ESCOLA TÉCNICA ESTADUAL PROFESSOR MASSUYUKI KAWANO
TÉCNICO EM REDES DE COMPUTADORES

BOTNET (REDE ZUMBI)

GUILHERME MASSARI MARQUEZIN
KELI DE FÁTIMA DO NASCIMENTO DA SILVA
WENDER FLÁVIO PINTO

TUPÃ – SP
NOV/2021

ESCOLA TÉCNICA ESTADUAL PROFESSOR MASSUYUKI KAWANO
TÉCNICO EM REDES DE COMPUTADORES

BOTNET (REDE ZUMBI)

GUILHERME MASSARI MARQUEZIN
KELI DE FÁTIMA DO NASCIMENTO DA SILVA
WENDER FLÁVIO PINTO

Trabalho de Conclusão de Curso, apresentado a Escola Técnica Estadual Prof. Massuyuki Kawano de Tupã, Curso Técnico em Redes de Computadores, como parte dos requisitos para a sua conclusão.

Orientador:
Paula Regina Garcia Zanini

Tupã – SP
NOV/2021

GUILHERME MASSARI MARQUEZIN
KELI DE FÁTIMA DO NASCIMENTO DA SILVA
WENDER FLÁVIO PINTO

BOTNET (REDE ZUMBI)

Trabalho de Conclusão de Curso, apresentado a Escola Técnica Estadual Prof. Massuyuki Kawano de Tupã, Curso Técnico em Redes de Computadores, como parte dos requisitos para a sua conclusão.

Tupã, 29 de novembro 2021.

BANCA EXAMINADORA

_____	_____
Prof.ª Paula Regina Garcia Zanini Orientador	Prof. Anderson T. Berengue Coordenador de Área
_____	_____
Prof. Joel Coutinho De Souza Prof.º Convidado	Ewerton José da Silva Prof.º Convidado

Dedicamos este trabalho de conclusão de curso aos discentes envolvidos em sua confecção pelo engajamento, esforço e tempo dedicado. Aos nossos familiares pelo apoio e incentivo ao estudo e por fim o corpo docente da ETEC Professor Massuyuki Kawano, pelo suporte pedagógico e crescimento profissional dos que elaboraram este trabalho.

AGRADECIMENTOS

Agradecemos a Deus, razão da nossa existência, pela oportunidade e pelo privilégio de vivenciarmos tamanha experiência, e, conseguirmos perceber ao longo do curso a relevância de temas que não faziam parte, em profundidade, do nosso cotidiano.

Nossa gratidão à nossa orientadora Prof.ª Paula Regina Garcia Zanini, pelo incentivo e presteza no auxílio às atividades e discussões sobre o andamento deste Trabalho de Conclusão de Curso.

Nosso agradecimento a todos os professores pelo carinho, dedicação e competência demonstrados ao longo do curso.

Agradecemos aos nossos familiares por acreditar e incentivar nossa constante busca pelo conhecimento.

.

[...] O modo como você reúne, administra e usa a informação determina se vencerá ou perderá [...]”

Bill Gates

RESUMO

As redes de computadores podem ser definidas como um conjunto de equipamentos, que além de compartilhar dos mesmos recursos, também podem trocar informações entre si. Os recursos são por exemplo: a conexão com a internet, divididas entre todas as máquinas conectadas a uma determinada rede. Ela possibilita o compartilhamento de dados equipamentos e a comunicação entre usuários. Atualmente a grande maioria dos usuários dessa rede de computadores mundial, não tem conhecimento dos perigos que a internet pode oferecer. Acessam links desconhecidos, e-mails ou ofertas inacreditáveis, e é nesse momento que o usuário pode ser infectado por ameaças cibernéticas como a botnet, entre tantos outros tipos de malware. A botnet é um tipo de malware que possibilita ao hacker ou cracker obter controle completo através do uso remoto de um computador infectado, transforma o computador infectado em um zumbi, para realizar tarefas automatizadas na Internet. Essa rede de agentes de software ou bots são executados de maneira autônoma sem conhecimento do usuário, e podem ser usados para gerar novas infecções, infectando novos PCs com os quais interage através da rede local ou por meio de dos endereços de contatos armazenados no PC. Uma botnet pode conter centenas ou milhares de computadores infectados. Quanto mais dispositivos conectados à botnet, mais poderoso o ataque será. Por isso é importante que o usuário saiba detectar e se proteger de possíveis infecções em seu computador ou rede local.

