# RW10k: Combating Spam as Network Operators
## An anti-spam toolkit case study

22 September, 2016

### RW10k: Combating Spam as Network Operators

The Rwanda Information & Communication Technology Association (RICTA) learned a tough lesson in 2016 when their web servers were attacked and used to send out thousands of spam messages. The attack, while now resolved, impeded the project from quickly reaching its goals. In this case study, we outline some lessons learned and the steps undertaken by RICTA to alleviate the problem, protect themselves against future attacks, and restore their clients' trust.

> While the association did not have difficulty with incoming spam, large amounts of outgoing spam were sent by their servers.

### Introduction

RICTA's RW10k project provides local hosting services for their clients through servers using CPanel, a cloud hosting platform. The project aims to relocate ten thousand Rwandan websites hosted abroad to servers in Rwanda. The Rwandan servers provide both web hosting and email functionality for their customers. This project is particularly important for a landlocked country like Rwanda which has to rely on neighboring countries for international submarine cable access. By hosting websites in Rwanda, RW10k reduces the load on transnational Internet connections. This helps to reduce website loading times for its users, and eventually for other consumers, thus improving user experience.

RW10k was created by RICTA in 2016 in collaboration with the Internet Society to provide incentives for Rwandan domain name registrars to host their websites locally.

During the pilot phase, three virtual private servers (VPSs) were made available to RICTA members (domain name registrars based in Rwanda) to migrate their websites from the United States and Europe to Rwanda. After the pilot phase, some members migrated fully to servers in Rwanda.

In 2016, shortly after migrating registrars' websites to the VPSs, RW10k began having problems with spam. While the association did not have difficulty with incoming spam, large amounts of outgoing spam were sent by their servers. As a consequence, legitimate notifications sent by websites using a functionality on CPanel were being flagged as spam by other email services. The notifications were not reaching their intended destinations. After considerable effort, the project's servers are no longer sending spam. However, RICTA will still have to continue to monitor its servers, train its staff, and attract lost users back to the service.

### The Spam Problem and Immediate Solutions

The reputation of the servers' IP addresses suffered as a result of the large number of spam emails originating from the servers. Google, and other email service providers, blacklisted the servers' IP addresses. Due to the blacklisting, legitimate notifications sent from the servers of RW10k clients stopped reaching their intended recipients. Some emails were delivered to junk or spam folders, and others were blocked entirely, rendering the email service virtually unusable. Without a usable email service, registrars were reluctant to transition their websites to the local servers.

RICTA took several steps to find, mitigate, and fix RW10k's spam problem.

1. They first determined the source of the problem. By analyzing the logs on one of the servers, they concluded that malicious scripts installed through weaknesses in outdated Content Management Systems (CMSs) used by the registrars were the cause of the spam. The scripts were periodically generating thousands of junk emails. The malicious scripts had been uploaded by exploiting known vulnerabilities in outdated CMSs. It is important to note that by using outdated versions of CMSs, the websites were fairly easy for botnets to find and exploit.

2. After the source of the spam was located, steps had to be taken to remove the source and mitigate its impact. As a short term solution, another virtual private server was used to analyze and filter out spam emails from legitimate outgoing emails. RW10k servers were configured to forward all outgoing emails to this virtual private server for filtering, before the emails were sent out on to the Internet. This solution successfully filtered spam emails from legitimate emails with a high degree of accuracy.
3. To eliminate the source of the spam emails, the malicious scripts were removed and security software was installed on the servers. This software will periodically check for malicious scripts, along with other malware, and quarantine them.
4. Clients were encouraged to update their CMS to ensure that they had the latest security features, or to obtain a new release and/or product if their CMS was no longer supported.

All hosting providers are confronted with similar problems with their clients' CMSs. Like RW10k, the majority filter outgoing emails for spam to mitigate the impact on the network. This is an example of collective responsibility[1] at play – providers taking steps locally to protect others on the network and the ecosystem at large. Large hosting providers also make it easy for users to automatically install CMSs by offering Installatron, a multi-platform application installer. By using Installatron, or a similar tool, the host enables and encourages automatic updates by setting it as a default. This helps to guard against known vulnerabilities while the CMS is supported.

## Long Term Impacts and Solutions

Despite successfully filtering outgoing spam emails and removing malicious code, RW10k will need to continually monitor and update its email and web hosting services to avoid similar incidents in the future.

One consequence of RW10k's spam problem is a loss of users and user trust. The registrars impacted by the problem did not fully migrate their websites to the RICTA servers based in Rwanda. After they encountered problems on the virtual private servers, they decided to return to servers hosted outside the country. By remaining on a foreign server based outside of Rwanda, the benefits from local hosting were not obtained. RICTA has alerted their clients that the spam problem has been alleviated and is actively attracting users to their service.

RICTA, as with all hosting providers, will also have to take action to protect against future attempts by spammers to exploit their service, such as:

- Training their registrars in better security techniques. This includes training on CPanel security settings to prevent future malicious scripts from being introduced, and training on email filter management.
- Advising registrars how to configure email services for their clients to ensure better security. Some examples are: using secure ports to send and receive email, as well as accurately configuring DNS entries to ensure email is delivered properly.
- Disabling unnecessary CPanel services as they could be potential security holes, and consistently monitoring and analyzing logs of all online services to detect unusual activity.
- Ensuring that CMS installations are regularly updated to protect against attackers.

> it can be difficult for local providers to compete, and to reclaim any lost business as a result of a security incident.

## Conclusion

The RW10k case provides a practical example of the everyday problems faced by new hosting providers. It also shows the importance of strong security for network and service operators, not just for themselves, but also for the Internet as a whole. The RW10K project, which was focused on helping Rwandans host local content locally, did not build in the necessary security features from the start. This is an important lesson for all of us. However, through identifying and fixing the spam problem, the association and its registrar members are now practicing better security techniques that will ensure

[1] For more information, see the Internet Society Collaborative Security approach

they are better prepared against future attacks by spammers.

The RW10k case also demonstrates the importance of strong security practices for not only the technical, but also the commercial, success of a service provider. For RW10k, the loss of email functionality for websites hosted on its servers resulted in a loss of clients. For smaller providers in the developing world, such as RICTA with RW10k, this often means a move from small local providers to large foreign providers. As large foreign providers often have more name recognition and resources, it can be difficult for local providers to compete, and to reclaim any lost business as a result of a security incident. For this reason, it is particularly important that providers focus on security.

Equipping yourself with the knowledge and skills needed to protect against spam threats is essential, not only in your personal life, but also to ensure the success of your business or organization. To learn more about what you can do to protect yourself and others against spam, visit the Internet Society's Anti-Spam Toolkit. The toolkit provides resources and suggestions for users, network operators, and policymakers on defending against spam and mitigating its impacts. You can also take our free online training class Combating Spam and Mobile Threats.