EUIPO
UFFICIO DELL'UNIONE EUROPEA
PER LA PROPRIETÀ INTELLETTUALE

IDENTIFICAZIONE E ANALISI DI MALWARE SU SITI WEB SELEZIONATI SOSPETTATI DI VIOLAZIONE DEL DIRITTO D'AUTORE

SINTESI

Settembre 2018

Riassunto

I contenuti sospettati di violare il diritto d'autore rappresentano una significativa violazione dei diritti di proprietà intellettuale. Vi sono siti web che condividono tali contenuti pubblicamente, a volte anche a titolo gratuito, senza alcuna registrazione. Oltre a questi contenuti, i siti web distribuiscono comunemente vari tipi di software maligni (malware) e programmi potenzialmente indesiderati (PUP), invitando gli utenti a scaricare e avviare tali file. Il presente studio fornisce una panoramica degli esempi più aggiornati di malware e PUP rinvenuti su siti web sospettati di violazione del diritto d'autore. Tali programmi si avvalgono di tecniche ingannevoli e di ingegneria sociale, come ad esempio le installazioni «vuote» di giochi e software apparentemente «utili», per indurre ingannevolmente gli utenti finali a divulgare informazioni sensibili. Nel corso dello studio sono stati scoperti diversi PUP, quali software «utili», falsi installatori di giochi e falsi clienti per le piattaforme di streaming video. Un tale software non presenta necessariamente pericoli diretti per il software o l'hardware dell'utente. Tuttavia, attraverso trucchi di ingegneria sociale, un utente potrebbe essere convinto a divulgare dati personali sensibili o relativi alla sua carta di pagamento. Inoltre, le informazioni sul computer stesso potrebbero essere trasferite ad altre parti senza il consenso esplicito degli utenti.

Gruppo di ricerca

Il gruppo di ricerca è costituito da Francesca Bosco, responsabile del programma UNICRI, e da Andrii Shalaginov, dottorando di ricerca in sicurezza delle informazioni presso il dipartimento per la sicurezza delle informazioni e della comunicazione (Digital Forensic Group), facoltà di tecnologie dell'informazione e ingegneria elettrica, Università norvegese di scienza e tecnologia.

Clausola di esclusione della responsabilità

In tale contesto, va sottolineato che l'unico scopo della ricerca è stato determinare le caratteristiche tecniche dei malware e PUP rilevati durante lo studio e in cui gli utenti di Internet potrebbero imbattersi durante la ricerca di contenuto sospettato di violare il diritto d'autore. I campioni di malware e PUP documentati non sono da considerarsi esaustivi, né lo scopo dello studio (o dei suoi risultati) è stato quello di fornire una valutazione della probabilità complessiva o del rischio di infezione da malware e PUP a cui un utente di Internet sarebbe esposto durante la ricerca di contenuto sospettato di violare il diritto d'autore.

Prefazione

Le presunte violazioni online del diritto d'autore possono essere finanziate in vari modi, tra cui le quote di sottoscrizione, le donazioni, il pagamento per servizi ausiliari e il reddito da pubblicità online.

Tuttavia, non tutti i mezzi di finanziamento sono altrettanto innocui come gli esempi addotti. Da anni la diffusione di infezioni da malware e di altri tipi di programmi potenzialmente indesiderati (PUP) è stata di fondamentale importanza in relazione al finanziamento di presunte violazioni del diritto d'autore su Internet.

Gli utenti abituali di Internet iniziano ad acquisire consapevolezza dei rischi di potenziali infezioni quando accedono a siti web o applicazioni mobili sospettate di violare il diritto d'autore.

Il quadro di valutazione del rapporto tra i giovani e la PI 2015 dell'EUIPO ha dimostrato che il 52 % dei giovani ritiene che la sicurezza su un sito web sia un elemento importante quando si accede a contenuti online. Complessivamente, il 78 % dei giovani dichiara che ci penserebbe due volte se fosse consapevole del rischio che il computer o il dispositivo potrebbero essere infettati da virus o malware. Complessivamente, l'84 % dichiara che ci penserebbe due volte se fosse consapevole del rischio di furto dei dati relativi alla propria carta di credito.