Palavras Chaves: Redes de Computadores, Malware, Botnet

LISTA DE ABREVIATURAS E SIGLAS

BOT	Robô
PC	*Personal Computer* (Computador Pessoal)
IRC	*Internet Relay Chat* (Protocolo para conversa em tempo real)
DSL	*Digital Subscriber Line* (Linha Digital do Subscritor)
DDoS	*Distributed Denial of Service* (Serviço de Negação Distribuído)
LAN	*Local Area Network* (Rede Local)
MAN	*Metropolitan Area Network* (Rede Metropolitana)
WLAN	*Wide Local Area Network* (Rede Local sem Fio)
WMAN	*Wide Metropolitan Area Network* (Rede Metropolitana sem Fio)
SAN	*Storage Area Network* (Rede de Armazenamento)
PAN	*Personal Area Network* (Rede Pessoal)
NAC	*Network Access Control* (Controle de Acesso a Rede)
MIT	*Massachussetts Institute of Tecnology* (Instituto de Tecnologia de Massachussetts)
ARPA	*Advanced Research Projects Agency* (Agência de Projetos de Pesquisa Avançada)
IMP	*Interface Message Processors* (Processadores de Mensagens de Interface)
NCP	*Network Control Protocol* (Protocolo de Controle de Rede)
DARPA	*Defense Advanced Research Projects Agency* (Agência de Projetos de Pesquisa Avançada de Defesa)
TCP	*Transmission Control Protocol* (Protocolo de Controle de Transmissão)
IP	*Internet Protocol* (Protocolo de Internet)
UDP	*User Datagram Protocol* (Protocolo de Datagrama do Usuário)
XNS	*Xerox Network Systems*
SNA	*Systems Network Architecture*
CSNET	*Computer Science Net* (Rede de Ciência de Computadores)
NSFNET	*National Science Foundation Network* (Rede da Fundação Nacional de Ciências)
DNS	*Domain Name System* (Sistema de Nome de Domínio)

EUA	Estados Unidos da América
CERN	Organização Europeia para Pesquisa Nuclear
HTML	*HyperText Markup Language* (Linguagem de Marcação de HiperTexto)
HTTP	*HyperText Transfer Protocol* (Protocolo de Transferência de Hipertexto)
RNP	Rede Nacional de Pesquisas

SUMÁRIO

INTRODUÇÃO

Atualmente a grande maioria dos usuários desconhecem ou não se preocupam com os perigos que a internet pode oferecer. Muitas vezes por simples curiosidade, acabam acessando links desconhecidos em e-mails com ofertas imperdíveis, processos judiciais recebidos via e-mail, premiações por participação em concursos no qual desconhecem, e é nesse momento que o usuário pode ser infectado por ameaças cibernéticas como o Bot.

As botnets são ações efetuadas por meio de códigos maliciosos, em geral *malwares,* que permitem que o invasor controle remotamente uma rede de máquinas infectadas, podendo dar comandos e realizar tarefas sem que o usuário perceba. Além de se propagar para outros computadores através do envio de e-mails maliciosos, o *malware* também pode coletar informações pessoais do usuário, como dados bancários, documentos pessoais, dados de cartão de créditos e enviá-los ao invasor.

De acordo com a Forbes (2018), o Brasil lista entre os 10 principais países fontes de spam e ocupa a 5ª posição, dos 10 maiores países por porcentagem de usuários infectados.

A partir dessa problemática, a justificativa de tratar sobre o tema botnet, que apesar de se tratar de um *malware* antigo, nascido no final do ano de 2009, teve pouco sucesso na época. Neste novo contexto, em que estamos vivendo sob a pandemia do COVID – 19, com o êxodo das empresas para o home office (trabalho remoto), esse *ranswer* veio a reaparecer ainda mais complexo e se disseminando cada vez mais na rede mundial de computadores. Isso se deve aumento crescente de dispositivos conectados a redes domésticas, que em sua grande maioria não possuem o mínimo de segurança adequada, o que se tornou um prato cheio para aqueles que operam e tiram o proveito desse *malware* (botnet).

O objetivo principal deste trabalho é alertar aos usuários sobre os riscos contidos ao acessar uma rede desconhecida, fazer downloads de arquivos mal-intencionados, conscientizando e precavendo os possíveis vazamentos de informações sigilosas e uso do computador pessoal para práticas ilegais.

