Nuove vulnerabilità in Android consentono di effettuare un attacco di phishing che permette di rubare le credenziali utente da qualsiasi applicazione e per qualsiasi versione del sistema operativo.

La scoperta e la soluzione di un gruppo di ricercatori UniGe ed EURECOM

Un gruppo di ricercatori dell'Università di Genova, Dipartimento di Informatica, Bioingegneria, Robotica ed Ingegneria dei Sistemi (DIBRIS), e di EURECOM Graduate School and Research Center in Digital Science (Biot Sophia Antipolis, Francia) ha individuato nuove **vulnerabilità in Android**, il più diffuso sistema operativo per dispositivi mobili, che consentono di realizzare un **attacco di *phishing***, semplice da attuare ed estremamente efficace, che permette di rubare le credenziali dell'utente (login e password) **da ogni applicazione installata e su qualsiasi versione del sistema operativo sviluppata finora.**

I ricercatori hanno proposto al team sicurezza di Android alcune soluzioni per sanare tali vulnerabilità, che verranno probabilmente rilasciate già nei prossimi aggiornamenti del sistema operativo.

Non è la prima volta che la collaborazione tra UniGe ed EURECOM porta a risultati significativi in questo campo di studio. Nel 2018, lo stesso gruppo di ricerca è riuscito ad ingannare i più famosi *password manager* forzandoli a consegnare le credenziali salvate ad app malevole (link), anche in questo caso tramite un attacco di *phishing*. Mentre all'epoca l'attacco di *phishing* abusava di alcune nuove funzionalità introdotte in Android 8, questa nuova scoperta si basa su una funzionalità disponibile fin dalla prima versione del sistema operativo. Per questo motivo, il nuovo attacco è attuabile a prescindere dal dispositivo o dalla versione del sistema, e ha un impatto molto maggiore.

Il *phishing* è un attacco informatico volto a ingannare l'utente, il quale sarà portato a consegnare le proprie credenziali ad una applicazione malevola invece che a una applicazione legittima, nota all'utente, della quale lo stesso si fida. Per risultare efficace, un attacco di *phishing* richiede che l'applicazione malevola:

1. sia identica a quella originale;
2. venga eseguita al posto dell'originale;
3. si mostri all'utente nel momento preciso in cui lo stesso si aspetta di interagire con l'applicazione originale.

Sebbene il primo punto sia abbastanza facile da realizzare in quanto richiede all'attaccante di creare una copia apparentemente identica (dal punto di vista grafico) dell'applicazione originale, i sistemi di sicurezza di Android, estesi e migliorati negli anni, hanno reso finora estremamente difficile realizzare i punti 2 e 3.

Tuttavia, i ricercatori Antonio Ruggia e Alessio Merlo del Computer Security Lab (http://csec.it) del DIBRIS, Università di Genova, Simone Aonzo, Dario Nisi e Andrea Possemato di EURECOM, hanno scoperto una serie di vulnerabilità collegate a una funzionalità del sistema operativo – ***inotify*** – che permettono di aggirare facilmente tali protezioni.

In breve, *inotify* permette ad un'applicazione di ricevere una notifica qualora un'altra applicazione venga avviata. Data la potenziale pericolosità di un servizio di questo tipo, il sistema operativo Android permette alle applicazioni di usarlo solo sotto determinate e stringenti condizioni. Ciononostante, il lavoro dei ricercatori ha portato alla scoperta di una serie di vulnerabilità causate da sbagliate configurazioni che permettono di trarre vantaggio dalle funzionalità di **inotify**, di fatto permettendo ad un'applicazione malevola di essere *notificata* nel momento preciso in cui una qualsiasi applicazione bersaglio venga avviata o, più in generale, cambi di stato. In questo modo, l'applicazione malevola può avviarsi concorrentemente con l'originale per eseguire l'attacco (ad esempio, sostituendosi alla stessa), realizzando facilmente i punti 2 e 3 dell'attacco di *phishing*.

L'efficacia e l'impatto dell'attacco di *phishing* descritto possono essere valutati in un video (https://www.youtube.com/watch?v=k3FO-Tews04) in cui risulta evidente l'impossibilità per l'utente umano di distinguere l'applicazione malevola da quella originale.

Va infine sottolineato come l’applicazione malevola possa implementare una variante di questo attacco senza bisogno di particolari privilegi; inoltre, il risultato più allarmante è che **tutte le applicazioni e tutte le versioni del sistema operativo Android sviluppate finora sono potenzialmente vulnerabili a questo tipo di attacco.**
Maggiori informazioni e dettagli tecnici completi sono disponibili al link:
https://www.s3.eurecom.fr/post/2023/03/06/android-notify-me-when-it-is-time-to-go-phishing/