Nonius, o nível de Segurança da Internet Portuguesa.

F. Rente$^{\phi}$, M. Rela$^{\lambda}$, H. Trovão$^{\xi}$, S. Alves$^{\mu}$
{frente, htrovao, salves}@cert.ipn.pt$^{\phi,\xi,\mu}$, mzrela@dei.uc.pt$^{\lambda}$

CERT-IPN, IPNlis, Instituto Pedro Nunes
Rua Pedro Nunes 3030-199 Coimbra, Portugal

Resumo

O projecto **Nonius** ambiciona produzir um histórico fidedigno de dados indicadores do nível de segurança da Internet Portuguesa. O sistema que o sustenta executa um rastreio, e sucessiva carga de testes, a todo o endereçamento IPv4 alocado a Portugal. Os dados recolhidos passam por um processo de anonimização sendo, posteriormente, publicados segundo um conjunto de métricas pré-definidas.

1 Introdução

No âmbito do projecto **Nonius** foi desenvolvido um sistema computacional que, através de um rastreio ao espaço de endereçamento IPv4 português, produz dados indicadores do estado e do nível de segurança da Internet Portuguesa. Projecto este que se encontra integrado nos serviços de disseminação do CERT-IPN.
O CERT-IPN é um núcleo CSIRT[1], do Laboratório de Informática e Sistemas do Instituto Pedro Nunes (IPNlis), uma instituição de utilidade pública sem fins lucrativos, que tem como missão a transferência de tecnologia entre a Universidade de Coimbra e o tecido económico Português. Os serviços de disseminação são um conjunto de serviços de natureza comunitária, em que o CERT-IPN se afirma como entidade socialmente activa, disposta a contribuir e apoiar o desenvolvimento do conhecimento na área da Segurança de Informação.[3]
Sendo o **Nonius** um sistema de medição do nível de segurança da Internet Portuguesa, um aspecto preliminar para a definição clara do âmbito do projecto é definir o que se entenderá como Internet Portuguesa no seio do **Nonius**. Neste contexto compreende-se como Internet Portuguesa o conjunto de todos os endereços IPv4 alocados a Portugal no RIPE-NCC[4].
Naturalmente esta definição não engloba na totalidade o que realmente é a Internet Portuguesa uma vez que, *p.ex.*, entidades/organizações Portuguesas podem assentar as suas infra-estruturas em endereços IP não alocados a Portugal. Contudo a abrangência da definição usada é suficientemente elevada para dar credibilidade e consistência aos dados estatísticos que o **Nonius** produz.
Os objectivos gerais do **Nonius** podem ser englobados em dois grupos distintos. Num grupo é representada a perspectiva social do projecto, e no outro a perspectiva de Engenharia:

- **Produção de dados indicadores do nível de segurança da Internet Portuguesa** - Sempre com a intenção de criar um histórico fidedigno e consistente, o **Nonius** produzirá iteração[2] após iteração uma série de dados estatísticos relativos a vulnerabilidades técnicas e à presença de *malware* [3] em toda a Internet Portuguesa.
- **Consciencialização Nacional para a problemática gerada à volta da Segurança de Informação** - Esta frase define claramente o objectivo principal do **Nonius** na sua vertente social. A necessidade de uma consciencialização deste tipo é urgente para uma realidade como a que se vive actualmente em Portugal. A título de exemplo, é generalizado o desconhecimento relativo à importância da protecção de dados, à

[1] Computer Security Incident Response Team
[2] Uma execução total do sistema, incluído varrimento e carga de testes.
[3] Sotware Malicioso

necessidade de políticas de segurança de informação, e à facilidade e proliferação dos ataques informáticos contemporâneos. Estes são apenas alguns exemplos das lacunas que o **Nonius** pretende ajudar a reduzir ou minimizar com as suas publicações.

O presente artigo serve como objecto de apresentação e descrição sumária do projecto **Nonius**. Encontra-se subdivido em sete secções, sendo a primeira, onde foi feita uma introdução ao projecto e respectivos objectivo. De seguida é apresentada a arquitectura do sistema computacional que sustenta o projecto. Posteriormente, na terceira secção, são descritas as várias fases de cada iteração. Na quarta secção, são expostos de forma sucinta os vários testes que compõem a actual carga de testes. De seguida, são apresentados os resultados obtidos na primeira iteração do sistema. Por último é explanado um pouco do que será o futuro do **Nonius** e algumas conclusões referentes ao estado actual do projecto.

2 Arquitectura do sistema

O desenho da arquitectura do sistema teve em conta a possibilidade da infra-estrutura técnica, que suporta cada um dos componentes descritos de seguida, estar em localizações geográficas distintas, bem como a possibilidade da existência de mais de um exemplar do componente referido de seguida como *Crawler*. Tal situação levaria à utilização de um ou mais canais de comunicação seguro, p.ex., estabelecido sobre a Internet.
O **Nonius** é constituído por dois componentes conceptuais distintos, o *Crawler* e o *Digester*. A figura 1 representa a visão geral da arquitectura do **Nonius**.

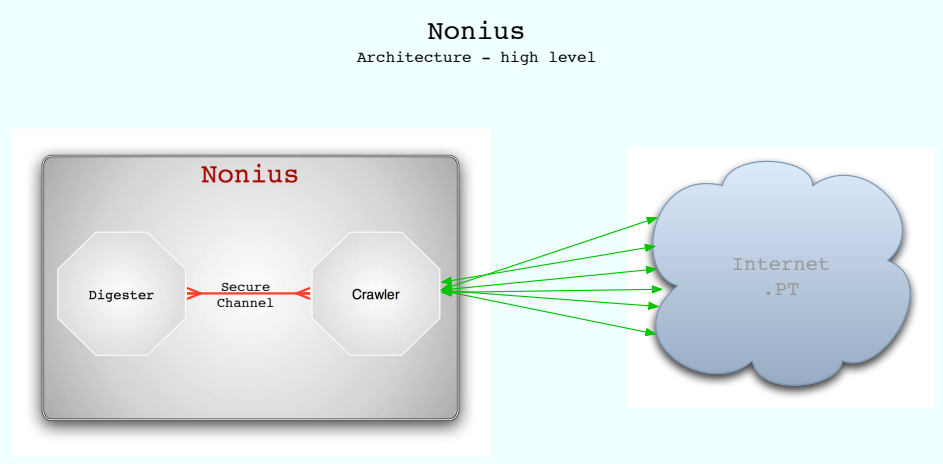

Figura 1: Arquitectura Geral do Nonius.