Nella ricerca per il presente studio, l'Ufficio ha deciso di affrontare un compito estremamente impegnativo dal punto di vista tecnico, vale a dire individuare e documentare esempi di malware e PUP che un utente di Internet potrebbe incontrare quando tenta di accedere a film, musica, videogiochi e titoli televisivi contraffatti.

In tale contesto, è opportuno sottolineare che l'unico scopo della ricerca era quello di determinare le caratteristiche tecniche dei malware e dei PUP incontrati nel corso dello studio e in cui gli utenti di Internet potrebbero imbattersi durante la ricerca di contenuto sospettato di violare il diritto d'autore. I campioni di malware e PUP documentati non sono da considerarsi esaustivi, né lo scopo dello studio (o dei suoi risultati) è stato quello di fornire una valutazione della probabilità complessiva o del rischio di infezione da malware e PUP a cui un utente di Internet sarebbe esposto durante la ricerca di contenuto sospettato di violare il diritto d'autore.

La ricerca è stata condotta in diverse fasi, in stretta collaborazione con il Centro europeo per la lotta alla criminalità informatica (EC3), presso Europol.

I risultati mostrano una serie di programmi maligni e PUP diversi che un utente Internet può incontrare cercando del contenuto che viola il diritto d'autore. La maggior parte dei software maligni e dei PUP documentati possono essere descritti come Trojan o altri software indesiderati in grado di ottenere un accesso ingiustificato ai dati personali degli utenti di Internet. Questi esempi saranno pertinenti e di interesse non solo per il titolare dei diritti di proprietà intellettuale, ma anche per le autorità incaricate dell'applicazione della legge e, non da ultimo, per i consumatori preoccupati per l'accesso ai loro dati personali senza la loro autorizzazione.

Sintesi

Lo studio fornisce una panoramica degli esempi più aggiornati di programmi maligni (malware) e di programmi potenzialmente indesiderati (PUP) individuati in siti web sospettati di violazione del diritto d'autore. Tali programmi si avvalgono di tecniche ingannevoli e di ingegneria sociale, come ad esempio le installazioni «vuote» di giochi e software apparentemente «utili», per incoraggiare gli utenti finali a divulgare informazioni riservate.

L'obiettivo dello studio è quello di scoprire e documentare la diffusione di software maligni o indesiderati su siti web selezionati, sospettati di violare il diritto d'autore e di classificare i campioni individuati in base alle varie tassonomie di malware. In tale contesto, è opportuno sottolineare che lo studio ha come unico scopo quello di determinare le caratteristiche tecniche dei malware e dei PUP rilevati durante la ricerca e in cui gli utenti di Internet potrebbero imbattersi durante la ricerca di contenuto sospettato di violare il diritto d'autore. I campioni di malware e PUP documentati non sono da considerarsi esaustivi, né lo scopo dello studio (o dei suoi risultati) è stato quello di fornire una valutazione della probabilità complessiva o del rischio di infezione da malware e PUP a cui un utente di Internet sarebbe esposto durante la ricerca di contenuto sospettato di violare il diritto d'autore. Ai fini del presente studio, i programmi televisivi, i film, la musica e i videogiochi sono considerati contenuti protetti dal diritto d'autore.

