Nicolosi, 29 aprile 2023

Al personale
Agli alunni
Alle famiglie

Oggetto: Glossario sulla Sicurezza Informatica - parte seconda

Di seguito una raccolta dei termini più comunemente utilizzati nel campo della sicurezza informatica, ognuno con il relativo significato- seconda parte.

MALWARE
Crasi dei termini inglesi "Malicious Software" (software malevolo in inglese), malware è un termine generico utilizzato per indicare qualunque tipologia di programmi o stringhe di codice che possono mettere a rischio dati e informazioni presenti nella memoria del dispositivo attaccato. Sono esempi di malware i worm, i virus, gli stalkerware, gli spyware, i ransomware, gli adware e qualunque altra famiglia di programma creata per attaccare device elettronici.

PASSPHRASE
È l'evoluzione della password: una chiave d'accesso composta da più parole di senso compiuto che, da un lato, rende più complesso il lavoro di chi prova a rubare password con metodi automatizzati (tramite i cosiddetti "attacchi dizionario", ad esempio) e, dall'altro lato, fa sì che le chiavi d'accesso siano facilmente ricordabili.

PASSWORD MANAGER
Buona norma vorrebbe che utilizzassimo una password differente per ogni account che abbiamo. I password manager nascono proprio per facilitarci in questo compito: dove non arriva la memoria, arrivano programmi ad hoc che archiviano le credenziali in un database sicuro e crittografato. Le credenziali così salvate verranno poi riproposte non appena si tenterà di effettuare l'accesso a uno dei propri account.

PASSWORD
Letteralmente "parola d'accesso", è la chiave d'accesso che impostiamo e utilizziamo per accedere ai profili web (posta elettronica, social network, banca online e altro).

Sito web www.ipssatchinnicinicolosi.edu.it **C.F.** 93128180879 **CUF** UFDFIK
Sede Centrale Via F.lli Gemmellaro s.n.c 95030 Nicolosi (CT) Tel. 095.6136609 - Cod.Min. CTRH05000N
Sede coordinata Via Mirti s.n.c 95038 Santa Maria di Licodia (CT) Tel. 095.6136631 - Cod.Min. CTRH05001P
Corso serale Via F.lli Gemmellaro s.n.c 95030 Nicolosi (CT) Tel. 095.6136609 - Cod.Min. CTRH050503
Email: ctrh05000n@istruzione.it **PEC:**ctrh05000n@pec.istruzione.it

PATCH

In italiano sta per "toppa", un termine che descrive alla perfezione il suo ruolo nel mondo informatica. Le patch sono infatti delle piccole porzioni di codice o piccoli programmi rilasciati per correggere una precisa vulnerabilità di sicurezza (o comunque un numero limitato di bug).

PENETRATION TEST

Serie di strumenti e programmi che consentono di valutare la sicurezza di una rete, di PC o di un sito web provandone a superare (o penetrare, in gergo tecnico) i sistemi di difesa.

PHISHING

Il phishing è una delle tecniche di attacco informatico maggiormente utilizzate. Si tratta di un tentativo fraudolento di ottenere dati e informazioni personali di un utente come le sue credenziali di posta elettronica o social, i dati della carta di credito e altri. Solitamente, un attacco phishing viene condotto tramite messaggi di posta elettronica, ma sempre più spesso vengono utilizzati i servizi di messaggistica istantanea e i social network, che consentono di raggiungere un numero di persone più ampio in minor tempo (e senza "filtri" a difenderli) Il phishing, così come lo abbiamo descritto, rientra nel più ampio settore dell'ingegneria sociale, che sfrutta informazioni private degli utenti per poterli truffare o rubare loro informazioni personali.

RANSOMWARE

Tra le famiglie malware più pericolose, è anche una delle ultime ad aver fatto la sua comparsa. I ransomware, o software del riscatto, sfruttano una combinazione di ingegneria sociale e phishing per infettare un computer e infiltrarsi in una rete informatica. Una volta che il virus è all'interno del PC o dello smartphone, l'utente può ben poco: il ransomware crittografa immediatamente tutti i dati presenti nella memoria e riavvia il dispositivo. Alla riaccensione, l'utente visualizza un messaggio di riscatto ("ransom" in inglese) da pagare solitamente in bitcoin.

ROOTKIT

Tra le famiglie malware più pericolose, i rootkit consentono a un cracker di ottenere i permessi di root del sistema operativo. Ciò consente al cybercriminale di controllare ogni singolo aspetto del PC, sia a livello software sia a livello hardware. I permessi di root, infatti, sono i cosiddetti "permessi da amministratore", che conferiscono potere assoluto sulla gestione del sistema operativo.

