RECIT
Revista Eletrônica Científica Inovação e Tecnologia

Revista Eletrônica Científica Inovação e Tecnologia
ISSN: 2175-1846

https://periodicos.utfpr.edu.br/recit

DESCOBERTA DE BOTNETS POR MEIO DE ANÁLISE DE TRÁFEGO DNS

Thales Nicolai Tavares.
tavares@redes.ufsm.br
https://orcid.org/0000-0003-1200-6031
Universidade Federal de Santa Maria – UFSM –Santa Maria – Brasil

RESUMO

Algumas botnets utilizam de técnicas de endereçamento dinâmico como ip-flux e domain-flux para a comunicação entre os bots e o servidor de comando e controle, tornando-as assim mais robustas para a operação, e consequentemente mais difíceis para a detecção. Este artigo detalha um método para realizar a detecção de botnets através da análise do tráfego DNS junto com a engenharia reversa de código malicioso. O método é um conjunto de procedimentos que devem ser seguidos para a obtenção de hosts caracterizados como bots. São apresentados dois estudos de caso que obtiveram êxito com a aplicação deste método.

PALAVRAS-CHAVE: Botnets, DNS, descoberta.

INTRODUÇÃO

Em toda a Internet recursos e sites são pesquisados por seu nome ou endereço IP, sendo necessário o uso do DNS (Domain Name System) para tal atividade. Logo o DNS é o serviço básico e essencial para o correto funcionamento da pesquisa na Internet. Entretanto devido ao acesso livre e distribuído do protocolo DNS, aplicações maliciosas também podem fazer consultas para realizar ataques, dentre elas botnets que podem ser definidas como um conjunto de máquinas comprometidas que permitem ao atacante o controle remoto dos recursos computacionais para realizar atividades fraudulentas ou ilícitas [McCarty 2003b, Freiling et al. 2005]. Tais máquinas utilizam um software chamado de bot (da palavra robô), o qual liga os computadores infectados a uma infraestrutura de Comando e Controle (C&C).

Alguns trabalhos propuseram sistemas, ferramentas e arquiteturas para detecção e mitigação de botnets, como [Ceron J. 2010] que definiu uma arquitetura baseadas em assinatura de rede de máquinas comprometidas por bots, [Laufer 2005] propôs um sistema de rastreamento de pacotes para descobrir a origem de ataques, [Hossain 2010] propôs a mineração do tráfego DNS para detecção de aplicações de envio de Spam, e [Kaio 2014] apresenta uma metodologia utilizando teoria dos grafos para distinguir consultas padrões de anômalas no tráfego DNS.

Motivado pelos problemas citados o presente artigo tem como objetivo, definir um método híbrido composto pela análise do tráfego de rede e a engenharia reversa, para detecção de botnets que utilizam o serviço de DNS para se proliferar e controlar seus bots. A intenção.

deste trabalho é ser um guia para a detecção com êxito de botnets que especificamente utilizam o serviço de DNS.

Para validar o método proposto, o mesmo foi executado em um ambiente real: uma empresa com diversos tipos de dispositivos, entre eles smartphones, desktops, servidores e notebooks. São apresentados dois estudos de caso, onde no primeiro foi possível detectar um Spyware que se conectava a um domínio do serviço No-IP, e no segundo uma botnet criada dentro da própria rede para fins de avaliação deste método.

O restante deste artigo está organizado da seguinte forma: A seção 2 apresenta o detalhamento do método proposto, a seção 3 apresenta os dois estudos de casos e os resultados obtidos, e a seção 4 apresenta as conclusões.

