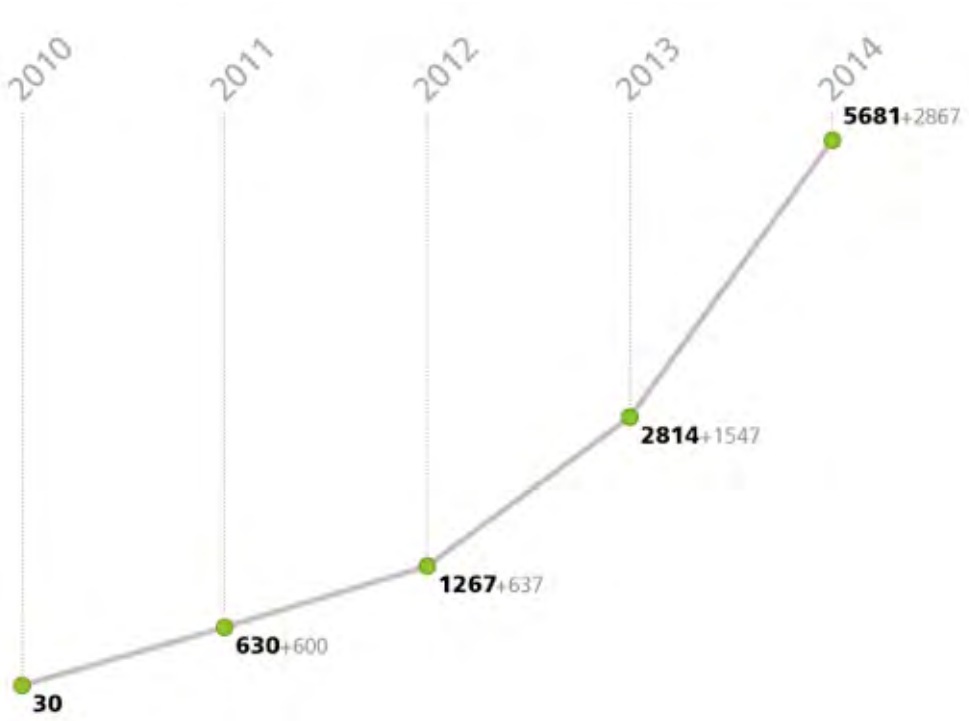
Ruberia mobile

Android è il sistema operativo per smartphone e tablet più popolare ed è il secondo più preferito dopo Windows dal punto di vista degli autori dei virus. I primi programmi malevoli per Android comparvero nel 2010.

La maggior parte dei programmi malevoli viene creata per infettare i dispositivi mobili gestiti da Android – a causa dell'utilizzo su larga scala e del codice aperto di questo SO, nonché della possibilità di installare applicazioni ottenute da varie fonti.

Questo grafico mostra com'è aumentato il numero di record per i programmi malevoli per SO Android nel database dei virus Dr.Web



Nel 2014 il numero di record è aumentato del 102%!

Dal 2010 il numero di record è aumentato di 189 volte!

Secondo i dati del 1° aprile 2015, il numero di firme antivirali aggiunte al database dei virus Dr.Web per il rilevamento delle applicazioni malevole Android ha raggiunto pressoché 7 mila.

Cioè solo nei tre primi mesi del 2015, il database si è accresciuto di più del 25%!

Si dovrebbe tenere presente che attraverso una firma antivirale Dr.Web può rilevare più di un programma malevolo.

La maggior parte dei programmi malevoli per Android viene creata allo scopo di FURTO.

I dispositivi mobili possiedono ricche funzioni, e i creatori dei trojan Android rubano tutto quello che si può rubare:

- Denaro — dall'account di telefonia mobile, dal conto bancario tramite sistemi di online banking e dalle carte di credito
- Login e password — credenziali di accesso ai sistemi di online banking e di pagamenti elettronici, ad account in social network e così via
- Messaggi SMS
- Chiamate
- Messaggi di posta elettronica
- Fotografie — si possono usare per ricattare la potenziale vittima o per causarle il danno morale pubblicando le foto in Internet
- Registrazioni delle conversazioni del proprietario del dispositivo mobile — se non è l'utente che attiva la registrazione, può farlo il trojan
- Indirizzi dalla rubrica
- Coordinate del dispositivo — cioè la posizione del proprietario e le informazioni sui suoi spostamenti
- Qualsiasi informazione tecnica circa il dispositivo (identificatori IMEI/IMSI/SID, numero di cellulare, versione del SO, versione SDK del sistema, modello del dispositivo, informazioni su produttore)

In molti casi gli utenti stessi scaricano e installano programmi malevoli su dispositivi mobili!

