Ai Docenti
Al Personale ATA
Agli Studenti
Alle Famiglie

Nicolosi, 3 marzo 2023

Oggetto: Famiglie di malware

Come dimostrano recenti sondaggi nel nostro Paese viene registrato più di un evento di sicurezza al secondo, con almeno una vittima di attacco informatico al secondo.
Questo a dimostrazione che "Ignorare i pericoli legati agli attacchi informatici non fa che aumentare le probabilità di finire nella rete di un hacker". **La tattica dello struzzo non è oramai una soluzione accettabile**.
Fra tutti i possibili attacchi, a farla da padrone sono gli attacchi via malware - software malefico - (48% dei casi registrati), seguiti da quelli phishing e di social engineering e molti dei quali registrati all'interno delle Pubbliche Amministrazioni, scuole comprese.
Nel complesso, tutti i software che tentano di infiltrarsi nei nostri sistemi sono parte di una decina di "macrocategorie" di seguito descritte:

VIRUS: Si tratta della forma più "comune" di malware. Come quelli biologici, sono capaci di autoriprodursi ed infettano i files presenti nel sistema danneggiandolo e, nei casi più gravi, rendendo del tutto inutilizzabile il computer.

WORM: Come i virus, anche i worms sono caratterizzati dalla capacità di autoriprodursi ma, a differenza dei primi, sanno anche diffondersi autonomamente. Solitamente, i worms sfruttano strumenti come la posta elettronica per riprodursi nei dispositivi dell''intera lista dei contatti e infettare il numero maggiore possibile di altre macchine.

TROJAN HOURSE: Letteralmente vuol dire "Cavallo di Troia", un nome tutt'altro che casuale. I Trojan Horse, infatti, identificano una tecnica di attacco al sistema creando delle aperture nelle difese del sistema informatico camuffandosi da"software comune" e non malefico.

ADWARE: sono tra i meno pericolosi per la stabilità del sistema, ma forse sono tra i più fastidiosi per gli utenti. Si tratta, infatti, di "software pubblicitario", che mostrano banner e annunci pubblicitari mentre navighiamo online o mentre lavoriamo con il PC.

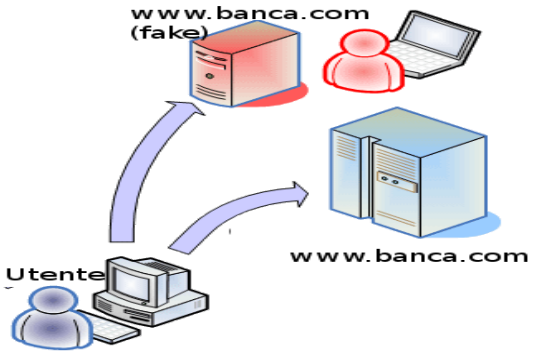
Sito web www.ipssatchinnicinicolosi.edu.it **C.F.** 93128180879 **CUF** UFDFIK
Sede Centrale Via F.lli Gemmellaro s.n.c 95030 Nicolosi (CT) Tel. 095.6136609 - Cod.Min. CTRH05000N
Sede coordinata Via Mirti s.n.c 95038 Santa Maria di Licodia (CT) Tel. 095.6136631 - Cod.Min. CTRH05001P
Corso serale Via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

SPYWARE: Come dice il nome, si tratta di "software spia" che, una volta installato, sottraggono informazioni di ogni tipo dal dispositivo infetto. Può rubare file e documenti archiviati, accedere alle immagini della webcam e all'audio del microfono.

RANSONWARE: Tra le famiglie malware più recenti, sono anche una delle più pericolose. Detto anche "software del riscatto", il ransomware crittografa tutti i dati presenti nella memoria e riavvia il PC. Una volta che il processo viene completato, l'utente non può più accedere ai propri documenti. Se vuole farlo, deve ottenere la chiave di sblocco dal cracker che ha realizzato il malware, pagandogli un riscatto (ransom, in inglese)normalmente in valuta non tracciabile come i Bitcoin.

0BOT: in ambito di sicurezza informatica ci si riferisce a computer infetti da software in grado di "prenderne il controllo" in un qualunque momento. Detti anche "computer zombie", i bot sono solitamente utilizzati per attacchi DDoS di grande portata che risultano essere molto dannosi.

Pharming: L'obiettivo del pharming è il medesimo del famosissimo phishing, ovvero carpire i dati personali della vittima.
La tecnica utilizzata è molto più complessa: si indirizza la vittima verso un "server fake" clone del server reale a cui si sostituisce in modo trasparente appropriandosi quindi delle vere credenziali di accesso al servizio



KEYLOGGER: E un'altra tipologia di "software spia" utilizzato per trafugare dati sensibili come nome utente, password e altri codici di accesso.
I keylogger, una volta installati in un computer, iniziano a registrare tutte le parole che l'utente digita sulla tastiera e le invia a sua insaputa verso un server remoto collegato via internet.

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

ROOTKIT: Tra le varie famiglie è una delle più pericolose. Si tratta di kit di un insieme di strumenti che consentono di ottenere i permessi di root del dispositivo. Di fatto, l'hacker diventerà amministratore di sistema e potrà disporne nella maniera che preferisce, come per esempio potrà installare e disinstallare programmi, potrà cancellare file a piacimento,etc.

Il responsabile delle sicurezza informatica

Ing. Prof. salvatore Musumeci

Salvatore
Musumeci
03.03.2023
17:07:17
GMT+01:00

Il Dirigente

Luciano Maria sambataro

LUCIANO MARIA
SAMBATARO
03.03.2023 19:50:18
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