementato per proteggere le proprie reti.

Sostanzialmente, utilizzate questa guida come primo passo nella progettazione della vostra strategia di difesa approfondita. I professionisti IT devono comprendere a fondo il rischio per l'impresa ed essere consapevoli che la sicurezza IT non offre soluzioni miracolose. Malgrado quanto affermano i fornitori, non esiste una tecnologia che, da sola, possa evitare il verificarsi di scenari dannosi.

Gli attacchi informatici, il malware e le vulnerabilità dei sistemi sono stati mistificati ed esagerati dai media oltre ogni sorta di analisi ragionevole. Infatti le strategie IT più efficaci contro le minacce, sia sconosciute sia note, sono solitamente le stesse.

Applicare patch e aggiornare il sistema operativo, applicare patch e aggiornare le applicazioni di terzi, limitare l'accesso come amministratori e utilizzare le difese contro il malware. Queste raccomandazioni derivano da anni di analisi svolte da organizzazioni governative e di sicurezza in tutto il mondo.

Infine, il reato crea la difesa. Ciò significa che i provider di servizi IT devono imparare a vedere le reti dei loro clienti come bersagli. Non è certo auspicabile che vengano scatenati attacchi informatici distruttivi su clienti inconsapevoli, ma è possibile migliorare la difesa e l'individuazione di attacchi alle reti con la creazione di un laboratorio virtuale di difesa informatica e la possibilità di scaricare strumenti gratuiti per analizzare le vulnerabilità.

È utile ricordare che, in qualità di professionisti IT, siete parzialmente o interamente responsabili della riservatezza, integrità e disponibilità dei sistemi IT di cui vi occupate. Non semplificate l'accesso ai criminali, rendetelo complesso tramite livelli di difesa di rilevazione, prevenzione e forense.

# INTRODUZIONE

Discussioni sulla sicurezza con fornitori IT e MSP inevitabilmente ricadono sull'efficacia delle difese anti-malware; in particolare la domanda sulla efficacia del software antivirus contro il ransomware. Per rispondere a questa domanda, è utile comprendere la relazione fra exploit, trojan e payload.

Il diagramma alla pagina successiva è un adattamento della Cyber Kill Chain® di Lockheed Martin, che descrive le diverse fasi di un'infezione malware dall'exploit iniziale all'esecuzione di un payload su un bersaglio endpoint.[1] La Cyber Kill Chain è un fantastico modo per spiegare come il malware completi il proprio viaggio dalla distribuzione dell'attacco da parte dell'endpoint e, infine, (nella maggior parte dei casi) all'esecuzione di un payload ransomware sull'endpoint preso di mira.

Questo e-Book è studiato per aiutare gli MSP e i fornitori di servizi IT a comprendere il diagramma e le varie tecnologie ed eventi che portano al successo di un'infezione da parte di criminali informatici. Ciò vi aiuterà ad individuare al più presto una compromissione e a conoscere la migliore risposta.

*“La relazione fra exploit, trojan e payload è fondamentale.”*

*"La maggior parte di MSP e di provider di servizi IT ricade nella categoria di servizi di informazioni sulle minacce."*

## LA CYBER KILL CHAIN DI LOCKHEED MARTIN

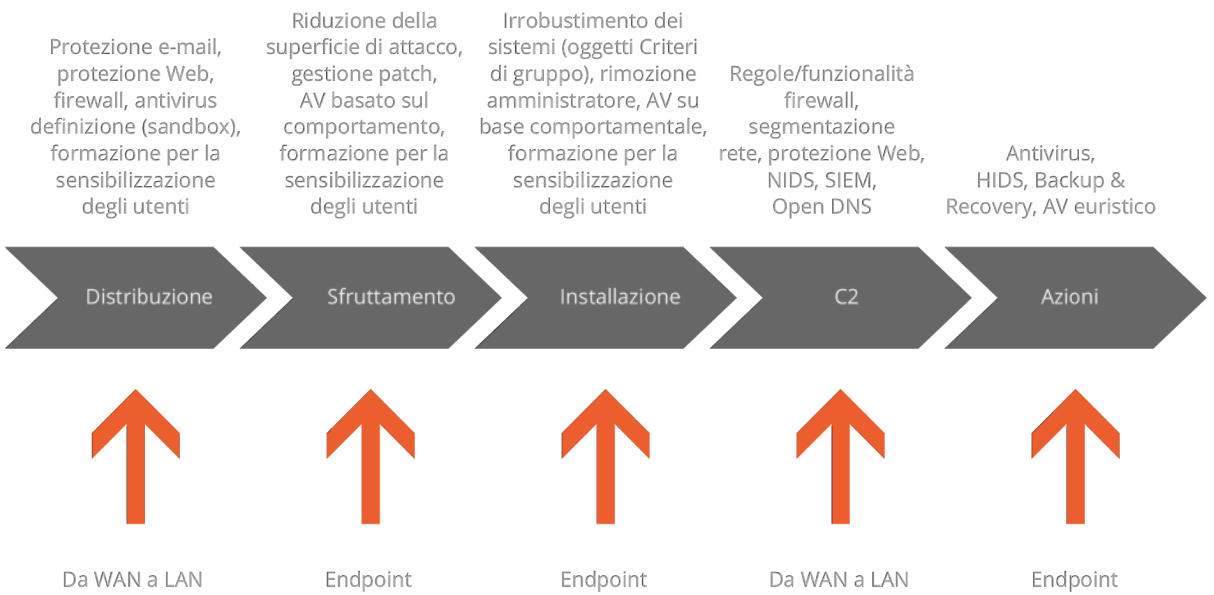

Il diagramma precedente mostra la Cyber Kill Chain completa, con due frecce grigie sotto ricognizione e armamento. Queste due aree sono, in genere, fuori dall'ambito per tutti, tranne le organizzazioni di maggiori dimensioni: la maggior parte di MSP e di provider di servizi IT ricade nelle categorie di servizi di informazioni sulle minacce.

Nel corso del tempo, grazie ad una migliore consapevolezza del settore del ciclo di vita di un attacco malware, l'apprendimento della macchina e l'intelligenza artificiale possono aiutare a fornire avvisi relativi ad un attacco imminente durante le prime due fasi della Kill Chain. Tuttavia, al momento, poco può essere fatto per degradare le capacità dei criminali informatici durante queste prime due fasi.

In realtà, psicologia/sociologia criminale, disparità geopolitiche, economiche e regionali motiveranno individui e gruppi a scandagliare i social network e a creare kit di exploit, programmi trojan sofisticati e payload malware/ransomware.