Risultati dello studio

I contenuti sospettati di violare il diritto d'autore rappresentano una violazione significativa dei diritti di proprietà intellettuale. Vi sono siti web che condividono tali contenuti pubblicamente, a volte anche a titolo gratuito, senza alcuna registrazione. Oltre a questi contenuti, i siti web distribuiscono comunemente vari tipi di software maligni (malware) e programmi potenzialmente indesiderati (PUP), invitando gli utenti a scaricare e avviare tali file. Durante l'identificazione dei siti web sulla base della classifica dei 500 siti principali realizzata da Alexa, oltre alla simulazione delle ricerche effettuate dall'utente medio utilizzando motori di ricerca ben noti, come Google, Yahoo, e Bing, si è riscontrato che la serie dei siti web è cambiata tra i due cicli dello studio. Questa modifica è probabilmente il risultato degli sforzi compiuti dai motori di ricerca per eliminare i legami con i siti web sospettati di violare il diritto d'autore, mentre nuovi siti web sospetti continuano a manifestarsi. Per quanto riguarda l'identificazione dei siti web, una conclusione interessante è relativa al fatto che la stragrande maggioranza dei siti web sono ospitati negli Stati Uniti o hanno nomi di dominio collegati a servizi di hosting negli Stati Uniti. Al contrario, solo pochi si trovano sui server all'interno dell'UE. Inoltre, .com e.net sono i nomi di dominio di primo livello più frequenti usati sui siti web sospettati di violazione del diritto d'autore. Ciò può essere dovuto al fatto che, a differenza dei settori specifici di ciascun paese, questi ultimi potrebbero non richiedere l'identificazione dell'utente con un passaporto o altri documenti di identificazione. In media, fra i due cicli di identificazione è stato aggiunto un 20 % di nuovi siti web e soppresso un 20 % dei vecchi siti web. Inoltre, quasi l'8 % dei siti web individuati in entrambi i cicli è stato caratterizzato come maligno dalla piattaforma VirusTotal. Con l'aiuto di vari sistemi di gestione dei contenuti, creare un sito web e fornire contenuti agli utenti, anche di natura dolosa, è divenuta un'attività molto semplice.

Prima della raccolta dei malware, lo studio ha condotto un esame documentale delle minacce malware rilevate nel 2017 e una categorizzazione dello stato dell'arte. Tali conoscenze sono state altresì utilizzate durante l'analisi del malware per seguire i principi riconosciuti dalla comunità relativi ai tipi di malware e all'identificazione delle famiglie. In totale sono stati raccolti 106 file durante entrambi i cicli di raccolta dei dati. Tra questi figurano file scaricati direttamente da siti web sospettati di violare il diritto d'autore, nonché file creati durante l'esecuzione dei file scaricati. Nel corso dello studio sono stati scoperti diversi PUP, quali software «utili», falsi installatori di giochi e falsi clienti per le piattaforme di streaming video. Tali software non costituiscono necessariamente dei pericoli diretti per il software o

l'hardware dell'utente. Tuttavia, attraverso trucchi di ingegneria sociale, un utente potrebbe essere convinto a divulgare dati personali sensibili o relativi alla sua carta di pagamento. Inoltre, le informazioni sul computer stesso potrebbero essere trasferite ad altre parti senza il consenso esplicito degli utenti.

Il malware oggetto della raccolta è stato analizzato inizialmente con strumenti open source per comprenderne la logica interna, individuare eventuali attività dolose e valutarne la pertinenza rispetto all'attuale studio malware. Oltre all'analisi preliminare effettuata con strumenti open source, i campioni di malware raccolti sono stati analizzati dalla piattaforma Europol di analisi dei malware (EMAS). Ciò ha portato all'individuazione di numerosi artefatti diversi e di attività dolose. Le relazioni EMAS comprendono un'analisi completa dei file che utilizzano quattro versioni di Microsoft Windows, in cui il traffico di rete, le chiamate di funzione e le attività del disco sono integralmente registrate ai fini di ulteriori analisi. Inoltre, la piattaforma evidenzia tutte le attività sospette rilevate durante le procedure di esecuzione dei file. Dopo aver analizzato tutte le relazioni, EMAS ha rilevato 35 tipi di attività dolose aggregate in 17 classi di eventi dolosi. Tali attività spaziano da anomalie generali (ad esempio, processi di lancio dei sistemi o processi presenti in memoria) ad azioni inequivocabilmente dolose (ad esempio, keylogger, rootkit e manomissioni del traffico di rete).

