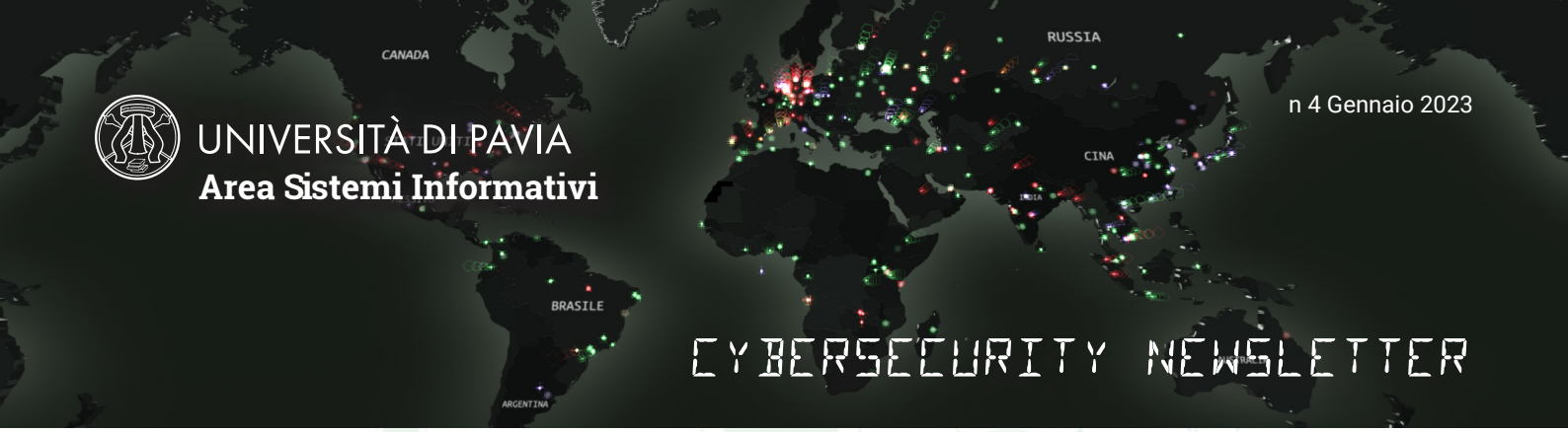


UNIVERSITÀ DI PAVIA
Area Sistemi Informativi

n 4 Gennaio 2023

Attacchi informatici: le misure di difesa dell'Ateneo nell'ultimo mese

I tentativi di intrusione nei sistemi informatici o di raccolta illecita di informazioni sono un fenomeno da monitorare e fronteggiare quotidianamente in Ateneo.

Ad oggi non ci sono state perdite di dati grazie alle misure di protezione adottate che hanno ben anticipato le intenzioni malevole e messo al sicuro il lavoro interno svolto.

La sicurezza collettiva dipende molto anche dalla responsabilità del singolo nell'utilizzare i propri dispositivi, tenerli aggiornati e relazionarsi con l'Area Sistemi Informativi qualora non si senta adeguatamente protetto.

I numeri sotto riportati evidenziano infatti ancora margini di miglioramento nel comportamento di ciascuno di noi oltre alla necessità di un costante lavoro interno ad ogni struttura al fine di acquisire consapevolezza dei rischi e quindi di adottare comportamenti adeguati alle condizioni di sicurezza.

In questo mese abbiamo avuto 96 pc infetti che sono stati segnalati e bonificati e circa 13.700 comunicazioni C&C rilevate e bloccate.

Queste tipologie di attacchi rappresentano uno dei primi fenomeni da monitorare poiché potrebbero nascondere malware, cryptolocker o altri fenomeni malevoli che approfondiremo nei successivi numeri di questa newsletter.

In questo quarto numero della newsletter relativa alla cybersecurity affronteremo il tema dei "trojan"

Malware and Attacks

96
computers infected with bots

13.7K
communications with C&C* sites

* C&C - Command and Control.
If proxy is deployed, there might be additional infected computers.

1 known malware downloaded by **198** users

2 Zero-days downloaded

Zero-days downloaded present a unique count of old or new malware variant with un-known anti-virus signature.

377
unique software vulnerabilities were attempted to be exploited

Indicates potential attacks on computers on your network.

High Risk Web Access

5
high risk web applications

898.8MB

Potential risks: opens a backdoor to your network, hides user activity, causes data leakage or malware infections.

0
high risk web sites

0 hits

Potential risks: Exposure to web-based threats and network infection. Examples: Spam, malicious, phishing web sites.

