Projecto 0

Ricardo Santos @ CERT-MZ TechTalk
ricardo@cert.mz - facebook.com/cert-mz - www.cert.mz

Análise de Vulnerabilidades do Espaço Cibernético Moçambicano

Parte 1

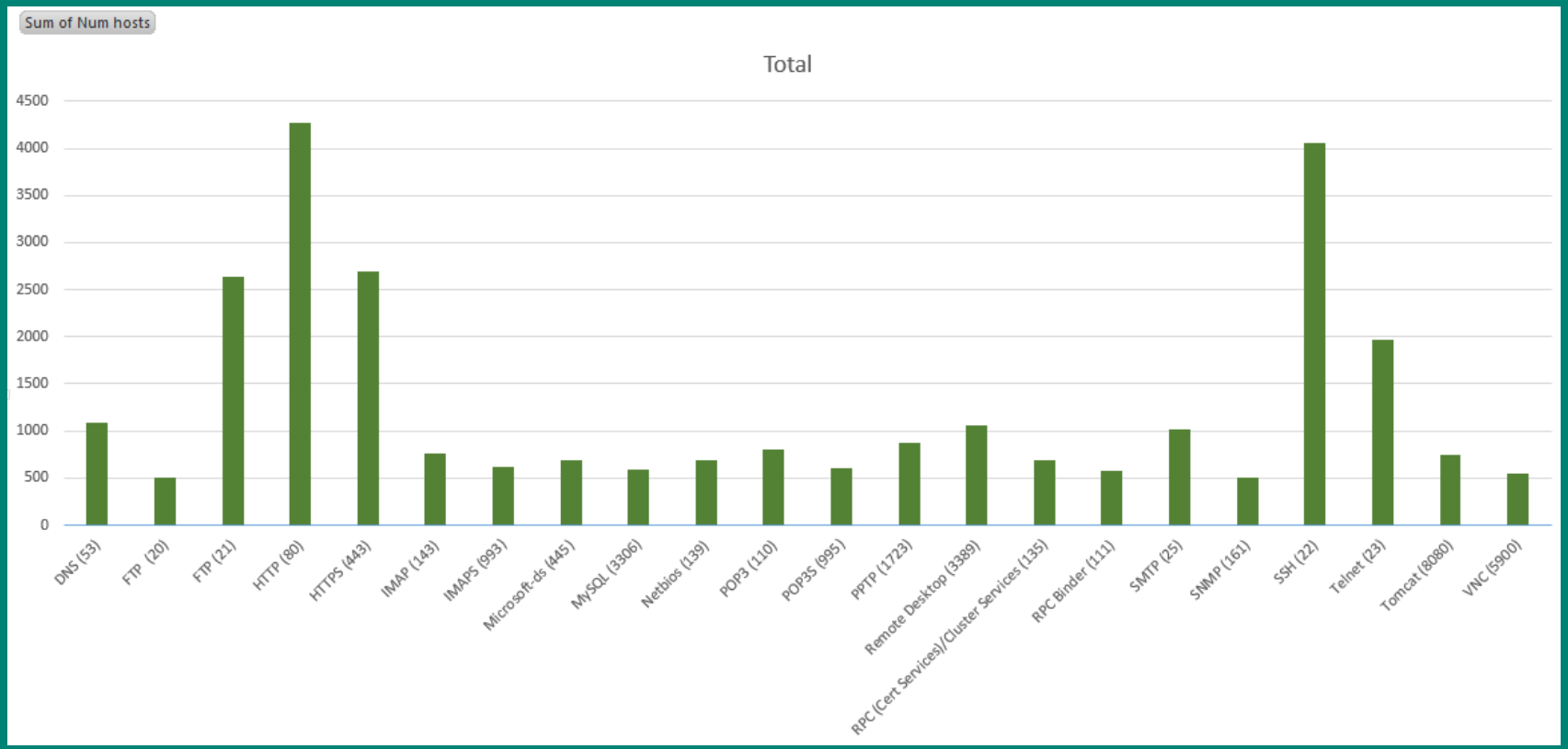
Universo

- 15 entidades com endereços IP públicos
- 27965 Hosts
- Scan efectuado em 14 / Abril / 2017
  (Mais de um ano atrás !!!)
- A partir da rede do CIUEM (IP origem: 196.3.103.67)

