White Paper

La sicurezza a strati

LA CYBERSICUREZZA, UNO STRATO DOPO L'ALTRO

Il tema della **sicurezza IT multi-layer o multi-strato** è oggi ampiamente discusso, e per un ottimo motivo.

Sgombero subito il campo dagli equivoci: **non si tratta di una trovata di marketing** degli operatori del settore per moltiplicare le soluzioni da proporre ai loro clienti, **né del tentativo di colmare i possibili gap di un'applicazione di sicurezza** (per esempio un antivirus) affiancandone altre due o tre simili ma di altri produttori nella speranza che ciò che sfugge a una venga invece bloccato da un'altra.

Il problema è che la sicurezza IT non fa altro che seguire un'evoluzione allineata a quella dei metodi utilizzati per gli attacchi.

Poiché i "cattivi" sfruttano arsenali sempre più diversificati e sofisticati, va da sé che la protezione dei sistemi informatici delle aziende, compresa la tua, **debba mettere in campo un corrispondente mix di sistemi di difesa**.

Quando parliamo di **"strati" di sicurezza ci riferiamo allora a soluzioni diverse tra loro**, **ciascuna di esse responsabile di uno specifico mattoncino della muraglia difensiva** informatica con la quale cerchi di ripararti dai malintenzionati.

E quante motivazioni hanno questi malintenzionati per colpirti!

Indipendentemente dal ramo di attività o dalle dimensioni del business, oggi che la vita personale, professionale ed economica di tutti si svolge in gran parte all'interno di una dimensione digitale**, un cybercriminale ha solo l'imbarazzo della scelta** per arricchirsi illecitamente a tue spese. Sottrazioni di dati, furti di identità, ricatti, spionaggio industriale, infiltrazione di reti e sistemi... ecco il menu dei nuovi pericoli del XXI secolo, talmente diffusi da non essere più materia confinata a qualche rivista specializzata ma frequente oggetto di notizie sui normali organi di informazione generalisti.

Nessuno ne è più immune: la cybersicurezza è diventata una necessità per tutti, dal momento che **i dati sono il bottino più appetitoso che possa esistere oggi**.

Perché allora non è più sufficiente il buon, vecchio antivirus piuttosto che il firewall o qualsiasi altra singola soluzione che sei stato abituato a usare finora?

Semplicemente perché la tua "impronta digitale" nel mondo è ormai talmente ampia e multiforme che offre ai criminali **un incredibile ventaglio di opportunità per colpire** dove e quando non te lo aspetti aggirando le vecchie difese tradizionali.

Dedica qualche minuto per fare un **veloce inventario**:

- quanti sono i PC, i laptop, i tablet, i telefonini e gli altri dispositivi smart che usi per il tuo lavoro e la tua vita personale?
- Quante informazioni mantieni internamente alla tua azienda e quante invece affidi ai vari servizi e applicativi in cloud?
- Quante sono le caselle email che utilizzi? E cosa ne dici dei servizi di messaggistica su smartphone e su PC?
- Quante ore trascorri navigando sul Web, quanti sono i siti che possiedono le tue credenziali e i tuoi dati personali?

Come vedi, l'uso dell'informatica si è talmente diversificato che **diventa sempre più difficile tenere traccia di tutto quanto**. I malintenzionati lo sanno e ne approfittano, diversificando a loro volta tecniche e metodi.

Proviamo infatti a considerare tutto quel che c'è nella cassetta del perfetto scassinatore informatico di oggi: per lo meno ci troveremo una serie di spyware, adware, bot, programmi per registrare quanto digitato alla tastiera, rootkit, virus, trojan, worm e app fasulle.

Tutte cose che in genere ci vengono recapitate per posta elettronica tramite campagne di phishing o spear-phishing, queste ultime estremamente personalizzate grazie al patrimonio di informazioni personali che quotidianamente disseminiamo in maniera più o meno consapevole su Internet.

Ma ci sono anche **altri canali di ingresso** come quelli forniti da **siti Web compromessi** che colpiscono l'ignaro visitatore scaricando sul suo browser **script indesiderati**, primo passo per assumere il controllo del computer e magari della rete aziendale a cui esso è connesso.

