Nicolosi, 21 aprile 2023

Al personale
Agli alunni
Alle famiglie

Oggetto: Glossario sulla Sicurezza Informatica - parte prima

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

ADWARE
A differenza di moltissime altre famiglie di malware, quella degli adware è probabilmente tra le meno pericolose. Si tratta di programmi malevoli che infettano il PC o lo smartphone per mostrare video pubblicitari e banner. Lo scopo, in questo caso, non è quello di rubare dati o distruggerli, ma semplicemente di guadagnare sulla visualizzazione di pubblicità da parte degli utenti.

ANTIMALWARE
Come gli antivirus, anche gli antimalware si pongono l'obiettivo di proteggere computer e smartphone da infezioni di software malevolo di ogni genere. Lo "scudo" offerto dagli antimalware è più mirato e si concentra su famiglie malware magari meno conosciute ma, proprio per questo, più difficili da scovare.

ANTIVIRUS
Con il nome di antivirus vengono indicati tutti quei software pensati e sviluppati per proteggere PC e smartphone da tentativi di infezione e intrusione. Inizialmente questi programmi agivano esclusivamente (o quasi) contro virus; oggi, invece, offrono una protezione molto più ampia, rilevando, bloccando ed eliminando (o mettendo in quarantena) in tempo reale le potenziali minacce. Per riuscire in questa "impresa", gli antivirus utilizzano
varie tecniche: le più efficaci sono quella euristica e quella "signature based".

ATTACCO DDOS
Acronimo di "Distributed Denial of Service" ("Interruzione distribuita del servizio" in italiano), l'attacco DDoS è tra i più temuti dei big della Rete. Si tratta di una minaccia di "alto livello", ma che fa sentire i suoi effetti anche agli utenti finali. Gli attacchi di questo genere sono solitamente rivolti a CDN (acronimo di Content delivery network, rete di distribuzione dei contenuti) o datacenter e mirano a comprometterne il funzionamento. I cybercriminali "inondano" di traffico dati questi nodi di rete, sino a quando non riescono più a sopportarne il flusso e smettono di funzionare. In gergo

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

tecnico si dice che il nodo è saturo e tutti i contenuti "presenti" a quell'indirizzo non sono più raggiungibili. Solitamente, questa tipologia di attacco viene utilizzata per "mettere offline" siti e portali web, anche di grandi dimensioni.

ATTACCO MAN IN THE MIDDLE

Si tratta di una delle tecniche di cyberspionaggio più utilizzate. Come dice il nome, l'attacco consiste nel "mettersi nel mezzo" di una comunicazione tra due utenti (o due nodi della rete), così da intercettarne tutte le comunicazioni e il traffico.

BLACK-HAT HACKER

Detto anche cracker, è un esperto informatico che sfrutta le proprie conoscenze nel campo della programmazione e sicurezza personale per ricavarne un vantaggio personale.
Ad esempio, può sfruttare una vulnerabilità presente in un software per spiare utenti o controllare da remoto i loro dispositivi. O, ancora, può vendere queste informazioni al miglior offerente, ricavandone somme ingenti.

BOTNET

Letteralmente "rete di bot", si tratta di un insieme di dispositivi informatici infetti e controllati a distanza da un hacker. Le botnet sono solitamente composte da centinaia di migliaia – se non milioni – di device di ogni genere, definiti in gergo "device zombie". Una volta infetti sono "assoggettati" al volere del cybercriminale che controlla il malware e ne eseguono tutti i comandi. Sono così utilizzati per creare un flusso dati "artificiale" utile per saturare la banda dati di un nodo e realizzare un perfetto attacco DDoS.

BUG BOUNTY PROGRAM

Promossi da software house e organizzazioni varie, i programmi "Bug bounty" sono rivolti a white-hat hacker ed esperti di programmazione informatica. Tramite questi programmi, infatti, le case sviluppatrici ricompensano (bounty, in inglese, vuol dire "premio") chi trova falle nel codice sorgente di software e applicazioni e non li sfrutta a proprio vantaggio. In questo modo, le software house possono risolvere il problema prima che diventi di dominio pubblico, evitando che possa causare la diffusione di malware o compromettere il funzionamento dei programmi.

BUG

Letteralmente "baco", "piccolo insetto", indica un errore di programmazione in un software (vedi anche vulnerabilità) che consente a un cybercriminale di introdursi in un sistema informatico. Il nome risale agli albori dell'informatica, quando il primo errore in un software venne causato da uno scarafaggio (un bug, per l'appunto), che era finito tra le schede perforate del programma.