# COMPRENDERE LA DISTRIBUZIONE DELL'ATTACCO INFORMATICO

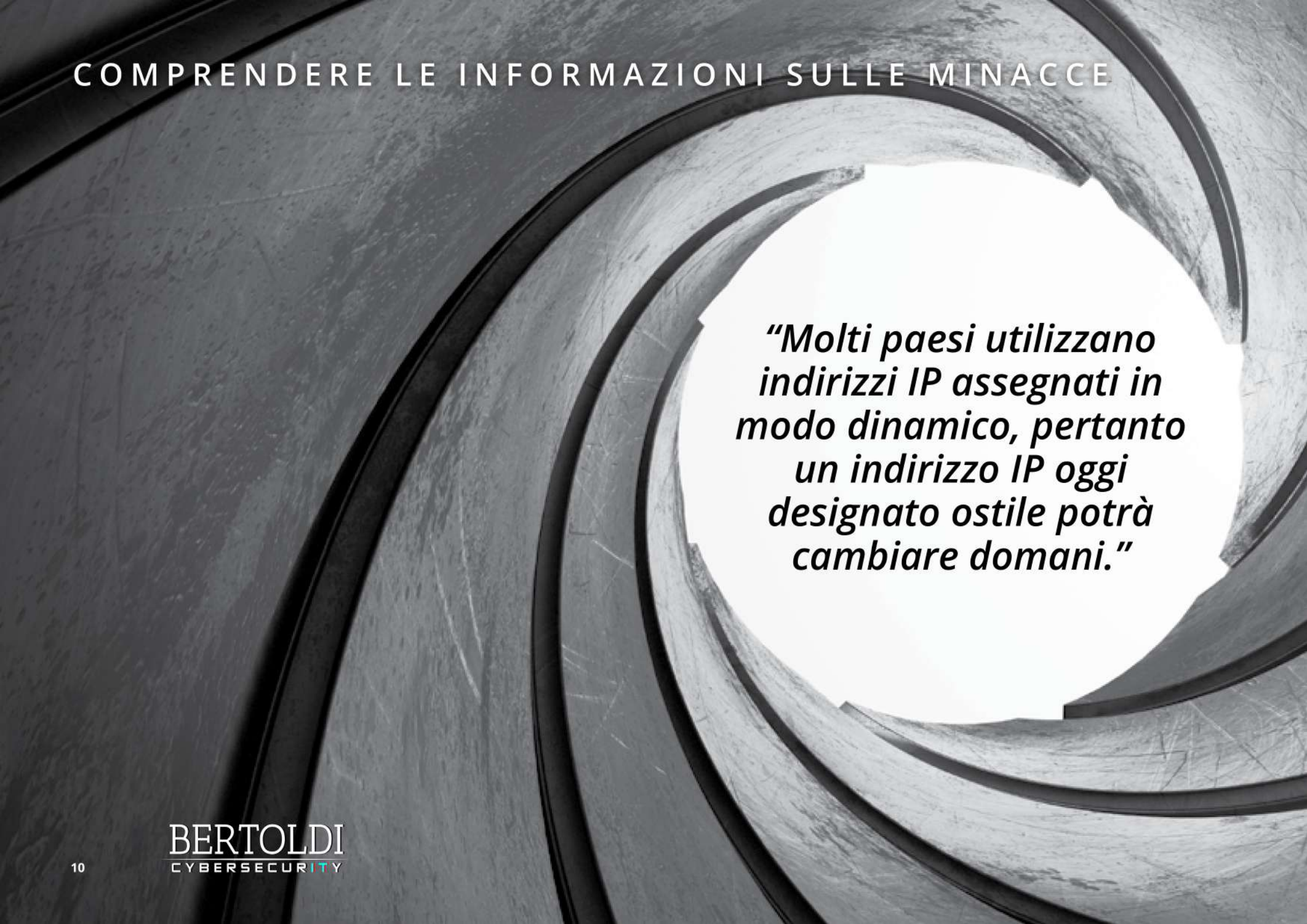
## ADATTATO DALLA CYBER KILL CHAIN DI LOCKHEED MARTIN




Lungo la parte superiore del nostro diagramma "Kill Chain" adattato è presente un elenco non esclusivo delle soluzioni di mitigazione, fra le quali formazione per la sensibilizzazione degli utenti e una serie soluzioni tecnologiche, mappate alle varie fasi dell'infezione. La sezione intermedia mostra le varie fasi della Cyber Kill Chain di Lockheed Martin. Le sezione inferiore visualizza le fasi di infezione e dove sia presente l'opportunità di rilevare, prevenire e ripristinare dall'attacco dei criminali informatici.

BERTOLDI CYBERSECURITY

# COMPRENDERE LE INFORMAZIONI SULLE MINACCE






BERTOLDI CYBERSECURITY

I servizi di informazioni sulle minacce devono essere avvicinati con una nota di cautela. La semplice ricezione di un elenco di indirizzi IP e l'aggiornamento di soluzioni firewall non è un approccio pratico. Molti paesi utilizzano indirizzi IP assegnati in modo dinamico, pertanto un indirizzo IP oggi designato ostile potrà cambiare domani. Inoltre, gli amministratori occasionalmente eliminano il malware dalle macchine. Senza un contesto per le informazioni sulle minacce, potrebbe non essere rilevante bloccare un indirizzo IP che non stia effettuando un attacco.

È consigliabile che organizzazioni che cercano di estendere le proprie difese nelle prime due fasi della Cyber Kill Chain creino e mantengano un ambiente "honeypot", una trappola tesa per rilevare o deflettere l'attività di criminali informatici da una rete. L'offerta corrente di servizi di informazioni sulle minacce presenta una pletora di dati senza contesto. Sapere che un indirizzo IP sudcoreano stia attaccando un indirizzo IP russo può essere interessante, ma se la vostra attività non si trova in uno di questi paesi, non è un'informazione utile. L'impostazione di un proprio "honeypot" per raccogliere informazioni su attacchi effettivi alla vostra infrastruttura aiuta a mitigare queste sfide.

# COMPRENDERE LE INFORMAZIONI SULLE MINACCE

*"Semplicemente sapere che un indirizzo IP sudcoreano stia attaccando un indirizzo IP russo può essere interessante, ma se la vostra attività non si trova in uno di questi paesi, non è un'informazione utile."*

A meno che MSP, provider IT e organizzazioni non siano preparati ad investire sforzo tecnologico e ad implementare hardware specifico, i budget e le risorse IT limitati li forzeranno a concentrare le difese degli endpoint sulle ultime cinque opportunità della Cyber Kill Chain per prevenire, rilevare e reagire ad un attacco di criminali informatici.

