КИБЕР АТАКИ В МОБИЛНА СРЕДА

Росен Пасарелски

Александър Иванов

CYBER ATTACKS IN MOBILE ENVIRONMENT

Rosen Pasarelski

Alexander Ivanov

The large amount of intended attacks and criminal activities experienced in recent years has exposed the Internet to serious danger regarding the security of users. These malicious attacks are made to inflict harmful effects to many different targets through Internet. The most successful attacks are made with so called botnets – collection of infected machines (bots) controlled by the bot-master to launch devastating attacks and crime activities. It is very important to detect, analyze and terminate suck overlay networks before they become active. A different research on botnet activity is mostly related to detection and disruption of the thread.

1. Обхват на действие на съвременните кибер-атаки

Терминът кибер-атака или още наричан мрежова компютърна атака (Cyber Network Attack - CNA) се дефинира като - "Зловреден компютърен код или друг умишлен акт, предназначен да променя, да наруши, да деградира, или да унищожи информация, пребиваваща или съхранявана в компютри и компютърни мрежи или да повреди самите тях". С увеличаването на потреблението на Интернет и телекомуникационни услуги, с модернизирането на компютърната и комуникационна техника се увеличава и ръста на злонамерените кибератаки. Списък с известни кибератаки и възможни тенденции за заплаха на населението в областта на информационните и телекомуникационни технологии може да бъде представен, както следва:

- интернет атаки чрез социалните мрежи
- подслушване на мрежата /Network sniffers/
- прихващане на IP пакети /Packet spoofing/
- отвличане на сесия /Session-hijacking/
- промишлен шпионаж /Industrial espionage/
- Email разпространение на зловреден код /Email propagation of malicious code/
- Анти-криминалистични техники /Anti-forensic techniques/
- Широкомащабно използване на червеи / Wide-scale use of worms/

Съвременните кибер-атаки разглеждат утвърдените и разпознаваеми практики за атакуване на компютри в мобилна среда. В най-честия случай става въпрос за атаки, наблюдявани върху персонални компютри, лаптопи и т.н. Еволюцията на компютрите от десктоп до мобилни архитектури пренася атаките от десктоп средите към мобилните устройства. Причината за увеличаващите се атаки на мобилни устройства е непрестанното увеличение на използването на подобен тип устройства. Проучвания показват, че до 2020 г. мобилните устройства ще са над 6 млрд. Поради този факт, хакерите все повече се съсредоточават към прилагането на атаки към мобилни устройства – смартфони, таблети, pda устройства и др.

Лидери на пазара на мобилни операционни системи са Android, iOS, Windows Phone, BlackBerry OS. Повечето инструменти, с които се осъщесвяват кибер атаките са насочени главно към тези платформи

2. **Атаки на незащитени и защитени мрежи - MITM (Man-In-The-Middle)**

Едни от най-често срещаните мрежови атаки, използвани срещу голям брой организации и единични потребители , са man-in-the-middle(MITM) атаки. Считана като атака чрез активно подслушване, MITM работи чрез установени връзки между устройствата на потребителите и препредаващи се съобщения между тях. В случаи като тези, жертвата вярва, че комуникира директно с друг потребител, докато всъщност комуникационния поток до хоста се пренасочва. Крайния резултат е че атакувания хост не само се подслушва, но може също така да бъде манипулиран потока от данни през него с цел бъдещ контрол на потрбителите му

3. **Атаки чрез SMS Flood посредством Skype**

Един от най-успешните и практикувани методи за D-DoS (Denial of Service) атаки. При този метод се залага на атакуване на дадена цел (domain, сайт, услуга) от многобройни места с безкрай заявки. Самия D-DoS представлява невъзможността на даден сайт или услуга да обработва и обслужва прекалено много заявки едновременно. Атаките могат да бъдат разделени на няколко групи:

