УДК 004.056.53

Антон Олександрович НОВИЦЬКИЙ,
магістр факультету № 6
Харківського національного університету внутрішніх справ

АНАЛІЗ РИНКУ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ МОБІЛЬНОГО БАНКІНГУ

Загрози для мобільних платформ значно еволюціонували в плані кількості і рівня складності. Це пов'язано з тим, що все більше хакерських програм, що спочатку створювалися для ПК, були «переорієнтовані» на мобільні платформи. Якщо говорити про мобільні загрози в цілому, то, в порівнянні з аналогічним періодом минулого року, кількість нових сімейств шкідливих програм для Android (які як і раніше становлять до 99% всіх мобільних загроз) в цьому році впевнено зростає, причому мова не тільки про зростання активності відомих загроз, але про появу нових категорій ПЗ. Користувачі продукції Apple також не можуть вважати себе повністю захищеними від цих небезпек. Кіберзлочинці прагнуть «освоїти» цю широку, а тому привабливу аудиторію потенційних жертв. Не дивно, що кожен рік число фішингових атак на користувачів платформ Apple зростає.

За словами експерта з кібербезпеки компанії IBM Лімор Кессі (Limor Kessem), за останні кілька місяців ринок шкідливих програм для мобільних пристроїв дуже активізувався. Сьогодні їх використовують різні кіберзлочинці, від професіоналів, до недосвідчених користувачів форумів, які купують шкідливий програмний продукт, покладаючись на програмні установки за замовчуванням і підтримку послуг від підпільних постачальників.

Одним з найдавніших і дорогих на чорному ринку троянів є GM Bot. Ціна нової версії в порівнянні зі старою виросла з $ 5000 до $ 15000. Завдяки витоку його вихідного коду в лютому 2016 року з'явилося кілька послідовників GM Bot. У троянів немає такого розмаїття властивостей, як у GM Bot, але коштують вони на порядок дешевше (від $ 3000 до $ 6000). Вони здатні накладати додатковий шар поверх легітимних сторінок, зокрема банківських. З його допомогою зловмисник отримує логіни і паролі жертв. Злочинець може самостійно змінювати налаштування форм, в тому числі для викрадення даних платіжних карт. Серед таких троянів-послідовників можна виділити Bial Bot, Cron Bot і KNL Bot.

Дослідники IBM X-Force розповіли, що автор популярного мобільного банкера GM Bot нещодавно був заблокований на найбільших торгових майданчиках даркнета через конфлікт з покупцем. За відсутності головного конкурента, автори трьох інших троянів для Android виступили вперед і тепер змагаються за лідерство на чорному ринку.

Аналітики IBM відстежують банківський троян GM Bot з 2014 року. Згідно з їхніми даними, малваре за ці роки вже встигла поміняти власника, пережила не один витік вихідних кодів, але продовжує залишатися успішним продуктом, популярним серед кіберзлочинців.

Після того як вихідні коди GM Bot в черговий раз стали надбанням громадськості в лютому 2016 року, його автор не розгубився і вже в березні представив нову версію банківського трояна. Разом з релізом нової версії розробник втричі підвищив ціну малварі: вона зросла з $ 5000 до $ 15000.

Дослідники IBM X-Force повідомляють, що в квітні 2016 року у автора трояна GM Bot відбувся певний конфлікт з одним із клієнтів, в результаті чого розробника заблокували майже у всіх основних магазинах даркнета. Через це обставини, а також в силу недавнього підвищення ціни, активізувалися автори конкурентних шкідників, які давно усвідомили, наскільки перспективним є сегмент Android-малваре. Зараз за вакантне місце топового мобільного банкера змагаються шкідники Bilal Bot, Cron Bot і KNL Bot.