Così per esempio, il malware Android.Plankton, che può raccogliere le informazioni circa il dispositivo compromesso e trasmetterle ai malfattori, fu stato scaricato manualmente dagli utenti 150.000 volte (!) dal sito ufficiale Android Market (il nome precedente di Google Play) prima che fu rimosso dall'amministratore del catalogo.

Secondo le statistiche di Dr.Web per Android, circa il 50% dei nostri utenti utilizza sul dispositivo l'opzione che permette di scaricare applicazioni da sorgenti sconosciute (diverse da Google Play). Questo significa che gli utenti stessi potrebbero installare un'applicazione malevola scaricata da un forum o sito non attendibile.

I metodi del social engineering consentono ai criminali informatici di distribuire i trojan tra gli utenti su larga scala. Per esempio, **più di 30 mila** utenti sudcoreani dei dispositivi Android hanno scaricato il trojan banker Android.SmsBot.75.origin aprendo una pagina fraudolenta con le informazioni su una "spedizione postale".

La maggior parte degli utenti pensa che possa accorgersi dell'attività di un trojan sul dispositivo mobile.

Un trojan ben fatto però è un trojan che è impercettibile per l'utente.

Gli autori dei virus l'hanno capito da qualche tempo.

Nella maggior parte dei casi, si può scoprire l'attività dei trojan più di successo, progettati per il furto di denaro, solo dopo che tutto è stato già rubato.

- Per esempio, il trojan-dialer Android.Dialer.7.origin, per diminuire la probabilità che la sua attività indesiderata venga scoperta dall'utente, disattiva l'altoparlante del dispositivo mobile per il tempo della "conversazione telefonica" da esso fatta, e per celare completamente la sua attività malevola, rimuove tutte le relative informazioni dal registro di sistema e dall'elenco chiamate.
- Possono nascondersi bene anche quei trojan che rubano denaro dall'account di telefonia mobile, abbonando l'utente a qualche servizio a pagamento.

Di solito un servizio a pagamento manda sms di conferma dopo la fine di un'operazione — i trojan celano questi messaggi affinché l'utente non se ne accorga della ruberia. Alcuni programmi malevoli possono mandare automaticamente gli sms con il codice di conferma per l'autenticazione in servizi a pagamento — e spesso anche tali messaggi vengono intercettati e celati.

- Alcuni trojan progrediti sono camuffati da software legittimi e una volta scaricati e avviati, rimuovono la loro icona e in seguito funzionano in un modo invisibile agli utenti.
- Vi sono dei trojan che i malfattori incorporano dentro il sistema operativo oppure in un'immagine firmware. In tali casi, il malware ha i poteri avanzati e può eseguire una vasta gamma di azioni indesiderate senza farsi scoprire dall'utente.
- Per raggirare i programmi antivirus, alcuni trojan utilizzano la funzione della resistenza a software di sicurezza: possono bloccare il funzionamento degli antivirus e persino rimuoverli completamente dal dispositivo.

Trojan-banker

Sono famiglie di trojan Android create allo scopo di rubare denaro da carte di credito e bancomat e da sistemi di pagamenti online.