In generale, i campioni binari dei malware e dei PUP che sono stati raccolti hanno messo in luce alcuni modelli commerciali generali diversi: programmi «utili», che dichiarano di ripulire vecchi file sul computer dell'utente a fronte del pagamento di un abbonamento; simulatori di installazione di giochi che richiedono i dati personali dell'utente; e programmi gratuiti che offrono accesso a piattaforme che distribuiscono contenuti piratati, ad esempio attraverso BitTorrent tracker. I due cicli dell'identificazione dei siti web e della raccolta di malware hanno prodotto risultati promettenti in termini di comprensione dei metodi di diffusione dei malware e di ingegneria sociale nel rubare informazioni sensibili e identificabili. Inoltre, la crescente popolarità dei dispositivi mobili negli ultimi anni è evidente alla luce del rilevamento di molti PUP per lo strumento operativo Android, disponibili attraverso le piattaforme sospettate di distribuire contenuti che violano il diritto d'autore. La correlazione delle analisi ha permesso di giungere alla conclusione che le minacce rappresentate dalla distribuzione di malware attraverso siti web che violano il diritto d'autore sono più sofisticate di quanto potrebbero apparire a prima vista. Tra i software scoperti, alcuni possono essere classificati come Trojan, adware, backdoor e agenti. A ciò si aggiunge il fatto che sono state rilevate anche molte famiglie specifiche di malware, quali WisdomEyes, DealPly e FileRepMalware. Inoltre, una tale categorizzazione completa si applica analogamente alla piattaforma Android, non solo a Microsoft Windows. Esiste un'ampia gamma di minacce per le risorse degli utenti, tra cui, ma non solo, il furto di credenziali sensibili, dati personali, informazioni sulla configurazione hardware e la modifica del traffico di rete. Pertanto, anche se il software individuato può essere un PUP, esso può comunque avere un impatto sugli utenti, soprattutto nei casi che coinvolgono un utente medio che potrebbe non essere pienamente al corrente delle pratiche e delle misure di sicurezza online di base.

Un esempio dei risultati dello studio è riportato in basso.

Sito web 03

Il sito web incoraggia gli utenti a utilizzare un'installazione di giochi falsa; l'intero processo di acquisizione delle informazioni sensibili dell'utente è cambiato tra il primo e il secondo ciclo di raccolta di malware. L'utente di questo servizio scarica un archivio che contiene materiale «mascherato» sotto forma di attività di gioco e non un file eseguibile esplicitamente binario che può essere rilevato come dannoso da un programma antivirus. L'archivio criptato concede

Sito web 09

Il sito offre l'accesso a qualsiasi tipo di contenuto video disponibile attraverso torrent tracker con l'aiuto di uno strumento software. Questo strumento richiede meno interazioni tra gli utenti rispetto ad altri tracker di BitTorrent. Sono sufficienti pochi clic per scaricare contenuti da fonti sconosciute, mentre l'utente non è protetto, né esercita il controllo su quanto viene scaricato.

Sito web 08

(Android) Il sito web consente di accedere a una gamma di applicazioni mobili gratuite senza registrazione. Con un'unica applicazione si ha accesso illimitato allo streaming di spettacoli televisivi e di film. Non viene fatta alcuna richiesta esplicita di fornire informazioni sensibili o dettagli sui pagamenti per l'acquisto di video protetti dal diritto d'autore. Tuttavia, l'utente deve disattivare le impostazioni di sicurezza che consentiranno l'installazione di applicazioni diverse da quelle che provengono dal mercato delle applicazioni

Metodologia

Al fine di svolgere la ricerca, è stato necessario adottare una rigorosa metodologia per trattare la selezione di titoli e siti web, nonché il compito tecnicamente difficile di individuare e documentare gli esempi di malware e PUP rilevati. Una breve panoramica della metodologia è descritta qui di seguito.

1. Nella fase I della ricerca UNICRI, in collaborazione con l'Osservatorio europeo sulle violazioni dei diritti di proprietà intellettuale (Osservatorio), è stato istituito un gruppo di esperti al fine di fornire consulenza sulla metodologia di ricerca, sulla selezione dei siti web utilizzati per l'analisi e di valutare le ricerche svolte in ciascuna fase dell'attuazione del progetto. Il gruppo di esperti era composto da rappresentanti delle parti interessate dell'Osservatorio, organizzazioni titolari di diritti, università, autorità preposte all'applicazione della legge e agenzie dell'UE.