SCANSIONE "SIGNATURE BASED"

Detta anche "analisi delle firme", è alla base del funzionamento della gran parte dei software antivirus. Ogni programma di sicurezza ha un database di "firme", una porzione di software di tutti i malware noti da confrontare con file e programmi presenti nella memoria del PC o dello

Sito web www.ipssatchinnicinicolosi.edu.it **C.F.** 93128180879 **CUF** UFDFIK
Sede Centrale Via F.lli Gemmellaro s.n.c 95030 Nicolosi (CT) Tel. 095.6136609 - Cod.Min. CTRH05000N
Sede coordinata Via Mirti s.n.c 95038 Santa Maria di Licodia (CT) Tel. 095.6136631 - Cod.Min. CTRH05001P
Corso serale Via F.lli Gemmellaro s.n.c 95030 Nicolosi (CT) Tel. 095.6136609 - Cod.Min. CTRH050503
Email: ctrh05000n@istruzione.it **PEC:**ctrh05000n@pec.istruzione.it

smartphone. In caso di corrispondenza tra la firma e il software analizzato, quest'ultimo verrà "immunizzato", mettendolo in quarantena o eliminandolo dalla memoria.

SCANSIONE EURISTICA

Detta anche "analisi euristica", si contrappone a quella basata sulle firme perché, anziché limitarsi allo studio e al confronto del codice del software malevolo, ne studia anche il comportamento. Gli antivirus ad analisi euristica valutano così come si comporta un determinato software e, in caso ci siano delle analogie con il comportamento di malware noti, lo mette in quarantena, così da renderlo innocuo. In questo modo è possibile individuare virus e malware non ancora conosciuti o per i quali non sono ancora disponibili delle "firme".

SEXTORTION

Neologismo inglese nato dall'unione di "Sex" ed "Extortion", è una truffa a sfondo sessuale condotta sul web. Le vittime di sextortion ricevono email o messaggi sui social network da sconosciuti che sarebbero entrati in possesso di loro immagini compromettenti (foto nude o in atteggiamenti sessuali) e sarebbero pronte a diffonderle pubblicamente. Per evitare che ciò accada, alle vittime viene chiesto il pagamento di una somma a mo' di "riscatto": una truffa bella e buona, dato che nella stragrande maggioranza dei casi le immagini compromettenti non esistono.

SICUREZZA INFORMATICA

Con il termine "sicurezza informatica" si intendono tutte quelle tecniche e quelle strategie volte a difendere server, datacenter, computer, smartphone, dispositivi IoT e qualunque device elettronico da attacchi di natura informatica. Gli attacchi sono solitamente diretti ad accedere, modificare o distruggere informazioni presenti all'interno dei dispositivi, a estorcere denaro o "prendere possesso" da remoto degli stessi dispositivi.

SMISHING

Lo smishing è un tentativo di truffa telematica condotto via SMS (il suo equivalente "informatico" è il phishing, per intendersi). In quello che potremmo definire "caso tipo", l'utente riceve un messaggio dalla propria banca per un tentativo di accesso anomalo al conto corrente online e per questo è necessario modificare la password del profilo. In realtà, il sito su cui si viene indirizzati è un "falso realizzato ad arte", che permette ai cybertruffatori di accedere indisturbati al conto corrente online.

SPAM

Invio massivo di messaggi di posta elettronica non richiesti, solitamente di carattere pubblicitario o promozionale. Anche se si tratta di una pratica in netto calo rispetto al passato, si calcola che tra il 55% e il 60% delle email inviate ogni giorno siano di spam e, dunque, inutili. Di per sé lo spam non

Sito web www.ipssatchinnicinicolosi.edu.it **C.F.** 93128180879 **CUF** UFDFIK
Sede Centrale Via F.lli Gemmellaro s.n.c 95030 Nicolosi (CT) Tel. 095.6136609 - Cod.Min. CTRH05000N
Sede coordinata Via Mirti s.n.c 95038 Santa Maria di Licodia (CT) Tel. 095.6136631 - Cod.Min. CTRH05001P
Corso serale Via F.lli Gemmellaro s.n.c 95030 Nicolosi (CT) Tel. 095.6136609 - Cod.Min. CTRH050503
Email: ctrh05000n@istruzione.it **PEC:**ctrh05000n@pec.istruzione.it

è pericoloso, ma potrebbe anche trattarsi di una tattica per "nascondere" mail di phishing e trarre così in inganno un utente.

SPYWARE

Il nome è piuttosto evocativo: spyware nasce infatti dall'unione dei termini inglesi spy (spiare) e ware (per software). Si tratta di un malware che infetta PC, smartphone e sistemi informatici con l'obiettivo di spiare l'utente, trafugare informazioni presenti nella memoria del dispositivo e inviarle a server remoti gestiti dagli stessi hacker – oppure organizzazioni criminali – che hanno creato il malware.

STALKERWARE

Tra gli ultimi arrivati sul panorama della sicurezza informatica mobile, gli stalkerware sono app che consentono a un utente di spiare e controllare ogni singolo aspetto di uno "smartphone obiettivo". Si tratta di una tipologia particolare di spyware che, una volta installata su un dispositivo mobile, permette di accederne a tutte le risorse: fotocamera, galleria fotografica, rubrica, app per SMS, social network e piattaforme di messaggistica istantanea.

