UNIVERSITÀ DI PAVIA
Area Sistemi Informativi

n 1 Luglio 2022

Numero di attacchi informatici: le misure di difesa dell'Ateneo

I tentativi di intrusione nei sistemi informatici o di raccolta illecita di informazioni sono un fenomeno da monitorare e fronteggiare quotidianamente in Ateneo, sia sui PC dei singoli utenti sia sui dispositivi in rete all'interno di aule e laboratori.

In questo mese 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 alla rete dell'Ateneo.

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 Dipartimento al fine di acquisire consapevolezza dei rischi e quindi di adottare comportamenti adeguati alle condizioni di sicurezza.

In questo mese abbiamo avuto 82 pc infetti che sono stati segnalati e bonificati e circa 86.000 comunicazioni C&C (cioè fenomeni non leciti di controllo del proprio pc da parte di una macchina remota).

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

Benvenuti dunque nel primo numero della newsletter relativa alla cybersecurity, dove affronteremo il tema del Phishing. La newsletter è composta da una parte iniziale di carattere generale che consente di apprendere il fenomeno fornendo anche alcuni consigli iniziali per riconoscerlo, e da un seconda parte di approfondimenti per chi sarà curioso di conoscerne i dettagli. In fondo alla newsletter trovate indirizzi utili cui rivolgervi per approfondimenti o per rappresentare casi specifici.

Malware and Attacks

82
computers infected with bots

86.8K
communications with C&C sites

* C&C - Command and Control. If proxy is deployed, there might be additional infected computers. See GDPR Article 49

10 known malware downloaded by

64 users

4 Zero-days downloaded

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

171
unique software vulnerabilities were attempted to be exploited

Indicates potential attacks on computers on your network.

High Risk Web Access

8
high risk web applications

151.7MB

Potential risks: opens a backdoor to your network, hides user activity, causes data leakage or malware infections. See GDPR Article 32

0
high risk web sites

0 hits

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

1
cloud applications

10.8KB

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

Phishing: come funziona e come evitarlo

Il phishing è un tipo di truffa effettuata per lo più su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.

Sfruttando una tecnica di ingegneria sociale, viene effettuato un invio massivo di messaggi che imitano, nell'aspetto e nel contenuto, messaggi legittimi di fornitori di servizi; tali messaggi fraudolenti richiedono di fornire informazioni riservate quali il numero della carta di credito o la password per accedere ad un determinato servizio. Oltre alla posta elettronica, anche il canale telefonico viene sfruttato per la messa in atto di possibili truffe tramite telefonate o l'invio di SMS.

Il phishing è una minaccia attuale, il rischio è ancora maggiore nei social media come Facebook e Twitter, che sono normalmente utilizzati a casa, al lavoro e nei luoghi pubblici. Gli hacker potrebbero infatti creare un clone del sito e chiedere all'utente di inserire le sue informazioni personali o aziendali.

Metodologia generale di attacco

I processo standard di un attacco di phishing può riassumersi nelle seguenti fasi:

1. l'utente riceve un messaggio e-mail graficamente uguale a quellodi un'istituzione nota (ad esempio la propria banca, il proprio provider web, un sito di aste online a cui è iscritto).
2. il contenuto dell'e-mail riporta quasi sempre avvisi relativi a problemi col proprio conto corrente/account (come un addebito enorme, la scadenza dell'account, ecc.) oppure un'offerta di denaro.
3. il destinatario è invitato a seguire un link, fornito nel messaggio, per evitare l'addebito e/o per regolarizzare la sua posizione con l'ente o la società simulati (Fake login).
4. il link, però, non porta al sito web ufficiale, ma a una copia fittizia apparentemente simile al sito ufficiale, situata su un server controllato dal phisher, allo scopo di chiedere e ottenere dal destinatario dati personali specifici; la scusa addotta è spesso una richiesta di conferma o la necessità di effettuare un'autenticazione al sistema; le informazioni vengono poi memorizzate su questo server e rimangono a disposizione del malintenzionato.
5. il phisher utilizzerà questi dati per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

Come evitare il phishing?

Prima di tutto, attenendosi a criteri di senso comune.

Mantenete la calma e non lasciatevi fuorviare da offerte incredibili o provocazioni: si tratta di due elementi basilari sia nelle truffe online sia nel vishing.

Esaminate con attenzione l'aspetto del link e dell'URL a cui vi volete connettere.

Se ricevete un link sospetto da un amico o collega di lavoro, chiedete conferma al mittente prima di cliccarci sopra.

Nel caso di attacchi di phishing, ricordate che nessun impiegato bancario insisterebbe mai nel chiedere il pin della vostra carta di credito.

Non visitate mai una pagina web facendo clic su un link sospetto: inserite sempre l'indirizzo manualmente.