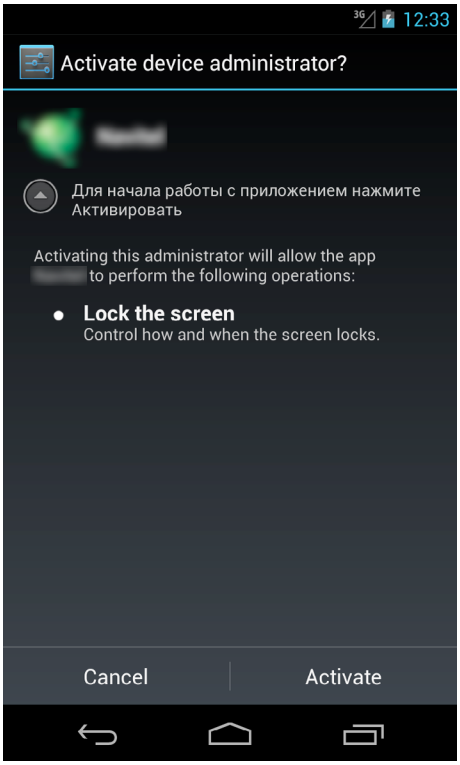
Il mobile banking è un servizio veramente utile. Molte banche offrono ai loro clienti le versioni Android delle applicazioni per l'online-banking. Vengono utilizzate non soltanto per fare le transazioni personali, ma anche i pagamenti aziendali. Di solito, questa possibilità viene usata dai top manager che hanno l'accesso al conto bancario della loro azienda.

Il furto del denaro è il principale vettore di attacco dei criminali informatici.

Android.BankBot.33.origin

È in grado di:

- ottenere le informazioni circa il saldo del conto corrente e l'elenco delle carte di credito e bancomat associate al cellulare dell'utente;
- rubare le credenziali dell'account di home-banking, caricando nel browser del dispositivo infetto un sito web fraudolento che imita l'aspetto del vero sito di una banca e offrendo alla vittima di immettere le informazioni di autenticazione;
- effettuare transazioni illegali con il denaro delle vittime, trasferendolo su un conto appartenente ai malintenzionati.



La vittima potrebbe per qualche tempo rimanere all'oscuro del furto accaduto, perché l Android.BankBot.33.origin può intercettare e nascondere gli avvisi via sms di transazioni effettuate.

Gli utenti STESSI installano questo trojan (è possibile se nelle impostazioni del sistema operativo è consentita l'installazione di programmi da fonti sconosciute)!

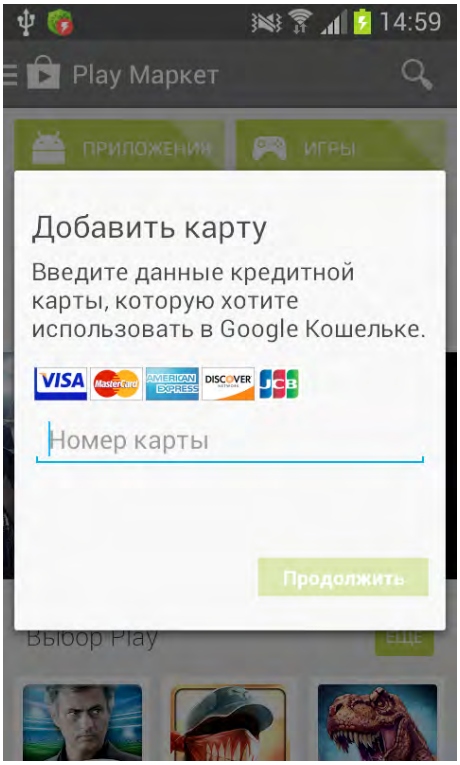
Da gennaio ad aprile 2015 questo programma malevolo è stato rilevato sui dispositivi degli utenti dell'Antivirus Dr.Web per Android 62.840 volte, il che costituisce lo 0,37% del numero totale di minacce rilevate in questo periodo.