Atribuem-se ao *Crawler* todas as funções relacionadas com o processo de rastreio, execução e sucessiva recolha de informação da carga de testes. Por outro lado ao *Digester* são atribuídas todas as funções de tratamento e anonimização da informação recolhida, bem como a sua publicação num *web-site*.
Mais pormenorizadamente, o *Crawler* contém os seguintes sub-conponentes: *Network Engine*; *Malware Detection*; *Technical Vulnerabilities Detection*.
O *Network Engine* é responsável pela gestão de todas comunicações geradas durante o processo de rastreio, o módulo de *Malware Detection* implementa os testes de presença de *Malware*, e por último, o módulo *Technical Vulnerabilities* implementa a carga de testes referente às vulnerabilidades técnicas.

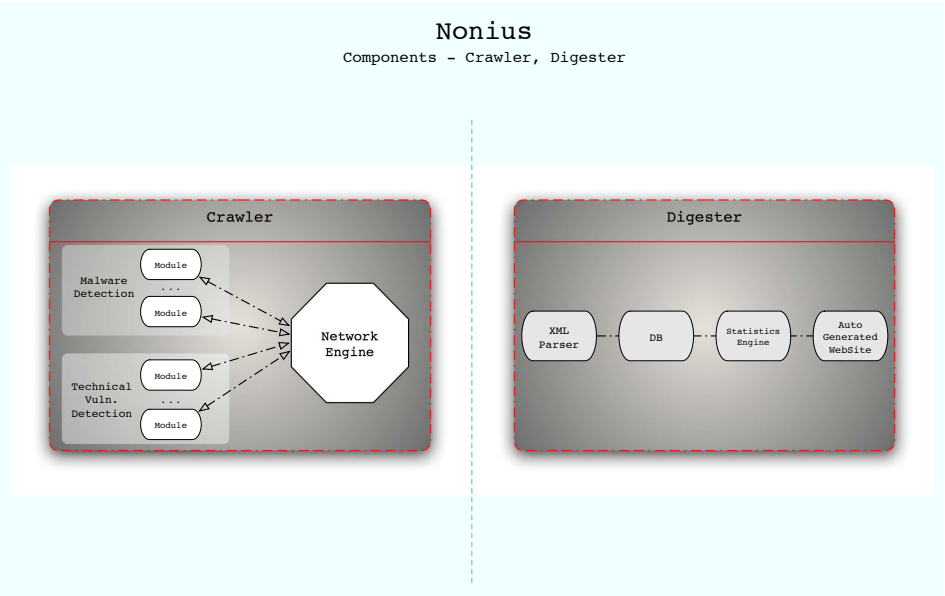

Figura 2: Componentes do Nonius.

Por sua vez, o *Digester* é subdividido nos seguintes sub-componentes: *XML Parser*; *DBMS*; *Statistics Engine*; *Auto Generated Web-Site*. Sendo o *XML Parser* responsável pelo processo de anonimização dos dados XML oriundos do *Crawler* e pela sua inserção na base de dados, o sub-componente *DBMS* (na figura, *DB*) representa o sistema de base de dados onde a informação será armazenada durante o seu processamento e, já agregada e anonimizada, no final de cada iteração do **Nonius**. O *Statistics Engine* é o sub-componente responsável pela produção dos vários dados estatísticos referentes a toda a informação contida no **Nonius**. Por último, o *Auto Generated Web-Site* é o sub-componente responsável pela criação automatizada do web-site onde serão publicados os resultados do **Nonius**. A figura 2 mostra o posicionamento de cada sub-componente no sistema.

3 Fases de cada iteração

Compreende-se por iteração do **Nonius**, o rastreio total a todo o endereçamento IPv4 e respectivos domínios *.pt* pretendidos.
Existem quatro estados distintos em cada iteração do **Nonius**, figura 3: *Host Discovery*, *Tests Payload*, *Data Anonymization*, *Published Data*.
Entende-se como *Host Discovery* o processo de rastreio que permite saber o número de endereços IPv4 vivos [4] num determinado espaço de endereçamento IP. No final deste processo alcança-se o estado ***Host Discovery***, onde existirá uma lista de endereços IPv4 considerados vivos e respectivos domínios *.pt*.
O Processo de *Host Discovery* desempenha um papel crucial na eficácia e abrangência dos resultados do **Nonius**, na medida que é este processo que permite definir a dimensão do âmbito de teste de cada iteração.
Este tipo de processos exigem uma grande optimização e especificação, na medida que têm

[4] Considera-se como *endereço IPv4 vivo* um determinado endereço IPv4 que responda a algum dos processos de sonda que lhe é feito.

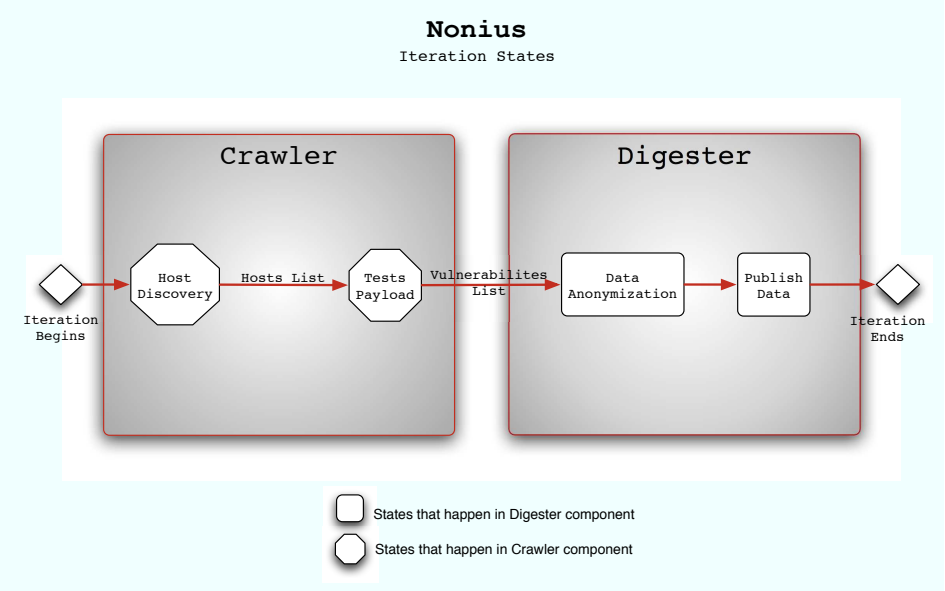

Figura 3: Vários estados de cada iteração.