Como objetivos específicos estão ajudar os usuários conectados a redes de computadores a identificar se seus dispositivos fazem parte de uma rede infectada por botnets; orientar os usuários verificar e reconhecer se seus dispositivos estão

infectados a partir de alguns sintomas; propor soluções para que os usuários não sejam infectados com a botnet e relacionar o que é possível fazer se seus dispositivos estiverem infectados e ligado a uma rede zumbi.

A pesquisa é de natureza aplicada, pois gera conhecimento para aplicações práticas, orientados a soluções de problemas específicos; como forma de abordagem qualitativa avaliando a existência de uma analogia dinâmica entre o mundo real e o problema (*malware)*; com objetivos exploratórios e explicativos, utilizando-se de estudos de casos através de pesquisas bibliográficas, visando identificar fatores que motivam ou contribuem para o acontecimento dos episódios.

1. REDES DE COMPUTADORES

1.1 HISTÓRIA DAS REDES DE COMPUTADORES

A história das redes de computadores iniciou por volta da década de 60, onde a rede telefônica, era a rede de comunicação que dominava o mundo, a voz era transmitida por comutação de circuitos a uma taxa constante entre a origem e o destino. O desenvolvimento de minis e microcomputadores de bom desempenho, com requisitos menos rígidos de temperatura e umidade, permitiu a instalação de considerável poder computacional em várias localizações, ao invés de em uma determinada área, mas faltava um meio para unir estes computadores. Apesar do alto custo dos computadores nesta década, pode-se dizer que com o surgimento da multiprogramação, começou a ocorrer à necessidade de interligar computadores de modo que se pudessem compartilhar informações entre diferentes usuários e diferentes regiões, esta necessidade surgiu naturalmente pela espera de acontecimentos futuros. O tráfego gerado por estes usuários, ocorreria em uma sequência de atividades, onde ao acionar um comando a um computador distante (remoto), este permaneceria por alguns instantes inativo, explorando e aguardando uma resposta.

Em busca de como transformar a comutação de circuitos em uma comutação de pacotes, três grupos de pesquisa separadamente iniciaram seus estudos. Sendo o primeiro em 1961, onde Leonard Kleinrock nos laboratórios MIT usou a teoria das filas, a comutação de pacotes baseada no tráfego em rajadas. Já

por volta de 1964 Paul Baran do Rand Institute começou a estudar o uso da comutação de pacotes para a segurança da transmissão de voz para redes militares, e na Inglaterra Donald Davies e Roger Scantlebury desenvolviam ideias sobre a comutação de pacotes no National Physical Laboratory. Estes trabalhos, junto com Lawrence Roberts também no MIT lideravam o projeto de ciência de computadores na ARPA (EUA - Agência de Projetos de Pesquisa Avançada).

Roberts por volta de 1967 publicou a ARPAnet (a precursora da grande rede mundial- a Internet), sendo a rede de computadores por comutação de pacotes. Os primeiros comutadores de pacotes ficaram conhecidos como IMPs (interface menssage processors), processadores de mensagens de interface, sendo fabricados pela empresa BBN.

Em 1969 o primeiro IMP foi instalado na Universidade da Califórnia com três IMPs adicionais, depois no Stanford Research Institute, em Santa Bárbara e na Universidade de Utah, todos supervisionados por Leonard Kleinrock (figura 1), sendo a primeira utilização um login remoto entre a Universidade da Califórnia com o Research Institute que acabou derrubando o sistema então com 4 nós. Por volta de 1972 a ARPAnet já tinha 15 nós e foi publicamente apresentada por Robert Kahn na Conferência Internacional de Computadores. O primeiro protocolo de controle de rede deste sistema foi o NCP (network-control protocol), sendo elaborado também o primeiro programa de e-mail por Ray Tomlinson na BBN. Devido a ARPAnet ser única na época era uma rede fechada e para se comunicar com suas máquinas era preciso estar ligado a um de seus IMPs.

Na foto abaixo o primeiro IMP com Leonard Kleinrock.

Por volta da década 70 começaram a surgir outras redes de comutação de pacotes como:

- **ALOHAnet**: rede de micro-ondas via rádio que interligava as ilhas do Havaí;
- **TELENET**: comutação de pacotes comerciais da BBN baseada na tecnologia da ARPAnet;
- **TAYMNET e TRANSPAC**: rede de comutação de pacotes franceses.

