ERT Threat Alert

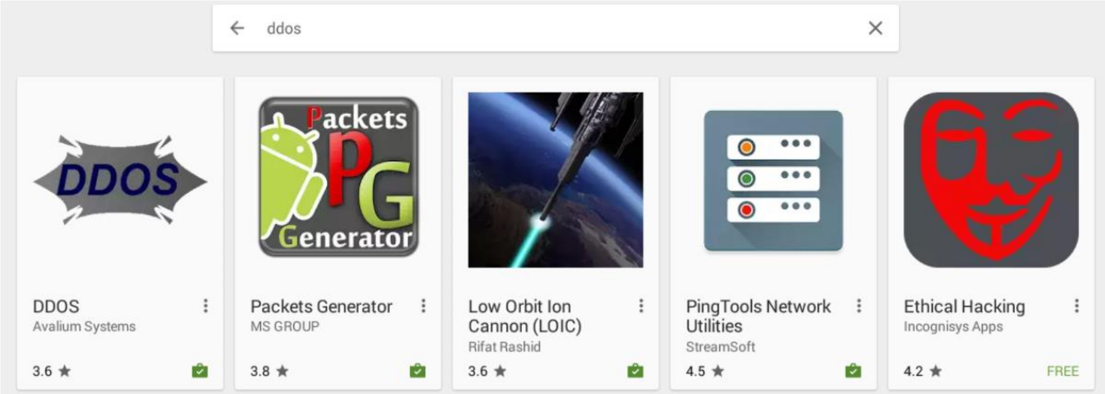
Cyber-Attacks in the Palm of Your Hand

August 29, 2016

Abstract

Smartphones. What began as the next generation of mobile phones has morphed into portable computers which combine the capabilities of a personal computer with the features for mobile and handheld use. These devices are powerful enough to perform many of the operations of a PC, and as a result, are now the catalyst for launching cyber-attacks on the go.

Equipped with a multicore processor, GBs of RAM and large capacity storage, the can easily be turned into a cyber weapon to carry out attacks. These devices are passively vulnerable to various kinds of exploits, bots and remote access tools (RATs) such as DroidJack (Android) and SideStepper (iOS), which are often found in third–party app stores. Not only can they be used to conduct small-scale DoS and SQL-based attacks from applications found in the Google Play store (see Figure 1), but they can be used to connect to a cloud-based platform loaded with attack scripts via SSH.

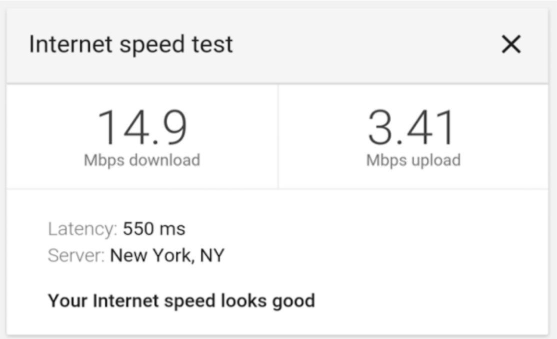


ddos

DDOS Avalium Systems 3.6 ★	Packets Generator MS GROUP 3.8 ★	Low Orbit Ion Cannon (LOIC) Rifat Rashid 3.6 ★	PingTools Network Utilities StreamSoft 4.5 ★	Ethical Hacking Incognisys Apps 4.2 ★ FREE

Figure 1 – Denial of Service apps found on Google Play

When perpetrators connect via SSH from their mobile device to a cloud platform loaded with attack scripts, they can easily leverage it to launch a variety of assaults. While most mobile networks offer limited or throttled speeds around 10-20Mbps, cloud platforms offer a capacity of 1Gbps and more. This is a primary reason why only a limited number of network and application attack tools are being developed for mobile devices. Most hackers use their phones to log into their pre-loaded attack cloud where they have access to their tools plus a high capacity connection.