que ser capazes de lidar com inúmeros (muitas vezes imprevisíveis) cenários. É esta variedade de cenários que pode distorcer os resultados obtidos durante o processo. Situações como a utilização de *traffic shapping*, *NAT*, sistemas de *QoS*, *IDS/IPS*, *firewalls* ou outros sistemas que de alguma maneira interfiram com o tráfego IP em algum ponto do caminho percorrido pelo *flow* em questão, tornam o processo de *Host Discovery* uma tarefa em que é difícil obter resultados cem por cento completos e exactos.
No sentido de tentar contornar estes obstáculos da maneira mais eficiente possível, o processo de *Host Discovery* do **Nonius** foi segmentado em três fases distintas e correlacionadas por uma ordem de preferência, relativa a exactidão e performance. Cada uma das fases distingue-se pela utilização de uma técnica distinta, sendo estas: o *reverse-DNS scan*, o *TCP SYN scan* e o *UDP Empty scan*. Cada uma destas técnicas oferece vantagens e desvantagens largamente conhecidas, de modo que não serão especificadas neste artigo.
A correlação e ordem de preferência dos resultados de cada uma das fases encontra-se descrito na seguinte tabela:

Técnica	**Inclusão dos resultados**
reverse-DNS scanning	apenas se for identificado em pelo menos mais uma técnica
TCP SYN scanning	inclusão directa
UDP Empty scanning	inclusão directa

O segmento referente aos domínios *.pt* é obtido através de, um conjunto de pesquisas a motores de busca [5], de dados oriundos do *reverse-DNS scanning* e, por último, por um conjunto de pesquisas à base de dados *WHOIS* do RIPE-NCC.
Através da lista obtida no estado *Host Discovery*, são executados os testes referentes à presença de *malware* e às vulnerabilidades técnicas. No fim desta carga de testes e após a recolha dos resultados dos mesmos, o **Nonius** encontra-se no estado *Tests Payload*. Neste estado o **Nonius** conta com uma lista das vulnerabilidades encontradas em cada endereço IPv4 testado, portanto, informação não anonimizada.

[5]Motores de busca utilizados: Google, Live Search, Sapo.

Esta lista de pares (Vulnerabilidades, endereço IPv4) passa por uma fase de anonimização, que consiste basicamente na contagem de ocorrências de cada vulnerabilidade no espaço de endereçamento testado, o que resulta num quadro de dados nos formatos: (*Vulnerabilidade X, Numero de ocorrências Y*); (*Vulnerabilidade X, Numero de ocorrências no ISP Y*). Quando este quadro estiver finalizado o **Nonius** encontra-se no estado *Data Anonymization*. Por último são gerados os dados e gráficos estatísticos baseados nas métricas internas, de maneira a ser criado/actualizado o web-site. No final deste processo o **Nonius** está no estado *Published Data*.

4 Vulnerabilidades e Presenças de Malware Testadas

A escolha das vulnerabilidades teve em conta duas preceptivas distintas, uma representativa do que se pode designar por sector organizacional, e outra representativa dos utilizadores caseiros.
Num sentido lato, os principais riscos para o sector organizacional estarão, de uma forma ou de outra, ligados com a fuga/perca de informação. Já para os os utilizadores caseiros, a fuga de informação surgirá paralela à possível utilização das seus computadores para a execução de crimes informáticos a terceiros. Estas duas premissas estiveram por de trás das decisões relativas à carga de testes que o **Nonius** executa.
De seguida é apresentada uma breve descrição das várias vulnerabilidades testadas actualmente pelo **Nonius**.

1 Acesso por SNMP com permissões apenas de leitura, e de leitura e escrita em simultâneo
A possibilidade de aceder a um sistema usando SNMP pode, no mínimo, representar a maneira de um possível atacante obter informação descritiva desse sistema. Dependendo do sistema, as informações obtidas podem variar entre simples identificações de fabricante até à totalidade das configurações usadas no sistema, ou até mesmo à identificação de software que esteja a ser executado localmente. Independentemente do tipo de informação possível de obter, o acesso por SNMP com permissões de leitura é considerada uma vulnerabilidade grave. Se a possibilidade de um atacante ter acesso a informações descritivas e/ou de configuração, de um determinado sistema é considerada uma vulnerabilidade grave, a possibilidade de alteração dessa informação é, certamente, uma vulnerabilidade crítica. Torna-se evidente que a exploração desta vulnerabilidade por parte de um atacante, pode levar facilmente a um compromisso integral da integridade e funcionamento do sistema. Juntando a isto o facto de exploração poder ser remota, torna o acesso por SNMP com permissões de escrita e leitura, umas das vulnerabilidades mais criticas das testadas pelo **Nonius** actualmente.

2 Permissão de transferências de Zona de DNS por AXFR
O AXFR é um protocolo para transferências de zonas de DNS entre servidores de DNS. A possibilidade de terceiros poderem aceder à informação contida numa zona de DNS é considerada uma vulnerabilidade grave. Vulnerabilidades deste tipo podem, entre outros, representar uma fuga de informação suficiente para um atacante identificar a estrutura e topologia da rede associada ao domínio em causa.