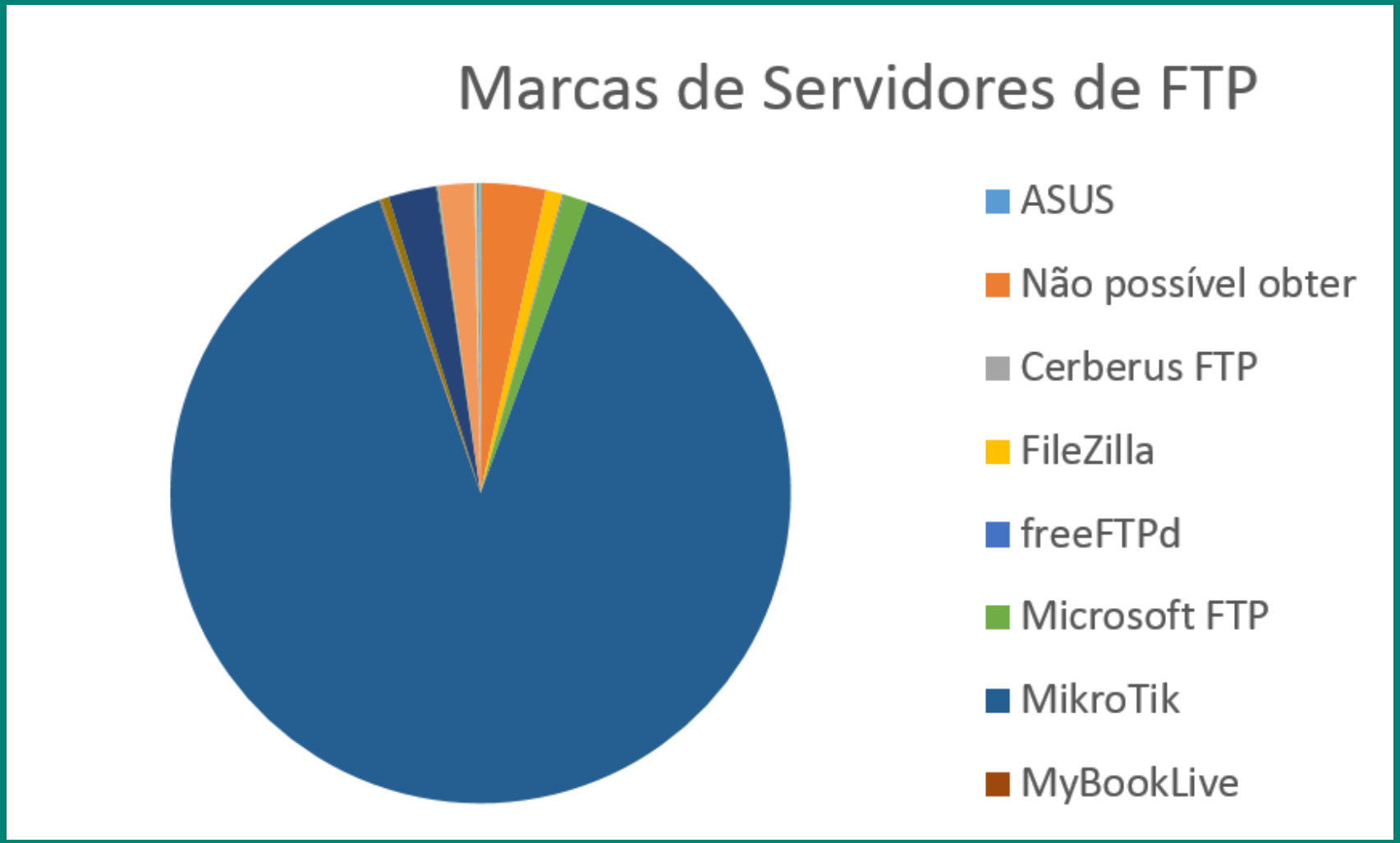
Metodologia

- masscan para todos os hosts fazendo scan aos portos mais utilizados
- grep, awk, sort e uniq -c para tirar estatísticas básicas
- script em python para retirar o banner de alguns protocolos
- Análise do Banner - marca, modelo e versão
- Pesquisa de CVEs para o banner identificado
- Análise não intrusiva, rápida e simples

Distribuição de Protocolos



FTP


Marcas de Servidores de FTP
ASUS
Não possível obter
Cerberus FTP
FileZilla
freeFTPd
Microsoft FTP
MikroTik
MyBookLive