Android.SpyEye.1

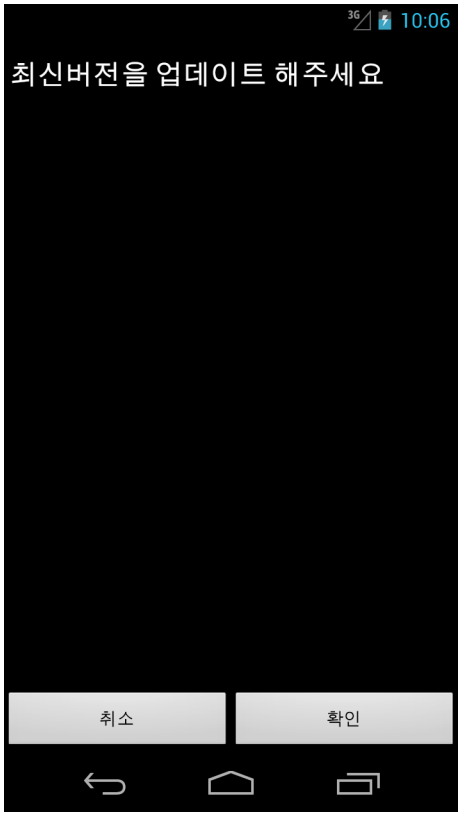
Se l'utente del desktop o del notebook visita un sito di banca di cui l'indirizzo è presente nel file di configurazione del trojan bancario che ha infettato il suo computer, il programma malevolo incorpora nella pagina visualizzata un testo o un modulo web per l'inserimento delle credenziali di accesso al conto. La vittima, che non sospetta nulla, carica nel browser la pagina web della banca in cui ha un conto corrente e scopre un messaggio che dice che la banca ha messo in atto nuove misure di sicurezza, senza osservare le quali l'utente non può accedere al sistema di home-banking, e inoltre offre di caricare sul telefono un aggiornamento del client mobile, che in realtà contiene un trojan. Questo programma è capace di intercettare e di mandare ai malintenzionati le password inviate via sms, necessarie per accedere al sistema di home-banking.

Android.BankBot.21.origin

Per ottenere i dettagli di pagamento della carta di credito o bancomat in uso e per rubare il denaro, l' Android.BankBot.21.origin controlla se sul dispositivo mobile è attiva la finestra dell'applicazione Google Play e se è così, visualizza un falso modulo per l'associazione della carta all'account utente. Le informazioni digitate dalla vittima vengono trasmesse sul server appartenente ai malfattori. Il successivo furto del denaro è già una cosa facile.



Android.BankBot.29.origin



Il trojan prova a ottenere i privilegi di amministratore sul dispositivo mobile — nasconde la relativa richiesta di sistema dietro la propria finestra di dialogo, e come risultato la potenziale vittima con l'alta probabilità potrebbe assegnare all'app malevola i privilegi richiesti. Il successivo furto del denaro è già una cosa facile.

Furto degli SMS in arrivo

Direste che il furto di un messaggino è una cosa di poco conto. Dipende dallo scopo con cui è stato mandato sul vostro telefono l'sms rubato dai malintenzionati.

Quali sms, la perdita dei quali può portare a danni finanziari, vengono rubati dai trojan?

- SMS che confermano o chiedono l'autorizzazione per l'abbonamento a servizi mobile premium o servizi di contenuti. I malintenzionati intercettano tali sms affinché la vittima più a lungo possibile rimanga all'oscuro dell'abbonamento a tali servizi e non prenda provvedimenti per interrompere l'attività del trojan.
- SMS con gli avvisi dei sistemi di home-banking che contengono codici mTAN.

Gli sms rubati vengono trasmessi sul server di controllo del trojan in possesso dei malintenzionati. Questa funzionalità è disponibile nei trojan di diverse famiglie.

Furto del denaro tramite l'invio degli sms in uscita

Per esempio, i trojan della famiglia **Android. SmsSend** rimettono denaro dall'account mobile dell'utente a favore dei malintenzionati inviando sms a costo elevato dal telefono della vittima.

Secondo le statistiche ottenute mediante Dr.Web per Android, nel 2014 i trojan della famiglia Android.SmsSend sono stati rilevati 20.223.854 volte.

I trojan della famiglia **Android.SmsBot** anche possono inviare, intercettare e cancellare messaggi sms.

Secondo le statistiche ottenute mediante Dr.Web per Android, nel 2014 i trojan della famiglia Android.SmsBot sono stati rilevati 5.985.063 volte.

Furto del denaro tramite le chiamate a numeri premium

I dialer sono trojan per Android che effettuano chiamate a numeri premium (chiamate a costo elevato) all'insaputa del proprietario del dispositivo mobile. È un altro modo di guadagni illeciti, popolare tra gli autori dei virus.

Secondo le statistiche ottenute mediante Dr.Web per Android, nel 2014 i trojan della famiglia Android.Dialer sono stati rilevati 177.397 volte.