- TCP атаки на IPv4 адрес (TCP/IPv4 flooding) (подаване на прекалено много заявки на услуга използваща IPv4 адресация с цел претоварване на системата)

- TCP атаки на IPv6 адрес (TCP/IPv6 flooding) (подаване на прекалено много заявки на услуга използваща IPv6 адресация с цел претоварване на системата)

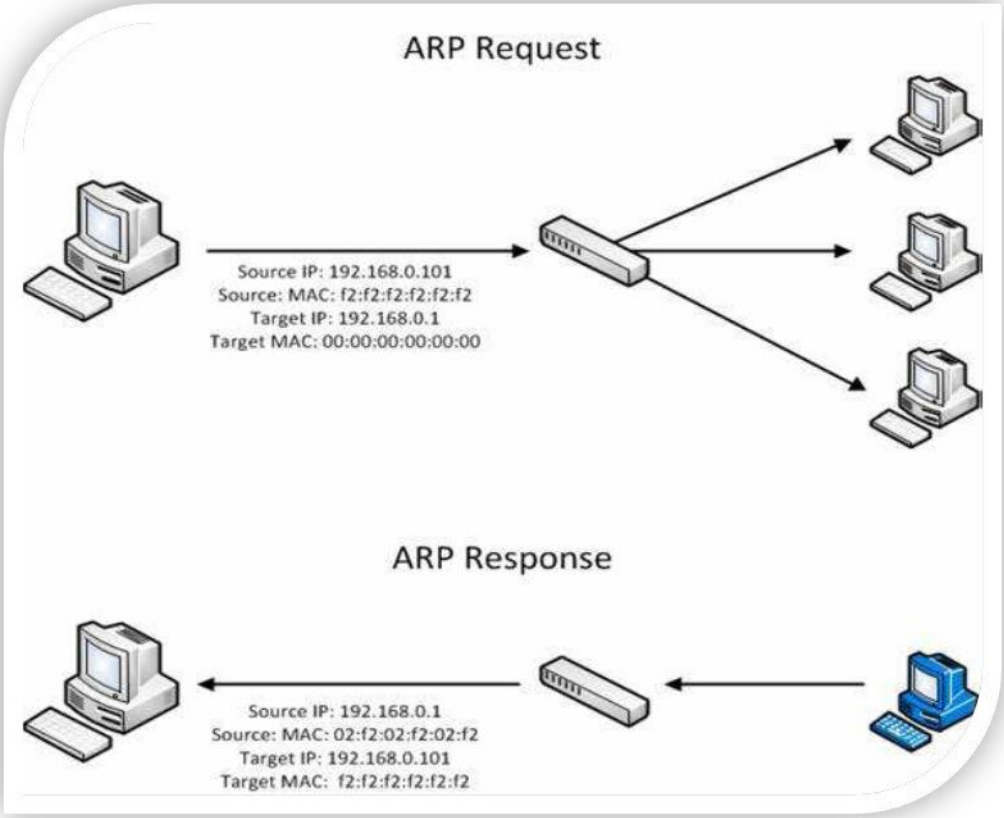
- SYN атаки (SYN & ICMP) (подаване на прекалено много заявки към дадена услуга с цел да се попречи използването на мрежовия ресурс)

- UDP атаки на несъществуващ порт (пример: целта има отворен само порт TCP 80 за уеб услуга, атаката се прави на UDP порт 80 – резултата е kernel panic (пробива се ядрото на системата)

По аналогичен начин, дупка в услугата за мигновенни съобщения, може да бъде използвана за "наводняване" на мобилно устройство, посредством SMS. Чрез изпълняване на html код и след въвеждане на мобилен номер, атакуващия използва метод за възстановяване на парола в Skype за да атакува мобилен телефон. HTML кодът добавя цикличност на това действие, в резултат на което могат да бъдат изпратени безброй SMS към даден мобилен номер. Поради факта, че Skype работи с всички страни по света, този метод работи към всички мобилни оператори, при това без способност да бъде локализиран (пълна анонимност). SMS известията се получават от името на Skype и така атакуващият заличава следите си.