0
cloud applications

0B

Risk of data loss and compliance violations. Examples: Dropbox, Google Drive, OneDrive.

Data Loss

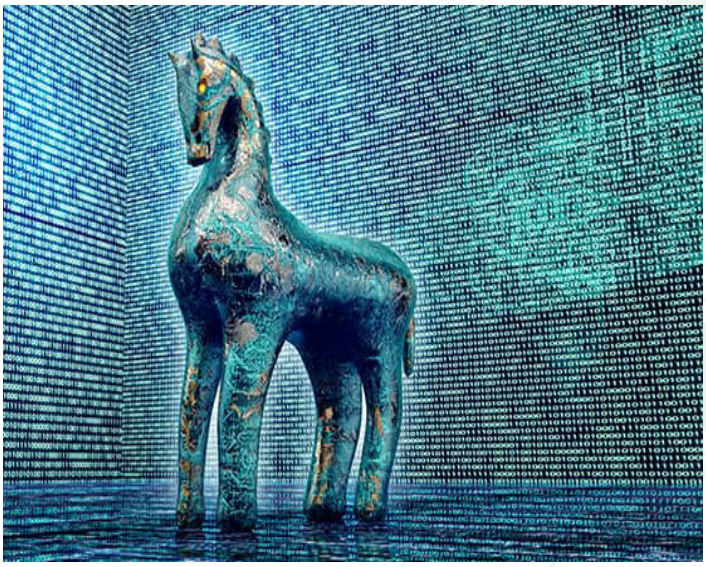
0
potential data loss incidents

0
sensitive data categories

Indicates information sent outside the company or to unauthorized internal users. Information that might be sensitive. See GDPR Article 5

Trojan: che cos'è

Un trojan o trojan horse (in italiano "cavallo di Troia"), nell'ambito della sicurezza informatica, indica un tipo di malware. Il termine deriva dall'antica storia greca dell'ingannevole Cavallo di Troia che portò alla caduta della città. Il trojan, come il cavallo dell'antica storia greca, si nasconde all'interno di un altro programma apparentemente utile e innocuo: l'utente, eseguendo o installando quest'ultimo programma, attiva inconsapevolmente anche il codice del trojan nascosto.



L'attribuzione del termine "cavallo di Troia" ad un programma (o file eseguibile) è dovuta al fatto che esso nasconde il suo vero fine, in questo modo l'utente è indotto ad eseguire il programma.

Spesso il trojan viene installato dallo stesso attaccante, quando prende il controllo del sistema, acquisendone i privilegi amministrativi. In questo caso il trojan serve a "mantenere lo stato di hacking", cioè a mantenere il controllo remoto del computer, senza che il legittimo proprietario si accorga che alcuni programmi nascondono altre funzioni, per esempio di intercettazione di password o di altri dati sensibili.

Il trojan è un programma appositamente progettato per eseguire azioni non autorizzate da parte dell'utente-vittima; i Trojan, ad esempio, cancellano, bloccano, modificano o copiano dati, oppure compromettono il normale funzionamento di computer o reti di computer.

Utilizzo

Con il termine "trojan" ci si riferisce normalmente ai malware ad accesso remoto (detti anche RAT dall'inglese Remote Administration Tool), composti generalmente da 2 file: il file server, che viene installato nella macchina vittima, ed un file client, usato dall'attaccante per inviare istruzioni che il server esegue.

Spesso i trojan sono usati come veicolo alternativo ai worm e ai virus per installare delle backdoor o dei keylogger sui sistemi bersaglio.

I trojan sono sempre più diffusi e non tutti sono riconoscibili prontamente dagli antivirus. Per aumentare la loro efficacia possono nascondersi in modo tale che nemmeno l'antivirus sia in grado di eliminarli, permettendo così di danneggiare il computer. Se questo accade, il trojan può essere individuato e rimosso solo tramite la reinstallazione totale del sistema operativo.

Metodo di diffusione

I trojan non si diffondono autonomamente come i virus o i worm e non sono in grado di replicare sè stessi. Quindi richiedono un'azione diretta dell'aggressore per veicolare il software maligno alla vittima.

A volte però worm e trojan agiscono insieme: un worm viene iniettato in rete con l'intento di installare dei trojan sui sistemi. Spesso è la vittima stessa che involontariamente, non prestando attenzione ai siti che sta visitando, scarica un trojan sul proprio computer. Una tecnica che i cracker amano usare è quella di inserire queste "trappole", ad esempio, nei videogiochi piratati. In generale sono riconosciuti da un antivirus aggiornato, come un normale malware.