O número de pequenas redes crescia cada vês mais sendo apresentado por Robert Metcalfe os princípios de uma rede local, uma **ETHERNET** Que mais tarde originariam LANs de curta distância.

O trabalho pioneiro da interconexão de redes foi supervisionado pela **DARPA** (Agência de Projetos de Pesquisa Avançada de Defesa), por Vinton Cerf e Robert Kahn, criando uma arquitetura, uma rede de redes baseados na criação de um protocolo, o **TCP** (transmission control protocol) responsável pela entrega sequencial e confiável de pacotes. Com o tempo o serviço deste foi modificado devido à procura de um controle maior do fluxo de informações, sendo então dividido o protocolo **TCP**, ficando responsável somente pela organização na chegada dos pacotes, retirando a função do envio de pacotes, destinando essa ao protocolo **IP** e

criando outro protocolo o **UDP** que ficou responsável pelo controle do fluxo de voz nos pacotes.

Além das pesquisas realizadas pela DARPA, no Havaí Norman Abramson com a rede Aloha desenvolveu um protocolo, o **ALOHA** que permitiu o compartilhamento de informações com um único meio de comunicação através de ondas eletromagnéticas, com frequência de rádio (**broadcast**) em diferentes localizações geográficas. Este protocolo de múltiplo acesso foi aprimorado por Metcalfe e Boggs desenvolvendo a **Ethernet** para redes compartilhadas com fios, cujo esquema está na figura 1, que surgiu pela necessidade de conectar diversos PCs, impressoras, discos etc. Este protocolo foi de muita importância, pois, cada rede local (**LAN**) é uma rede diferente. Já com um grande número destas pequenas redes, aumentava ainda mais a necessidade de uma rede maior interligando-as.

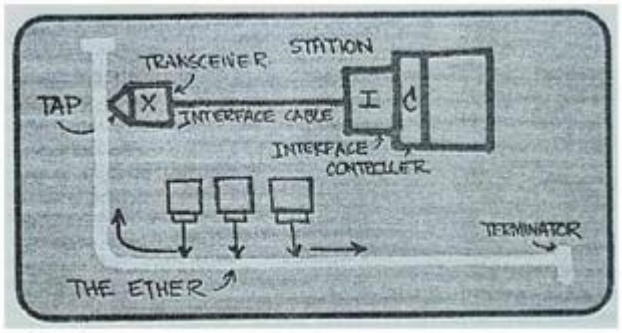


Fig. 1| Esquema da Ethernet desenvolvido por Metcalfe.

Outras empresas também desenvolveram suas próprias arquiteturas de redes, a Digital Corporation que lançou sua primeira versão de rede em 1975, a DECnet interligando apenas dois computadores PDP-11, que continuou evoluindo com o conjunto de protocolos OSI (interconexão de sistemas abertos). A Xerox com arquitetura XNS e a IBM com arquitetura SNA, também se destacam os pesquisadores Fraser e Turner com arquitetura TM, cujos reconheciam os pacotes como células e tinham tamanhos fixos.

No final da década de 80 aproximadamente 200 máquinas estavam conectadas a ARPAnet não só devido a pesquisas, mas também por ser utilizada para comunicação militar na Guerra Fria onde toda a comunicação passava por um computador central que se encontrava no Pentágono, ao passar esta época de guerra a ARPAnet não tinha mais importância para os militares sendo passada então para maioria das universidades e outros pesquisadores que foram estendendo a comunicação por outros países chegando à década de 80 com cem mil máquinas

interligadas formando uma grande rede mundial que passou a ser conhecida como Internet.

A transferência de arquivos e o processamento de e-mails entre as universidades dos EUA eram feitas pela BITnet (rede de bits), e a comunicação com outras universidades não interligadas pela ARPAnet eram feitas pela CSNET. No dia primeiro de janeiro de 1983 o protocolo TCP/IP tornou-se oficial, sendo obrigatório estar em todas as máquinas. Em 1986 surgiu o NSFNET o backbone primário que fornecia acesso a outros centros de computação. Também nesta época foi desenvolvido o DNS (Domain Name System), usado para conversão dos endereços em forma de letras e palavras, pois são de mais fácil memorização para nós, na forma de endereço IP de 32 bits, a linguagem dos computadores.