TROJAN HORSE

Come Ulisse entrò a Troia sfruttando un cavallo di legno, gli hacker sono soliti crearsi delle "aperture" nei sistemi di difesa di PC, smartphone e altri sistemi informatici utilizzando i trojan horse (letteralmente "cavallo di Troia"). Si tratta di software che, una volta all'interno del dispositivo, crea un accesso remoto che un cybercriminale può utilizzare sia per trafugare dati, sia per accedere al device e prenderne possesso a distanza.

VIRUS

I virus sono una delle famiglie malware più importanti e conosciuti. Si tratta di programmi che infettano un PC o un sistema informatico per tentare di distruggerne i dati, corromperne i file di sistema o alternarne le prestazioni. A differenza di altri malware, i virus sono in grado di autoreplicarsi e diffondersi in altri computer o smartphone sfruttando la connessione a Internet o altri sistemi di comunicazione.

VPN

Acronimo di Virtual Private Network, la VPN è una rete informatica virtuale protetta da crittografia. Molto utilizzata a livello aziendale, ma sempre più apprezzata anche da utenti "normali", la VPN viene creata attraverso una tecnica detta di "tunneling", ossia uno "scudo crittografico" che forma una connessione a "prova di cracker" tra due punti di una rete. Tutti i dati che passano sotto questo "scudo" sono crittografati e, per questo, indecifrabili e inutilizzabili in caso di attacco man-in-the-middle.

Sito web www.ipssatchinnicinicolosi.edu.it **C.F.** 93128180879 **CUF** UFDFIK
Sede Centrale Via F.lli Gemmellaro s.n.c 95030 Nicolosi (CT) Tel. 095.6136609 - Cod.Min. CTRH05000N
Sede coordinata Via Mirti s.n.c 95038 Santa Maria di Licodia (CT) Tel. 095.6136631 - Cod.Min. CTRH05001P
Corso serale Via F.lli Gemmellaro s.n.c 95030 Nicolosi (CT) Tel. 095.6136609 - Cod.Min. CTRH050503
Email: ctrh05000n@istruzione.it **PEC:**ctrh05000n@pec.istruzione.it

VULNERABILITÀ
Difetto di progettazione, codifica o configurazione di un software (ma anche di protocolli informatici) che consente a un hacker o cybercriminale di compromettere l'integrità del sistema. Sfruttando una vulnerabilità del sistema operativo (o di un software installato su PC), ad esempio, è possibile accedere alle informazioni archiviate nella memoria del dispositivo oppure ottenere i privilegi di amministratore e spiare tutte le attività dell'utente.

WHITE-HAT HACKER
Detto anche hacktivist, è la "nemesi" del Black-hat hacker. Si tratta di un hacker "etico", specializzato in penetration test e altre metodologie di prove il cui scopo è di verificare il livello di sicurezza e affidabilità di reti informatiche. Il solo scopo di un White-hat hacker è quello di portare alla luce falle e vulnerabilità insite nei sistemi di network informatici, in modo che i gestori della rete possano correre ai ripari.

WORM
Letteralmente "verme", è una famiglia di malware che sfrutta le macchine infettate per replicarsi e diffondersi su altri PC (nella stragrande maggioranza, il worm si "auto-invia" sfruttando la posta elettronica). Il worm, solitamente, non viaggia mai solo: funge infatti da "apripista" per altri malware, come keylogger, backdoor o spyware.

ZERO DAY
Attacco informatico che sfrutta vulnerabilità non ancora rese pubbliche per le quali non è ancora disponibile una patch o un aggiornamento. Si tratta di una delle minacce più gravi, dal momento che non esistono soluzioni disponibili.

Il Responsabile della Sicurezza Informatica
Ing. Prof. Salvatore Musumeci

Salvatore
Musumeci
29.04.2023
09:01:31
GMT+01:00

LUCIANO MARIA
SAMBATARO
30.04.2023
18:58:10
GMT+01:00

Il Dirigente
Luciano Maria sambataro

Sito web www.ipssatchinnicinicolosi.edu.it **C.F.** 93128180879 **CUF** UFDFIK
Sede Centrale Via F.lli Gemmellaro s.n.c 95030 Nicolosi (CT) Tel. 095.6136609 - Cod.Min. CTRH05000N
Sede coordinata Via Mirti s.n.c 95038 Santa Maria di Licodia (CT) Tel. 095.6136631 - Cod.Min. CTRH05001P
Corso serale Via F.lli Gemmellaro s.n.c 95030 Nicolosi (CT) Tel. 095.6136609 - Cod.Min. CTRH050503
Email: ctrh05000n@istruzione.it **PEC:**ctrh05000n@pec.istruzione.it