Altre volte gli stessi trojan possono essere usati per diffondere virus all'interno di una rete difficile da attaccare per gli hacker. Oppure possono essere usati per aprire porte di comunicazione sui sistemi o server che normalmente invece dovrebbero essere chiuse.

Tipi di trojan

- **Trojan backdoor** - Sono uno dei tipi di trojan più semplici, ma potenzialmente più pericolosi. Agendo come un gateway, sono infatti in grado di caricare in un sistema ogni sorta di malware o quanto meno di fare in modo che il computer sia vulnerabile agli attacchi. Una backdoor viene spesso utilizzata per configurare le botnet. Senza che l'utente se ne accorga, il computer diventa parte di una rete zombie usata per diffondere gli attacchi ad altri computer o reti.

- **Exploit** - Gli exploit sono programmi contenenti dati o codice, che sfruttano una vulnerabilità di un'applicazione installata nel computer.

- **Rootkit** - I rootkit sono progettati per nascondere determinati oggetti o attività nel sistema. Spesso il loro obiettivo principale è impedire il rilevamento di programmi nocivi, al fine di prolungare il periodo di esecuzione dei programmi su un computer infetto.

- **Trojan dropper/downloader** - Uno dei più noti trojan dropper è il malware Emotet, ormai innocuo, che, al contrario di un trojan backdoor, non può eseguire codice direttamente nel PC. Porta invece con sè altri malware, ad esempio il trojan bancario Trickbot e il ransomware Ryuk. I dropper sono quindi simili ai downloader con la differenza che questi ultimi hanno bisogno di una risorsa di rete per estrarre il malware. I dropper contengono già gli altri componenti dannosi nel pacchetto del programma. Entrambi i tipi di trojan possono essere aggiornati da remoto dai programmatori responsabili, in modo che, ad esempio, gli scanner anti-virus non riescano a rilevarli con le nuove definizioni.

- **Trojan bancari** - I trojan bancari sono tra quelli più diffusi, considerando il crescen-

te utilizzo del banking online. Questi attacchi hanno l'obiettivo primario di carpire le credenziali di accesso ai conti bancari. A questo scopo, utilizzano tecniche di phishing indirizzando le potenziali vittime a una pagina manipolata dove l'utente immetterà le proprie credenziali di accesso. Pertanto, quando si effettuano operazioni bancarie online, è fondamentale utilizzare metodi sicuri per la verifica, (ad esempio l'app della banca), e non immettere mai i dati di accesso in un'interfaccia Web.

- **Trojan DDoS** - Questo trojan solitamente viene installato su più macchine per creare una botnet (cioè una rete composta da dispositivi infettati da malware). Dopo aver fatto ciò viene usato per eseguire un attacco di tipo DoS (Denial of Service), che consiste nell'inviare richieste in modo massivo ad un determinato indirizzo in modo da creare un disservizio o bloccare il server. Il comportamento di una botnet è all'apparenza normale, tuttavia è in grado di operare anche in background per portare a compimento gli attacchi. A consentirlo è un trojan con un componente backdoor che resta silente e inosservato nel computer e, se necessario, viene attivato dal suo operatore. Se un attacco botnet o un attacco DDoS viene portato a termine, siti Web o addirittura intere reti non sono più accessibili.

- **Trojan anti-virus falsi** - I trojan anti-virus falsi sono particolarmente insidiosi, infatti invece di proteggere i dispositivi, li mettono a rischio. Il loro obiettivo è quello di ingannare gli ignari utenti comunicando loro di aver individuato un virus e spingendoli ad acquistare una protezione efficace.

- **Trojan GameThief** - Questo tipo di programma ruba informazioni dall'account degli utenti che giocano online.

- **Trojan IM (Instant Messaging)** - I programmi trojan IM rubano i dati di accesso e le password dai programmi di messaggistica istantanea come ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype etc.. Tuttavia, neppure i nuovi servizi di messaggistica sono immuni dai trojan. Anche Facebook Messenger, WhatsApp, Telegram o Signal possono diventare obiettivi dei trojan. Di recente, a dicembre 2020, un trojan per Windows è stato attivato attraverso un canale Telegram.

- **Trojan ransom** - Questo tipo di trojan può modificare i dati sul computer per danneggiarne il funzionamento e per impedire all'utente di utilizzare dati specifici. L'hacker. Normalmente, ripristinerà le prestazioni del computer oppure sbloccherà i dati solo dopo che l'utente avrà pagato il riscatto richiesto.