No outro lado do mundo o governo francês desenvolvia o projeto Minitel, uma rede pública de comutação de pacotes baseada num conjunto de protocolos chamado X.25 que usava circuitos virtuais, terminais baratos e modems embutidos, porém de baixa velocidade, disponibilizava sites de listas telefônicas e outros, havia também sites particulares onde eram pagas taxas pelos usuários conforme o tempo de uso. Em 1990 a Minitel já oferecia 20 mil serviços diferentes, e já era usada por mais de 20% da população Francesa, gerando mais de 1 bilhão de dólares por ano, e 10 mil novos empregos.

Um fato interessante é que a grande rede de computadores na França já estava presente nas empresas, no comércio, nas residências 10 anos antes dos norte-americanos ouvirem falar em uma rede de computadores e menos ainda em uma desenvolvida Internet.

No final da década de 70 aproximadamente 200 máquinas estavam conectadas a ARPAnet não só devido a pesquisas, mas também por ser utilizada para comunicação militar na Guerra Fria onde toda a comunicação passava por um computador central que se encontrava no Pentágono, ao passar esta época de guerra a ARPAnet não tinha mais importância para os militares sendo passada então para maioria das universidades e outros pesquisadores que foram estendendo a comunicação por outros países chegando à década de 80 com cem mil máquinas interligadas formando uma grande rede mundial que passou a ser conhecida como Internet.

A transferência de arquivos e o processamento de e-mails entre as universidades dos EUA eram feitas pela BITnet (rede de bits), e a comunicação com

outras universidades não interligadas pela ARPAnet eram feitas pela CSNET. No dia primeiro de janeiro de 1983 o protocolo TCP/IP tornou-se oficial, sendo obrigatório estar em todas as máquinas. Em 1986 surgiu o NSFNET o backbone primário que fornecia acesso a outros centros de computação. Também nesta época foi desenvolvido o DNS (Domain Name System), usado para conversão dos endereços em forma de letras e palavras, pois são de mais fácil memorização para nós, na forma de endereço IP de 32 bits, a linguagem dos computadores.

No outro lado do mundo o governo francês desenvolvia o projeto Minitel, uma rede pública de comutação de pacotes baseada num conjunto de protocolos chamado X.25 que usava circuitos virtuais, terminais baratos e modems embutidos, porém de baixa velocidade, disponibilizava sites de listas telefônicas e outros, havia também sites particulares onde eram pagas taxas pelos usuários conforme o tempo de uso. Em 1990 a Minitel já oferecia 20 mil serviços diferentes, e já era usada por mais de 20% da população Francesa, gerando mais de 1 bilhão de dólares por ano, e 10 mil novos empregos.

Um fato interessante é que a grande rede de computadores na França já estava presente nas empresas, no comércio, nas residências 10 anos antes dos norte-americanos ouvirem falar em uma rede de computadores e menos ainda em uma desenvolvida Internet.

Na década de 1990 a ARPAnet deixou de existir, a Milnet e a Rede de Dados de Defesa passaram a controlar maior parte do tráfego do Departamento de Defesa dos EUA e a NSFNET passou a ser o backbone de conexão entre os Estados Unidos e todas as redes do exterior, mas perdeu seu valor comercial em 1995, pois essa tarefa passou a ser encargo dos provedores de Internet.

O destaque da década de 90 foi o funcionamento da World Wide Web, nos lares e empresas de milhões de pessoas espalhadas por todo mundo, para fins comerciais, bancários, empresariais, educacionais e para própria diversão. A Web foi inventada no CERN (Centro Europeu para Física Nuclear) por Tim Berners Lee no período de 1989 a 1991, baseados em trabalhos realizados por Bush e Ted Nelson respectivamente nas décadas de 40 e 60. Berners Lee e seus companheiros desenvolveram versões iniciais de HTML, HTTP, um servidor web e um Browser.

O Brasil entrou na rede em 1990 criando a RNP (rede nacional de pesquisas). Em 1992 foi criada a Internet Society e já existiam 200 servidores web em operação, nesta época as pesquisas estavam mais voltadas para o desenvolvimento

de browsers com interface gráfica, por exemplo, Marx Andreesen com a versão beta do GUIMosaic em 1993 e James Baker com a Mosaic Communications em 1994 que mais tarde transformou-se na Netscape Communications Corporation. Também nesta época a Embratel disponibilizou o acesso à rede de empresas e usuários particulares.