4. Атаки чрез заразяване на DNS услуга - DNS Poisoning (ARP Cache)

Една от най-старите форми на модерната MITM атака е ARP(address resolution protocol) Cache Poisoning , също позната като ARP Poison Routing. Тя позволява на атакуващ от същата подмрежа като на жервите да подслушва целия мрежови трафик между тях. Тя е една от най-просто изпълнимите атаки, но е считана като една от най-ефективната атака използвана някога от хакерите. ARP протокола е проектиран поради необходимост от улеснение на препредаването на мрежовите адреси между второто и третото ниво на OSI модела(канален и мрежови слой). Каналното ниво използва MAC адреси, които хардуерните устройства могат да използват за директна комуникация по между си. Мрежовото ниво използва IP адреси за да създаде големи мащабируеми мрежи, комуникиращи с други мрежи из целия свят. Всеки слой притежава собствена адресираща схема, като те трябва да работят заедно за да се осъществи мрежовата комуникация. За тази цел ARP протокола беше създаден като An Ethernet Address Resolution Protocol.

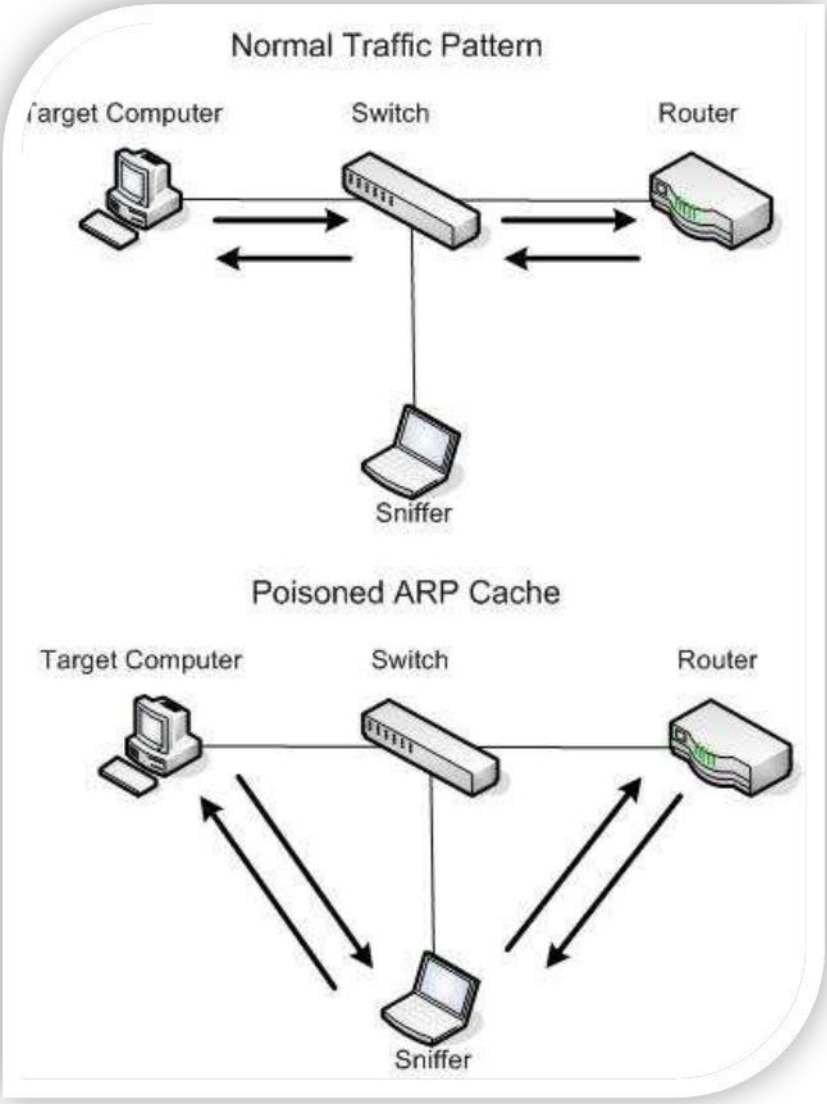


Фиг. 1 – ARP комуникационен процес