- **Trojan SMS** - I trojan SMS, ad esempio il malware per Android Faketoken, si mimetizza nel sistema come una normale app per SMS e invia messaggi SMS in massa a costosi numeri internazionali. Il proprietario del cellulare dovrà quindi pagarne i costi. Altri trojan SMS, invece, stabiliscono connessioni a costosi servizi SMS premium.

- **Trojan spy** - I programmi trojan spy possono spiare tutto ciò che l'utente sta ricercando attraverso i suoi device, ad esempio tenendo traccia dei dati immessi

con la tastiera, catturando screenshot del monitor o procurandosi un elenco delle applicazioni in esecuzione.

- **Trojan mailfinder** - Questi programmi, normalmente,raccolgono gli indirizzi e-mail dai computer infetti.

Recentemente sono state scoperte nuove minacce di tipo trojan, come quelle sotto riportate.

Triada: un trojan che colpisce i cellulari Android.
Questo trojan è stato creato usando come base altri 3 trojan (Ztorg, Gorp e Leech). Il trojan viene trasmesso tramite lo scaricamento di app dal Play Store e tende a colpire più efficacemente i sistemi Android precedenti alla versione 4.4.4. Questo trojan una volta installato ottiene i privilegi di sistema, leggendo quindi informazioni, inviando messaggio o estraendo dati da altre applicazioni.

Nemucod: questo trojan viene diffuso come archivio ZIP normalmente allegato ad una mail. L'archivio contiene uno script che viene eseguito una volta che l'archivio viene aperto. Lo script eseguito fa scaricare un altro virus solitamente un Cryptolocker. Per proteggersi è opportuno mantenere sempre l'antivirus aggiornato e non aprire o scaricare allegati da mail di provenienza sospetta.

Modalità di attacco

La prima cosa da considerare è che un trojan è un programma eseguibile che per installarsi necessita dell'input da parte dell'utente. Purtroppo ci sono molti modi in cui un programma può fingersi benevolo, quindi l'unico modo per evitarlo è imparare a diffidare dei programmi dalla provenienza dubbia o sospetta e a integrare il software antivirus con sistemi anti-malware.

Inoltre è consigliato prestare attenzione ai file eseguibili, ad esempio quelli con estensione exe, 'vbs', 'bat', 'js' in particolare se arrivano attraverso email, anche da mittenti conosciuti.

Un altro modo per trasmettere un trojan è quello di veicolarlo attraverso le macro di un documento: per esempio nei formati di Word, Excel, PDF e altri. Anche per queste tipologie di file bisogna prestare attenzione ai file anche se provenienti da mittenti conosciuti.

Prevenzione

La regola principale per evitare di essere infettati è di essere sicuri della sorgente e del contenuto di ogni file che si scarica.

Prestare attenzione ai file ricevuti in quanto alcuni trojan possono essere inviati come

allegati di posta elettronica da computer a loro volta infettati da un virus. In questo caso si dovrebbe dubitare della ricezione di file non richiesti da persone sconosciute.

Di seguito alcune semplici regole per evitare di essere infettati quando si vuole scaricare un file da internet

- Conoscere la sorgente da cui si stanno scaricando i file.
- Controllare che non vengano scaricati altri file insieme al file di interesse.
- Controllare che il file scaricato sia conforme come formato e come nome a ciò che ci si aspetta, ad esempio se si scarica un file di un'immagine controllare che non sia un file di altra estensione o un eseguibile.
- In ogni caso una volta scaricato il file controllare l'eventuale presenza di virus o trojan tramite un antivirus e un anti-malware.
- Non usare le funzioni di anteprima soprattutto sui file di cui non si conosce la provenienza o dei quali non si ha l'assoluta certezza.
- Non eseguire in modo automantico qualsiasi programma scaricato, prima è opportuno salvarlo, quindi controllarlo con un antivirus e infine eseguirlo.
- E'una buona norma non diffondere informazioni personali come mail, password, numeri di telefono o carte di credito su siti o applicazioni di cui non si ha conoscenza o che non possono garantire una adeguata sicurezza delle informazioni.

Per saperne di più...

- per informazioni: **https://trasformazionedigitale.unipv.it**
- per contattare l'Area Sistemi Informativi: **https://sos.unipv.it**
- se sei uno studente scrivi a questo indirizzo: **smart@ unipv.it** oppure contatta un tecnico del tuo dipartimento per ottenere informazioni
- informazioni in tempo reale su attacchi informatici: **https://www.csirt.gov.it**

Fonti

- Wikipedia portale sicurezza informatica - *Trojan*
- Kaspersky Lab - *Cos'è un Trojan e quali danni può provocare?*