Il primo passaggio pratico dove la tecnologia può aiutare a prevenire il verificarsi dell'intera Cyber Kill Chain, si verifica nella fase di distribuzione di un attacco informatico. Nella grande maggioranza dei casi, il vettore della minaccia è molto evidente. Il grafico a pagina 13 è tratto dal Verizon Data Breach Investigations Report 2016 e mostra i metodi più frequenti di distribuzione di malware.[2]

Il tasso di successo delle e-mail di phishing, con un incredibile tasso di apertura del 30%[3], rende gli allegati malevoli delle e-mail e i collegamenti incorporati in esse, l'epicentro dalla lotta contro gli attacchi di criminali informatici. I dati mostrano inoltre che non dovremmo trascurare i pericoli della navigazione Web non protetta. È difficile obiettare il fatto che filtraggio di e-mail, filtraggio Web e formazione per la sensibilizzazione dell'utente siano le chiavi per interrompere con successo attacchi informatici alla fase di distribuzione nella Cyber Kill Chain.

## CINQUE PRINCIPALI VETTORI DI MALWARE

# IL RUOLO DEI SERVIZI BASATI SU CLOUD

Grazie ad una pletora di servizi basati su cloud, fra i quali Gmail e Office 365, la fase di distribuzione è oggi forse la meno costosa durante la quale le attività possono implementare intercettazione del malware. È inoltre relativamente semplice da implementare, con un impatto minimo o nullo sulle attività aziendali. La scansione di e-mail e i servizi proxy di navigazione Web situati on-premise o nel cloud offrono la maggioranza delle difese contro attacchi informatici in questa fase.

I servizi basati su cloud spingono le difese fuori del perimetro dell'organizzazione e offrono valore di difesa informatica impedendo persino che l'attacco arrivi all'endpoint. Sebbene molti di questi servizi dispongano di più motori di definizione dei virus e capacità di analisi euristica, i criminali informatici, in effetti, di tanto in tanto infiltrano malware attraverso queste difese utilizzando astuzia e scaltrezza "vecchia maniera", seducendo un dipendente in modo che faccia clic su un collegamento e/o esegua un payload.

L'attacco senza malware per la compromissione di e-mail aziendale, o "CEO fraud", è un esempio di attacco informatico che aggira persino le difese di filtraggio e-mail più robuste. Pertanto, la formazione di sensibilizzazione degli utenti, che insegna alle persone di verificare qualsiasi richiesta o allegato non richiesto/sospetto tramite conferma verbale, può aiutare a salvaguardare contro questi sempre più sofisticati attacchi di social engineering. I cosiddetti attacchi "CEO fraud" spesso si traducono in vasti profitti per i criminali informatici rispetto al ransomware, in quanto si presentano come trasferimento di denaro autorizzato da un executive verso un partner commerciale.

***"I servizi basati su cloud spingono le difese fuori del perimetro dell'organizzazione e offrono valore di difesa informatica impedendo persino che l'attacco arrivi all'endpoint."***

Inoltre l'attacco CEO fraud può avere altri fini oltre facilitare trasferimenti illeciti di denaro. I criminali informatici possono anche intendere sottrarre dati dei dipendenti. Secondo un fornitore SIEM, "oltre un terzo degli intervistati in un recente sondaggio hanno riferito che i loro executive sono caduti vittima di un'e-mail di CEO fraud e l'80% riteneva che i loro executive sarebbero potuti cadere vittime di truffe di phishing mirati. Queste preoccupazioni sono ben fondate. Solo durante l'ultimo periodo fiscale, oltre 50 organizzazioni, comprese Snapchat e Care.com, hanno subito attacchi riusciti con e-mail di CEO fraud che richiedevano informazioni sul W-2".[4]

È giusto affermare che il primo livello di difesa informatica deve essere progettato per sconfiggere l'attacco prima ancora che raggiunga l'endpoint. Tuttavia, quando l'attacco si verifica sotto forma di e-mail fraudolenta, ma dall'aspetto legittimo, la formazione di sensibilizzazione dei dipendenti è il miglior investimento le aziende possono effettuare per prevenire perdite su larga scala.

# PARTE 2—IL RUOLO DELL'ANTIVIRUS E DELLA GESTIONE DELLE PATCH

In questa sezione ci concentreremo sullo sfruttamento del vettore di attacco dell'endpoint, presupponendo che la fase di distribuzione dell'exploit sia eseguita con successo contro l'endpoint di destinazione.

Dal punto di vista del kit di exploit, l'endpoint sotto attacco si troverà in uno di quattro stati, illustrati nelle prossime pagine.

*"La modalità di autenticazione Windows è meno vulnerabile agli attacchi brute force, in quanto è più probabile che l'aggressore incontri un blocco del login dopo un certo numero di tentativi di attacco."*



BERTOLDI CYBERSECURITY

## **STATO 1:** LE PATCH SONO APPLICATE ALLA MACCHINA, L'ANTIVIRUS È INSTALLATO E AGGIORNATO

Le sole vulnerabilità che sono qui presenti sono "umane" (utente finale ingannato affinché installi il malware) o attacchi/exploit zero day che non vengono rilevati dall'antivirus.

Chiaramente, la formazione di sensibilizzazione dell'utente è la sola efficace difesa contro "inganni" o attacchi basati su social engineering. Solo se gli avvisi sono ignorati l'exploit può consegnare con successo il proprio payload. Questo è ciò che avviene con exploit tramite macro Visual Basic in e-mail di phishing. Antivirus robusti, che offrono definizioni di firme malware, rilevamento euristico di attività di exploit e analisi basate sul comportamento delle attività di exploit, possono proteggere l'endpoint, ma spesso ciò non avviene.

STATO: **VERDE**

# IL RUOLO DELL'ANTIVIRUS E DELLA GESTIONE DELLE PATCH

## **STATO 2**: LE PATCH NON SONO APPLICATE ALLA MACCHINA, L'ANTIVIRUS È INSTALLATO E AGGIORNATO

Qui le vulnerabilità sono correlate ad exploit sviluppati per la mancanza di una patch specifica. Sebbene l'antivirus possa essere aggiornato, è discutibile che l'exploit venga effettivamente rilevato. In questo scenario, la macchina può essere facilmente infettata da un exploit progettato per aggirare l'antivirus. Ricerche condotte da Recorded Future indicano che Adobe Flash, Java e Internet Explorer sono i bersagli più frequenti di kit di exploit.[5] Non installare, in primo luogo, il software attaccabile è l'unica difesa effettiva.

STATO: **GIALLO**

*"La macchina può essere facilmente infettata da un exploit progettato per aggirare l'antivirus."*



BERTOLDI CYBERSECURITY

## **STATO 3**: LE PATCH NON SONO APPLICATE ALLA MACCHINA, L'ANTIVIRUS È INSTALLATO, MA NON È AGGIORNATO

Le vulnerabilità qui sono notevolmente elevate rispetto ai primi due stati, in quanto la macchina è aperta ad una vasta gamma di exploit, non solo alle ultime versioni di kit di exploit. Analogamente allo Stato 2, una macchina in questo stato può essere facilmente infettata. Tuttavia, è anche probabile verrà infettata più volte. I fornitori IT e gli MSP si trovano troppo spesso in questa situazione. L'attenzione deve essere posta sulle patch a causa dell'abilità del pacchetto di exploit di eseguire e inviare un trojan il quale, a sua volta, invia un payload verso una macchina senza patch. Le definizioni degli antivirus includono le firme aggiornate del malware, ma più sofisticati aggiornamenti comportamentali ed euristici del motore forniscono all'antivirus "indizi da ricercare" (quale traffico di rete verso una determinata serie di indirizzi IP) o "eventi sospetti" quali richiamare JavaScript da un documento in un'e-mail. Tutti questi sono indizi rivelatori di un endpoint che sta per ricevere un Trojan.

