Abstract

The hacktivist group Anonymous has upped the ante in its cyber-assault against corporations and government that "enable and perpetuate corruption on the African continent." Since Radware's previous ERT alert on February 16, 2016, the OpAfrica operation has grown with the assistance from a collection of Anonymous-affiliated groups, including the hacktivist group, New World Hackers (see Figure 1), Team Hack Argentino, and others.

Background

OpAfrica is an Anonymous operation that is focused on fighting corruption, child abuse and internet censorship across the continent. Since the launch of the operation in February, Anonymous has targeted the governments of Rwanda, Uganda, South Africa, Tanzania, Zimbabwe and Sudan with defacements, data dumps and massive DDoS attacks. As predicted in the previous ERT Alert, Anonymous has issued an expanded target list for the second phase[i] of the operation, claiming they will not stop anytime soon.

Figure 1: New World Hackers claim support for OpAfrica

Upon joining, New World Hackers attacked the DNS server portals for a number of government sites in South Africa (see Figure 2), resulting in outages for the following:

- gov.za
- capetown.gov.za
- News.co.za
- dod.mil.za
- treasury.gov.za
- entenders.gov.za
- icd.gov.za
- weterncape.gov.za
- educationweek.co.za

Figure 2: New World Hackers down gov.za

Operation Information

Attackers

- World Hacker Team
- New World Hackers
- Team Hack Argentino
- Hanom1960
- Greater Anonymous collective

Communication

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

Original Target List

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

Updated Target List

- Burundi Government
- Togo Government
- Kenya Government
- Burkina Faso Government
- Central African Republic Government
- Algeria Government

Recently Targeted [ii]

- Rwanda Government IT – World Hacker Team (WHT)
- South African Government Communication and Information System (GCIS) – WHT
- South African Department of Water Affairs – WHT
- Tanzania Telecommunications Company LTD – WHT
- vreport.co.za – WHT
- A staggering 2,532 South African websites – Team Hack Argentino – Tobitow
- Parliament of Malawi – LulzSec
- Central Bank of Nigeria – LulzSec
- Government of Zimbabwe's Network – LulzSec
- Uganda Revenue Authority – LulzSec
- Seed Marketing Co. – New World Hackers
- Assembly of Niger – NWH
- BokoHaram.net – NWH

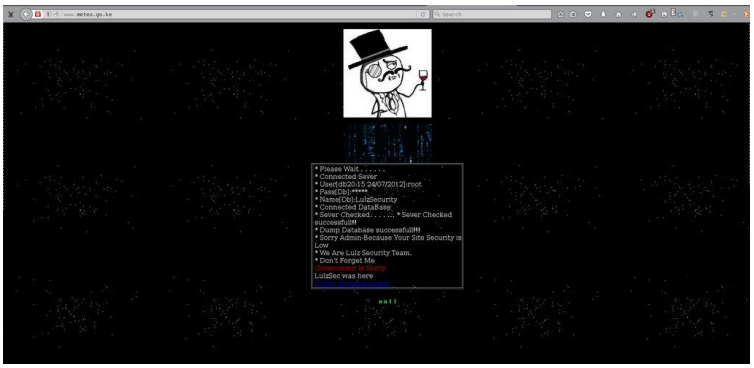

Figure 3: Deface of meteo.go.ke by Hanom1960

Figure 4: Image used on defaced sites for OpAfrica

Reasons for Concern

Many sites suffered SQL injections, data dumps and service outages caused by network crippling DDoS attacks. OpAfrica is expected to continue as it enters the second phase of operations, moving on to their next targets. These targets can expect to experience similar attacks to those used during the first phase. Radware also expects to see a new target list in the future and the continued support from the greater Anonymous collective.

Effective Protection Considerations

Enterprises and government agencies should consider a comprehensive defense system to detect and mitigate multi-vector, volumetric denial of service, and Web application attacks. Enterprises should 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.

Here are several considerations for a seamless security solution:

- 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 Web application security protection solution via a Web Application Firewall (WAF) or a cloud WAF service, that can protect against sophisticated web-based attacks and website intrusions to prevent defacement and information theft.
- An integrated, synchronized solution that can protect from multi-vector attacks combining DDoS with web-based exploits such as website scraping, Brute Force and HTTP floods.
- 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.

Additional important considerations when choosing a solution to defend from web-based attacks:

- IP-agnostic device fingerprinting – Having the ability to detect attacks beyond source-IP using by developing a device fingerprint that enables precise activity tracking over time
- Automatic and real time generation of policies to protect from 0-day, unknown attacks
- Shortest time from deployment to security

Need 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/operation_africa_phase_two/
[ii] https://ghostbin.com/paste/8795b