Основните етапи на ARP комуникациите са ARP заявака и ARP отговор. Целта на заявката и отговора е да се открие MAC адреса , който отговаря на дадения IP адрес, така че трафика да може да достигне до крайната дестинация от мрежата. Пакета за заявката се изпраща до всички устройства в мрежовия сегмент. В нея се записват IP и MAC адреса на източника и IP адреса на крайния получател. Това устройство, което разпозане своя ip адрес в тази заявка, отговаря с IP-то си и търсения MAC адрес. Веднъж като се е осъществил този процес, предаващите устройства си обновяват свойта ARP кеш таблица и устройствата имат възможност да комуникират по между си.

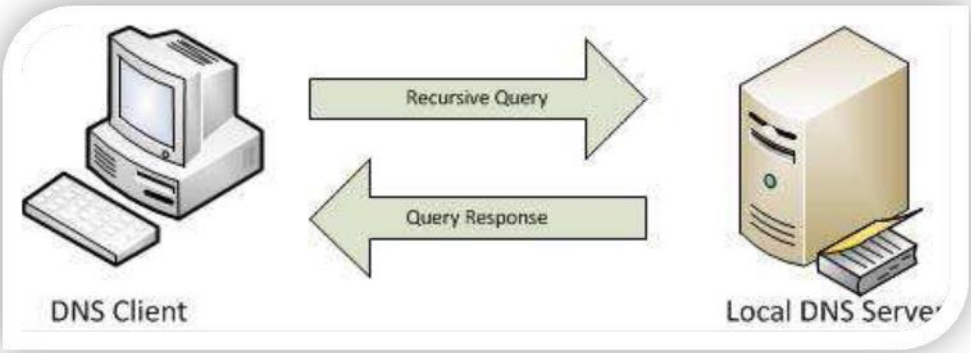
Poisoning the Cache : ARP cache poisoning използва незащитената част от ARP протокола. Докато протоколи като DNS, които могат да бъдат конфигурирани да приемат само защитени динамични ъпдейти, устройствата, които използват ARP, ще приемат всички и по всяко време. Това означава , че всяко устройство може да изпрати ARP отговор до даден хост за да обнови неговия ARP кеш с зловредна информация. Изпращането на ARP отговор, когато не е генрирана заявка, се нарича gratuitous ARP(безпричинен). Когато злонамерена намеса предоставя резлутата от няколко добре известни gratuitous ARP пакети, може да

предизвика хоста да си мисли, че комуникира с един хост, но всъщност комуникира с атакуващия, който го подслушва.