Non parliamo poi delle **vulnerabilità di applicazioni e sistemi operativi**, le più pericolose delle quali sono quelle cosiddette "zero-day" o del giorno zero, così chiamate perché nessuno ne conosce l'esistenza fino al giorno in cui vengono scatenate sul campo per attaccare utenti e aziende.

Capirai facilmente come **non sia possibile fermare un frullato di tutto questo con un'unica soluzione** o, peggio, con strumenti pensati e realizzati in un tempo passato nel quale lo scenario della sicurezza era decisamente più semplice e lineare. Né puoi pensare di isolare sistemi e applicazioni tagliando i ponti con l'esterno, perché equivarrebbe a tagliar fuori dal mondo la tua attività o addirittura la tua vita personale.

Quel che puoi fare invece è che siano capaci di coordinarsi tra loro mediante capacità di analisi e correlazione degli eventi in modo da ottenere quella che viene chiamata "visione olistica" della difesa informatica, ovvero la capacità di percepire l'insieme di segnali differenti che presi singolarmente non sarebbero fonte di preoccupazione ma che, messi in fila e inquadrati nel giusto contesto, possono far scattare tutti gli allarmi e le contromisure del caso salvaguardando i tuoi dati.

La sicurezza multi-strato non è altro che questo, ed è qualcosa alla quale non è più possibile rinunciare.

UN LABIRINTO DI DIFESE PER SCORAGGIARE GLI ATTACCANTI

Cos'è allora questa famigerata sicurezza multi-strato? Come si concretizza nella pratica?

Per capirne il funzionamento generale prova a **considerare la faccenda dal punto di vista di un attaccante**.

Il lavoro di un cybercriminale non è quello che si vede nei film, dove l'hacker di turno si collega al computer della vittima, indovina la password del sistema, scarica l'intero patrimonio informativo di una mega-azienda su una chiavetta USB, spegne e se ne va.

Piuttosto, si tratta di un paziente lavoro di composizione di tanti piccoli tasselli fino a comporre il quadro generale.

Inizia magari con un messaggio di phishing per dirigere la vittima su un sito compromesso dal quale verrà automaticamente scaricato e **installato un programma** che tenterà di analizzare l'ambiente informatico nel quale si trova per rilevare vulnerabilità e tenere aperto un canale di comunicazione con l'attaccante.

Da qui le strade possono divergere a seconda degli obiettivi desiderati: crittografare i dati della vittima per chiedere un riscatto, sfruttare le risorse IT per fare mining di criptovalute, inviare spam o scatenare campagne DDoS, spiare singole persone per preparare le cosiddette "truffe del CEO", appropriarsi di password e credenziali per svuotare conti bancari o carte di credito...

La buona notizia è che in genere un cybercriminale si specializza su un unico obiettivo, per esempio il ransomware. La cattiva notizia è che, **una volta raggiunto il proprio obiettivo, lo stesso cybercriminale può "vendere" la sua vittima ad altri colleghi specializzati su altri illeciti**, un po' come fanno certe bande di sequestratori.

Fatto sta che un cybercriminale deve vedersela con una quantità notevole di elementi: fisici, tecnologici e anche umani (un phishing efficace richiede una buona conoscenza della vittima e delle tecniche di persuasione psicologica). Proteggere ciascuno di questi elementi con una soluzione ad hoc permette di ottenere la sicurezza multi-strato di cui stiamo parlando.

Una breve **panoramica dei diversi strati** della sicurezza ti aiuterà a capire meglio l'ambito di cui stiamo parlando.

STRATO DELL'UTENTE UMANO

Il primo, fondamentale livello di una strategia di sicurezza multi-strato completa **corrisponde a quello che probabilmente è l'anello più debole dell'intera catena: l'essere umano**. Disattenzione, credulità, errori, interesse personale possono provocare notevoli disastri all'interno di un'azienda e del suo ambiente informativo – spesso anche senza bisogno di un cybercriminale che muova i fili dall'esterno.