Internet speed test

14.9 Mbps download

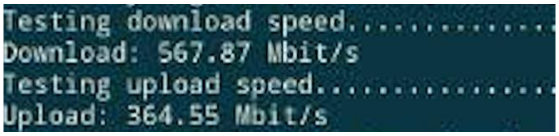
3.41 Mbps upload

Latency: 550 ms

Server: New York, NY

Your Internet speed looks good

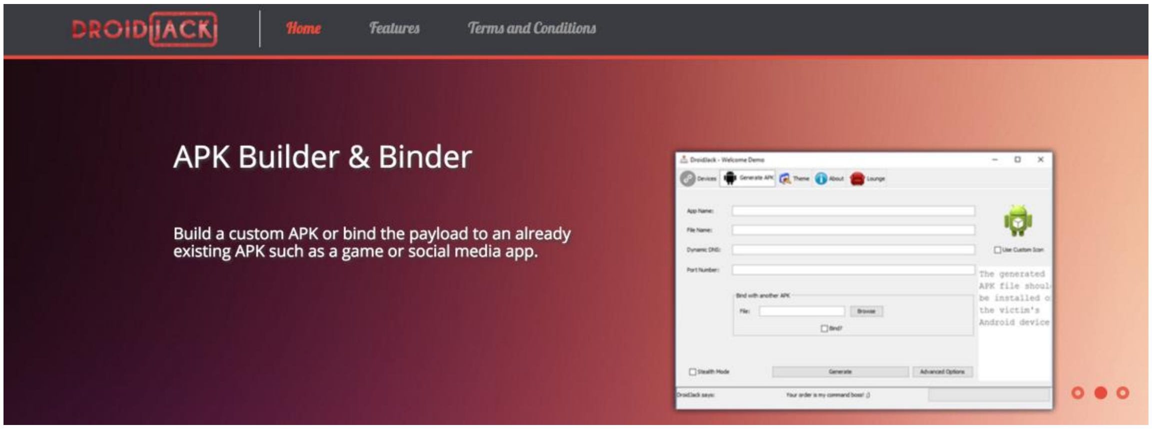
Figure 2 - Local mobile speed test



```
Testing download speed.............
Download: 567.87 Mbit/s
Testing upload speed...............
Upload: 364.55 Mbit/s
```

Figure 3 - Cloud speed test

Targeting a Device
Android devices are highly vulnerable to malware and users rarely secure their device, making it a target rich environment. Malicious apps found in the Google Play store and drive-by download are just a few examples of infection methods. Using RATs, attackers can force the device to perform certain tasks such as recording audio and video, taking photos, sending text messages, opening webpages, stealing user data, deleting files, launching DoS attacks via HTTP floods and preforming Web injections. Recently it was argued by researchers that Pokemon Go apps, Parrot Copter and Viking Jump found in the Google Play store contained a RAT enslaving the targeted device into the attacker's mobile botnet.



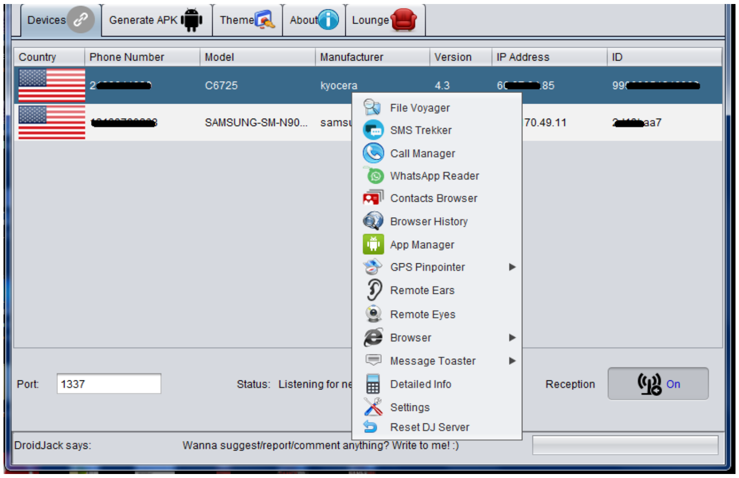
APK Builder & Binder

Build a custom APK or bind the payload to an already existing APK such as a game or social media app.

The generated APK file should be installed on the victim's Android device

Figure 4 – DroidJack.net – Android RAT

Attacking Devices
Attackers infect Android application packages and APK files by binding malware into them to take over a victim's phone. The attacker usually selects a popular Android application and binds the malicious server APK to it. Next, the attacker encrypts the APK, renames the package and removes any unwanted features and permissions. The hacker is than able to distribute the malicious application by uploading the APK file to a third-party app store. Once a device is infected, the hacker is able to execute a number of tasks on the victim's device, including the ability to launch layer 7 HTTP attacks. A mobile botnet is more than capable of generating hundreds of thousands of requests from unique IPs per second, resulting in the appearance of legitimate traffic.