KNL Bot вважається найбільш просунутим рішенням з перерахованої трійки. Автор малварі хвалиться, що його дітище володіє практично всіма тими ж функціями, що і GM Bot, зате коштує вдвічі менше: тоді як найдешевша версія GM Bot оцінювалася в $ 8000 в місяць, KNL Bot можна придбати за $ 4000 в місяць. У рекламі шкідника заявлено, що KNL Bot здатний: перехоплювати вхідні SMS, а також відправляти вихідні повідомлення; здійснювати голосові виклики або встановлювати їх переадресацію; перекривати екран оверлеєм, щоб змусити жертву повірити, що вона як і раніше працює в легітимному додатку; працювати в прихованому режимі (відключивши екран, звук і вібрацію). Автор трояна заявляє, що KNL Bot «неможливо видалити», тобто гарантує стійкий root-доступ. Також розробник надає опціональну можливість управління шкідником за допомогою SMS-повідомлень.

Bilal Bot являє собою трохи більш просте рішення, але і його ціна складає всього $ 3000 на місяць (плюс автор надає клієнтам безкоштовні патчі). Розробник Bilal Bot використовує найбільш агресивний маркетинг з усієї трійці. Автор трояна не соромиться поносити конкурентів, наприклад, заявляє, що GM Bot вже став занадто відомий і його дуже легко виявити, а також має досить велику кількість багів і не може похвалитися гарною підтримкою. Згідно з заявою творця, Bilal Bot вже сьогодні є одним з найбільш ефективних банкерів (хоча знаходиться в стадії розробки). Хоча малваре вже зараз має всі необхідні функції, основну фішку автор обіцяє представити в недалекому майбутньому. Розробник обіцяє, що незабаром фішингові оверлеї можна буде редагувати прямо з контрольної панелі малварі.

Cron Bot – зовсім новий шкідник, експерти вперше помітили його на початку квітня 2016 року. Основна відмінна риса Cron Bot - кросплатформеність. Заявлено, що троян працює як на iOS, так і на

Android. Ціна шкідника варіюється від $ 4000 до $ 7000 в місяць, в залежності від набору функцій.

Cron Bot комплектується набором різних модулів: hVNC, stealer, injects, SOCKS5, loader, keylogger, cmd і так далі. Крім того, троян може похвалитися маленьким розміром (всього 400 Кб) і поставляється з білдером для модифікацій.

Автор шкідника, так само як і його конкуренти, обіцяє стійкий root-доступ, перехоплення SMS-повідомлень, перенаправлення голосових викликів, збір і розкрадання будь-яких даних з зараженого пристрою, перекриття вікон інших додатків фальшивками і так далі.

Як можна помітити, всі шкідники поширюються по підписці, як послуга. Аналітики IBM відзначають, що схема malware-as-a-service на сьогодні вже набрала більшу популярність. Так автори шкідливого програмного забезпечення намагаються унебезпечити себе, захищаючись від можливих витоків і копіювання коду.

Експерти IBM X-Force відзначають, що поки не фіксували великих шкідливих кампаній з використанням перерахованих вище троянів і не піддавали шкідників детальному аналізу.

Більшість Android-пристроїв заражається під час скачування додатків з неофіційних сайтів. Однак шкідники можуть проникати і в офіційні магазини і встановлюватися разом з легітимними програмами.

Фахівці компанії Avast попереджають, що різних модифікацій банківського трояна GM Bot (також відомого під назвами Acecard, SlemBunk і Bankosy) стає все більше.

Фахівці Avast повідомляють, що після витоку коду, цілком передбачувано, був зафіксований значний ріст аналогів GM Bot. Тільки за останні три місяці користувачі мобільних додатків Avast зіткнулися з трояном понад 200 000 разів. Шкідники на базі GM Bot маскуються під додатки більш ніж п'ятдесяти різних банків з усього світу. Серед жертв малварі опинилися клієнти мобільних додатків Citi Bank, ING, Bank of America і інших великих банків в США, Канаді, Австралії та країнах Європи.