Per questo **occorre formare e sensibilizzare se stessi e il proprio personale** aziendale in modo efficace e coinvolgente. Le iniziative migliori sono quelle che si integrano nel normale corso delle attività lavorative e che prevedono simulazioni periodiche basate sulle ultime tendenze degli attacchi che sfruttano la buona fede degli individui.

Grande attenzione in questo strato deve essere rivolta alla **corretta gestione della posta elett**ronica, il principale canale usato per contattare le potenziali vittime. Dalle **applicazioni che bloccano lo spam a quelle che impediscono l'apertura di allegati e link pericolosi**, fino alle semplici **regole di comportamento per gli utenti**, c'è tutta una serie di soluzioni che possono essere dispiegate per minimizzare i rischi spediti per email.

L'obiettivo è quello di allenarsi a sentire la puzza del phishing quando ancora è sufficientemente distante. Non hai idea di quanti credano ancora a sconosciuti desiderosi di regalare milioni di dollari, comunicare vincite a lotterie e concorsi o piazzare ricchi ordinativi di merce... spesso dettagliati in presunti "documenti" allegati che fanno scattare il trappolone.

STRATO FISICO

Va bene che il cloud ci fa pensare a un'informatica dematerializzata ed eterica, ma si tratta di un'illusione: alla fine abbiamo sempre a che fare con computer, server e storage che da qualche parte devono pur risiedere. **Che siano all'interno della tua azienda piuttosto che in qualche data center professionale, l'ambiente fisico dove si trovano le tue risorse IT dovrebbe essere dotato delle misure necessarie a evitare sorprese** che derivano in genere da due categorie di problemi:

- **disastri ambientali**: per perdere i dati non sempre c'è bisogno di un cybercriminale. Allagamenti e incendi sono più frequenti di quanto si pensi, ma con le giuste contromisure le probabilità che possano creare danni si abbattono radicalmente. L'importante è pensarci per tempo.

- **accessi non autorizzati**: alle attrezzature IT non dovrebbe fisicamente avvicinarsi nessuno che non abbia un buon motivo per farlo. Ci sono sistemi di controllo basati su tecniche biometriche che risultano molto efficaci, come dimostra il loro utilizzo da parte dei data center più attenti alla sicurezza.

Porte blindate, riprese video, registrazione degli ingressi e delle uscite, sistemi antincendio e antifurto possono sembrare un investimento eccessivo ma sono quello che spesso fa la differenza tra un'azienda che continua a lavorare e una che è costretta a chiudere i battenti.

Se invece preferisci affidare i tuoi sistemi a un data center terzo, fatti consegnare il documento che spiega le misure di sicurezza esistenti e le procedure di accesso adottate; se ti è possibile, fai anche una visita di persona alla struttura di cui intendi avvalerti.

STRATO DEGLI ENDPOINT

Con il nome **"endpoint" si intendono tutti quei dispositivi che si trovano nelle mani degli utenti**. Fino a qualche tempo fa corrispondevano ai PC aziendali ma oggi, tra laptop, tablet, smartphone e computer di casa, la famiglia degli endpoint **si estende al di fuori del perimetro tradizionale comprendendo anche apparecchi di proprietà personale**.

Questo ha semplificato la vita dei malintenzionati, che ora possono scavalcare le protezioni che circondano le reti professionali sfruttando, per esempio, le vulnerabilità di un router domestico o il comportamento poco attento di un utente collegato al wi-fi di un Internet cafè per ottenere un pratico cavallo di Troia con cui entrare in azienda.

Non parliamo poi dei frequenti **smarrimenti di computer e dispositivi elettronici**, che nonostante il loro valore costituiscono per esempio il 40% di tutti gli oggetti dimenticati dai proprietari sulle Frecce Trenitalia[1]. Persino utenti alle prese con dati estremamente sensibili non sono immuni ad abbandonare i propri endpoint in giro: i dipendenti del Ministero britannico della Difesa perdono almeno un laptop al giorno[2], e scommettiamo che se altre nazioni fossero altrettanto trasparenti nell'ammettere problemi del genere ne sentiremmo delle belle anche altrove.

Per fortuna **un endpoint può essere rinforzato con diversi accorgimenti** che vanno dalla cifratura delle informazioni memorizzate al suo interno al blocco delle porte USB, dal controllo delle applicazioni autorizzate alla protezione con antivirus/antimalware e così via.