STATO: **ROSSO**

***"Tutti questi sono indizi rivelatori di un endpoint che sta per ricevere un Trojan."***

## **STATO 4**: LE PATCH SONO APPLICATE ALLA MACCHINA, L'ANTIVIRUS È INSTALLATO, MA NON È AGGIORNATO

Questo stato è simile allo Stato 1, ma i criminali informatici avranno maggiore successo in quanto la maggioranza delle difese informatiche è fornita dall'installazione delle patch. La superficie di attacco è la stessa dello Stato 1, tuttavia la macchina è più suscettibile verso vulnerabilità "umana" in quanto un'intera gamma di Trojan (installati tramite e-mail di phishing) può infettare la macchina. Questo è probabilmente il secondo scenario più comune, poco dopo l'applicazione delle patch agli endpoint. Con le patch installate, il provider IT o l'MSP riducono considerevolmente la probabilità di infezione. Tuttavia, il pericolo di trojan inviati tramite e-mail permane. La combinazione di attacchi tramite e-mail di phishing e social engineering può essere condotta utilizzando famiglie di trojan più vecchi, se l'antivirus del bersaglio non è aggiornato.

STATO: **GIALLO**

*"La macchina è più suscettibile verso vulnerabilità "umana"."*

Negli Stati 3 e 4, dove l'antivirus è obsoleto, il modo migliore di agire è eseguire l'aggiornamento alle definizioni più aggiornate ed eseguire una scansione completa sugli endpoint. Vi è un'ottima probabilità che il malware possa essere stato installato quando le difese antivirus della macchina erano "abbassate". Molti utenti non ammetteranno di avere accidentalmente fatto clic su qualcosa che non dovevano, pertanto un trojan potrebbe essere in agguato sull'endpoint, in attesa di scaricare un payload tenuto a bada alle altre difese di rete.

Su sistemi per impieghi speciali, quali libri paga, contabilità e punti vendita, la rimozione di software spesso infettati, le patch settimanali e l'aggiornamento di software sensibile ad exploit, quale il citato Adobe Flash, è essenziale. Se il software non può essere rimosso, un robusto antivirus con frequenti aggiornamenti delle firme contro il malware e dotato di analisi comportamentale ed euristica offre la soluzione migliore per la protezione di questi sistemi.

Presupponendo la presenza di una formazione per la sensibilizzazione degli utenti, le situazioni precedenti dovrebbero indicare le priorità operative per MSP e provider di servizi IT. Questo lavoro deve essere concentrato sul test e sulla distribuzione delle patch in modo rapido ed efficiente sulla rete: essere ossessionati da definizioni e funzionalità dell'antivirus scelto non è certamente un'attività prioritaria.

Immediatamente dopo robusti backup dei dati, l'applicazione di patch e l'aggiornamento dovrebbero essere le priorità per impedire che il sistema cada nelle mani di criminali informatici.

# PARTE 3—RIDUZIONE DELLA SUPERFICIE DI ATTACCO E ANTIVIRUS BASATI SUL COMPORTAMENTO

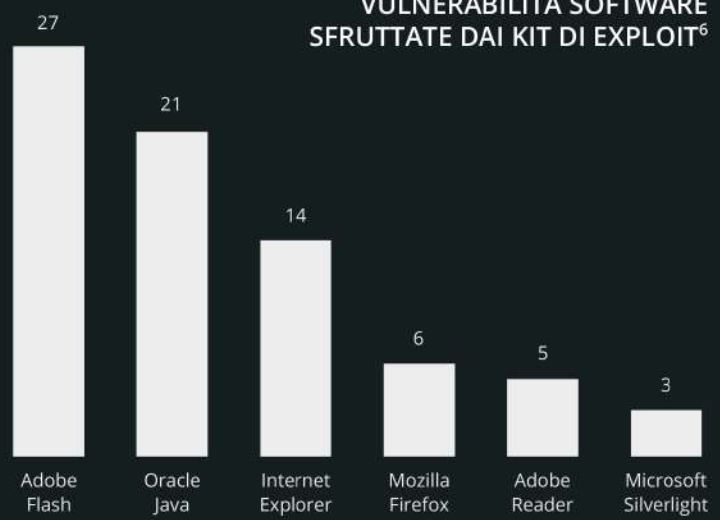
Secondo la tabella in basso a destra, se non fosse possibile impegnarsi per una rapida applicazione delle patch all'endpoint, spesso è possibile migliorare la sicurezza semplicemente rimuovendo il software che viene più spesso preso di mira. Vi sono vari motivi per i quali un'attività potrebbe non sentirsi in grado di impegnarsi in un programma di rapida applicazione delle patch, fra i quali la mancanza di un processo o di uno strumento automatizzato, ansia istituzionale verso tempo di inattività autoinflitto o mancanza di attenzione o procedure da parte del servizio IT verso questa attività.

Un approccio alla sicurezza dell'organizzazione che richieda autorizzazione manageriale per l'installazione e utilizzo dei "terribili 5" (Adobe Flash, Java, Internet Explorer, Firefox e Silverlight), può essere la chiave per l'implementazione di robusta sicurezza senza dover ricorrere a spese significative per protezioni più tecnologiche. In un ambiente aziendale, la rimozione di Adobe Flash, Java o Internet Explorer (IE), oppure l'impegno a mantenerli aggiornati con le versioni più recenti, riduce significativamente il potenziale di sfruttamento dell'endpoint.

Una workstation aziendale nella quale non vi sia Flash, Java, IE, Firefox, Adobe Reader o Silverlight attaccata da un moderno exploit potrà uscirne completamente indenne, in quanto il kit di exploit non sarà in grado di trovare una via di attacco. Questo è un risultato molto significativo per settori regolati o per organizzazioni preoccupate della confidenzialità e integrità dei loro sistemi di dati.