3 DNS Snooping
Se um determinado servidor de DNS permitir pedidos não recursivos a terceiros, possibilita a um atacante executar um ataque conhecido como *DNS Snooping*. Este tipo de ataques fornece ao atacante dados sobre a informação contida na *cache* do servidor de DNS, permitindo assim ao atacante, *p.ex.*, saber se determinado domínio foi resolvido recentemente. Numa primeira avaliação este tipo de vulnerabilidade pode ser conotado de um nível baixo

de importância, contudo, se se fizer um enquadramento com a actual dinâmica do mundo empresarial e a sua respectiva dependência das Tecnologias da Informação, essa perspectiva muda: a possibilidade de um atacante obter informação sobre fornecedores de determinados serviços (como *p.ex.* de *backup* remoto, serviço de e-mail externos, servidores de reenvio de E-mail...), ou a possibilidade de identificação de parceiros estratégicos que não sejam de conhecimento público, pode certamente representar um grave fuga de informação.
Supondo que um atacante pretendia atacar determinada entidade (X), que por sua vez requisitava um serviço de *backups* remoto a uma outra entidade (Y). Caso um dos servidores DNS da entidade X tivesse vulnerável a *DNS Snooping*, o atacante poderia identificar facilmente o(s) domínio(s) da entidade Y, e focar o seu ataque nesses domínios. Caso o atacante fosse bem sucedido no ataque à entidade Y, a informação da entidade X seria comprometida.

4 Uso de SSH versão 1.x

O uso das versões 1.33 e 1.5 do protocolo SSH permite a um atacante, que consiga interceptar o fluxo de comunicação, comprometer na totalidade a integridade da informação transitada nessa comunicação.

5 Uso de certificados SSL gerados pelo pacote do OpenSSL Debian com versões vulneráveis, em SSH[6]

No dia treze de Maio de 2008[1], o Projecto *Debian* anunciou a existência de uma vulnerabilidade no pacote do software *OpenSSL* que o projecto publicava. A vulnerabilidade em causa deveu-se a um erro do responsável pelo pacote de software que, ao comentar linhas no código do software em causa, interferiu radicalmente com a capacidade de entropia necessária para os processos de cifragem do *OpenSSL* serem considerados seguros. Mais concretamente, a vulnerabilidade debilitou o *Pseudo Random Number Generator (PRNG)* por completo. O conjunto de chaves possíveis para a cifragem viu-se assim reduzido ao minúsculo número de 32767 possibilidades, tornando assim a "adivinha"das chaves de cifragem um processo trivial, mesmo usando os tão pouco produtivos, processos de força bruta. Um dos serviços em que esta vulnerabilidade pode ter um impacto destruidor, é no *SSH (Secure Shell)*. Um servidor de *sshd* que use chaves geradas pelo pacote *Debian* do *OpenSSL* vulnerável, pode ser comprometido usando técnicas de força bruta em poucos instantes. No caso de sucesso, o atacante fica com permissões Administrador (*root* nos sistemas operativos baseado *Unix*).

6 Uso de Telnet

O uso de Telnet é considerado inseguro, umas vez que os dados em trânsito não usam qualquer tipo de cifra. O que permite a terceiros ter acesso a toda informação que circular nas comunicações geras por este serviço, incluído por exemplo credenciais de autenticação e outros dados confidenciais.

7 SMTP Relay público

Um serviço *SMTP* que permita retransmissão de mensagens para outro domínios que não o ou os que forem da sua responsabilidade, representa uma vulnerabilidade grave. Uma vez que permite a criminosos usarem o serviço em causa para proliferação de *spam*. Embora esta vulnerabilidade não ponha risco a infra-estrutura onde corre, sem contar com o uso indevido de recursos, considera-se uma vulnerabilidade bastante grave uma vez é uma das fontes de *spam*.

8 Uso de Finger

O serviço Finger tem como objectivo fornecer informações sobre os utilizadores do sistema,

[6]Uma vez que quando esta vulnerabilidade foi publicada já se encontrava a decorrer a primeira iteração do **Nonius**, na primeira iteração o teste da mesma está restringido apenas a dados recolhidos aquando dos testes relativos ao uso de *SSH1.1*.

incluído em certos casos se estes se encontram ligados ao sistema.
Este tipo de informação pode ser utilizada por um atacante para, entre outros, obter informação sobre *usernames* para, *p.ex.*, o uso posterior em ataques de força bruta.

9 Acesso público a partilhas de CIFS/SMB
O acesso público a partilhas de CIFS/SMB, vulgo partilhas de *Windows*, para além do evidente acesso directo à informação partilhada, pode ter um papel crucial em determinados tipos de ataques, nomeadamente em processos de *fingerprinting* do sistema.

10 Acesso público a partilhas de CIFS/SMB em que pelo umas delas seja C:\ou C:\windows Se o acesso público a informação que não esteja directamente relacionada com o sistema operativo em si é considerada uma vulnerabilidade grave, sê-lo-á ainda mais se a informação disponível for relacionada com o sistema operativo, onde um atacante pode facilmente obter um perfil altamente detalhado do sistema operativo da máquina em causa.

11 Uso de certificados SSL expirados
O uso de certificados SSL expirados coloca em risco a privacidade dos utilizadores do serviço em causa. Na medida em que facilita e favorece ataques, como por exemplo ataques *Man-In-The-Middle*(MITM)[7].

12 Uso de protocolos consideradas vulneráveis
O uso da versão número dois do protocolo SSL é considerada um risco. O SSL 2.0 detêm várias falhas nos seus processos criptográficos [2]. O seu uso é totalmente desaconselhado uma vez que torna possível a execução de ataques *MITM* e da decifragem, por parte de um atacante, do tráfego gerado por comunicações que façam uso de SSL 2.0.