Em 1995 os estudantes usavam diariamente os browsers Mosaic e Netscape para navegar, e pequenas e grandes empresas começaram a utilizá-los para transações comerciais, já existindo 10 milhões de servidores.

Em 1996 a Microsoft entrou com tudo na web com o browser Internet Explorer. Como o desenvolvimento avançava a cada dia, iniciaram pesquisas por roteadores e roteamento de alta velocidade para redes locais. e recursos como o comércio eletrônico e textos, imagens, multimídia e outros.

Para finalizar sobre o histórico das redes de computadores, temos 1996 em diante, com a enorme evolução do serviço em redes tanto em empresas como em lares surgiram além das redes Ethernet que são redes locais, redes Intranet que são redes locais ligadas a grande rede mundial, muito utilizada pelas empresas hoje para diversos fins, como comunicação com filiais, comunicação entre setores através de um sistema em rede etc.

A grande rede formada por redes menores é hoje o componente mais importante na área da comunicação a popular e grande rede global de computadores a Internet, ainda não parou de crescer e com certeza não parará, pois o número de usuários tanto para fins empresariais como pessoais aumenta a cada dia, pois, hoje o custo para aquisição, ou acesso a uma rede é menor e tende a ficar cada vez mais barato, e ainda as maiores dificuldades seriam condições técnicas.

Não podendo esquecer que a grande rede ainda continua com os 3 protocolos TCP, IP e UDP criados no fim da década de 70, é claro que aperfeiçoados. As estatísticas apontam que hoje há no mundo em torno de mais de 900 milhões de usuários devido à grande utilidade no gerenciamento empresarial, nas políticas, nas residências, escolas, projetos de inclusão digital e enfim na sociedade em geral e que o acesso hoje além do computador ocorre pelo celular, PDAs e outros.

A rede sempre irá mudar, devido a demandas do tempo e do mercado, pois o tempo passa e os recursos devem passar também, é claro que os recursos úteis sempre irão ficar. Se formos analisar blogs, vídeos, chats, msn, pesquisas, sites de relacionamentos entre outros são a base da internet hoje.

1.2 TIPOS DE REDES DE COMPUTADORES

Atualmente existem diferentes tipos de redes, como redes cabeadas, redes sem fio, redes locais, redes externas, redes virtuais privativas entre outros tipos. Nomenclaturas como LAN, MAN, WLAN, WMAN, WWAN, SAN e PAN geralmente se fundem em apenas dois conceitos: redes locais e redes remotas.

Malhas de comunicação usadas dentro de uma empresa ou residência geralmente são classificadas apenas como LAN, enquanto redes de longa distância como as que provem acesso à internet são chamadas de WAN.

As redes podem ser públicas ou privadas. Enquanto qualquer pessoa pode acessar a internet pública, o acesso às redes privativas exige que o usuário tenha informações de acesso, como credenciais ou certificados para poder se conectar à rede.

Dentro de corporações, os sistemas de controle de acesso à rede (NAC) normalmente usam políticas de segurança para controlar o acesso à rede da empresa. Isso quer dizer que os dispositivos devem ter permissão para se conectar, atendendo os requisitos de autenticação e segurança estipulados pela empresa. Tais controles são fornecidos e administrados por políticas de um sistema de controle central e a maioria pode se utilizar de um controlador de domínio para controlar os acessos dos usuários, garantindo que assim que eles tenham as permissões necessárias e não possam acessar determinados locais que podem expor os dados da empresa, ou trazer acessos externos que podem transformar a rede interna em uma botnet.

2. BOTNET

Para começarmos a entender sobre o que este trabalho irá abordar, iniciaremos este capítulo conceituando o tema “Botnet” e posteriormente suas causas efeitos.

A palavra botnet é composta pela junção das palavras em inglês "robot" (robô) e "network" (rede); é um tipo de malware que possibilita ao hacker ou cracker obter controle completo através de uso remoto de um computador afetado. Ou seja, transforma um computador em um “zumbi” para realizar tarefas de forma automatizada na Internet, sem o conhecimento do usuário. Uma botnet, por sua vez,

é uma rede de agentes de software ou bots que são executados de maneira autônoma. Os sistemas infectados passam a ser usados como cobertura para uma série de atividades ilegais, incluindo novas infecções, onde um computador pode infectar PCs com os quais interage através da rede local ou por meio dos endereços de contatos armazenados no PC. O bot pode se infiltrar tanto em servidores de IRC ou em um canal específico de uma rede pública IRC quanto em roteadores e modems DSL.