2. In parallelo è stato selezionato il gruppo di ricerca. Nel quadro della presente relazione non era tecnicamente possibile[1] effettuare ricerche su tutti gli Stati membri dell'UE; durante la fase II sono stati scelti a caso 10 paesi campione selezionati fra i 28 Stati membri dell'UE.

3. Nella fase III sono stati identificati film, programmi televisivi, canzoni e videogiochi famosi. Tale popolarità ha riguardato la popolarità a livello mondiale e la popolarità in solo uno o più dei 10 paesi campione all'inizio del periodo di raccolta dei dati, ovvero al 23 giugno 2017. Nelle fasi successive dello studio, tali titoli campione sono stati sistematicamente utilizzati nelle ricerche online per trovare siti web e applicazioni mobili che violano il diritto d'autore. Ciascun titolo soddisfa due o più dei seguenti criteri:

   - popolare al momento della raccolta dei dati negli Stati membri dell'UE,
   - popolare al momento della raccolta dei dati su scala globale,
   - storicamente popolare a livello mondiale, e
   - classificato come film, programma televisivo, canzone o videogioco.

   Sono stati selezionati cinque titoli cinematografici, cinque titoli televisivi, cinque titoli musicali e cinque giochi per videogiochi, per un totale di 20 titoli di campioni. È stata prestata particolare attenzione alle fonti utilizzate per individuare la popolarità di un particolare titolo, il che ha comportato una procedura di selezione sistematica per garantire che i dati di partenza fossero disponibili per tutti gli Stati membri o per la maggior parte di essi.

4. Nella fase IV sono stati identificati siti web sospettati di fornire accesso illegale a materiale protetto dal diritto d'autore a livello mondiale e/o tra i 10 paesi campione al 26 giugno 2017 (primo ciclo di raccolta di malware). In una fase successiva dello studio, tali siti web sono stati analizzati per individuare la presenza di malware e programmi potenzialmente indesiderati.

   La metodologia per individuare i casi di sospetta violazione del diritto d'autore è stata messa a punto con il contributo del gruppo di esperti individuato nella fase I, nonché a seguito del riesame da parte dell'UNICRI della letteratura esistente. È stata specificamente concepita per generare un campione di siti web che:

   - siano popolari tra i diversi Stati membri dell'UE, garantendo un'ampia copertura geografica;
   - rappresentino tipi diversi di siti web sospettati di violazione del diritto d'autore, compresi siti web di streaming, siti web di link, siti web di hosting, cyberlocker e siti web torrent;

[1] Il numero di paesi selezionati avrà un impatto diretto (ovvero, un aumento) del numero di casi selezionati su siti web che violano il diritto d'autore e dei relativi file binari da analizzare. Si è pertanto deciso di concentrarsi solo su un campione di paesi per essere in grado di realizzare efficacemente la parte pratica dello studio entro un periodo di tempo determinato.

- rappresentino una vasta gamma di contenuti sospettati di violazione di diritto d'autore, compresi film, titoli televisivi, musica e videogiochi; e
- rappresentino siti web in cui l'utente medio di Internet ha la probabilità di imbattersi nel tentativo di accedere a materiale sospetto di violazione del diritto d'autore.

Per la selezione dei siti web sospettati di violazione del diritto d'autore, sono state seguite cinque fasi. Le prime tre fasi sono state concepite per individuare i siti web più popolari che violano il diritto d'autore tra gli Stati membri dell'UE. Questo metodo riproduce gli scenari in cui un utente medio può cercare i siti web sospettati di violazione del diritto d'autore senza specificare, ad esempio, il titolo di un film o di una canzone. Le ultime due fasi sono state concepite per individuare i siti web sospettati di violazione del diritto d'autore in cui un utente medio potrebbe imbattersi nella ricerca di soluzioni per scaricare un titolo popolare senza specificare un sito web. Questa fase è stata particolarmente significativa, data la presenza di presunti siti web dannosi che effettuano attività di avvelenamento dei risultati della ricerca, tramite la quale sfruttano argomenti di tendenza attraverso l'ottimizzazione di motori di ricerca. I due approcci insieme hanno contemplato i vari modi che un utente medio di Internet ha a disposizione per trovare online materiale sospetto che viola il diritto d'autore.