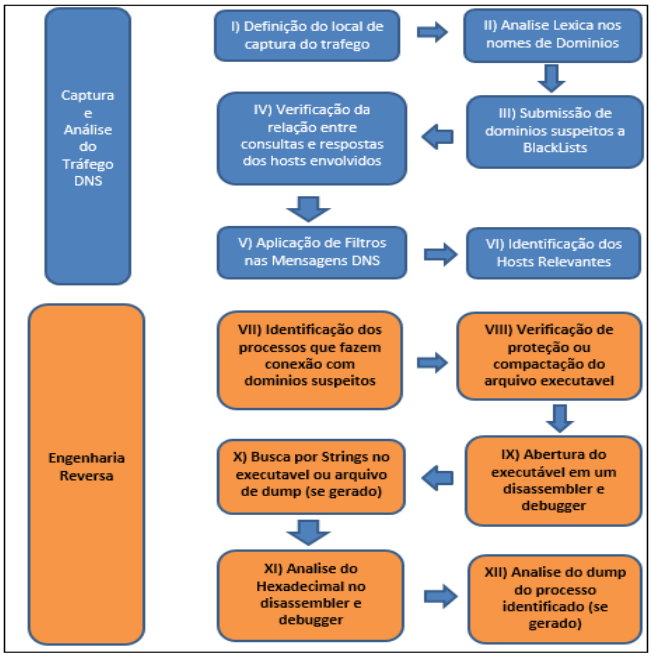
METODOLOGIA

Método de descoberta proposto

O método proposto neste trabalho é um roteiro de atividades que deve ser seguido, para descoberta de botnets. Este método é dividido em duas partes: a primeira parte trata da captura e análise do tráfego DNS. A segunda parte trata da engenharia reversa feita no código malicioso. A Figura 1 exibe o diagrama da ordem de execução e a própria estrutura do método. Neste trabalho foram utilizadas ferramentas conhecidas pelo autor para executar cada etapa do método,

porém cabe ressaltar que outras ferramentas também podem ser utilizadas para a execução do método, desde que cumpram o propósito definido em cada etapa.

Figura 1 – Diagrama Estrutural do Método



Fonte: Acervo pessoal (2018).

RESULTADOS

Estudos de caso

Nas seções 3.1 e 3.2 são apresentados dois estudos de casos, nos quais o método proposto foi aplicado. Em ambos os casos a análise do tráfego DNS tem como objetivo diminuir o escopo de hosts a serem analisados pela engenharia reversa.

Detecção de um Spyware

Neste estudo de caso, é apresentado como se obteve a identificação de um spyware, capturando e analisando o tráfego DNS a partir de um servidor de segurança com funções de firewall, gateway e roteador.

Para a captura do tráfego foi executada a seguinte linha de comando em ambiente Unix: <tcpdump -i eth1 src port 53 or dst port 53 -w capturaDNS-Dia_Hora.pcap> Posteriormente foi efetuado a analise léxica e submissão dos domínios a BlackLists. A Figura 2 demostra esta avaliação.

Figura 2 – Confirmação de Domínios listados em BlackLists

Fonte: Acervo pessoal

Após obter os domínios classificados como ameaça, efetuou-se a verificação no dump de rede, de quais endereços IPs consultaram os domínios listados.

Para entender o padrão de comunicação entre os hosts identificados como possíveis bots, é necessário relacionar o total de consultas realizadas, com o total de respostas, isto é possível através da visualização de conversações efetuadas entre os hosts.

Fazendo a relação entre as consultas, foi examinado o formato das mesmas, verificando- se a integridade e conteúdo de cada uma. A primeira tarefa foi à verificação da má formação das consultas, através das flags das mensagens DNS, como: “dns.flags.rcode == 1” e “dns.flags.rcode ==3” no filtro do Wireshark, é possível obter as consultas que retornaram com o status de MXDOMAIN (No Such Name), que podem corresponder a servidores de comando e controle. De posse dos hosts relevantes e os domínios suspeitos, efetuou-se nova análise no tráfego DNS em todos os arquivos de captura, fazendo-se a correlação entre quais os hosts que acessaram quais domínios, assim como a frequência em que acessavam. O comando para a verificação dos domínios em cada arquivo de captura foi: dns.qry.name contains "nomeDoDominio". A Tabela 1 mostra a correlação dos hosts que acessaram os domínios listados em BlackLists, e que também enquadraram-se em algum parâmetro dos filtros aplicados.