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

CLOUD COMPUTING

Con il termine cloud computing si intendono tutte quelle tecnologie che consentono di usufruire di risorse hardware e software attraverso Internet. Con il cloud computing aziende e fornitori di servizi possono mettere a disposizione l'accesso a server, potenza di calcolo, database, spazio di archiviazione, software e altri servizi. Solitamente il cloud computing viene suddiviso in PaaS (acronimo di Platform as a Service), SaaS (acronimo di Software as a Service) e IaaS (acronimo di Infrastructure as a Service). Negli ultimi anni, però, il cloud viene utilizzato anche per diffondere e vendere malware, tramite piat taforme MaaS (ossia Malware as a Service).

CLOUD STORAGE

Un servizio cloud storage mette a disposizione degli utenti spazio di archiviazione online di svariate decine di gigabyte, accessibile da qualunque dispositivo dotato di connessione a Internet. In questo modo un utente potrà archiviare file online senza occupare spazio sul disco rigido del PC o nella memoria dello smartphone, ma avendoli comunque a disposizione: basterà fare il login al proprio account per accedere allo spazio online e scaricare tutto ciò di cui ha bisogno.

CRITTOGRAFIA

Tra le tecniche di sicurezza informatica più utilizzate (e utili per l'utente finale), la crittografia consiste nel convertire, tramite l'utilizzo di particolari algoritmi, una serie di dati da un formato leggibile a un formato codificato. Pur esistendo diversi metodi crittografici per "rendere illeggibili" dei file archiviati sul PC o inviati via Internet, quelli più utilizzati sono due: cifratura a chiave simmetrica (nella quale la "chiave di lettura" del messaggio è inviata in allegato con il messaggio stesso) e cifratura a chiave asimmetrica (nella quale vengono utilizzate due "chiavi di lettura", una pubblica e una privata, in modo che solo il destinatario possa effettivamente decifrare il messaggio).

CRYPTOJACKER

Famiglia malware nata in seguito al "boom" delle criptovalute, non produce danni diretti al sistema informatico. Almeno in apparenza: i cryptojacker, infatti, sfruttano la potenza di calcolo del PC per creare criptovalute ("minare", in gergo tecnico), che verranno però accreditate sul conto del cybercriminale, e non dell'utente. Come detto, però, l'innocuità è solo apparente: un cryptojacker, infatti, mette sotto stress tutte le componenti del PC, abbreviandone l'aspettativa di vita.

CYBER TERRORISMO

Equivalente cibernetico e digitale del terrorismo "armato". Si tratta quindi di operazioni, a sfondo politico e/o ideologico, che prevedono l'utilizzo di attacchi informatici per mano mettere il funzionamento di sistemi informatici di infrastrutture critiche o per entrare in possesso di informazioni di rilievo.

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

CYBERBULLISMO
Potremmo definirlo come la versione digitale del bullismo e sta a indicare tutte quelle offese, minacce, insulti e attacchi condotti per via telematica. Rivolto principalmente verso giovani e adolescenti, il cyberbullismo si manifesta principalmente sulle piattaforme di messaggistica istantanea e social network, dove un soggetto viene preso di mira e deriso (oppure offeso) da un gruppo di persone.

CYBERCRIME
Traducibile in "Crimine informatico" in italiano, indica tutte quelle attività compiute da cracker o black-hat hacker tese a compromettere le difese di sistemi informatici. I crimini informatici permettono al pirata informatico di prendere il controllo sia dell'hardware sia del software del sistema colpito.

CYBERCRIMINALE
Vedi hacker.

CYBERWARFARE
Detta anche "Guerra cibernetica", indica l'utilizzo di dispositivi informatici e tecniche hacking per attaccare una nazione, causando danni comparabili a quelli di un conflitto armato. Una tipica azione di cyberwarfare è quella dell'attacco ai sistemi di controllo di centrali elettriche o telefoniche, così da mettere fuori uso il sistema energetico o comunicativo di una nazione nemica.