In particolare, **gli endpoint possono trarre grande beneficio dalle recenti tecnologie che tengono monitorato costantemente il comportamento di utenti e applicazioni per evidenziare (e bloccare) eventuali attività sospette**, aprendo così una sorta di ombrello protettivo su una vasta gamma di pericoli cui sono soggetti gli apparecchi smart che ci piace (o che dobbiamo) utilizzare.

Utilissime anche le soluzioni che permettono alle aziende di gestire il parco degli endpoint tenendo traccia delle risorse installate su ciascuno di essi, lo stato degli aggiornamenti, le autorizzazioni concesse e così via. In caso di smarrimento del dispositivo o di uscita dell'utente dall'azienda, soluzioni di questo tipo permettono di bloccare e cancellare facilmente tutto quel che occorre evitando così grattacapi più grossi.

1 https://www.ecodibergamo.it/stories/bergamo-citta/smemorati-sul-treno-si-perde-di-tuttoce-chi-lascia-le-scarpe-e-la-fede-nuziale_1200709_11/

2 https://www.dailymail.co.uk/news/article-4057056/MoD-staff-lose-one-laptop-day-Nearly-800-containing-sensitive-information-lost-stolen-2015-election.html

STRATO DELLA RETE

In ogni epoca e area geografica, i banditi hanno sempre fatto in modo di intercettare le loro vittime lungo le strade che dovevano percorrere. Con il cybercrimine la cosa non è molto diversa, se non che le strade in questione esistono oggi in forma virtuale sotto forma delle reti che collegano un sistema all'altro attraverso percorsi spesso tortuosi che passano attraverso una moltitudine di server e apparecchiature di proprietà di svariati operatori.

Dal punto di vista di un attaccante, **la rete è un obiettivo che fa gola** perché può essere usata per due scopi:

- **spiare le informazioni che vi scorrono attraverso** (il furto perfetto, perché i dati arrivano comunque a destinazione senza che vi sia traccia dell'avvenuta sottrazione);
- **penetrare nei sistemi della vittima nascondendosi all'interno del traffico** che legittimamente essa riceve.

Ecco perché grandi risorse vengono dedicate dai cybercriminali per trovare vulnerabilità in questo campo. L'industria dell'informatica lo sa bene e propone adeguate contromisure. Vediamone alcune.

- ***VPN Virtual Private Network***: Una **VPN** non è altro che una sorta di tunnel riservato "scavato" all'interno delle normali comunicazioni Internet. Una rete VPN permette di stabilire una connessione cifrata (e quindi potenzialmente inviolabile) tra due interlocutori, per esempio il tuo smartphone e il server della contabilità che si trova nella tua azienda. Qualunque sia il percorso che la comunicazione deve compiere dallo smartphone al server – percorso che ricordiamo non è quasi mai diretto – un eventuale osservatore non autorizzato non avrà modo di decifrarne i contenuti salvaguardando così la riservatezza delle informazioni.
- ***Firewall***: Un apparecchio fisico o virtuale che filtra i pacchetti di rete in ingresso e in uscita secondo regole di traffico prestabilite. Ciò permette di restringere le attività di rete a determinate porte e determinati servizi così da minimizzare i rischi. Un po' come se decidessimo di murare tutte le finestre di casa nostra lasciando aperte solamente quelle che riteniamo indispensabili, magari tenendole sotto controllo.
- ***IPS Intrusion Prevention System***: Un'evoluzione del firewall è l'IPS, che oltre alle regole di traffico si occupa di analizzare anche i contenuti effettivi dei pacchetti di rete in transito – sempre che non siano cifrati tramite protocolli sicuri come HTTPS, SSH, SFTP e simili – bloccando tutti quelli sospetti. Quando un IPS si limita a segnalare i pacchetti sospetti a solo scopo di reportistica senza bloccarli prende il nome di IDS, Intrusion Detection System.
- ***NGFW Next Generation Firewall***: Il mix tra firewall, IPS e IDS nato per semplificare la protezione delle reti con un unico apparato completo che può essere potenziato con funzioni supplementari come il rilevamento del malware. Esistono versioni più semplici e meno costose rivolte alle piccole e medie aziende, che prendono il nome di UTM o Unified Threat Management.