Furto degli indirizzi dei contatti

Anche quest'attività costituisce un business. Ogni contatto reale può essere venduto, e ci sono diverse categorie degli acquirenti.

1. Spammer. Lo spamming è un business che prospera. Non è soltanto l'invio di innocua pubblicità.

Sempre più spesso i malintenzionati inviano in massa messaggi sms che includono un link per il download di un programma malevolo: al momento questo è un popolare modo per distribuire minacce Android.

Per esempio il worm **Android.Wormle.1.origin** può diffondersi via sms, inviando messaggi a tutti i contatti del proprietario del dispositivo compromesso. Alla fine di novembre 2014, risultavano infettati dal worm **Android.Wormle.1.origin** oltre 15.000 dispositivi mobili Android in circa 30 paesi.

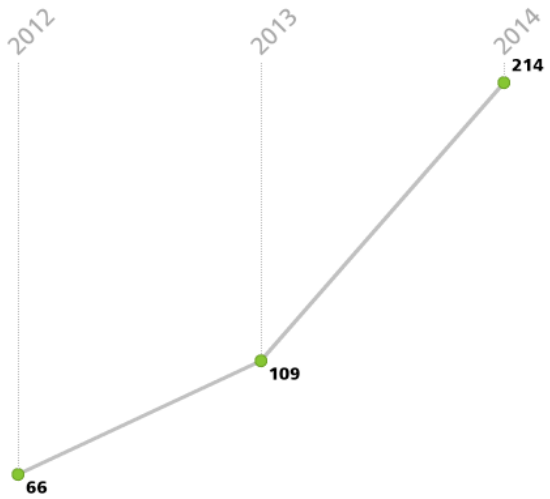
2. Phisher. Raccolgono contatti per mandare messaggi che includono falsi link di siti di banche o di sistemi di pagamento. Se l'utente entra in tale sito, il phisher potrà ricavare le sue credenziali di autenticazione per l'accesso al sistema di home-banking o i dettagli della sua carta di credito. E l'utente stesso tradirà le sue informazioni segrete, digitandole nei moduli creati dal phisher, pensando che siano quelli della banca.

3. Organizzatori di attacchi DDoS — hanno un disperato bisogno dei contatti dei proprietari dei dispositivi mobili i quali loro possono infettare e quindi utilizzare per attuare attacchi DDoS contro, per esempio, un concorrente di un loro cliente.

4. Spie (servizi segreti, concorrenti). Ogni contatto è una manna per la spia o per il ricattatore. Gli spioni possono leggere messaggi dell'utente, registrare le sue conversazioni, caricare le sue foto su un server remoto.

Per esempio, il trojan Android.Spy.130.origin invia ai malintenzionati le informazioni circa i messaggi sms in arrivo e in uscita e le chiamate effettuate, le coordinate GPS attuali, e inoltre può fare una chiamata a un numero impostato all'insaputa dell'utente e in questo modo trasforma lo smartphone o il tablet infetto in un dispositivo di ascolto.

Aumento del numero di record per i trojan della famiglia Android.Spy nel database dei virus Dr.Web.



Utilizzate spesso i servizi

- Google Play
- Google Play Music
- Gmail
- WhatsApp
- Viber
- Instagram
- Skype
- "VKontakte"
- "Odnoklassniki"
- Facebook
- Twitter...?

I truffatori metteranno a frutto le informazioni che ci conservate — le venderanno o le useranno per il ricatto!

Dr.Web protegge i dispositivi Android dalla ruberia mobile

Componenti di protezione

Antivirus
Protegge dai trojan e dagli altri programmi malevoli

Antifurto
Vi aiuterà a trovare il vostro dispositivo mobile se smarrito o rubato e, se necessario, consentirà di cancellare da esso le informazioni confidenziali su remoto

Antispam
Difende da chiamate ed SMS indesiderati

Filtro URL basato su cloud
Restringe l'accesso alle risorse Internet indesiderate a prescindere dallo stato dei database dei virus nel vostro Dr.Web per Android installato

Firewall
Controlla l'attività delle applicazioni in rete

Auditor della sicurezza
Valuta lo stato del dispositivo, rileva problemi della sicurezza e propone le soluzioni per risolverli

Link utili

Progetto informativo "Ruberia mobile"