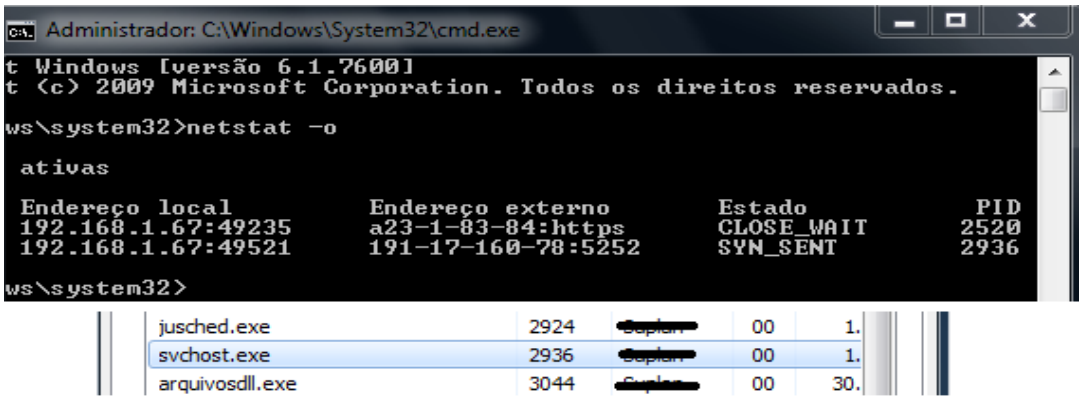
Tabela 1 – Correlação Domínios X Hosts

Correlação entre os Dominios listados em BlackLists e os Hosts Relevantes						
Dominio	**20**	**21**	**25**	**26**	**27**	**28**
nxtck.com	53	53	53	53,56	53,56	53
mininova.org	67	67				
xnxx.com				123	67	100,12
summonerswarskyarena.info				63		
tinyurl.com				63		
njrattttttttt.ddns.net	67	67		67	67	
ssp.lkqd.net	56,67,70	70	55,56,57,70		55,70	53,56,62
x.cnt.my	53	56,62	53,56	53,56	53	
bidswitch.rtb.adx1.com	70,123	55	56			56
anonycrackd123.ddns.net	67			67	67	
absolutosistema.no-ip.org	67	67		67	67	

Fonte: Acervo pessoal (2018)

Pelo fato do host com endereço IP 192.168.1.67 ser o host com mais entradas em domínios suspeitos, chamou-se a atenção para uma investigação mais profunda no mesmo. Ao inicializar o sistema operacional deste host, que por sua vez possui o sistema Windows, foi verificado o status das conexões ativas através do comando “netstat -o”, pois o parâmetro “-o” permite identificar o PID do processo que está em execução. Visto que nenhum programa de rede como gerenciador de e-mail, navegador web, ou outro tinha sido iniciado, este host já possuía conexões com um endereço IP. A Figura 3 mostra as conexões e o processo envolvido.

Figura 3 – Status das Conexões e Identificação do Processo

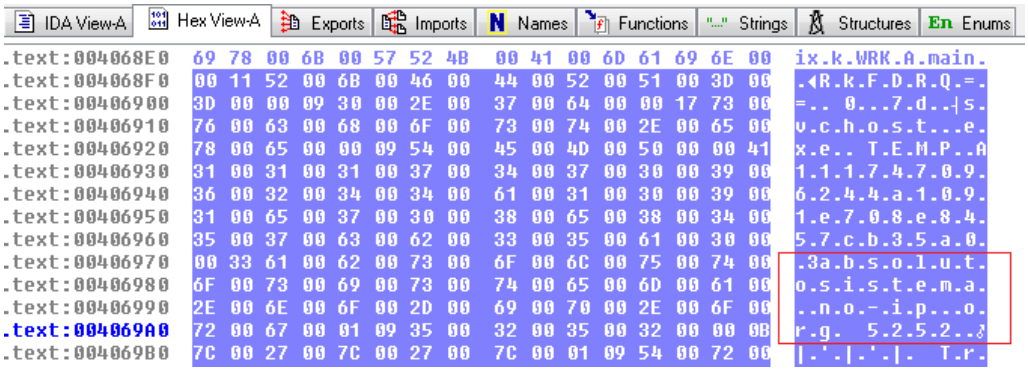


Fonte: Acervo pessoal (2018)