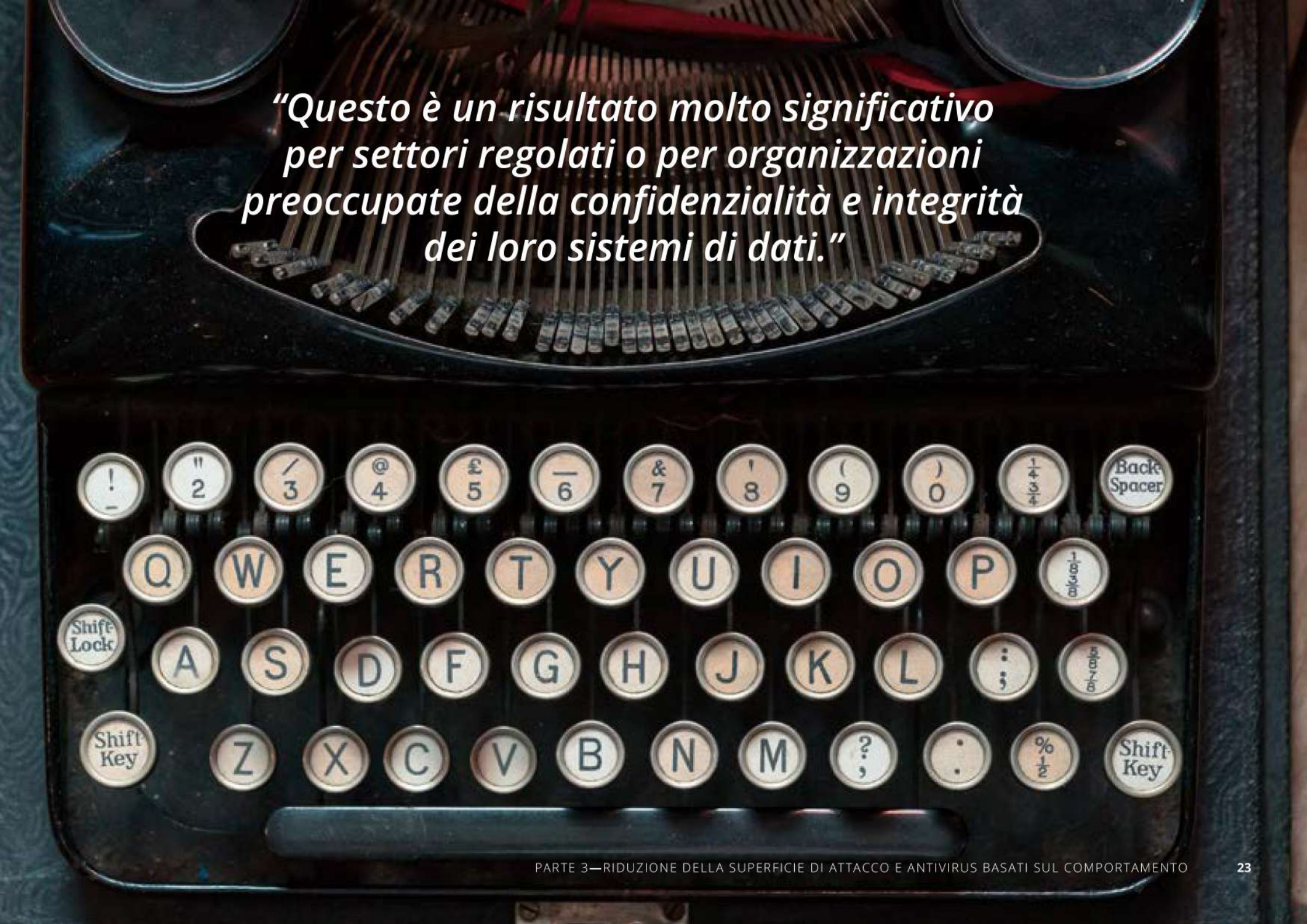
Nella Parte 1 abbiamo discusso di come le tecnologie anti-malware basate sulle definizioni, quali antivirus endpoint, filtraggio/protezione Web e scansione e-mail, combinati con formazione per la sensibilizzazione degli utenti, possano essere utili per arrestare la distribuzione di trojan e payload. Vi è anche un ruolo significativo per l'antivirus endpoint dotato di funzionalità basate sul comportamento nonché per la formazione per la sensibilizzazione degli utenti al punto di sfruttamento.

