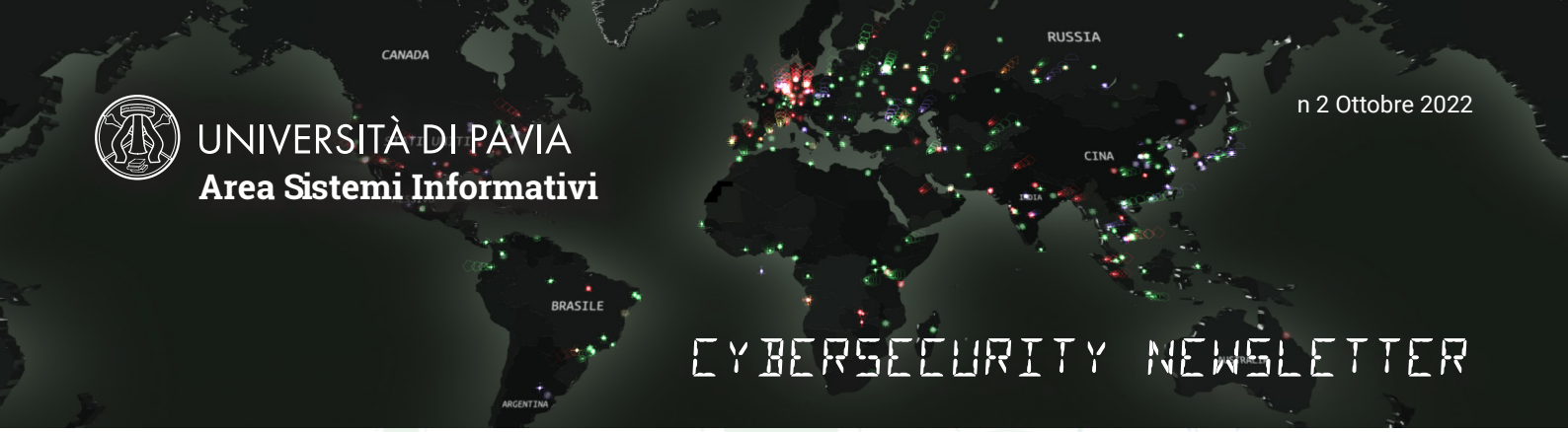

UNIVERSITÀ DI PAVIA
Area Sistemi Informativi

n 2 Ottobre 2022

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 146 pc infetti che sono stati segnalati e bonificati e circa 6.800 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 secondo numero della newsletter relativa alla cybersecurity affronteremo il tema del Ransomware.

Malware and Attacks

146
computers infected with bots

6.8K
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 **211** users

1 Zero-days downloaded

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

211
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

79.5MB

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

1
high risk web sites

2 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

Ransomware: che cos'è

Un ransomware è un tipo di malware che limita l'accesso al dispositivo che infetta richiedendo il pagamento di un riscatto (ransom in inglese) per rimuovere la limitazione. Alcune forme di ransomware bloccano il device e intimano all'utente di pagare per sbloccare il sistema, altri invece cifrano i file dell'utente chiedendo un esborso per riportare i file cifrati in chiaro.

Il ransomware cerca su un disco rigido informazioni che presumibilmente hanno valore per l'utente (come documenti, tabelle, immagini e database) e cifra tutto ciò che trova, rendendo inutilizzabili i file. Successivamente, il malware mostra un messaggio che richiede il pagamento di un riscatto per ripristinare i dati.

A fronte di un pagamento, i criminali informatici in genere si comportano in uno dei seguenti modi:

- *inviano effettivamente la chiave di decifrazione con le istruzioni;*
- *non inviano alcuna chiave e spariscono;*
- *non sono loro stessi in grado di recuperare i dati, in quanto alcuni ransomware danneggiano i file in modo irrimediabile.*

Un ransomware può entrare in un computer in vari modi, per esempio, mediante una chiavetta infetta o attraverso file scaricati da siti potenzialmente compromessi oppure che distribuiscono materiale illegale (es. software pirata). Le fonti di infezione più comuni sono le e-mail con allegati pericolosi o che contengono link a siti dannosi. L'aspetto più grave di molti programmi ransomware è la loro capacità di diffondersi tra i dispositivi della stessa rete, così come alle memorie di massa rimuovibili che vengono collegate al computer infetto. Questo significa che se il vostro computer di casa viene colpito dal malware ed avete l'abitudine di usare, ad esempio, una chiavetta USB per trasferire dati da casa al lavoro, potete infettare il computer dell'ufficio e diventare quindi fonte di diffusione del ransomware anche all'interno della rete d'Ateneo.

Metodologia generale di attacco

I ransomware tipicamente si diffondono, come altri tipi di virus, penetrando nel sistema attraverso un file scaricato o sfruttando una vulnerabilità del device. Il software malevolo, una volta presente sul dispositivo, esegue un payload (cioè un insieme di istruzioni) che cripta i file personali sull'hard disk. I ransomware più sofisticati utilizzano sistemi ibridi di criptazione adottando una chiave privata casuale e una chiave pubblica fissa. L'autore del malware è l'unico a conoscere la chiave di decriptazione privata. Alcuni ransomware invece eseguono un payload che non cripta, ma che limita

l'interazione col sistema, agendo sulla shell di Windows e rendendola non operativa e controllata dal malware stesso.
I payload dei ransomware fanno anche uso di scareware per estorcere denaro mostrando notifiche fasulle ma dall'aspetto verosimile che simulano la provenienza da Enti o Aziende note e che affermano che il sistema è stato usato per attività illecite o che contiene materiale illegale, pornografico o piratato, spingendo così l'utente a pagare una multa o sottoscrivere un abbonamento fasullo.