De seguida serão descritos os teste a presença de *Malware* que o **Nonius** executou na sua primeira iteração. O testes de *Malware* executados cobrem um total de quatro espécies distintas, das quais o **Nonius** é capaz de identificar 12 estirpes diferentes.
De uma forma geral, pode-se afirmar que o grau de certeza dos teste de *Malware* é bastante mais baixo do que os testes de Vulnerabilidades técnicas. Este facto deve-se não só às características furtivas deste tipo de software, que tem como um dos principais objectivos garantir que não sejam detectados, mas também às dificultadas técnicas impostas por razões de foro legal, naturalmente adjacentes a este tipo de processos. Se é tecnicamente difícil detectar a presença de *Malware* num determinado sistema onde se detém total acesso e total permissão de uso, muito mais o será em sistemas onde esse nível de acesso e permissão não existem, como é o caso do **Nonius** e dos sistemas que testa.
Pode-se ainda referir o acréscimo de dificuldade, relativo ao facto de se tratarem de testes remotos, ao invés dos típicos testes locais de *Malware*.
Tendo isto em conta, a filosofia adoptada foi: tentar enquadrar o máximo possível de espécimens de *Malware* e apenas quando for possível fazerem-se testes com maior precisão; garantir a coerência dos resultados finais através de uma adequada distribuição dos pesos a cada um dos testes (quanto mais preciso for o teste, mais peso no resultado final terá).
A escolha dos espécimens a testar teve por base dois factores: vestígios possíveis de detectar remotamente; grau de actividade.
Na lista que se segue são apresentados as quatros espécies de *Malware* testados, acompanhadas da indicação das várias estirpes suportadas pelos teses.

[7] Ataques em que através de adulteração dos dados identificativos dos vários pontos de comunicação, o atacante, consegue passar a interceptar toda a comunicação.

NetSky

Tipo: *worm*

In the Wild:[8] Sim

***Ranking* de preexistência:** 2º lugar no ano de 2007 com 21.94% das infecções detectadas (25161383 infecções); 1º lugar no mês de Abril de 2008 com 21.17%.

Principais métodos de propagação: E-Mail

Sistema Operativo: Windows (95, 98, 98 SE, NT, ME, 2000, XP, 2003

Estirpes detectadas: AA, S, T e Z

Principais Efeitos: Geração de SPAM, modificações no *Registry* do Windows, efectua ataques DoS

Vestígios Remotos: *backdoor* nos portos 665 (estirpes AA e Z) e 6789 (estirpes S e T).

Alias: Symantec: W32.Netsky.Z@mm ; Mcafee: W32/Netsky.z@MM ; Kaspersky: Email-Worm. Win32.NetSky.aa ; TrendMicro: WORM_NETSKY.Z ;F-Secure: W32/Netsky.Z@mm

Traços Históricos:

•Ataque DoS aos domínios: www.nibis.de, www.medinfo.ufl.edu e www.educa.ch (02/05/2004 e 05/05/2004); www.cracks.am, www.emule.de, www.kazaa.com, www.freemule.net, www.keygen.us (14/04/2004 e 23/04/2004)

•Datas de descoberta: NetSky.S -04/04/2004, NetSky.T -06/04/2004, Worm/NetSky.Z -21/04/2004, Worm/NetSky.AA -22/05/2005

MyTob

Tipo: *worm*

In the Wild: Sim

***Ranking* de preexistência:** 3º lugar no ano de 2007 com 16.43% das infecções detectadas (18839787 infecções); 4º lugar no mês de Abril de 2008 com 12.37%.

Principais métodos de propagação: E-Mail, rede local através de exploração das vulnerabilidades expressas nos boletins da Microsoft, MS03-049 e MS04-011

Sistema Operativo: Windows (95, 98, 98 SE, NT, ME, 2000, XP, 2003)

Estirpes detectadas: F, CF

Principais Efeitos: Geração de SPAM, modificações no *Registry* do Windows, bloqueia o acesso a sites de fabricantes de software de Segurança (impedindo assim por exemplo a actualização de software Anti-Vírus), instala outro Malware (nomeadamente *Rootkits* [9]), rouba informação confidencial, torna o sistema num *Zombie* de uma *botnet* baseada em *IRC* (*p.ex.* no canal #.hellbot no servidor bmu.q8hell.org)

Vestígios Remotos: Servidor de *FTP* no porto 10087 e 10487 com o *banner* "220 StnyFtpd 0wns j0".

Alias: Symantec: W32.Mytob.AH@mm ; Kaspersky: Net-Worm.Win32.Mytob.t, Net-Worm.Win32.Mytob.x; TrendMicro: WORM_MYTOB.BW,WORM_MYTOB.BR; F-Secure: Net-Worm.Win32.Mytob.t

Traços Históricos: Datas de descoberta: Mytob.IJ -07-07-2005, Worm/Mytob.CF -27/04/2005

Zafi

Tipo: *worm*

In the Wild: Sim

***Ranking* de preexistência:** 7º lugar no ano de 2007 com 3.00% das infecções detectadas (3437391 infecções); 9º lugar no mês de Abril de 2008 com 3.09%.

Principais métodos de propagação: E-Mail, redes *Peer to Peer*

Sistema Operativo: Windows (95, 98, 98 SE, NT, ME, 2000, XP, 2003

[8]Expressão utilizado para indicar que um determinado espécimen de *Malware* ainda se encontra em proliferação.

[9]Tipo de software malicioso que permite o controlo total do sistema por parte do atacante, de maneira furtiva (ou seja, sem o proprietário se aperceber)

Estirpes detectadas: B, D, F
Principais Efeitos: Geração de SPAM, modificações no *Registry* do Windows, desactiva ou destrói software de protecção.
Vestígios Remotos: instala uma *backdoor* que usa o porto 2121 e 8181 para interacção com o atacante e para actualização do próprio *malware*
Alias: Symantec: W32/Zafi.d@MM, W32.Erkez.B@mm; Mcafee: W32/Zafi.d@MM; Kaspersky: Email-Worm.Win32.Zafi.d, Email-Worm.Win32.Zafi.b; F-Secure: Email-Worm.Win32.Zafi.b
Traços Históricos: Datas de descoberta: Worm/Zafi.D -14/12/2004, Worm/Zafi.B -11/06/2004