**VULNERABILITÀ SOFTWARE SFRUTTATE DAI KIT DI EXPLOIT[6]**






BERTOLDI CYBERSECURITY

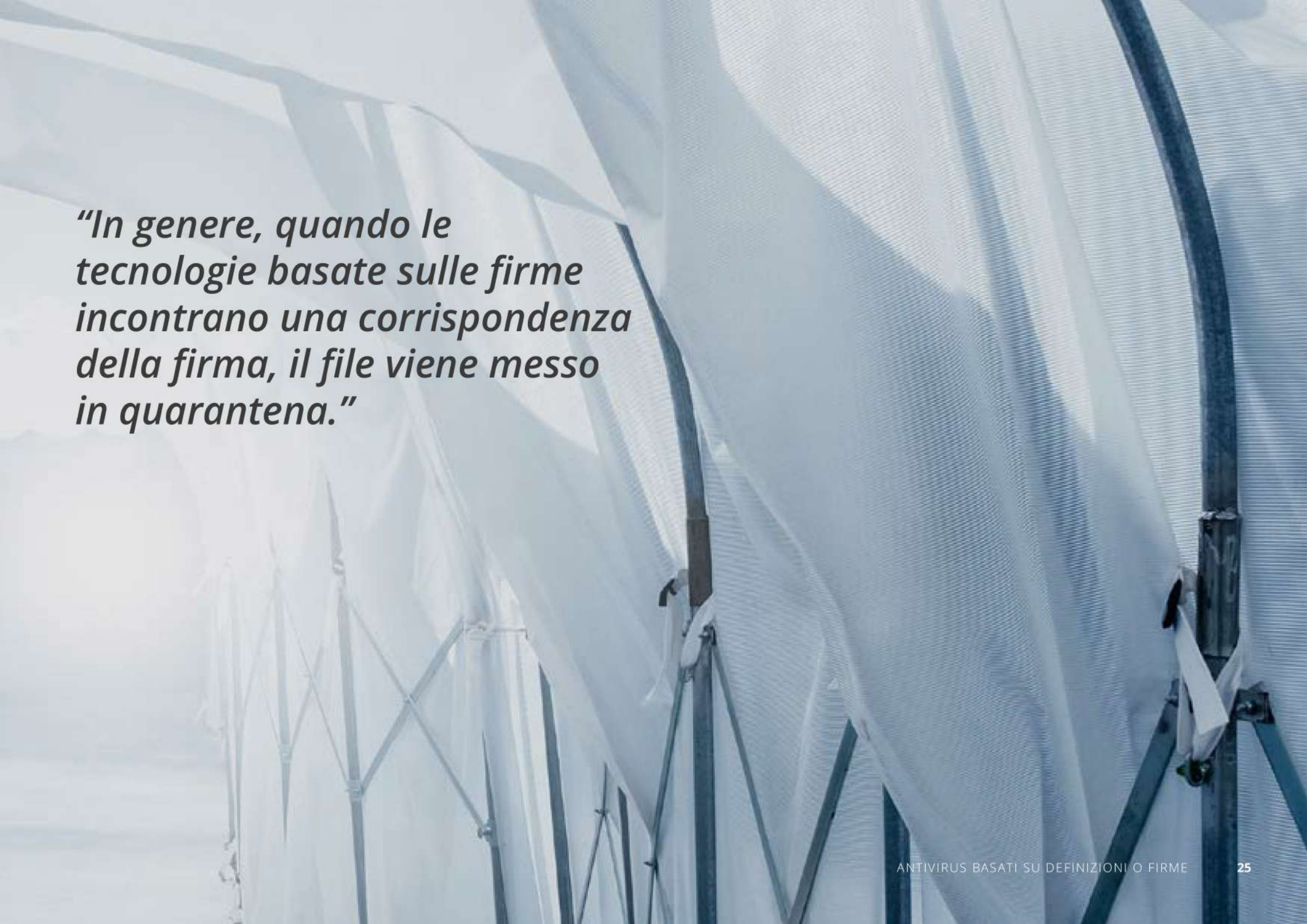


*"Questo è un risultato molto significativo per settori regolati o per organizzazioni preoccupate della confidenzialità e integrità dei loro sistemi di dati."*

# ANTIVIRUS BASATI SULLE DEFINIZIONI

Gli antivirus basati sulle definizioni (o basati sulle firme) confrontano le firme (hash MD5 o SHA-1) dei file presenti per stabilire se corrispondano ad un elenco di malware conosciuti. In funzione delle funzionalità del software, questo potrebbe analizzare l'interno del file per indizi rivelatori di malware. In genere, quando le tecnologie basate sulle firme incontrano una corrispondenza della firma, il file viene messo in quarantena.

I criminali informatici che scrivono exploit e trojan sono consapevoli che il loro malware potrebbe incontrare antivirus endpoint, pertanto spesso includono codice dannoso che disattiva l'antivirus e impedisce gli aggiornamenti o le comunicazioni di rete. In attacchi altamente specializzati, la presenza del software antivirus può essere in effetti utilizzata per installare il codice dannoso. A maggio 2016, un ricercatore della sicurezza, Tavis Ormandy, ha identificato un overflow sfruttabile nel "core del motore antivirus Symantec utilizzato nella maggior parte dei prodotti antivirus a marchio Symantec e Norton".[6]



*“In genere, quando le tecnologie basate sulle firme incontrano una corrispondenza della firma, il file viene messo in quarantena.”*

# ANTIVIRUS BASATI SUL COMPORTAMENTO

Gli antivirus basati sul comportamento elaborano segnali caratteristici di malware, quindi li confrontano con un elenco di comportamenti dannosi conosciuti. Ad esempio, in base all'elenco di pacchetti software vulnerabili sopra indicati, un documento aperto da un'e-mail che richiami JavaScript o Adobe Flash potrebbe essere considerato come "comportamento molto sospetto o simile a malware".

Il rilevamento basato sul comportamento è necessario in quanto molti creatori di malware hanno iniziato ad utilizzare tecniche di oscuramento quali segmenti di codice polimorfico o crittografato, per i quali è molto difficile creare una firma hash. Pertanto, un modo più semplice per identificarli è rilevare un particolare schema di comportamento.

Ovviamente, è molto consigliabile disporre di più livelli di difesa per intercettare la diffusione di exploit, trojan e payload prima che arrivino all'endpoint.

Tuttavia, se tali difese sono violate, la combinazione di rimozione del software preso di mira (riduzione della superficie di attacco), antivirus con motore basato sul comportamento, gestione aggressiva delle patch e formazione per la sensibilizzazione degli utenti può contribuire a scongiurare gli attacchi più persistenti, nonché visite accidentali a siti Web pericolosi.

# PARTE 4—MESSA IN SICUREZZA DELLE COMUNICAZIONI DA LAN A WAN

*"Dopo il suo arrivo ... il malware deve entrare in contatto con una rete bot di comando e controllo (C2) per ricevere istruzioni."*

BERTOLDI
CYBERSECURITY

Dopo il suo arrivo, o più specificamente dopo l'installazione del trojan sull'endpoint, il malware deve entrare in contatto con una rete bot di comando e controllo (C2) per ricevere istruzioni. Questa è forse una delle aree dove è più semplice implementare architetture firewall, registrazioni e controlli di rete per rilevare o prevenire la compromissione dell'endpoint.

L'infrastruttura C2 è fornita da server e workstation precedentemente infettati o compromessi. Tali reti possono essere affittate come sorgenti Crime as a Service (CaaS) oppure create specificamente dai criminali informatici per supportare un attacco trojan. Praticamente, tutto il moderno malware deve "risalire" ad una sorgente C2 per eseguire il download di un attacco con payload. In alcuni casi, parametri dettagliati sul successo dell'infezione, distribuzione geografica e informazioni dettagliate di sistema sono catturati per scopi di marketing CaaS. Proprio così: i criminali informatici cercano di raccogliere quanti più dati possibili su infezioni riuscite, così come le aziende moderne raccolgono informazioni su visite al sito Web e interazioni con i clienti.

Prendiamo, ad esempio, la comunicazione di rete "tipica" di un trojan che dispone di un dominio C2 hardcoded *twinpeakshockey.com* (vedere di seguito). Il trojan risale a questo dominio utilizzando una query DNS standard, quindi tenta di eseguire "GET" per il payload ransomware *GORsjo.exe* dal server C2.

In questo caso la comunicazione non è stata condotta di nascosto, né era crittografata (https). La maggior parte dei prodotti di filtraggio Web identificherebbero rapidamente l'indirizzo IP (69.89.31.222) o il dominio come sito pericoloso da visitare da parte di un endpoint. Tenete presente che protezioni DNS quali Open DNS e altri prodotti, forniscono un prezioso livello in grado di agire persino contro il malware che utilizza https per le comunicazioni. Inoltre, il download di un eseguibile (.exe) su un endpoint è un'azione che il firewall o un prodotto di protezione Web dovrebbe auspicabilmente bloccare.