Country	Phone Number	Model	Manufacturer	Version	IP Address	ID
	2[redacted]	C6725	kyocera	4.3	6[redacted].85	99[redacted]
	[redacted]	SAMSUNG-SM-N90...	samsu		70.49.11	2[redacted]aa7

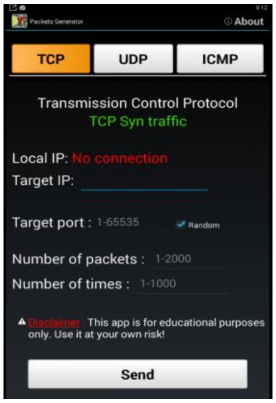
Port: 1337

Status: Listening for ne

DroidJack says: Wanna suggest/report/comment anything? Write to me! :)

Figure 5 – DroidJack Screenshot from DroidJack.net

Attacks are not always unwillingly generated from mobile devices. Some attackers install DoS tools like LOIC and Packet Generator with user-friendly interfaces from verified sources like Google's Play store. These tools are capable of generating HTTP, ICMP, UDP and TCP floods from mobile devices but are often too weak to cause major damage due to the limited capacity of a mobile network. These tools are provided for legitimate uses, such as testing a firewall, router ACLs and IDS attack signatures but are often abused by attackers looking to disrupt networks. All that is required to operate these tools are the URL or IP address, port number and threads. The attacker then selects the attack vector and clicks send.



Transmission Control Protocol
TCP Syn traffic

Local IP: No connection
Target IP:

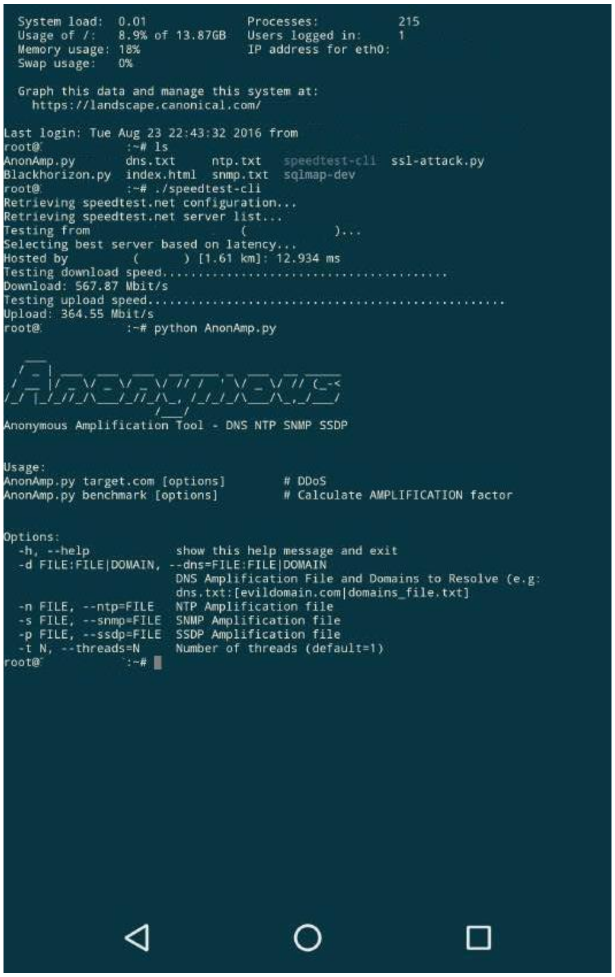
Target port : 1-65535 ☑ Random

Number of packets : 1-2000
Number of times : 1-1000

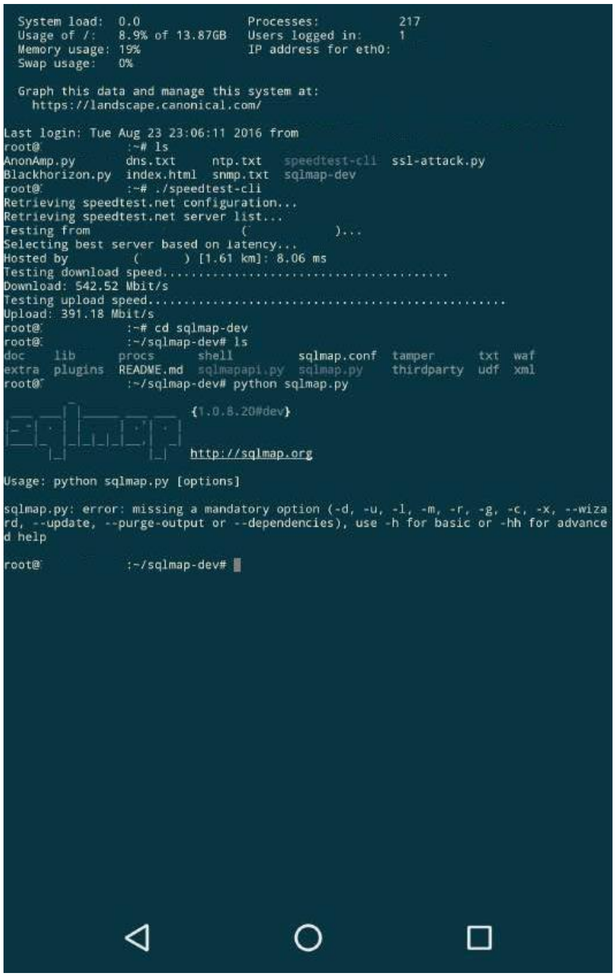
Disclaimer This app is for educational purposes only. Use it at your own risk!