Фиг. 2 – Комуникация при ARP cache poisoning

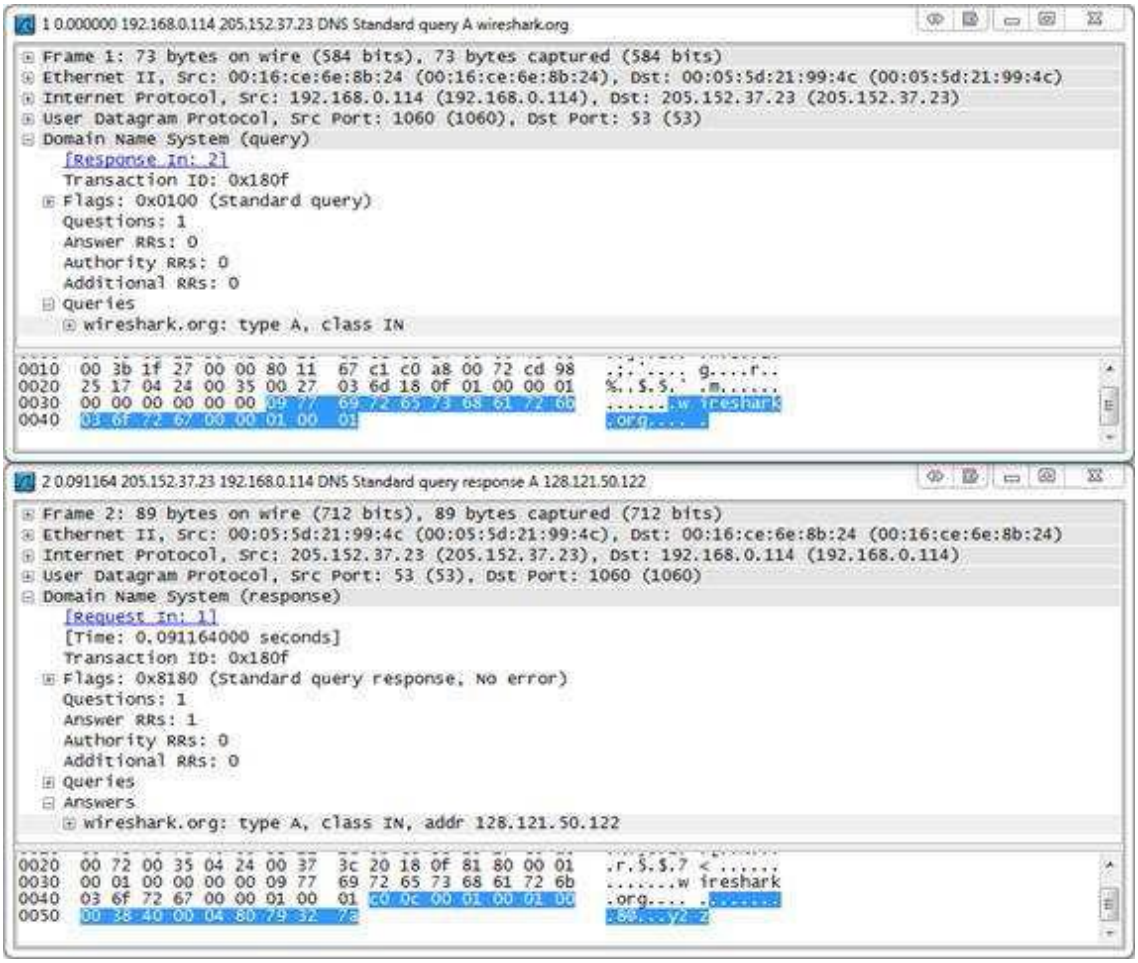
Domain Naming Sustme(DNS) протокола е считан за един от най-важните протоколи, които изграждат интернет. При въвеждане в браузера на web адрес се осъществява DNS заявка до DNS сървър с цел откриване на реалния IP адрес, който се свръзва с Web адреса. Това е необходимо, защото рутерите и устройствата за комуникация в интернет използват единствено IP адреси. DNS сървъра от своя страна работи като съхранява база от данни от карта с врзъки между IP адреси и DNS имена. Тази архитектура на DNS сървърите в интернет може да бъде малко сложна за обеснение.



Фиг. 3 – Основни DNS заявки(query) и отговори(response)

Когато клиента желае да преобразува(resolve) DNS име до IP адрес той изпраща запитване до DNS сървъра и той му отговаря с нужната информация. От гледна точка на клиента единствените видими пакети са заявката и отговора(фиг. 5). Това обаче се усложнава при отчитането на рекурсвината архитектура DNS сървърите в Internet. DNS сървърите трябва да имат възможност да комуникират по между си за да отговорят на запитванията от клиента, за които не съхраняват информация. От един локален DNS сървър може да се очавка да познава именованото пространство само на неговата локална мрежа. При към заявка него за адреси извън това пространство то се обръща рекурсивно към друг DNS сървър, който се намира по-високо в йерархията на DNS сървърите в интернет.(фиг. 4).