## ESEMPIO DELLA COMUNICAZIONE DI UN TROJAN CON UNA RETE C2

| | | | | |
|---|---|---|---|---|
| 11 4.177967 | 8.8.8.8 | 172.16.25.137 | ICMP | Echo (ping) reply (id=0x0200, seq(be/le)=7168/28, ttl=128) |
| 12 25.196459 | 172.16.25.137 | 172.16.25.2 | DNS | Standard query A twinpeakshockey.com |
| 13 25.674355 | 172.16.25.2 | 172.16.25.137 | DNS | Standard query response A 69.89.31.222 |
| 14 25.676099 | 172.16.25.137 | 69.89.31.222 | TCP | iascontrol-oms > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 15 25.676823 | 69.89.31.222 | 172.16.25.137 | TCP | http > iascontrol-oms [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 |
| 16 25.676879 | 172.16.25.137 | 69.89.31.222 | TCP | iascontrol-oms > http [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| 17 25.677229 | 172.16.25.137 | 69.89.31.222 | HTTP | GET /GORsjo.exe HTTP/1.1 |
| 18 25.677524 | 69.89.31.222 | 172.16.25.137 | TCP | http > iascontrol-oms [ACK] Seq=1 Ack=188 Win=64240 Len=0 |

*"La tecnica di spostamento laterale è stata progettata per creare trappole informatiche che rendono difficile per il trojan uscire dalla rete o infettare altri endpoint."*



BERTOLDI
CYBERSECURITY

A questo punto, le funzionalità comprendono segmentazione della rete, regole di uscita per il firewall e un sistema di gestione della sicurezza delle informazioni e degli incidenti (SIEM)/ una soluzione di gestione dei registri con funzionalità di avviso. Le regole del firewall, in particolare la necessità di aprire porte esterne, devono mappate a servizi aziendali.

Le seguenti regole concettuali di base del firewall aiutano a rilevare e prevenire le comunicazioni C2, nonché ulteriori sfruttamenti della rete utilizzando una tecnica denominata spostamento laterale. Queste regole sono progettate per creare trappole informatiche che rendono difficile per il trojan uscire dalla rete o infettare altri endpoint.

- Regole di rifiuto per subnet di workstation: nessun DNS, IRC, NTP, FTP, ICMP, SMTP, SNMP, RDP esterno
- Regole di rifiuto per amministratori (aperte come necessario): nessun DNS, IRC, NTP, FTP, ICMP, SMTP, SNMP, RDP esterno
- Regole di rifiuto per subnet di stampanti: rifiutare tutto. Nessuna stampante su Internet.
- Regole di rifiuto per i server. Solo DNS, NTP per IP specifici, HTTPS.

Come si può vedere, limitare le porte, i protocolli e le comunicazioni interne ed esterne nella rete a livello di architettura può prevenire e rilevare la presenza di attività di rete sospette o non autorizzate.

Se queste regole del firewall sono implementate e un trojan invisibile tenta di utilizzare il protocollo Internet Relay Chat (IRC) per raggiungere l'infrastruttura C2, questa attività sarà bloccata e se è stato implementato un SIEM, verrà attivato un avviso.

## ESEMPIO DI SPOSTAMENTO LATERALE

# LIVELLI ESSENZIALI NELLA VOSTRA DIFESA

Come altro esempio, "rifiutare" regole in rapporto a Simple Mail Transport Protocol (SMTP) su workstation rende più difficile per i criminali informatici utilizzare un endpoint compromesso come bot SPAM per diffondere ulteriori attacchi phishing tramite e-mail con allegati trojan.

Utilizzando una combinazione di regole in uscita per il firewall, segmentazione di rete e un SIEM per catturare informazioni di registro e avvisare della presenza di attività sospette, i tentativi del trojan di infettare e comunicare internamente ed esternamente sarà scoperto o impedito.

Per gli MSP e i provider IT, sviluppare un'architettura di rete segmentata standard e un pacchetto di regole di uscita per il firewall per il proprio cliente, vale il tempo e lo sforzo. In molti casi, la capacità di segmentare la rete e scrivere regole di uscita per il firewall può essere raggiunta con l'infrastruttura esistente. In unione con un SIEM per monitoring e ad avvisi relativi ad endpoint che tentano di violare una regola del firewall, l'MSP o il provider IT può rapidamente identificare il colpevole e agire di conseguenza.

*"Per gli MSP e i provider IT, sviluppare un'architettura di rete segmentata standard e un pacchetto di regole di uscita per il firewall per il proprio cliente, vale il tempo e lo sforzo."*

# PARTE 5—AZIONI DELL'ULTIMO ISTANTE E PULIZIA

Se si è ricevuto un exploit, la workstation è compromessa da un Trojan, sono stabilite comunicazioni in uscita e il payload è stato diffuso, allora si stanno per verificare problemi.

Nella situazione ideale dell'analisi della Cyber Kill Chain, le difese in ciascuna fase avrebbero fornito all'endpoint più opportunità per eludere la fase finale della compromissione, quando il payload viene eseguito. Per la grande maggioranza di SMB/SME, questo è ora un attacco ransomware.

Il malware varia in termini di qualità e funzionalità, da appena funzionante con effetti molto evidenti sul sistema, fino ad essere invisibile con subdoli effetti sul sistema. Nel caso di ransomware, non solo gli effetti sul sistema sono evidenti (ad esempio, file crittografati), ma l'attività è anche altamente rilevabile con sistemi euristici.

Se tutto va per il verso giusto, l'esecuzione di un attacco ransomware non è un'attività "normale". In generale, le workstation in un ambiente commerciale si comportano in modo prevedibile. Quando i cicli di CPU aumentano improvvisamente a causa di un processo e restano elevati e i file locali o in una condivisione di rete iniziano ad essere letti e modificati, un buon antivirus euristico potrà interrompere o chiudere il processo che ha causato questa improvvisa attività, in particolare se tale attività sembra essere sostenuta.

Questi sono gli indizi rivelatori che il rilevamento euristico di malware tenta di cercare. Come categoria di attacco, il ransomware è abbastanza palese da una prospettiva di sistema. Persino a livello di rete vi sarà un enorme incremento del traffico di dati e delle richieste di lettura/scrittura dall'endpoint infetto.

*“Nella situazione ideale dell’analisi della Cyber Kill Chain, le difese in ciascuna fase avrebbero fornito all’endpoint più opportunità per eludere la fase finale della compromissione.”*

# LINEE DI DIFESA DELL'ULTIMO ISTANTE

Persino in questa fase, non tutto è perduto. Vi sono comunque misure che possono essere adottate per limitare l'impatto dell'esecuzione del ransomware. L'utilizzo di Oggetti Criteri di gruppo (GPO) o di un'applicazione di terze parti per bloccare le directory %App/Data e %App/User e impedire l'esecuzione di file che si trovino in queste directory è un ottimo approccio. Per ulteriori informazioni, rivolgetevi al Ransomware Prevention Kit di Third Tier.[8]

Per ambienti Windows Active Directory più recenti, anche l'implementazione di whitelist delle applicazioni con Applocker o con un'applicazione di terze parti può fornire una difesa contro l'esecuzione del payload del ransomware. Per ulteriori approfondimenti, consultate la nota 9 nella sezione dei riferimenti, dove si discute l'utilizzo di AppLocker contro il ransomware. Per il suo funzionamento, gli utenti non devono possedere privilegi di amministratore di domini o di amministratore locale.