Figure 6 - Packet Generator from Google Play

VPS booters are cheap and easy to construct. For as low as $10 dollars a month, an attacker can create an attack platform capable of launching unlimited DDoS attacks for undefined periods, run custom scripts and set specific VPN and server configurations. The attacker only needs to find a hosting provider that allows spoofing. Once the VPS has been purchased, the attacker establishes their booter or scripts of choice. Once the VPS is completely configured, the attacker can access their server from their mobile device so they can launch attacks with a larger volume then if they had run the same scripts off their phone via a mobile network.



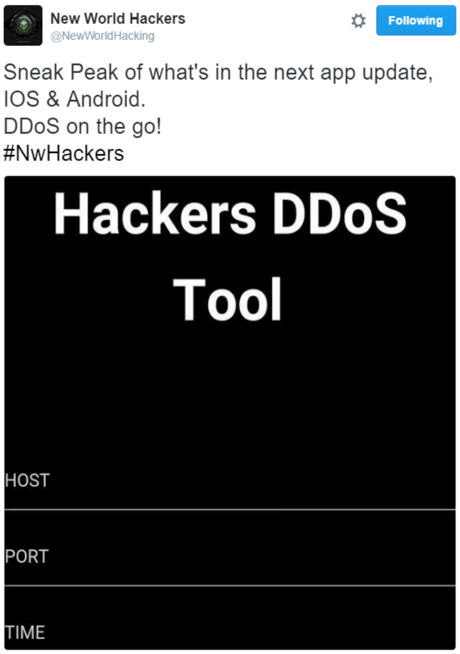
```
  System load:  0.01                Processes:           215
  Usage of /:   8.9% of 13.87GB     Users logged in:     1
  Memory usage: 18%                 IP address for eth0:
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

Last login: Tue Aug 23 22:43:32 2016 from
root@            :~# ls
AnonAmp.py       dns.txt     ntp.txt   speedtest-cli  ssl-attack.py
Blackhorizon.py  index.html  snmp.txt  sqlmap-dev
root@            :~# ./speedtest-cli
Retrieving speedtest.net configuration...
Retrieving speedtest.net server list...
Testing from                    (            )...
Selecting best server based on latency...
Hosted by        (      ) [1.61 km]: 12.934 ms
Testing download speed........................................
Download: 567.87 Mbit/s
Testing upload speed..................................................
Upload: 364.55 Mbit/s
root@            :~# python AnonAmp.py

Anonymous Amplification Tool - DNS NTP SNMP SSDP


Usage:
AnonAmp.py target.com [options]         # DDoS
AnonAmp.py benchmark [options]          # Calculate AMPLIFICATION factor


Options:
  -h, --help            show this help message and exit
  -d FILE:FILE|DOMAIN, --dns=FILE:FILE|DOMAIN
                        DNS Amplification File and Domains to Resolve (e.g:
                        dns.txt:[evildomain.com|domains_file.txt]
  -n FILE, --ntp=FILE   NTP Amplification file
  -s FILE, --snmp=FILE  SNMP Amplification file
  -p FILE, --ssdp=FILE  SSDP Amplification file
  -t N, --threads=N     Number of threads (default=1)
root@            :~# 
```



```
  System load:  0.0                 Processes:           217
  Usage of /:   8.9% of 13.87GB     Users logged in:     1
  Memory usage: 19%                 IP address for eth0:
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

Last login: Tue Aug 23 23:06:11 2016 from
root@            :~# ls
AnonAmp.py       dns.txt     ntp.txt   speedtest-cli  ssl-attack.py
Blackhorizon.py  index.html  snmp.txt  sqlmap-dev
root@            :~# ./speedtest-cli
Retrieving speedtest.net configuration...
Retrieving speedtest.net server list...
Testing from                    (            )...
Selecting best server based on latency...
Hosted by        (      ) [1.61 km]: 8.06 ms
Testing download speed........................................
Download: 542.52 Mbit/s
Testing upload speed..................................................
Upload: 391.18 Mbit/s
root@            :~# cd sqlmap-dev
root@            :~/sqlmap-dev# ls
doc    lib      procs      shell        sqlmap.conf  tamper      txt  waf
extra  plugins  README.md  sqlmapapi.py sqlmap.py    thirdparty  udf  xml
root@            :~/sqlmap-dev# python sqlmap.py

                         {1.0.8.20#dev}

                         http://sqlmap.org

Usage: python sqlmap.py [options]

sqlmap.py: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, -x, --wiza
rd, --update, --purge-output or --dependencies), use -h for basic or -hh for advance
d help

root@            :~/sqlmap-dev# 
```

