radware

ERT Threat Alert

OpAfrica

2/16/16

Abstract

The hacktivist group Anonymous is back, this time fighting corruption across the continent of Africa. #OpAfrica is an operation run by several hacktivists within Anonymous who are focused on targeting corporations and government that “enable and perpetuate corruption on the African continent”.[i]

Background

The operation is targeting corruption across the continent of Africa, including corporations and governments that are believed to be involved with or responsible for child abuse and labor. They are also targeting those involved with internet censorship and corruption across Africa. This operation is being run in parallel to OpNigeria and OpSouthAfrica, in hopes of freeing the continent of child exploitation and corruption. Like in many recent campaigns, perpetrators are using multiple attack vectors and techniques such as SQL injection and cross site scripting with volumetric network floods.

Phases of the Operation

- Public awareness
- Intelligence gathering on Government sites
- Trolling
- DDoS attacks
- Leaks and data dumps.

Communication

- Chat
  - irc.cyberguerrilla.org Port 6697
  - webchat.cyberguerrilla.org
- Channels
  - #Hack_Africa #OpSouthAfrica
- Video
  - https://vimeo.com/153705229
- Twitter
  - @opsouthafricaof

Recently Targeted

- Parliament of Malawi Defaced[ii]
- Anonymous Hacks Rwanda Government IT Company (BSC.rw)[iii]
- Anonymous Hacks vreport.co.za[iv]
- South African Government Communication and Information System[v]
- South African Government Department of Water Affairs[vi]
- Tanzania Telecommunication Company LTD[vii]

Reasons for Concern

As a result of OpAfrica, a number of organizations and government sites have and are currently experiencing SQL injections, data dumps and service outages cause by DoS attacks. The operation is expected to continue and a new group of targets will be added to the list. Those directly or indirectly related to the governments listed as targets could experience defacements and DoS attacks followed by data dumps.

First Target List

- Rwanda Government
- Uganda Government
- South Africa Government
- Zimbabwe Government
- Tanzania Government
- Sudan and South Sudan Government
- Ethiopia Government

How to Prepare

We recommend that organizations proactively prepare by taking the following steps:

- Inspect networks while looking for web and network vulnerabilities and patch systems accordingly in a timely manner
- Tune existing policies and protections to prevent false positives
- Allow identification of real threats if and when they occur
- Make sure to have all security solutions in place to protect from web and network based attacks

Organizations under Attack Should Consider

- 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 **protects against sophisticated web-based attacks** and website intrusions to prevent defacement and information theft.
- A cyber-security emergency plan that includes an **emergency response team** and process in place. Identify areas where help is needed from a third party.
- Automated solution that **recognizes malicious patterns in real time**, develops signatures and updates all security controls.
- Monitor security alerts and examine triggers carefully. Configure protections to prevent false positives and allow identification of real threats once occur.

Under Attack and in Need of Expert Emergency Assistance?

Radware offers a full range of solutions to help networks properly mitigate attacks similar to these. Our attack mitigation solutions provide a set of patented and integrated technologies designed to detect, mitigate and report todays most advanced DDoS attacks and cyber threats. With dedicated hardware, fully managed services and cloud solutions that protect against attacks, Radware can help ensure service availability. To understand how Radware's attack mitigation solutions can better protect your network contact us today.

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.

[i] https://www.cyberguerrilla.org/blog/opafrica-engaged/
[ii] https://www.cyberguerrilla.org/blog/lulzsec-is-back-parliament-of-malawi-defaced-for-opafrica/

[iii] https://www.cyberguerrilla.org/blog/anonymous-hacks-rwanda-government-it-company-for-opafrica/

[iv] https://www.cyberguerrilla.org/blog/anonymous-hacks-vreport-co-za-for-opafrica/

[v] https://www.cyberguerrilla.org/blog/anonymous-hacks-south-african-government-communication-and-information-system-gcis-for-opafrica/

[vi] https://www.cyberguerrilla.org/blog/anonymous-hacks-south-african-government-department-of-water-affairs-for-opafrica/

[vii] https://www.cyberguerrilla.org/blog/anonymous-hacks-tanzania-telecommunications-company-ltd-for-opafrica/