Mydoom
Tipo: *worm*
In the Wild: Sim
***Ranking* de preexistência:** 8º lugar no ano de 2007 com 2.49% das infecções detectadas (2850097 infecções); 6º lugar no mês de Abril de 2008 com 5.30%.
Principais métodos de propagação: E-Mail, redes *Peer to Peer*
Sistema Operativo: Windows (95, 98, 98 SE, NT, ME, 2000, XP, 2003
Estirpes detectadas: A, L, G, T
Principais Efeitos: Geração de SPAM, modificações no *Registry* do Windows, desactiva ou destrói software de protecção. Entre 10 e 20 minutos após a sua execução inicia um ataque de *DoS* contra o endereço www.symantec.com (a estripe Mydoom.G).
Vestígios Remotos: instala uma *backdoor* que usa os portos 1042 e 1034 5422 1080 para interacção com o atacante
Alias: Symantec: W32.Mydoom.L@mm, Backdoor.Zincite.A; Mcafee:
W32/Mydoom.n@MM; Kaspersky: Email-Worm.Win32.Mydoom.m;
TrendMicro: WORM_MYDOOM.L, WORM_MYDOOM.M
Traços Históricos: Datas de descoberta: Worm/Mydoom.L.2 em 19/07/2004, Tr/My- doom.BB.1 em 23/05/2006, I-Worm.MyDoom.gen (W32/MyDoom-Gen
ou Win32.Mydoom.S@mm) em 09-03-2004, W32/Mydoom.g@MM
(ou W32.Mydoom.G@mm) em 03-02-2004

Os dados apresentados referentes a *Malware* representam uma compilação de informação feita pelos autores através de recolhas empíricas por Análise de *Malware*, e através das seguintes fonte de informação públicas:

- *Malware prevalence Reports* - http://www.virusbtn.com/
- *Avira Virus Search* - http://www.avira.com/en/threats/
- *MacAfee Threat Center* - http://vil.nai.com/vil/
- *F-Secure Virus Description Database* - http://www.f-secure.com/v-descs/

A tabela 1, apresenta a classificação de cada Vulnerabilidade Técnica, e de cada Teste de presença de *Malware*, em termos de: Nível CVSS[5]; Vector CVSS; Nível de Precisão. O CVSS (Common Vulnerability Scoring System) é, como o próprio nome indica, um sistema métrico de classificação de vulnerabilidades. As suas classificações têm em conta três perspectivas distintas, a *base*, a *temporal*, e a *environmental*. Sendo a *base* responsável pela classificação do impacto, da complexidade e da dificuldade de exploração da vulnerabilidade, a *temporal* pela a avaliação das características que mudam com o passar do tempo, e por sua vez a *environmental*, as características especificadas de ambientes de utilização/execução.

Descrição	Nível CVSS	Precisão	Vector CVSS
SNMP, leitura	5.0	100%	(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
SNMP, escrita	7.5	100%	(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
DNS Zones, AXFR	5.0	100%	(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
DNS Snooping	5.0	90%	(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
SSH 1.1	2.9	100%	(CVSS2#AV:A/AC:M/Au:N/C:P/I:N/A:N)
SSH, Debian	10.0	100%	(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
Telnet	6.1	100%	(CVSS2#AV:A/AC:L/Au:N/C:C/I:N/A:N)
SMTP Open Relay	5.0	90%	(CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)
Finger	5.0	80%	(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
CIFS/SMB shares	5.0	100%	(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CIFS/SMB shares (C:)	7.8	100%	(CVSS2#AV:N/AC:L/Au:N/C:C/I:P/A:P)
SSL Expired	5.7	100%	(CVSS2#AV:A/AC:M/Au:N/C:C/I:N/A:N)
SSLv2	5.7	100%	(CVSS2#AV:A/AC:M/Au:N/C:C/I:N/A:N)
NetSky	7.6	50%	(CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)
MyTob	10.0	65%	(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
Zafi	9.3	50%	(CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)
MyDoom	9.3	50%	(CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

Tabela 1: Classificação das Vulnerabilidades Técnicas e dos Teste de presença de *Malware* (CVSS, Precisão e Vector CVSS)

5 Resultados da primeira iteração

Os resultados apresentados na tabela 2 foram obtidos numa população de **3 665 760** endereços *IPv4* e **11 304** domínios *.pt* associados a **9 320** *DNS Servers* distintos.Dessa população foi possível identificar **30 913** vulnerabilidades em **83 306** endereços *IPv4* [10], o que corresponde a 16.1% de um total de **516 213** endereços vivos.
A referida iteração demorou aproximadamente 330 horas (14 dias) a executar na sua totalidade. No referido intervalo de tempo foram executados os vários rastreiros, a respectiva carga de testes e o processamento de todos os dados recolhidos.
A tabela 2, o gráfico presente na figura 4, e o gráfico da figura 5 representam, respectivamente, a distribuição de ocorrências[11] das várias vulnerabilidades técnicas e os dados relativos às presenças de *Malware* detectadas.

O principal resultado do **Nonius** é um valor representativo do nível de Segurança da Internet Portuguesa (***NSIP***). O **NSIP**, tal como todos os resultados do **Nonius**, é um indicador com carácter estatístico, ou seja, é um dado indicador do nível de Segurança da Internet Portuguesa e não um valor exacto do que realmente é o referido nível. Até porque, o cálculo exacto do nível de Segurança de um segmento de endereçamento tão vasto e mutável como o referente a Internet Portuguesa, é difícil de alcançar, senão mesmo impossível. Este valor é obtido através de uma média ponderada dos resultados provenientes da carga de testes, onde o peso é o Valor *CVSS* e a percentagem de precisão de cada vulnerabilidade, ambos já apresentados.
O *NSIP* é calculado segundo a seguinte fórmula e corresponde a um valor entre zero e dez com uma casa decimal.

[10] Endereços onde foi possível efectuar pelo menos um teste.
[11] Uma ocorrência de uma determinada vulnerabilidade significa que o teste efectuado devolveu um resultado positivo.

NSIP, Nível de Segurança da Internet Portuguesa	
NSIP =	$\frac{\sum_{k=1}^{n}\left(\#Teste_k \ . \ CVSS \ . \ \%Prec\right)}{\#IPsTestados} = \mathbf{2.1}$
Legenda: **%Prec** - grau de precisão. **n** - número testes existentes no sistema. **CVSS** - valor CVSS de um determinado teste. #**IPs Testados** - número total de endereços IP onde foi possível executar pelo menos um teste.	