O arquivo svchost.exe foi submetido ao programa EXEinfoPE, e este informou que o mesmo estava protegido, com um ofuscador para códigos desenvolvidos na plataforma .Net. Para desofuscar/desproteger o arquivo svchost.exe foi utilizado o programa de4dot.exe especifico para a plataforma .Net.

Após o arquivo estar desprotegido, o mesmo foi aberto no Disassembler IDA Pro. Neste Disassembler foi verificado inicialmente as strings que compõem o código, porém não foi encontrado nenhuma palavra relevante, como um domínio, endereço de e-mail, ou endereço IP. Porem foi possível observar que existem várias strings que são comandos para obter informações do Sistema Operacional, como get_MachineName, get_UserName, ComputerInfo, get_OSFullName além de possuir nomes de Classes para programação de redes, como Socket, SocketFlags, NetworkStream, e para criptografia como MD5CryptoServiceProvider, entre outros como apagar logs no gerenciador de logs, deletar diretório e outros para diversos fins, como mostra a Figura 4.

Figura 4 – Analise do Hexadecimal no IDA Pro



Fonte: Acervo pessoal (2018)

Após fazer a busca por strings, foi retornado ao IDA Pro e efetuada a análise do Hexadecimal. Foi encontrado um nome de domínio, chamado “absolutosistema.no-ip.org”, onde ao executar o comando ping sobre este domínio, obteve-se justamente o endereço de IP que estava fazendo a conexão na porta 5252, verificado com o comando netstat.

Posteriormente executou-se o programa Netcat em modo listening, na porta 5252, para observar se seria apresentado algum dado em tela. A Figura 5 exibe o resultado.

Figura 5 – Netcat em Listening

Fonte: Acervo pessoal (2018).

Como pode ser observado, a maioria das strings está na codificação Base64, decodificado estas strings no site [https://www.base64decode.org/] é possível perceber que se trata de um Spyware, pois exatamente tudo o que é executado no host 67, é transmitido pela rede.

Detecção de botnet

Neste estudo de caso é apresentada a detecção de uma botnet através da análise do tráfego de DNS. Para demonstrar este estudo de caso, foram configurados um servidor DNS e um servidor de comando e controle (C&C) na rede interna da empresa. Para o servidor DNS foi utilizado o BIND versão 9, em um sistema Debian/Linux configurado como o servidor primário nas consultas da rede.

O domínio criado foi chamado de “botnetstolpe.net” fazendo-se com que o servidor DNS fosse autoritativo sobre este domínio. O ambiente no qual o método foi aplicado é de produção com tráfego de dados reais, composto por aproximadamente 60 dispositivos conectados á Internet, dentre eles estações de trabalho, notebooks, servidores e dispositivos moveis. A Figura 6 mostra parte dos arquivos de configuração.

Figura 6 – Descrição zona DNS

```
zone "botnetstolpe.net" {
        type master;
        file "/etc/bind/db.botnetstolpe";
        };

zone "1.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.botnetreversa";
        };
root@SRV-DNS:/etc/bind# cat db.botnetstolpe
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     SRV-DNS.botnetstolpe.net. root.botnetstolpe.net. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
botnetstolpe.net.       IN      NS      SRV-DNS.botnetstolpe.net.
botnetstolpe.net.       IN      A       192.168.1.210
SRV-DNS                 IN      A       192.168.1.210
SERVERBOT               IN      A       192.168.1.125
```

Fonte: Acervo pessoal (2018)

Para a configuração do servidor de comando e controle (C&C) utilizou-se o programa DarkDDoSer instalado em um sistema Windows 7. Neste programa é possível criar um cliente executável, onde a configuração é apenas o nome do servidor e a porta em que este cliente precisa conectar-se. Este executável torna a máquina infectada um bot, e é auto inicializável junto com o sistema operacional. Utilizando-se da mesma estratégia e ferramentas descritas na seção anterior para captura e analise do tráfego DNS, foram coletados 2 dias de tráfego.