L'accento è stato posto sull'analisi concomitante di malware e PUP specifici per applicazioni mobili su dispositivi, quali smartphone e tablet, come una delle principali minacce emergenti nella lotta alla criminalità informatica. L'analisi è stata limitata ai dispositivi Android a causa delle indicazioni contenute nella letteratura esistente di una maggiore presenza di malware negli store di applicazioni Android (ossia Google Play) rispetto allo store «iTunes» di Apple. La metodologia è stata concepita per generare un campione di applicazioni mobili che:

- siano molto popolari al momento della raccolta dei dati su scala mondiale;
- rappresentino diversi tipi di applicazioni (comprendenti applicazioni streaming, applicazioni torrent e applicazioni hosting);
- contengano o forniscano accesso a una vasta gamma di contenuti sospettati di violare il diritto d'autore (compresi film, titoli televisivi, musica e giochi per dispositivi mobili); e
- rappresentino ciò che un utente medio di un dispositivo mobile può incontrare nel tentativo di scaricare o utilizzare un'applicazione che facilita l'accesso a contenuti sospetti protetti dal diritto d'autore.

5. La fase V è consistita nella raccolta di malware e PUP, oltre alle applicazioni mobili sui siti web identificati, da esaminare in una fase successiva per una corretta classificazione. La fase di acquisizione dei dati ha previsto due cicli di attività di raccolta e analisi di malware svolte durante l'estate 2017. Il primo ciclo di raccolta di malware ha evidenziato 1 054 nomi di dominio unici, mentre la seconda ha individuato 1 057 nomi di dominio unici in 10 Stati membri dell'UE selezionati. Il malware è stato raccolto sia in maniera manuale, sia automatica al fine di simulare l'esperienza media dell'utente.

Raccolta manuale. Questo metodo prevedeva l'esame manuale dei domini individuati nella fase precedente. Grazie alla raccolta manuale, l'esperto è stato in grado di simulare l'esperienza di un utente medio di Internet cliccando su messaggi pubblicitari e interagendo con siti che richiedevano prompt.

Raccolta automatica. Questo metodo ha previsto l'utilizzo di un web crawler automatico sviluppato da un esperto per seguire tutti i link disponibili su un sito web sospettato di violazione del diritto d'autore. Su un dato sito web, il crawler ha raccolto in primo luogo le informazioni dai link verso la home page. In un secondo momento, il crawler ha seguito ciascuno di questi link a siti secondari. In una terza fase, il crawler ha seguito ciascuno di questi link a siti terziari. In ciascuna fase, il crawler rileva file binari che potrebbero essere d'interesse per la successiva analisi manuale, compresi malware e programmi potenzialmente indesiderati sospetti o potenziali. Questo processo è proseguito fino a un massimo di 1 000 collegamenti per sito web.

6. Una volta raccolti, i file binari sono stati analizzati in un ambiente di calcolo sicuro per comprendere la loro funzionalità interna e per una corretta classificazione. L'analisi preliminare si è basata su strumenti open source per essere in grado di correlare i risultati con le relazioni sulle minacce informatiche. I campioni di software raccolti sono stati quindi forniti a EMAS per essere analizzati; l'analisi EMAS è stata quindi confrontata con i risultati preliminari.