Фиг. 4 – Основни DNS заявки(query) и отговори(response)



Фиг. 5 –DNS query и response пакети

5. Атаки чрез заглушаване на WiFi сигнал - Killing WiFi signal

Заглушаването на WiFi сигнал се изразява в спирането на комуникацията между даден потребител (мобилен телефон, таблет и т.н.) и маршрутизатора, осигуряващ му интернет. Програмата използва метода на ARP Cache poison, като отклонява трафика на потребителя от точката за достъп. В резултат на това, атакуващият може да прекъсне трафика между точката за достъп и мобилното устройство, ползващо безжична мрежа чрез набор от инструкции към собствена Firewall система (iptables chains & rules). С инструкция (правило) “REJECT“ атакуващия спира целия трафик към атакуваното устройство за неопределен период от време. Самата програма не може да бъде засечена при наблюдението на трафика на точката за достъп поради факта, че използва единкъв физически (MAC address) с нея.

6. Методи за защита

MITM атаките са трудни за предотвратяване поради това , че атаката е пасивна по природа. Типично е потребителите изобщо да не узнават за подменена DNS информация и кога са били пренасочени към зловредни хостове. Това, което виждат най-често е уеб страницата, която очакват. Щетите от подобни действия на виртуалните престъпници могат да бъдат много значителни.
Можем да посочим няколко важни неща, които могат да се направят за да се защитим от този род атаки:

- **Висока степен на сигурност на вътрешната мрежа** и устройствата към нея. Атаките като тази, най-често се изпълняват от вътрешната мрежа на хоста. Ако мрежовите устройства са сигурни тогава съществува по-малък шанс за компроментирани хостове да бъдат използвани за Spoofing атаки.

- **Не трябва да се разчита на DNS като защитена система.** За високо чувствителни и защитени системи, които типично няма да достъпваме през браузерите в интернет, много често се прилага добрата практика да не се използва DNS. Ако даден софтуер разчита на именовани хостове за да функционира, то тогава те може да се опишат в специализирани, ръчно създадени файлове на хоста.

- **Използване на IDS:** Система засичаща инструкциите, която да засича не-типично поведение в ARP и DNS комуникацията.

- **Използване на DNSSEC:** DNSSEC е нова алтернатива на DNS, която използва цифрово подписани DNS записи за да осигури валидация на заявките и отговорите. DNSSEC не е все още широко разпространена, но е широко приета като бъдещето на DNS. Тя осигурява много висока степен на защита от подобен род атаки и не случайно ще се използва от всички военни и правителствени домейни в САЩ от тази година.

7. Заключение

Развитието на комуникационните мрежи и технологии води до неизменно обединяване на предлаганите услуги – като телефония, интернет, телевизия и др. Мобилната среда дава свобода на потребителите да използват хиляди приложения навсякъде, където се придвижват. С повишаване на ръста на мобилните абонати и услуги нарастват и заплахите от атаки в мобилна среда. Голяма част от кибер атаките са изключително опасни за потребителите, защото водят до присвояване на лични данни и

самоличност, банкови акредетиви, e-mail и facebook акаунти и много други. Съществуват и атаки водещи до откази на цели корпоративни системи и огромни загуби за бизнеса. Срещу кибер атаките и хората, които ги осъществяват трябва да се води ежедневна борба за противодействие и държавата, телекомуникационните оператори и бизнеса не трябва да пестят усилия и ресурси.

Използвана литература:

1. http://windowsecurity.com/
2. http://www.windowsecurity.com/articles/Understanding-Man-in-the-Middle-Attacks-ARP-Part1.html
3. http://www.windowsecurity.com/articles/Understanding-Man-in-the-Middle-Attacks-ARP-Part2.html
4. http://www.oxid.it/cain.html
5. http://ettercap.sourceforge.net/