Altri payload imitano le notifiche di attivazione del sistema operativo (ad es. attivazione di Windows), affermando che il computer sta utilizzando una distribuzione del sistema operativo contraffatta, che va quindi regolarizzata e a tal fine chiedono di acquistare una nuova licenza. Queste tattiche forzano l'utente a pagare l'autore del malware per rimuovere il ransomware, sia con un programma che decritti i file, sia con un codice di sblocco che elimini le modifiche apportate dal malware.

Tecniche di protezione

La prima regola per proteggere il computer da attacchi ransomware come dalla maggior parte delle minacce informatiche è adottare comportamenti prudenti durante la navigazione in rete, prestando attenzione ai siti e all'apertura di e-mail sospette. Se si ha il dubbio che un attacco sia in corso o se esso viene rilevato nelle sue fasi iniziali, occorre agire prontamente rimuovendo il malware prima che tutti i dati siano criptati. Gli esperti di sicurezza suggeriscono misure precauzionali per tutelarsi dai ransomware, come l'uso di software o di altre procedure di sicurezza per bloccare i payload noti prima della loro esecuzione, o il backup offline dei dati in aree non accessibili al malware.

Come difendersi dai ransomware

1. Eseguire regolarmente i backup

Salvare regolarmente file e documenti importanti su un archivio su cloud e su un disco rigido esterno. Assicurarsi di eseguire il backup dei documenti importanti e attuali ogni pochi giorni o addirittura ogni giorno.

Avere un backup nel caso di un attacco ransomware farà sì che non venga perso nulla di importante.

Per un backup efficace, è opportuno seguire alcune regole importanti:

1. Collegare il disco rigido di backup solo quando serve per questo scopo. Qualsiasi unità collegata al computer al momento di un attacco ransomware sarà cifrata;
2. Proteggere l'accesso all'archivio su cloud con una password robusta e l'autenticazione a due fattori e non mantenere l'archivio cloud per il backup collegato al computer.

2. Fare attenzione ai messaggi

Gli allegati alle e-mail e i siti infetti sono i nascondigli più comuni per i Trojan ransomware, occorre quindi trattare tutte le e-mail e i messaggi inaspettati come potenziali fonti di pericolo.

Assicurarsi di conoscere il mittente, in caso contrario trattare il contenuto, gli allegati e i link delle e-mail provenienti da sconosciuti con diffidenza. Questa raccomandazione vale anche per i messaggi nelle app di messaggistica, sui social network e nei forum. Se si hanno dei dubbi, è consigliato spostare il messaggio nella cartella dello spam, oppure eliminarlo dall'account di posta.

3. Evitare siti web sospetti

I criminali informatici impiegano tecniche in ingegneria sociale per indurre le vittime a scaricare il malware. Se cliccando su un banner appare una risorsa web inaspettata o viene chiesto di scaricare qualcosa, chiudere immediatamente la pagina.

4. Aggiornare il software in modo tempestivo

Per accedere ai dispositivi, i criminali informatici spesso sfruttano vulnerabilità note che gli sviluppatori hanno già risolto. Chiunque non aggiorni regolarmente il proprio software è particolarmente a rischio. È buona prassi attivare gli aggiornamenti automatici quando possibile, e controllate regolarmente gli aggiornamenti per le app che non si aggiornano automaticamente.

5. Installare una soluzione di sicurezza

Le moderne soluzioni di sicurezza possono identificare e bloccare i malware in tempo reale. È consigliato quindi installare un antivirus e tenerlo costantemente aggiornato.

Cosa fare se si viene infettati

Se i cybercriminali riescono a cifrare i dati con un ransomware, non bisogna cedere al panico, potreste infatti essere ancora in grado di recuperare i vostri file:

- **Non pagate il riscatto.** Pagando si contribuisce economicamente allo sviluppo di altri malware e si incoraggiano i criminali informatici che così avranno la conferma che la loro tecnica funziona. È il caso di ricordare che è molto probabile che non si ottenga nulla neanche dopo aver pagato.
- Usate il servizio Crypto Sheriff sul sito No More Ransom (https://www.nomoreransom.org/) per scoprire quale malware ha infettato il vostro disco. Potrebbe già esistere un decryptor e, se così fosse, è possibile utilizzarlo per recuperare i dati senza spendere un centesimo. Il sito No More Ransom, creato grazie al sostegno di Europol e di aziende che combattono il crimine informatico, ospita decine di decryptor;

Esempi di ransomware

CryptoLocker
Questo ransomware a criptazione apparve nel settembre 2013: generava una coppia di chiavi RSA a 2048 bit, le caricava su un server “command-and-control” e criptava i file con estensioni di un particolare tipo. Il malware minacciava poi di cancellare la chiave privata se entro tre giorni dall’infezione non fosse stato versato un pagamento.

A causa della notevole lunghezza delle chiavi, gli analisti, e tutti coloro colpiti dal worm, ritennero Cryptolocker estremamente difficile da eradicare. CryptoLocker fu isolato a seguito della neutralizzazione del botnet Gameover ZeuS, annunciato ufficialmente dal dipartimento di Giustizia statunitense.

Si stima che prima della sua rimozione il malware abbia estorto almeno 3 milioni di dollari.

WannaCry
Venerdì 12 maggio 2017 ha iniziato a diffondersi in tutto il mondo un’ondata di ransomware che ha infettato oltre 230 000 computer in 150 paesi, con richieste di riscatto in BitCoin in 28 lingue differenti. Europol lo ha definito come il più grande attacco ransomware di sempre. L’attacco di WannaCry non si è diffuso tramite email come i precedenti, ma ha sfruttato un exploit Windows chiamato EternalBlue.

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**