Foi necessário relacionar o total de consultas realizadas com o total de respostas, procurando por diferentes endereços IPs consultando um único endereço IP, em um intervalo de tempo muito curto. Este fato pode ser observado em dois momentos no tráfego DNS do dia 11-11-16, onde alguns endereços IPs consultam o servidor DNS no mesmo segundo. No primeiro momento as 10:03:03 acontece a consulta de diferentes endereços procurando pelo servidor do domínio “botnetstolpe.net”. As Figuras 7 e 8 exibem o momento do ataque, com uma diferença de 24 segundos entre a consulta dos bots pelo domínio, e o ataque propriamente dito. Executou-se um ataque de DoS (Negação de Serviço) em um roteador na rede. No segundo momento as 11:35 acontece o segundo ataque, e o tráfego demonstra as consultas efetuadas pelos bots.

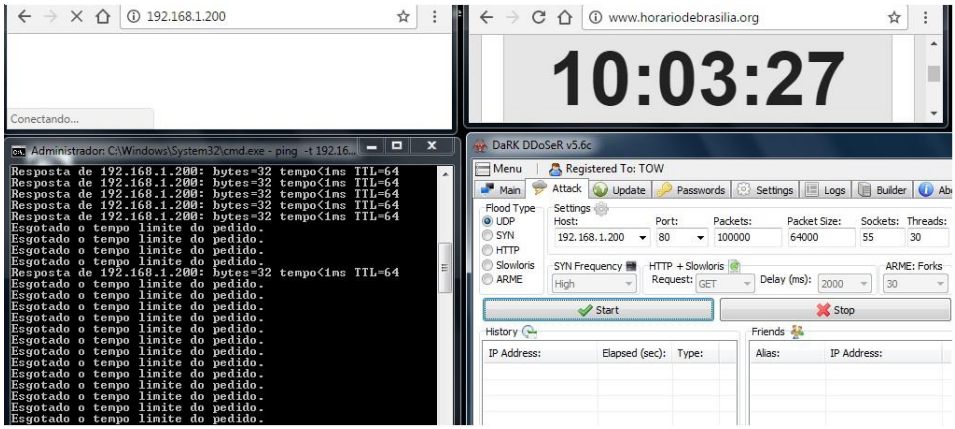
Figura 7 – Tráfego suspeito no servidor DNS

```
10:03:03  192.168.1.97   192.168.1.210  DNS     86 Standard query 0x648a A serverbot.botnetstolpe.net
10:03:03  192.168.1.210  192.168.1.97   DNS    150 Standard query response 0x648a A serverbot.botnetstolpe.net A 192.168.1.125
10:03:03  192.168.1.70   192.168.1.210  DNS     86 Standard query 0x16f8 A serverbot.botnetstolpe.net
10:03:03  192.168.1.210  192.168.1.70   DNS    150 Standard query response 0x16f8 A serverbot.botnetstolpe.net A 192.168.1.125
10:03:03  192.168.1.63   192.168.1.210  DNS     86 Standard query 0x98b4 A serverbot.botnetstolpe.net
10:03:03  192.168.1.210  192.168.1.63   DNS    150 Standard query response 0x98b4 A serverbot.botnetstolpe.net A 192.168.1.125
10:03:03  192.168.1.95   192.168.1.210  DNS     86 Standard query 0x81f2 A serverbot.botnetstolpe.net
10:03:03  192.168.1.210  192.168.1.95   DNS    150 Standard query response 0x81f2 A serverbot.botnetstolpe.net A 192.168.1.125
11:35:01  192.168.1.66   192.168.1.210  DNS     86 Standard query 0x644a A serverbot.botnetstolpe.net
11:35:01  192.168.1.210  192.168.1.66   DNS    150 Standard query response 0x644a A serverbot.botnetstolpe.net A 192.168.1.125
11:35:01  192.168.1.70   192.168.1.210  DNS     86 Standard query 0x7ac9 A serverbot.botnetstolpe.net
11:35:01  192.168.1.95   192.168.1.210  DNS     86 Standard query 0x4b45 A serverbot.botnetstolpe.net
11:35:01  192.168.1.210  192.168.1.70   DNS    150 Standard query response 0x7ac9 A serverbot.botnetstolpe.net A 192.168.1.125
11:35:01  192.168.1.210  192.168.1.95   DNS    150 Standard query response 0x4b45 A serverbot.botnetstolpe.net A 192.168.1.125
11:35:01  192.168.1.97   192.168.1.210  DNS     86 Standard query 0x055e A serverbot.botnetstolpe.net
11:35:01  192.168.1.210  192.168.1.97   DNS    150 Standard query response 0x055e A serverbot.botnetstolpe.net A 192.168.1.125
11:35:01  192.168.1.63   192.168.1.210  DNS     86 Standard query 0x1102 A serverbot.botnetstolpe.net
11:35:01  192.168.1.210  192.168.1.63   DNS    150 Standard query response 0x1102 A serverbot.botnetstolpe.net A 192.168.1.125
```