STRATO DELLE APPLICAZIONI

Si sa che i cybercriminali prosperano grazie alle **vulnerabilità del software**, i famosi "bug".

E cosa sono le applicazioni, se non prodotti software che tutti noi installiamo e adoperiamo fidandoci nella capacità dei loro autori di minimizzare (azzerare non è matematicamente possibile) la presenza di bug?

In azienda si trovano in genere **tre tipologie di applicazioni**: **quelle commerciali** necessarie allo svolgimento del business, come i pacchetti per l'ufficio, gli ERP, la contabilità, i software di progettazione, i database e così via; **quelle realizzate su misura dal personale IT** aziendale o da consulenti esterni; e **quelle che gli utenti si procurano per necessità personali**, specie sui loro dispositivi smart, fuori dal controllo dell'IT.

Per prima cosa è necessario **assicurarsi che tutte le applicazioni siano sempre adeguatamente aggiornate**, e i prodotti che si incaricano di questo permettono anche di gestire il patching dei sistemi operativi e dei driver dei dispositivi, altro elemento essenziale in un approccio completo alla sicurezza.

Chiaramente non è possibile controllare e certificare in maniera pratica e definitiva l'intero corredo di applicazioni, e allora come spesso accade ci si deve rivolgere alla tecnologia perché tenga a bada se stessa implementando degli appositi **scanner di vulnerabilità**, soluzioni concettualmente simili a quelle di monitoraggio comportamentale presenti sugli endpoint che possono aiutare a mettere in evidenza – ma la neutralizzazione è fuori dalla loro portata – falle e criticità presenti nell'ambiente applicativo.

Chi scrive software ha poi un'altra arma a disposizione, che in taluni settori regolamentati è addirittura obbligatoria, ed è il ricorso a particolari consulenti che ricoprono il ruolo di "hacker buoni" mettendo alla prova la sicurezza delle applicazioni attraverso vere e proprie campagne di attacchi simili a quelle che potrebbero essere scatenate da cybercriminali. Queste iniziative sono utilissime per trovare bug sfuggiti all'attenzione dei programmatori, e se la tua azienda si avvale di software fatto scrivere apposta da qualche software house specializzata potrebbe essere una buona idea verificare se quest'ultima ne faccia uso.

STRATO DEI DATI

Eccoci dentro il caveau informatico che rappresenta il sogno di qualsiasi delinquente informatico.

Le informazioni sono state definite "il petrolio della nostra epoca" e in effetti la definizione non si allontana molto dalla realtà, salvo che forse, in prospettiva, i dati sono destinati a diventare ancora più preziosi del greggio.

Per questo i dati **devono essere circondati da speciali attenzioni** che ne garantiscano l'accesso solamente a chi ha davvero un motivo legittimo per farlo, e senza che le procedure di sicurezza ne rendano l'utilizzo complicato, poco pratico o controproducente.

Per far ciò si ricorre in genere a una **combinazione di tecnologie e soluzioni**. Ecco le principali:

- ***Identity and Access Management (IAM)**:* l'anagrafe centrale che tiene traccia delle identità degli utenti permettendo di attivare e disattivare automaticamente la configurazione e i privilegi di accesso dei vari account.
- ***Single Sign-On (SSO)**:* il sistema che permette all'utente di autenticarsi una sola volta, magari con tecniche multi-fattore (ad esempio password e conferma di un codice una tantum spedito via SMS) per poter accedere a tutti i differenti servizi previsti dall'azienda.