Nº Vuln.	**Descrição**	**Número de Ocorrências/Presenças**	**Precisão**
1	SNMP, leitura	697	100%
2	SNMP, escrita	690	100%
3	DNS Zones, AXFR	1256	100%
4	DNS Snooping	1962	90%
5	SSH 1.1	3442	100%
6	SSH, Debian	241	100%
7	Telnet	15782	100%
8	SMTP Open Relay	21	90%
9	Finger	431	80%
10	CIFS/SMB shares	672	100%
11	CIFS/SMB shares (C:)	988	100%
12	SSL Expired	966	100%
13	SSLv2	3765	100%
14	NetSky	94	50%
15	MyTob	329	65%
16	Zafi	239	50%
17	MyDoom	60	50%

Tabela 2: Número de ocorrências de cada Vulnerabilidade Técnica.

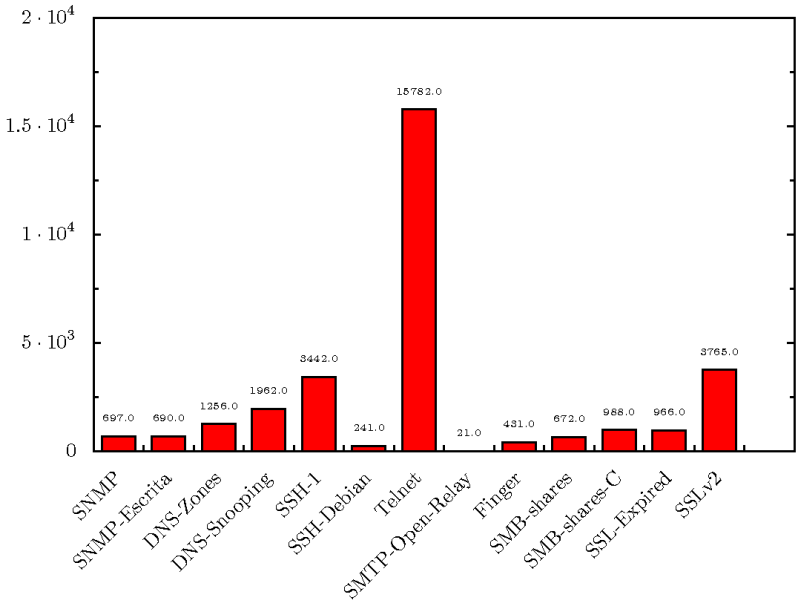

Figura 4: Ocorrências de cada Vulnerabilidade Técnica.

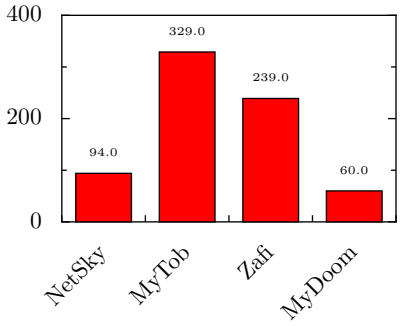

Figura 5: Presenças de *Malware* detectadas.

Resumindo, o *NSIP* corresponde ao racio entre o somatório de, o número de ocorrências de cada teste efectuado multiplicado pelo seu valor *CVSS* e pelo seu grau de precisão, e o número total de endereços *IP* onde foi possível efectuar pelo menos um teste.
Para facilitar a compreensão do significado do *NSIP* e consequentemente aumentar a abrangência da disseminação do **Nonius**, foi elaborada uma escala qualificativa que não é apresentada neste artigo, mas encontra-se totalmente descrita no *web-site* no projecto Nonius[12].
Uma das análise feitas aos resultados obtidos considerou a subdivisão entre um sector Estatal (infra-estruturas Estatais e Governamentais), e um sector Privado.
Contudo, esta subdivisão, não pode ser tida como exacta, uma vez que não é totalmente completa e pode conter falsas inclusões. O processo que suporta esta subdivisão tem um cariz não-automatizado, o que torna bastante difícil alcançar um nível de precisão completa dada a dimensão da população a ser testada, nomeadamente da lista de domínios *.pt*.

NSIP $=$	$\frac{\sum_{k=1}^{n}\left(\#Teste_k \ . \ CVSS \ . \ \%Prec\right)}{\#IPsTestados}$
Estatal	**NSIP = 1.6**
Privado	**NSIP = 2.2**

A tabela 3 e a figura 6, descrevem a variação dos dados globais apresentados anteriormente, pelas parcelas de endereçamento testado referentes ao Estado e ao sector privado.

A tabela 4 apresenta as percentagens de endereços com uma ou mais vulnerabilidades (endereços vulneráveis), no quadro geral, na parcela do endereçamento testado associado ao Estado, Organizações Estatais e Governamentais, e na parcela associada ao sector privado.

6 Trabalho Futuro

O futuro do **Nonius** passará obrigatoriamente por uma expansão do seu âmbito de execução, nomeadamente pelo aperfeiçoamento da detecção e diferenciação das parcelas de endereçamento referentes ao sector Privado e sector Estatal, e uma tentativa de aumento do número de domínios *.pt* a serem testados.
Para além disso será garantido que o resto do caminho a percorrer, afim de concretizar os objectivos inicialmente traçados, será concluído. Em concreto, uma maior difusão possível dos resultados obtidos e respectivos conteúdos de consciencialização.
Por último, é importante referir a ampliação da carga de testes e aperfeiçoamento da mesma. O esforço de aperfeiçoamento dos testes já existentes incidirá especialmente nos testes relativos à presença de *Malware*, uma vez que são os que apresentam menor taxa de preci-

[12]https://www.cert.ipn.pt/Nonius/tech.html

Nº Vuln.	Descrição	Nº de Ocor. (Estado)	Nº de Ocor. (Privado)	Precisão
1	SNMP, leitura	0	697	100%
2	SNMP, escrita	0	690	100%
3	DNS Zones, AXFR	415	841	100%
4	DNS Snooping	585	1377	90%
5	SSH 1.1	280	3162	100%
6	SSH, Debian	18	223	100%
7	Telnet	1453	14345	100%
8	SMTP Open Relay	9	12	90%
9	Finger	104	327	80%
10	CIFS/SMB shares	4	668	100%
11	CIFS/SMB shares (C:)	12	976	100%
12	SSL Expired	77	889	100%
13	SSLv2	418	3347	100%

Tabela 3: Ocorrências de cada Vulnerabilidade Técnica no sector Estatal e no sector Privado.