Fonte: Acervo pessoal (2018).

A identificação dos hosts relevantes seguiu a mesma métrica apresentada no estudo de caso I, efetuando-se o cálculo da quantidade de vezes que um determinado endereço IP é exibido em um dia e em um filtro. Ao todo se obteve 8 hosts que apresentaram alguma caraterística inerente aos filtros. E neste caso o fator que mais contribuiu para a relevância do host ser considerado suspeito, foi a sua inserção no grupo dos hosts acessando ao mesmo tempo um único IP.

Figura 8 – Ataque de negação de serviço (DoS) no roteador

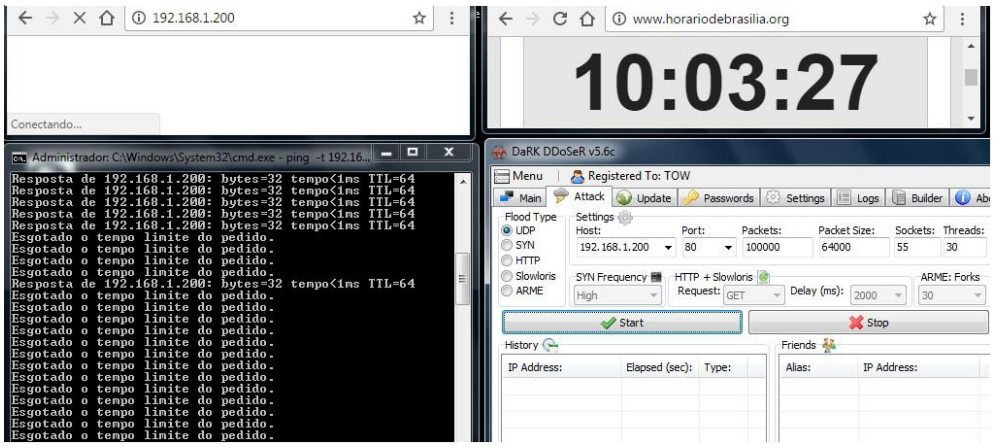


Fonte: Acervo pessoal (2018).

Ao abrir o executável no disassembler IDA PRO e no debugger OllyDBG, não foram encontradas nenhuma referência ao servidor, como nome do servidor, porta ou endereço IP, tanto na busca por strings quanto no hexadecimal. Apenas foram encontradas referências a classes de programação, chaves do registro do Windows, e System Calls do sistema operacional.