DARK WEB
Secondo alcune stime, la parte di Internet "visibile" agli occhi dei motori di ricerca - e, quindi, a quelli degli utenti - è appena il 4% della "dimensione totale" della Rete. La parte restante è formata da server e siti web che non vengono indicizzati e ricercati e da una nicchia di contenuti illegali. Questa ultima parte, che a grandi linee occupa la stessa dimensione del web "visibile" viene definito come Dark Web, ossia "Web Oscuro". Per accedere a questa parte della Rete è necessario utilizzare un software TOR (acronimo di The Onion Project), un programma che anonimizza la connessione e permette di navigare in assoluta sicurezza. Cosa si trova nel Dark Web? Un po' di tutto, basta che sia illegale. Fino a qualche anno fa nel Dark Web era disponibile una sorta di e-commerce chiamato The Silk Road ("La via della seta" in italiano) sul quale era possibile acquistare stupefacenti, armi e addirittura organi umani. Alcuni "shop" specializzati, invece, permettono di acquistare prodotti legati alla sicurezza informatica: kit di sviluppo malware (i cosiddetti Malware as a Service) o database di credenziali e password trafugati da siti web attaccati nei mesi e anni precedenti.

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

DEEP WEB

Anche se spesso vengono confusi, Dark web e Deep web sono due parti differenti della Rete. La prima, come visto poco sopra, è la parte "oscura" di Internet; la seconda è quella "sommersa", non indicizzata dai motori di ricerca ma comunque raggiungibile tramite un normale browser (a patto di conoscerne l'indirizzo esatto). Qui si possono trovare tutti i contenuti accessibili, ad esempio, dopo un login: l'estratto conto della banca, i risultati delle analisi del sangue, interi database e molto altro ancora. Ovviamente, anche nel deep web è possibile trovare materiale illegale, ma la sua percentuale è di gran lunga inferiore a quella del materiale legale.

DEEPFAKE

Tecnica di videoediting, sfrutta l'intelligenza artificiale per far assumere a una persona presente in un video le sembianze di un'altra, scambiandone i volti. I risultati ottenuti sono solitamente molto buoni, tanto che è impossibile riconoscere un video deepfake a occhio nudo. Pur non essendo direttamente correlata a minacce di sicurezza informatica, questa tecnica è considerata uno dei maggiori pericoli per la privacy e la protezione delle informazioni personali: sono sufficienti una manciata di foto di un volto per "assumere l'identità" di chiunque.

FALLA

Vedi vulnerabilità.

FIREWALL

Letteralmente "Muro di fuoco", si tratta di un programma di sicurezza che analizza il flusso di pacchetti dati in entrata e in uscita dal PC per verificare che non ci sia nulla di anomalo. In caso di pericolo (un cracker che prova a introdursi nel nostro sistema informatico o uno spyware che prova a "sifonare" dei dati dalla nostra memoria), il firewall interviene e interrompe la connessione, così da preservare l'integrità del sistema. Inoltre, l'utente può impostare regole predefinite che bloccano il traffico in entrata o uscita a prescindere, senza che ci sia bisogno di un evento malevolo.

FLEECEWARE

I fleeceware sono app legittime che ogni utente può scaricare sul proprio smartphone dall'App Store e dal Play Store, ma che nascondono una sorpresa. Dopo pochi giorni (o, in alcuni casi, poche ore) di utilizzo, viene attivato automaticamente un abbonamento da svariate decine di euro, senza che l'utente se ne accorga. Un metodo legale, o quasi, per spennare ("to fleece", in inglese) persone inconsapevoli di cosa sta per accadergli.

HACKER

Esperto informatico con conoscenze che spaziano dalla programmazione alla crittografia, passando per la sicurezza informatica. Un hacker utilizza così le sue abilità e la sua preparazione

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

per scovare vulnerabilità e falle all'interno del codice sorgente di app, software e protocolli, in modo da accrescerne la sicurezza. Da non confondere con la figura del cracker (o black-hat hacker), il cui scopo è esattamente opposto.

INTERNET OF THINGS

Spesso abbreviato in IoT, l'Internet delle Cose indica un sistema di "oggetti intelligenti" che comunicano tra loro sfruttando una connessione dati che può essere cablata o senza fili. Grazie al continuo scambio di dati e ai sensori di cui sono dotati, gli oggetti possono acquisire informazioni sull'ambiente che li circonda e "adattarsi" di conseguenza.

Potenzialmente, ogni oggetto della nostra quotidianità può diventare un dispositivo IoT: dalle lampade al termostato, dal frigo ai robot per la cucina, passando per TV, robot industriali e molti altri ancora.

Il Responsabile della Sicurezza Informatica
Ing. Prof. Salvatore Musumeci

Salvatore
Musumeci
21.04.2023
19:49:57
GMT+01:00

Il Dirigente
Luciano Maria sambataro

LUCIANO MARIA
SAMBATARO
24.04.2023 22:31:15
GMT+01:00

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