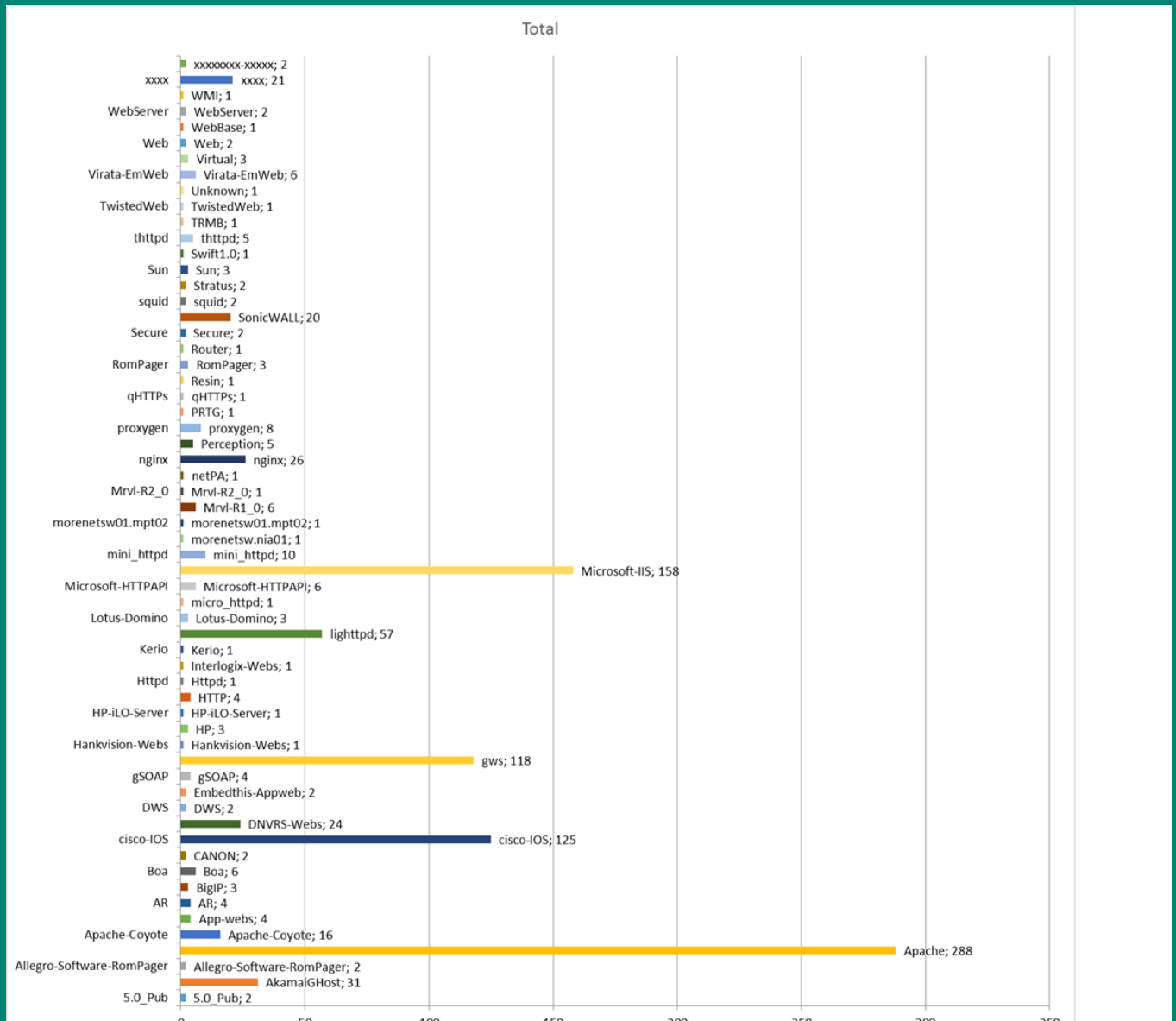
Vulnerabilidades FTP

Marca	Vulnerabilidade	CVSS
ProFTPD 1.3.5	CVE-2015-3306	10
ProFTPD 1.3.1	CVE-2011-4130	9
ProFTPD 1.3.4e	CVE-2015-3306	10
MikroTik 5.11	CVE-2012-6050	6.4 (DoS)
MikroTik 6.38.5	CVE-2017-7285	7.8 (Shutdown)
Fzilla 0.9.x beta	CVE-2007-2318	9.3
freeFTPd 1.0	CVE-2005-3683	7.5
ASUS RT-N16 FTP	CVE-2013-4937	10
ZTE FTP version 1.0	CVE-2014-4018	7.8 (Data)
Serv-U FTP Server v7.1	CVE-2011-4800	9

Conclusões FTP

- Equipamentos esquecidos sem update
- Muitos dos FTPs habilitados não são para transferência de ficheiros
- Banners com nome completo de pessoas, empresas e endereço IP interno

HTTP (porta 80)



Vulnerabilidades HTTP

Servidor	Num	CVE	CVSS
Apache/1.3.34	1	CVE-2010-0010	10
Apache/1.3.37	2	CVE-2010-0010	10
Apache/1.3.41	2	CVE-2010-0010	10
Apache/2.0.46	1	CVE-2010-0425	10
Apache/2.0.51	1	CVE-2010-0425	10
Apache/2.0.52	2	CVE-2010-0425	10
Apache/2.0.63	3	CVE-2010-0425	10
Apache/2.0.64	2	CVE-2011-3192	10