- ***Gestione dei permessi***: una soluzione che consente di associare utenti e gruppi ai dati che possono essere consultati a seconda della funzione aziendale di ciascuno. In questo modo, ad esempio, il personale dell'amministrazione può lavorare sui dati contabili senza che questi possano essere osservati o modificati dall'ufficio progettazione o dal marketing e viceversa, creando un ulteriore sbarramento di sicurezza contro gli estranei.
- ***Classificazione dei dati***: non tutti i dati nascono uguali né richiedono costantemente lo stesso trattamento. Distinguere tra dati critici e dati storici, dati attualmente in uso e dati da archiviare è un passo essenziale per segmentare correttamente quello che può essere consultato e modificato da chiunque.
- ***User behavior analytics (UBA)****:* anche nello strato dei dati è opportuno adottare soluzioni che osservano il comportamento degli utenti per lanciare l'allarme quando si verificano attività insolite e sospette. Un database che anziché essere salvato sul consueto sistema di backup viene esportato su una chiavetta USB è un buon motivo per andare a controllare, ma prima occorre chiaramente disporre di un software capace di accorgersi di una cosa del genere.

Sistemata la questione degli accessi, non bisogna dimenticare **che i dati devono essere protetti anche attraverso backup**, **segmentati a seconda dell'importanza e delle necessità di utilizzo, ripuliti da doppioni ed errori, allineati alle procedure normative come quelle previste per la privacy e i dati sensibili, e infine cancellati in maniera sicura quando non sono più necessa**ri. Anche se tutte queste attività non sono strettamente legate alla sicurezza informatica, tuttavia ne risultano intrecciate a livello di funzionalità: le soluzioni che permettono di risolvere un aspetto sono spesso le stesse che risolvono anche l'altro.

CONCLUSIONI

Come vedi, **gli strati della sicurezza non sono pochi e le soluzioni disponibili per ciascuno di essi sono numerose e variegate**; inoltre ogni giorno se ne aggiungono di nuove e si perfezionano le tecniche già esistenti. Ricorda: i cybercriminali non se ne stanno con le mani in mano, motivo per cui la sicurezza IT somiglia a un gioco a rimpiattino senza soluzione di continuità.

Lo schema visto sopra non è tuttavia che una sorta di mappa generale che deve poi essere **calata nella realtà della singola azienda**.

Non è detto che tutti debbano implementare ciascuno strato allo stesso modo, e comunque non è necessario che ciò venga fatto contemporaneamente.

A seconda delle tue priorità specifiche potrai scegliere di dare precedenza a determinate soluzioni piuttosto che altre per approfondire le contromisure che corrispondono alle tue esigenze, costruendo nel tempo il tuo perimetro difensivo ideale.

Il bello di una sicurezza a strati è che **ogni elemento collabora con tutti gli altri rafforzando la protezione complessiva**.

I malintenzionati si accorgono subito se una potenziale vittima dispone di adeguate contromisure o meno, e in genere **scelgono quella che offre la minor resistenza possibile**. A parità di potenziale bottino, tra una villa circondata da alte mura con telecamere, sensori perimetrali, cani da guardia, allarmi volumetrici, porte e tapparelle blindate e invece un appartamento protetto solo da una semplice serratura a doppia mappa, a quale obiettivo credi che un ladro preferirà dedicarsi? Anche nel crimine è sempre una questione di costo/risultato.

Certo, la materia non è semplicissima e soprattutto richiede competenze di vario genere che siano continuamente aggiornate.

Per questo **l'indicazione è quella di rivolgersi sempre a professionisti** esperti che possano fornirti la consulenza di cui hai bisogno e che ti seguano nel tempo con verifiche periodiche e aggiunte graduali ai tuoi sistemi di sicurezza, occupandosi di formare il tuo personale e di compiere anche tutti quegli adempimenti formali che possono essere necessari in taluni settori o qualora la protezione informatica si combini con questioni normative come per esempio il GDPR.

Si tratta di un investimento continuativo che puoi intraprendere al ritmo che ti è più congeniale: **uno strato dopo l'altro potrai comporre le difese più adatte per il tuo ambiente** acquisendo quella tranquillità che ti permetterà di concentrarti sulla tua attività senza correre rischi inutili.

Glossario

BEC Business Email Compromise – Una sofisticata truffa mirata che nella sua versione più diffusa assume l'aspetto di comunicazioni provenienti da un dirigente aziendale per convincere un altro dipendente a dare corso a pagamenti verso conti bancari riconducibili agli autori dell'illecito. Per dare credibilità alle richieste vengono spesso falsificati documenti ufficiali e creati domini Internet dal nome molto simile a quello delle aziende e degli enti coinvolti.

