DAILY POST
DAILYPOST.VU

TVL Cracks Down on Malicious Domains

Internet domain cleanup efforts date back to 2013

By Dan McGarry and Colin Cortbus

Even as it coped with a major Distributed Denial of Service—or DDoS—attack, Telecom Vanuatu Ltd confirmed this week that it has taken concerted action to stamp out malicious and illegal activity originating from the .VU internet domain space.

TVL staff declined to comment when asked whether the attack was in retaliation for the crackdown—a common scenario.

A Daily Post investigation has shed light on a dark corner of the internet.

Story continues on page 2

TVL Cracks Down on Malicious Domains

From Front Page

Unscrupulous business people have been on-selling subdomains in the .VU name space to customers engaging in such activities as fundraising for ISIS, propagating neo-Nazi ideology and attacking innocent computer users using 'phishing' scams to obtain passwords and other confidential data.

The telecommunications company, which is responsible for the administration of the .VU internet domain, reacted swiftly when a list of troubling domains was provided to them.

In a mid-week meeting with the newspaper, TVL representatives stated that these efforts were just the latest in a concerted clean-up operation that began in earnest in 2013.

Perhaps the worst example of domain abuse is the CO.VU domain. Originally registered in 2006, at a time when there was little to no oversight of the .VU domain space, the domain has been used as a platform to on-sell subdomains, many of which ended up pointing to websites hosting a wide variety of questionable and often illegal content.

An internet domain name is similar to a mailing address—an easy-to-remember sequence of letters or numbers that allow people to identify the site. The best-known domains are in the .COM (short for 'commercial') domain space. But each country has its own name, known as a country code Top Level Domain, or ccTLD.

Vanuatu's ccTLD is .VU. In the late 1990s, Telecom Vanuatu Ltd was asked by the government to administer the .VU domain. At that time, the entire internet domain system was run by a single person, a UCLA-based computer scientist named John Postel.

After Mr Postel's death in 1998, a global internet governance body was established to oversee domain management. The Internet Corporation for Assigned Names and Numbers, or ICANN, currently oversees the administration and governance of over a thousand top-level domains, and through its various administrative delegates, countless million subdomains.

To this day, TVL retains administrative and technical control of the .VU domain.

Company representatives complained to the Daily Post that the task of keeping the entire domain space clean and within the law is a vast and difficult process, requiring the cooperation of agencies and individuals throughout the world.

The CO.VU domain, for example, is registered to an address in Bangalore, India. The subdomain reselling service's website is hosted in the Amazon cloud, and many of its subdomains are automatically hosted on Google.

For the first few years of operation, abuse was rampant and went largely unchecked. In recent years, however, TVL technical staff began to wrestle with the problem of widespread unethical and even illegal activity originating from within the CO.VU domain.

In mid-2013, two .VU subdomains, DE.VU and CO.VU, were responsible for nearly 3% of all phishing activity, ranking them in the top 20 globally. A report from the Anti Phishing Working Group—a global body with members including the International Telecommunications Union, the OECD, ICANN, the EU and many others—stated that in the first six months of 2013, .VU domains were the source of 913 known phishing attacks.

In the latter half of 2013, that number dropped to 292. By mid-2014, the number was 52. The average duration of each attack also dropped by more than half.

Technical staff told the Daily Post that in the early going, they were receiving malicious activity reports concerning CO.VU domains almost every other week.

Their initial inclination was to drop the entire domain, but ICANN suggested to them that blacking out over 200,000 subdomains to stop a few dozen was an overreaction. TVL relented, and began a slow, painstaking process of bringing the domain operator into line. Using the threat of termination, they managed to drag the CO.VU domain administrator 'kicking and screaming' into compliance.

The domain has been the source of only two complaints in the last 12 months. That said, staff and management insisted that their patience was nearly exhausted, and they were prepared to shut down the entire domain at the first sign of a downturn.

Management of the .VU subdomain has been a bone of contention for many years now. There have been complaints about the domain's technical administration. Security experts have raised these concerns with the Government Chief Information Officer and the TRR in the past.

For their part, TVL representatives insist that they are improving, and that claim is borne out by the evidence. Troubling domains still exist as this article is being prepared. CEO Raj Beeharry likened the challenge to squashing bugs—no matter how many you get, there are always new ones emerging.

He argued that his company is a complex organisation working in a small market, and that its domain management unit lacks the vast resources available to larger, more prosperous entities who manage millions of domain names.

Pacific island countries have a decidedly spotty history of internet domain abuse. Palau, Christmas Island and Tokelau's domains, for example, host vast numbers of distasteful websites, some featuring content too revolting to describe here. Most of this content is not illegal in the country where the machines holding the material are located. But much of it is indisputably offensive to the sensibilities of citizens of the states whose domains are being used to access them.

Vanuatu's performance has improved, and compares favourably with the worst offenders, many of which are Pacific island domains. But technical and security experts have raised concerns repeatedly in the past, and although TVL's progress has been consistently positive, some have told the Daily Post that there is still much to be done.

Full disclosure: Dan McGarry has provided both free and paid advice to past telecommunications regulators concerning .VU domain governance.