Entretanto ao fazer o dump de memória com o processo em execução, gerou-se um arquivo chamado botClient.DMP, e este foi submetido ao IDA PRO para análise. Ao verificar este arquivo foi possível constatar o endereço do servidor de comando e controle chamado “serverbot.botnetstolpe.net”, ao qual o bot conectava-se, como mostra a Figura 9.

Figura 9 – Domínio encontrado no arquivo de despejo



Fonte: Acervo pessoal (2018)

Então, neste caso a detecção do domínio que liga o bot ao servidor de comando e controle, só foi possível através do arquivo de despejo de memória, executado sobre o processo em execução. Isso demostra que, mesmo sendo parte opcional do método proposto, são obtidos resultados satisfatórios.

CONSIDERAÇÕES FINAIS

O presente trabalho teve por objetivo descrever e aplicar um método híbrido composto pela análise do tráfego DNS em conjunto com a engenharia reversa de código malicioso, para detecção de botnets.

Após a aplicação do método, o mesmo mostrou-se satisfatório, pois além do objetivo principal que é a detecção de botnets, ele também consegue distinguir anomalias no tráfego de DNS, quando estas são causadas por algum tipo de malware, com mostrado no primeiro estudo de caso.

A contribuição acadêmica deste trabalho é importante por demonstrar que em algum momento entre a comunicação de programas maliciosos, com um servidor ou controlador de malwares, é possível detectar comportamentos estranhos ou anômalos para mitigar qualquer espécie de ameaça que utiliza o protocolo DNS contra uma rede de computadores.

BOTNETS DISCOVERY BY DNS TRAFFIC ANALYSIS

ABSTRACT

Some botnets use dynamic addressing techniques such as ip-flux and domain-flux to communicate between bots and the command and control server, making them more robust for operation and therefore more difficult to detect. This article details a method for performing botnet detection by analyzing DNS traffic along with reverse engineering malicious code. The method is a set of procedures that must be followed to obtain hosts characterized as bots. Two case studies that have been successful with the application of this method are presented.

KEYWORDS: Botnets, DNS, Discovery.

REFERÊNCIAS

CERON J., GRANVILLE L.,TAROUCO L. Uma Arquitetura Baseada em Assinaturas para Mitigação de Botnets. 2010.

CERON, JOÃO MARCELO ARQUITETURA Distribuida e Automatizada para mitigação de botnets baseada em analise dinamica de malwares. 2010.

CUNHA NETO, RAIMUNHO PEREIRA DA. Sistema de Detecção de intrusos em ataques oriundos de botnets utilizando metodo de detecção híbrido.- São Luis PPGEE. 2010

HOSSAIN, SORAYA S. Detecção de aplicações envio de Spam através da mineração do tráfego DNS. 2010.

!KAIO RAFAEL. Identificação e Caracterização de Comportamentos Suspeitos Através da Análise do Tráfego DNS. SBSeg 2014.

LAUFER RAFAEL PINAUD. Rastreamento de Pacotes IP contra Ataques de Negação de Serviço [Rio de Janeiro] 2005 XIII, 93 p. 29,7 cm (COPPE/UFRJ, M.Sc., Engenharia Elétrica, 2005).

Recebido: **14** abril. 2018.
Aprovado: 05 set 2019.
DOI: 103895/recit. v10n25.8032
Como citar: TAVARES, T. N. Descoberta de botnets por meio de análise de tráfego DNS. R. Eletr. Cient. Inov. Tecnol, Medianeira, v. 10, n. 25, p 18 – 29, jul/set, 2019 Disponível em: <https://periodicos.utfpr.edu.br/recit>. Acesso em: XXX.
Correspondência:
Thales Nicolai Tavares.
Av. Roraima, 1000 - Camobi, Santa Maria - RS, 97105-900Universidade Federal de Santa Maria – UFSM – Santa Maria – Brasil.