Dark web – Un vero e proprio web parallelo costituito da sistemi collegati a Internet attraverso software e configurazioni particolari, al cui interno si svolgono attività prevalentemente illegali di ogni genere. Il dark web rappresenta una componente del cosiddetto deep web, ovvero quella porzione del web che non è accessibile ai normali motori di ricerca.

DDoS – Distributed Denial of Service – Un attacco rivolto contro un sistema che viene contemporaneamente contattato con richieste di accesso o di traffico da migliaia di computer e dispositivi connessi al solo scopo di saturare la banda di comunicazione disponibile in modo da rendere inutilizzabile il sistema stesso. Nel Dark Web è possibile acquistare servizi DDoS gestiti da cybercriminali che controllano enormi quantità di computer (detti zombie) infettati da apposito malware quasi sempre veicolato mediante azioni di phishing.

Mining di criptovalute – La produzione di criptovalute come Bitcoin, Litecoin, Ethereum, Monero e altre è associata all'esecuzione di un massiccio quantitativo di calcoli matematici che richiede lunghi tempi di elaborazione da parte di un singolo computer. Per velocizzare queste operazioni e generare così nuove criptomonete, i cybercriminali sfruttano la potenza di calcolo di computer altrui su cui sia stato preventivamente installato del malware adeguato. Avendo a disposizione le risorse di calcolo di centinaia di migliaia o addirittura milioni di PC infetti, i cybercriminali possono arricchire la propria dotazione di criptovalute in tempi notevolmente ridotti.

Phishing – Una truffa diffusa principalmente tramite messaggi di posta elettronica e SMS attraverso i quali si tenta di carpire informazioni sensibili alle vittime facendo credere che la richiesta provenga da un interlocutore affidabile. I messaggi solitamente rimandano a pagine web fraudolenti che replicano l'aspetto di quelle ufficiali invitando il destinatario a inserire le proprie credenziali o i codici delle carte di credito con le scuse più diverse. A differenza delle truffe BEC, accuratamente personalizzate, il phishing si avvale di invii di messaggi in massa.

Ransomware – Un particolare tipo di malware che crittografa i file residenti sul computer colpito (e spesso anche su tutti gli altri dispositivi collegati alla stessa rete) che diventano così inaccessibili a meno di non pagare un riscatto per ottenere la chiave di decifrazione necessaria. Non sono rari i casi in cui anche la disponibilità di questa chiave non consenta il ripristino corretto dei sistemi, con gravi conseguenze per le aziende.

Spam – Messaggi indesiderati solitamente a carattere pubblicitario che rappresentano una porzione significativa del traffico mondiale di email. In molti Paesi l'invio di spam è reato e comunque quasi sempre contrario alle politiche d'utilizzo ammesse dagli Internet Service Provider. Per questo motivo, nonché per gli altissimi volumi di messaggi (anche alcuni miliardi) spediti da una normale campagna spam, i cybercriminali preferiscono effettuare l'invio attraverso computer di ignari utenti su cui sia stato precedentemente installato malware che ne permetta il controllo a distanza.

Spear phishing – Una variante del phishing estremamente personalizzata sul destinatario del tentativo di truffa. A differenza del normale phishing, i messaggi sono realizzati su misura dopo aver studiato il profilo della potenziale vittima attraverso le informazioni normalmente reperibili sul Web. Un accurato lavoro di preparazione permette di aumentare notevolmente l'efficacia dei messaggi prendendo alla sprovvista anche coloro che normalmente prestano poco credito alle comunicazioni indesiderate provenienti per posta elettronica.

Spyware – Una particolare tipologia di malware che ha lo scopo di raccogliere quante più informazioni possibili sull'utilizzatore del computer o del dispositivo sul quale risiede. A differenza del ransomware e di altri malware, lo spyware è scritto per restare ben nascosto più a lungo possibile raccogliendo dati sensibili che possono essere rilevati tramite sia la lettura dei file presenti sul sistema, sia il monitoraggio dei tasti premuti alla tastiera. Gli esemplari di spyware più sofisticati possono estendere il loro raggio d'azione anche alla rete alla quale è collegato il dispositivo infetto.