За даними Avast, варіації GM Bot вражають користувачів мобільних додатків наступних банків: США і Канада: BNC, American Express, Chase, CIBC, Citi Bank, ClairMail, Coinbase, Credit Karma, Discover, goDough, First PREMIER bank, Bank of America, JPMorgan Chase, Skrill, Western Union, PayPal, PNC, SunTrust, TD Bank, TransferWise, Union Bank, USAA, US Bank Access Online Mobile, Wells Fargo; Австрія: BAWAG P.S.K., easybank, ErsteBank / Sparkasse, Volksbank, Bank Austria, Raiffeisen; Австралія: Bank West, ING Direct, National Australia Bank, Commonwealth Bank, Bank of South Australia, St. George Bank, Westpac; Німеччина: Deutsche Bank, ING DiBa, DKB, Sparkasse, Comdirect, Commerzbank, Consorsbank, Volksbank Raiffeisen, Postbank, Santander; Франція: ING Direct, Crédit Mutuel de Bretagne, Crédit Mutuel Sud Ouest, Boursorama Banque, Téléchargements, Caisse d'Epargne, CIC, Crédit Mutuel, La Banque Postale, Groupama, MACIF,

Crédit du Nord, Axa, Banque Populaire, Crédit Agricole, LCL, Société Générale, BNP Paribas; Польща: Comarch, Getin Group, Citi Bank, Bank Pekao, Raiffeisen, BZWBK24, Eurobank, ING Bank, mbank, IKO, Bank Millennium; Туреччина: Akbank Direkt, QNB Finansbank Cep Şubesi, Garant, İşCep, Halkbank, VakıfBank, Yapı ve Kredi Bankası, Ziraat.

Фахівці нагадують, що найчастіше GM Bot як і його клони виглядає як невинна програма для Android і маскується під плагінів типу Flash або контент для дорослих. В основному малваре поширюється через сторонні каталоги програм, а аналоги GM Bot орієнтовані переважно на банківські програми. Так, при відкритті мобільного банку малваре підвантажує підроблену сторінку для введення логіну і пароля. Крім того, троян може перехоплювати SMS-повідомлення, так що двухфакторна автентифікація і одноразові коди проти нього не працюють. Якщо ж користувач мав необережність надати додатком права адміністратора, зловмисники зможуть контролювати все, що відбувається на інфікованому пристрої.

Одержано 06.11.2018

УДК 343.9.01+343.97

Наталя Анатоліївна ОРЛОВСЬКА,
доктор юридичних наук, професор,
начальник кафедри кримінального права та процесу
Національної академії Державної прикордонної служби України імені Б. Хмельницького

ПРО ВІКТИМОЛОГІЧНИЙ МОНІТОРИНГ ЯК ДЖЕРЕЛО ІНФОРМАЦІЇ ЩОДО ТОРГІВЛІ ЛЮДЬМИ

Належне інформаційне забезпечення запобіжної діяльності – одна з обов’язкових умов її ефективності. При цьому важливим є налагодження каналів отримання інформації про кримінологічну ситуацію, за рахунок чого стає можливим вивчення стану злочинності. Однак не менш нагальним є зворотний зв'язок, адже суспільство має бути зацікавленим в обізнаності у тому, що відбувається в країні. Громадська думка щодо злочинності – це не просто «стан масової свідомості», це колективне уявлення про оцінюваний об'єкт, і суспільство повинно прагнути, щоб це уявлення було максимально наближено до реальності.

У цьому контексті на особливу увагу заслуговує моніторинг – один з методів збору інформації. На відміну від технології статистичного обліку, моніторинг є цільовим спостереженням з орієнтацією на виявлення тенденцій розвитку з метою прогнозування ситуації, що змінюється. Зміст кримінологічного моніторингу складають процеси отримання, обробки й аналізу необхідної для формулювання кінцевих висновків інформації. Застосування відповідного методу не відрізняється особливою глибиною