Apache/2.2.11	1	CVE-2010-0425	10
Apache/2.2.12	1	CVE-2010-0425	10
Apache/2.2.13	1	CVE-2010-0425	10
Apache/2.2.14	3	CVE-2010-0425	10

Vulnerabilidades HTTP

Servidor	Num	CVE	CVSS
Apache/2.2.3	10	CVE-2010-0425	10
Apache/2.2.6	3	CVE-2010-0425	10
Apache/2.2.8	1	CVE-2010-0425	10
Apache/2.2.9	4	CVE-2010-0425	10
BigIP	3	CVE-2014-2927	9.3
HP-iLO-Server/1.30	1	CVE-2014-7876	10
Microsoft-IIS/6.0	14	CVE-2017-7269	10
Microsoft-IIS/7.0	15	CVE-2010-3972	10
Microsoft-IIS/7.5	55	CVE-2010-3972	10
Perception	5	CVE-2003-1144	10
RomPager/4.07	2	CVE-2014-9222	10
SonicWALL	20	CVE-2007-5603	9.3

Conclusões HTTP

- Apenas 2582 servidores web
- Internacionalmente Apache (50%); nginx em segundo lugar
- Em Moçambique Apache (28%); IIS em segundo lugar
- Muitos equipamentos Cisco (12%) e 1 HP ILO na porta 80
- Heterogeneidade e bastantes servidores Open Source

Próximos Passos

- Actualizar o scan
- Analisar os restantes protocolos
- Produzir um relatório a ser distribuído pela comunidade