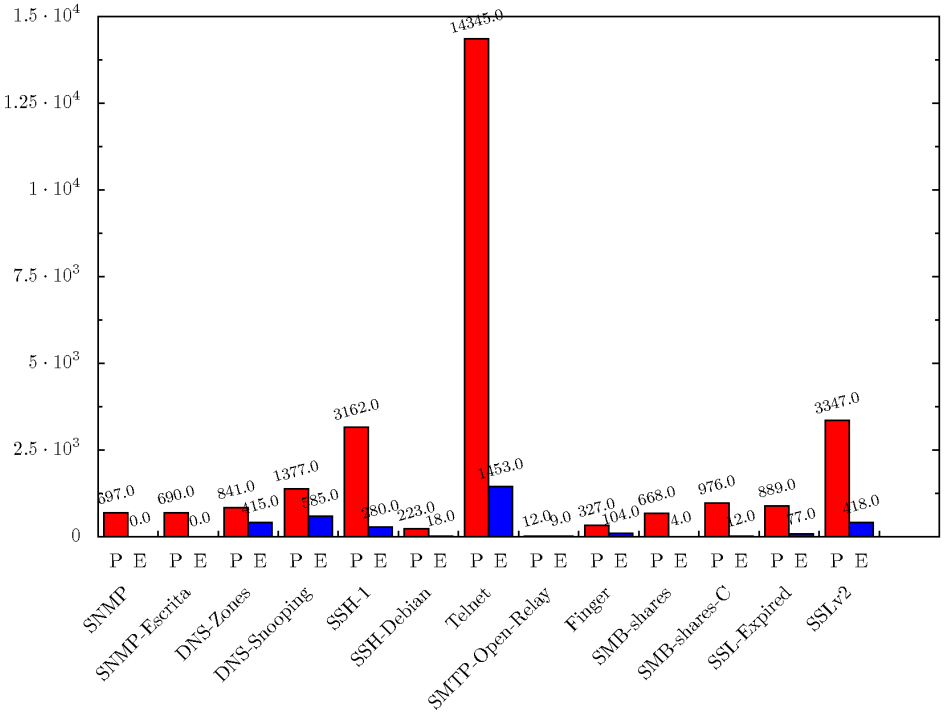

Figura 6: Variação das V.T. no sector Estatal e Privado.

são. Relativamente à implementação de novos testes, surgiram naturalmente algumas ideias ainda por concretizar. Como referência aponta-se a possibilidade de teste de *DNS Injection*, de *BGP Hijacking* ou de um conjunto de teste direccionados para as técnicas conhecidas como *Google Hacking*.

	Global	**Estatal**	**Privado**
Endereços vulneráveis	23 351	2 100	21 251
Endereços testados	83 306	11 380	71 926
Endereços vivos	516 213	16 607	499 606
Em relação aos endereços vivos	4.5%	12.6%	4.3%
Em relação aos endereços testados	28.0%	18.5%	29.5%

Tabela 4: Percentagem de endereços vulneráveis.

7 Conclusões

Evidentemente que, o trabalho aqui descrito representa apenas uma perspectiva do que poderá ser uma análise ao nível de segurança de um determinado segmento da Internet, até porque não se tratam de forma alguma de resultados exactos.
Contudo é importante reafirmar o carácter de alguma forma inovador do sistema, uma vez que não existem, pelo menos do conhecimento dos autores, sistemas que recolham o mesmo tipo de resultados de uma forma tão activa e focalizada, num âmbito de acção tão abrangente e definido. Poderão eventualmente ser comparados com o Nonius sistemas como, *Whats that site running?* e *Secure Server Survey* da Netcraft, o *Internet Threat Level*, ISS (IBM), ou *Threat Center* da Mcafee. Contudo, todos estes e muitos outros sistemas, ou são baseados em simples inquéritos, ou não abrangem um detalhe técnico tão aprofundado e um âmbito tão alargado como o Nonius, ou são baseados em recolhas passivas, ou simplesmente não revelam o processo que usam, o que demostra claramente que os resultados obtidos não poderão ser equiparados ao **Nonius**.
Paralelamente à concepção e implementação do **Nonius**, foi feito um estudo jurídico relativamente à viabilidade legal do Nonius. Estudo este que, de uma foram sucinta, diz que todos os processos e técnicas usadas pelo Nonius são completamente legais segundo a Lei vigente. Devendo-se isto, essencialmente ao facto de o Nonius se "limitar"a utilizar informação tida como pública, ou seja, não é feita nenhuma intrusão ou adulteração de sistemas de protecção e afins, para obtenção da informação utilizada.
Um outro aspecto que é interessante referir, é o facto de o sistema ter executado a primeira iteração em cerca de 14 dias, dado que teve um âmbito de acção consideravelmente alargado (cerca de 3.6 milhões de endereços IPv4 e 11 mil domínios *.pt*).
Relativamente aos resultados em si não haverá muito mais a acrescentar, são consideravelmente satisfatórios relativamente à sua expressividade e abrangência. Poderão não ser tão satisfatórios noutra perspectiva, na medida que apresentam valores de alguma forma preocupantes para a comunidade da internet Portuguesa. É importante referir, contudo, que os resultados poderiam ser bastante mais alarmantes, o que poderá vir a acontecer como consequência do alargamento do espectro da carga de testes. Todos os resultados apresentados neste artigo estão disponibilizados no *web-site* no projecto Nonius[13].

Referências

[1] *Debian Security Advisory: DSA-1571-1 openssl – predictable random number generator.* http://www.debian.org/security/2008/dsa-1571

[2] David Wagner - University of California- Berkeley, daw@cs.berkeley.edu; Bruce Schneier, Berkeley Counterpane Systems, schneier@counterpane.com *Analysis of the SSL 3.0 protocol.* http://www.schneier.com/paper-ssl.pdf .

[13] https://www.cert.ipn.pt/Nonius/

[3] *Serviços de Disseminação do CERT-IPN*. http://www.cert.ipn.pt/pt/disseminacao.html

[4] *RIPE Network Coordination Centre*. http://www.ripe.net/

[5] *Common Vulnerability Scoring System (CVSS-SIG)*. http://www.first.org/cvss/