Figure 7 & 8 - An "attack cloud" loaded with DDoS scripts, amplification list and SQLmap

Notorious DDoS groups like The New World Hackers - the group associated with the record breaking 602Gbps attack on the BBC - have already hinted that they are about to release a DDoS application for both Android and iOS. Other DDoS groups will likely follow suit and release their own attack applications. These new tools will probably hook into a booter or stresser service that allows reflective attacks, thus allowing an attack to conduct attacks of high volumes and packet rate.



New World Hackers
@NewWorldHacking

Sneak Peak of what's in the next app update,
IOS & Android.
DDoS on the go!
#NwHackers

Figure 9 - New World Hackers mention new app in development

Attack vectors

Denial-of-Service when perpetrators use computing resources to exhaust those of another machine, in order to prevent it from functioning normally.

Distributed Denial of Service – a DoS variant where perpetrators employ multiple machines (computers, servers, and mobile devices) to carry out a DoS attack simultaneously, thus increasing its effectiveness. The attack leverages a net of innocent infected zombie computers (bots) controlled by a Command and Control Server. Botnets are well-coordinated and could count millions of machines. Perpetrators use botnets to insure their anonymity, since the attack traffic originates from the bots' IPs rather than theirs.

Reflection Denial of Service – taking advantage of a legitimate third party component to send the attack traffic to a victim, ultimately hiding the attackers' identity. The packets are sent to the reflector servers with a source IP address set to their victim's IP therefore indirectly overwhelming the victim with the response packets. The disguise behind a legitimate server makes this kind of attack particularly difficult to mitigate. A common example for this type of attack is a Reflective DNS Response attack.

DNS amplification attack – a two-step sophisticated DoS attack: First, the attacker spoofs the IP address of the DNS resolver and replaces it with the victim's IP address, so all DNS replies will be sent to the victim's servers. Second, the attacker finds an Internet domain that is registered with many DNS records. During the attack, the attacker sends DNS queries that request the entire list of DNS records for that domain. The DNS server's replies are usually so big that they need to be split over several packets.

SQL Injection - This technique takes advantage of poor application coding. When the application inputs are not sanitized it becomes vulnerable. Attackers can modify an application SQL query to gain access to unauthorized data with administrator access, run remote commands on the server, drop or create objects in the database and more.

Organizations Under Threat Should Consider

- Deploy security controls on BYOD devices connected to the corporate network
- Provide employees with a mobile security solution to protect from infections
- Intercept any malicious outbound activity, such as communications with RATs and C&Cs or generating a high rate of HTTP/S requests
- Prevent installation of unauthorized applications

5 considerations for an effective DDoS Protection

- A security solution that can protect its infrastructure from multi-vector attacks including protection from network and application based DDoS attacks as well as volumetric attacks that can saturate the Internet pipe
- A hybrid solution that includes on premise detection and mitigation with cloud-based protection for volumetric attacks. This provides quick detection, immediate mitigation and protects networks from volumetric attacks that aim to saturate the Internet pipe.
- A solution that provides protection against sophisticated web-based attacks and web site intrusions to prevent defacement and information theft.
- A cyber-security emergency response plan that includes an emergency response team and process in place. Identify areas where help is needed from a third party.
- Monitor security alerts and examine triggers carefully. Tune existing policies and protections to prevent false positives and allow identification of real threats if and when they occur.

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you’re under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button".

Learn More at DDoS Warriors

To know more about today’s attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware’s Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.