Panoramica della metodologia

Campioni di malware e PUP rilevati

Al 28 luglio 2017 erano stati automaticamente controllati 5 240 siti (1 054 unici) durante il primo ciclo di raccolta, con 617 file pertinenti (musica, video, file torrent e software) recuperati di dimensioni complessive pari a 47 GB. Il lotto di file non sottoposti a cernita ha richiesto un'ulteriore analisi per decidere quali fossero pertinenti per lo studio. I campioni di siti web che violano il diritto d'autore erano simili in tutti i 10 paesi campione per ciascuno dei tipi di media (programmi televisivi, film, musica e videogiochi). Di conseguenza, il Belgio è stato scelto casualmente tra i paesi campione e tutti i siti identificati come siti di violazione del diritto d'autore per il Belgio sono stati verificati manualmente per la presenza di software dannosi o altresì indesiderati. Il 10 agosto 2017, dopo il secondo ciclo di raccolta, sono stati automaticamente individuati 3 665 file da siti web di tutti i paesi, per dimensioni complessive pari a 167 GB. Il numero complessivo delle URL uniche estratte per tutti i paesi era di 1 057 sui 5 606 siti web, questo ha reso impossibile controllare manualmente tutti i paesi.

Dopo un'analisi preliminare dei file raccolti, sono stati estratti 106 file binari unici per MS Windows, Android e Mac OS a seguito di entrambi i cicli di raccolta di malware. Più specificatamente, sono stati selezionati 41 file nel corso del primo ciclo e 65 nel corso del secondo ciclo, in particolare: 2 per Mac,

15 per Android e 89 per MS Windows. Di questi, 21 possono essere considerati come programmi dannosi noti, come i molteplici antivirus aggregati dalla piattaforma VirusTotal. Tra questi figurano i file scaricati direttamente da siti selezionati, sospettati di violare il diritto d'autore, nonché i file creati durante l'esecuzione dei file scaricati. Successivamente i campioni di software raccolti sono stati analizzati in ambiente SandBox e trasmessi a EMAS per un'analisi più approfondita di eventuali attività dolose. Complessivamente, sono stati rilevati 821 eventi pericolosi diversi in quattro relazioni EMAS (Windows 7 SP1, Windows7 SP1 64-bit, Windows 10 64-bit, Windows XP SP3) per tutti i file binari. Alcune delle relazioni non hanno evidenziato alcuna attività sospetta, mentre alcune di esse avevano fino a 10 attività dolose precedentemente note. Nella fase finale dello studio è stata effettuata la correlazione fra i risultati dell'analisi preliminare e quelli delle relazioni EMAS. Nella tabella seguente figura il riepilogo quantitativo dei risultati.

	Ciclo 1	**Ciclo 2**
Data	28 luglio 2017	giovedì 10 agosto 2017
Siti web scoperti in 10 paesi dell'UE	5 240	5 606
Siti web unici	1 054	1 057
File pertinenti	617	3 665[2]
Dimensioni dei file pertinenti GB	47	167
Trasmessi a EMAS		
Android	3	12
MAC OS	2	–
MS Windows	36	53
Dimensioni totali, byte	175 600 117	522 991 095

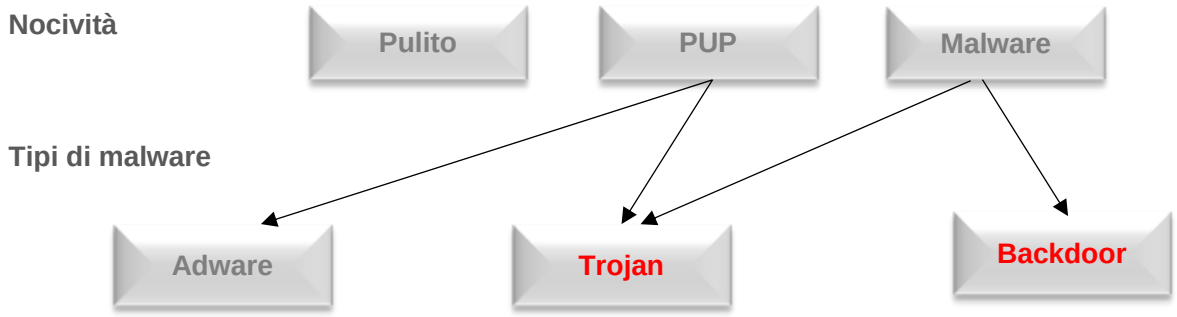
Soluzione di analisi dei malware di Europol (EMAS)