Se un utente sospetta che un attacco ransomware sia in atto, in conseguenza all'apertura di un allegato e-mail infetto o alla visita di un sito Web compromesso, la formazione deve includere l'interruzione dell'alimentazione del sistema o tenere premuto il pulsante di alimentazione fino allo spegnimento del computer. Se l'infezione non si è diffusa al server vero e proprio e il ransomware è in esecuzione sulla workstation, questa azione può evitare che molti file siano crittografati. I tecnici IT devono scollegare la macchina, senza dimenticare di disabilitare la modalità wireless, dalla rete dell'ufficio prima che sia sicuro accenderla nuovamente.

Quando si ha a che fare con un attacco ransomware, vi sono due componenti da considerare: primo, l'endpoint infettato che, se acceso, inizierà ad infettare i file quasi immediatamente dopo l'avvio (se ancora connesso alla rete) e, secondo, i file crittografati stessi.

*"Persino in questa fase avanzata del processo, non tutto è perduto."*

*“È consigliabile preservare la macchina per un esame professionale da parte di un team di Digital Forensic Incident Response (DFIR) o dalle forze dell’ordine”.*

Sull'endpoint infetto è necessario mitigare l'exploit (applicando patch o rimuovendo il software sfruttato), rimuovere il trojan e rimuovere il payload o il ransomware. Se uno di questi componenti rimane, vi sarà la possibilità che la macchina si colleghi ad Internet, si infetti nuovamente, esegua nuovamente il download del payload e l'attacco potrà riavviarsi. Una reinstallazione completa da una "gold image" .iso con script o da un'immagine valida nota da un supporto sicuro (non un recupero locale) può essere l'unico modo per rimuovere un'infezione in stato avanzato.

Un endpoint infetto può contenere preziose informazioni forensi su come la vostra sicurezza su più livelli sia stata aggirata e può includere le informazioni sui criminali informatici. Se l'attacco ha avuto un impatto significativo sulla vostra organizzazione, è consigliabile preservare la macchina per un esame professionale da parte di un team di Digital Forensic Incident Response (DFIR) o dalle forze dell'ordine.

Se intendete intraprendere la strada dell'utilizzo di un sistema isolato o offline, potrebbe essere consigliabile verificare la presenza di traffico sospetto sulla rete utilizzando Wireshark (in particolare per http o https) da una macchina ripulita recentemente prima di mandarla nuovamente in servizio. Purtroppo, il payload di ransomware più avanzato offre funzionalità di sottrazione di credenziali, pertanto tutte le password, comprese quelle memorizzate nei cookie del browser, possono essere compromesse. Pertanto sarà necessario modificare tutte le password.

# RICHIESTA DI BACKUP

*"Prestare attenzione quando si aggiornano file crittografati come dati campione."*



BERTOLDI CYBERSECURITY

Analogamente ai file crittografati, è auspicabile la vostra soluzione di backup basata su cloud sia in grado di eseguire rapidamente il restore dei file: il ransomware spesso tenta di distruggere qualsiasi backup locale.

Sfortunamente, in seguito ad un attacco ransomware riuscito, molte attività (o i loro MSP o provider IT) scoprono che la strategia di backup del cliente era tutto tranne robusta. Per un'azienda questo potrebbe essere catastrofico.

Se la vostra attività o quella del vostro cliente subisse un attacco ransomware, Heimdal Security offre una fantastica risorsa con circa 100 programmi online di decrittografia.[10] È decisamente una pagina Web da salvare. Tuttavia, un consiglio: prestate attenzione durante l'upload di qualsiasi file crittografato necessario per la decrittazione: non utilizzate nulla di confidenziale.

# PAGARE O NON PAGARE

*"È chiaro che pagare un riscatto non è nel migliore interesse di nessuno, tranne per i criminali informatici."*



BERTOLDI CYBERSECURITY

Nonostante le prime affermazioni controverse dell'FBI, è chiaro che pagare un riscatto non è nel migliore interesse di nessuno, tranne per i criminali informatici. Le uniche circostanze nelle quali si potrebbe considerare pagare il riscatto sono quelle nelle quali i dati sono incredibilmente preziosi per l'azienda e per le sue attività o se anni di ricerche sono in gioco. In entrambi i casi, svolgete un approfondito esame sul perché i dati non fossero protetti contro un attacco ransomware in primo luogo.

Tenete presente che coloro i quali hanno inviato, sfruttato e installato un trojan sul vostro sistema e quindi scaricato ed eseguito il ransomware sono criminali. Se è presente un'opportunità di estorcere ulteriore denaro, i criminali informatici non rinunceranno a tale opportunità, pertanto non spiegate quanto preziosi siano tali dati o il prezzo del recupero salirà ulteriormente. L'ultima cosa che è consigliabile fare è finanziare una migliore e più efficace versione di ransomware.

Tutti gli incidenti che coinvolgono ransomware sono crimini informatici e devono essere denunciati. Per denunciare un crimine informatico, contattate l'ufficio FBI locale[11] o sporgete denuncia presso l'Internet Crime Complaint Center.[12] Nel Regno Unito contattate Action Fraud,[13] nella UE contattate Europol[14] e in Australia contattate Acorn.[15]. Queste istituzioni vi consentiranno di reagire ai criminali informatici.

# CONCLUSIONE

Il contenuto delle Indicazioni di compromissione presentato da SolarWinds® MSP aiuterà nell'educazione di attività, MSP e provider IT nell'ambito delle meccaniche di un moderno attacco malware e i passaggi e le tecnologie che possono mitigare i danni.

Un attacco può avvenire in pochi secondi o minuti, in funzione di molti fattori ma l'implementazione delle difese per intercettare attività dannose tramite le fasi della Cyber Kill Chain e il potenziamento di tali difese con formazione di sensibilizzazione degli utenti, gli attacchi ransomware e la compromissione degli endpoint possono essere evitati.

# RIFERIMENTI


1 **Cyber Kill Chain Lockheed Martin®**
http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

2 **Verizon Data Breach Investigation Report 2016**
http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

3 https://blog.barkly.com/phishing-statistics-2016

4 https://www.alienvault.com/blogs/security-essentials/clicking-with-the-enemy

5 **Recorded Future**
https://www.recordedfuture.com/

6 **Digital Shadows**
https://www.digitalshadows.com

7 **Rapporto di Tavis Ormandy**
https://bugs.chromium.org/p/project-zero/issues/detail?id=820

8 **Third Tier Ransomware Kit**
http://www.thirdtier.net/ransomware-prevention-kit/

9 **Technet Blog**
https://blogs.technet.microsoft.com/askpfeplat/2016/06/27/applocker-another-layer-in-the-defense-in-depth-against-malware/

10 **Heimdal Security**
https://heimdalsecurity.com/blog/ransomware-decryption-tools/

11 **FBI**
https://www.fbi.gov/contact-us/field-offices

12 **IC3**
https://www.IC3.gov

13 **Action Fraud**
http://www.actionfraud.police.uk/report_fraud

14 **Europol**
https://www.europol.europa.eu/report-a-crime/report-cybercrime-online

15 **Acorn**
https://report.acorn.gov.au/