Inoltre, sempre bene ribadirlo, quandosi naviga su Internet, bisognerebbe sempre avere installata una robusta applicazione di sicurezza.

Non dimenticare di aggiornare regolarmente il vostro antivirus, specialmente se dotato di un modulo anti-phishing.

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**

Approfondimenti sulle tipologie di phishing

Phishing
Tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ottenere informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.

Spear phishing
Attacco mirato verso un individuo o una compagnia. Gli attaccanti potrebbero cercare informazioni sull'obbiettivo per poter incrementare le probabilità di successo.

Clone phishing
Tipo di phishing in cui una mail legittima viene modificata negli allegati o nei link e rimandata ai riceventi, dichiarando di essere una versione aggiornata. Le parti modificate della mail sono volte a ingannare il ricevente. Questo attacco sfrutta la fiducia che si ha nel riconoscere una mail precedentemente ricevuta.

Whaling
Termine coniato di recente per indicare attacchi di phishing indirizzati a figure di spicco di aziende o enti. Viene mascherata una mail/ pagina web con lo scopo di ottenere le credenziali di un manager. Il contenuto è creato su misura per l'obbiettivo, è spesso scritto come un subpoena legale, un problema amministrativo o il reclamo di un cliente. Sono state utilizzate anche mail identiche a quelle dell'FBI cercando di forzare il ricevente a scaricare e installare del software.

Manipolazione dei link

La maggior parte dei metodi di phishing usa degli exploit tecnici per far apparire i link nelle mail come quelli autentici.

È molto diffuso l'utilizzo di URL scritte male, l'uso di sottodomini (ad esempio http://www.tuabanca.it.esempio.com/ può sembrare a prima vista un sito legittimo, ma in realtà punta a un sottodominio di un altro sito).

Un altro espediente consiste nel registrare un dominio lavorando su lettere visivamente simili, ad esempio "a" ed "e" oppure, utilizzando lo stesso dominio, cambiando il suffisso da ".it" a ".com".

Infine è frequente l'inserimento del simbolo @ dopo l'indirizzo reale, seguito dall'indirizzo fraudolento, camuffando il secondo con un formato differente (ad esempio: IP); in questo modo l'utente truffato viene indirizzato all'indirizzo fraudolento, essendo il testo che precede la chiocciola ignorata dal browser.

Contraffazione di un sito web

Quando una vittima visita un sito di phishing l'attacco non è terminato. Nella pagina

possono essere infatti presenti comandi JavaScript per alterare la barra degli indirizzi. Tale operazione può essere attuata mettendo un'immagine nella barra degli indirizzi o chiudendo la finestra e aprendone una nuova con l'indirizzo legittimo.

Un attaccante può anche usare le vulnerabilità di un sito fidato e qui inserire i suoi scriptmalevoli. Questi tipi di attacco, conosciuti come cross-site scripting sono particolarmente problematici perché tutto sembra legittimo, compresi i certificati di sicurezza. In realtà tutto è fatto ad hoc per portare a termine l'attacco, rendendolo molto difficile da individuare senza conoscenze specialistiche. Un attacco di questo tipo è stato utilizzato nel 2006 contro PayPal.

Alcuni software, peraltro gratuiti, permettono di creare un sito web "clone". In pochi passaggi prelevano la struttura e le immagini in modo identico all'originale senza alcuno sforzo e/o senza necessità di possedere conoscenze informatiche. Solo a quel punto l'attaccante inserirà parloprio interno il login per catturare le credenziali di accesso, indirizzando le credenziali al suo database o più semplicemente in un file di testo.

Generalmente si adottano due principi: accettare tutte le password, senza alcuna correttezza delle informazioni inserite o rifiutare tutte le password, proponendo così di recuperare la password dimenticata.

Phishing telefonico

Non sempre il phishing implica l'utilizzo di un sito web o della mail. Talvolta il messaggio contiene un numero telefonico (gestito dal phisher, di solito si tratta di un numero Voice over IP) e se l'utente lo compone gli viene chiesto il proprio PIN. Il vishing (voice phishing) può utilizzare un finto numero di chiamante, in modo da dare l'apparenza di un'organizzazione fidata. In alcuni casi il phisher cerca di ottenere tramite WhatsApp, non dati finanziari o codici pin, ma copie di documenti d'identità che utilizzerà poi per successive truffe.

Phishing tramite SMS

Si chiama SMishing l'imbroglio perpetrato tramite [SMS].

Esistono sostanzialmente tre varianti di questa truffa:

1. vengono inviati messaggi sms relativi alla spedizione di un pacco;
2. vengono inviati messaggi sms che informano gli utenti di problemi con i loro account bancari;
3. vengono inviati messaggi sms contenenti Malware.