La soluzione di analisi dei malware (EMAS) di Europol è una soluzione dinamica e automatizzata di analisi dei malware fornita da Europol agli Stati membri dell'UE. EMAS offre la possibilità di elaborare relazioni di analisi, ma la sua caratteristica più rivoluzionaria è quella di produrre informazioni per gli investigatori di polizia. I controlli incrociati automatizzati possono mostrare dei legami tra gli attacchi effettuati in paesi diversi con lo stesso malware o con la stessa organizzazione criminale dietro la stessa famiglia di malware, che si collegano agli stessi settori e si riferiscono a indagini diverse all'interno o al di fuori dell'UE. Nel 2015 EMAS è diventata completamente automatizzata per consentire l'accesso diretto alle parti incaricate dell'applicazione della legge con le quali Europol ha concluso accordi operativi. Nel 2015: 525 108

Come illustrato nella figura riportata di seguito, i file binari raccolti possono in genere essere classificati in categorie a seconda della nocività come benigni (file che non provocano danni), PUP e malware nocivi. Inoltre, sono stati rinvenuti PUP anche per Android e per OS Mac, il che indica che gli sviluppatori di software maligni cercano di influenzare il maggior numero possibile di utenti utilizzando piattaforme diverse. I programmi potenzialmente indesiderati e i software maligni possono essere ulteriormente differenziati in base alle principali tipologie di malware, ossia Trojan, adware e backdoor. La maggior parte dei software rinvenuti rientrava nella categoria dei PUP. Il funzionamento dei PUP può essere associato ad uno dei seguenti modelli di business: l'installazione di giochi falsi con richieste di dati personali e coordinate bancarie, lo scaricamento di programmi «utili» che costringono gli utenti ad acquistare una versione a pagamento o a installare programmi gratuiti per accedere a piattaforme che violano il diritto d'autore. Tali applicazioni possono compromettere i dati personali degli utenti e la configurazione del computer. Attraverso trucchi di ingegneria sociale, possono essere altresì divulgati

[2] Per spiegare la differenza di numero tra il ciclo 1 e il ciclo 2, durante il ciclo 2 della raccolta automatizzata alcuni siti web hanno pubblicato serie multiple di file su ciascuna delle loro pagine web.

vari tipi di dati privati, come dati relativi alla carta di pagamento e credenziali relative agli account di accesso ai social media. Analogamente, la ricerca ha individuato 15 applicazioni Android da mercati di applicazioni terzi e, dopo l'analisi preliminare, si è concluso che tali applicazioni possono essere coinvolte nella distribuzione di contenuti che violano il diritto d'autore e nella divulgazione di dati personali.



Minacce per gli utenti finali

Nel corso dei due cicli di identificazione dei siti web e di analisi dei malware, non sono stati individuati file binari di tipo ransomware. In generale, la maggior parte dei malware raccolti può essere caratterizzata come Trojan, il che significa che questi possono essere rappresentati sui siti web come software benigni o software popolari, mentre in realtà possono rubare o divulgare informazioni private. Un utente inesperto potrebbe avere un grado elevato di fiducia nel software e non essere in grado di rilevare eventuali anomalie. Inoltre, l'analisi statica e le osservazioni dinamiche sul comportamento di tale software potrebbero non rivelare la piena funzionalità senza disporre di un codice sorgente. A seguito dell'analisi preliminare di malware, l'analisi EMAS ha rivelato attività dolose più specifiche. L'installazione del software sul computer dell'utente finale potrebbe avere conseguenze considerevoli e causare non solo perdite finanziarie, ma anche il furto di dati personali e altri rischi di accesso e di controllo indesiderati. Tali attività potrebbero comportare la raccolta e la trasmissione di dati personali a terzi in formato cifrato o aperto. Tali dati possono consistere, ad esempio, nelle credenziali di accesso al conto corrente del browser, in informazioni dettagliate sulla configurazione hardware e/o software, ovvero in ogni altro dato digitato attraverso la tastiera.

INDIVIDUAZIONE E ANALISI DI MALWARE SU SITI WEB SELEZIONATI SOSPETTATI DI VIOLAZIONE DEL DIRITTO D'AUTORE

SINTESI

Settembre 2018