Sobretudo, as botnets podem ser usadas para enviar mensagens de spam, disseminar vírus, atacar computadores e servidores, roubar informações bancárias e sigilosas, além de cometer outros tipos de crimes e fraudes.

Geralmente, uma botnet pode conter centenas ou milhares de computadores infectados, que acobertam ataques em sites e servidores, derrubando-os ou facilitando invasões. Isso dificulta a identificação dos invasores. Se o ataque for rastreado, a busca levará a uma máquina de um usuário que pode nem saber que seu computador era um “bot”. Quanto mais dispositivos conectados à botnet, mais poderoso o ataque será. A questão é que quase qualquer dispositivo conectado à Internet pode ser usado nesse tipo de ataque, incluindo coisas que você nem acha que usam a Internet, como câmeras de segurança e impressoras WiFi.

Muitas botnets já foram encontradas e removidas da Internet. No ano passado, por exemplo, foi encontrada e desativada uma botnet chamada Rustock, que chegou a enviar comandos para mais de um milhão de computadores zumbis.

Há muitas botnets em ação espalhadas pelo mundo. Algumas são pequenas com poucos "zumbis", já outras são enormes e sofisticadas. Atualmente, inclusive, existe uma que já infectou mais de 4,5 milhões de computadores em poucos meses e ainda está sob investigação.

A forma mais conhecida de usar uma botnet é organizar um ataque de negação de serviço (DDoS na sigla em inglês). Uma botnet simplesmente sobrecarrega um servidor com solicitações supérfluas o que ocasiona a falha ao processá-las tornando-se indisponível para usuários regulares.

Grandes botnets são capazes de fazer coisas realmente terríveis um exemplo foi o que aconteceu em outubro de 2016 onde criminosos usaram um ataque DDoS para interromper o trabalho de mais de 80 serviços na Internet dentre eles estão Twitter, Amazon, PayPal e Netflix. (Kaspersky, 2016).

2.1 TOPOLOGIAS DE COMUNICAÇÃO DA BOTNET

Para poder funcionar de maneira correta, os bots necessitam receber comandos de um servidor de *command-and-control* (C&C) que conversa com os agentes, através de sua rede.

A rede de bots pode trabalhar de diversas formas, dependendo da topologia (forma da estrutura) utilizada na sua elaboração.

Diversas topologias C&C podem ser empregadas com o intuito de disseminar os ataques. As principais topologias utilizadas nas redes botnets são: estrela, multi-servidor, hierárquica e randômica.

2.1.1 ESTRELA

A topologia estrela possui um único centralizado recurso de C&C para se comunicar com todos os demais bots. Cada bot recebe instruções diretamente do ponto central C&C

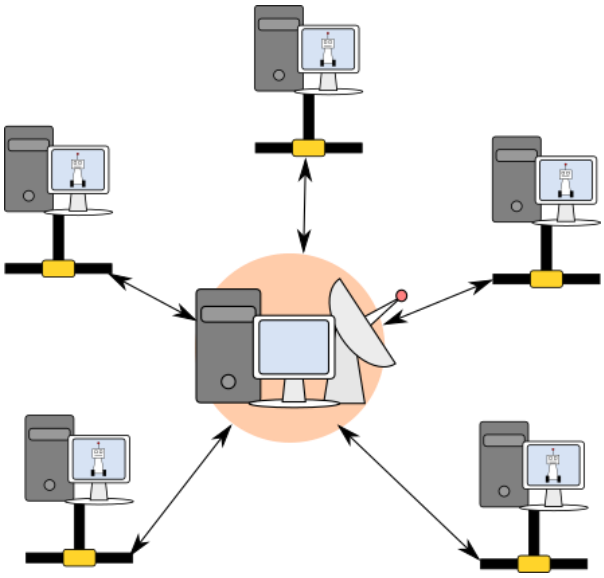


Figura 001 Topologia Estrela de botnets

Vantagens

- A comunicação direta entre o C&C e o bot agente possibilita a transferência de instruções (e dados roubados) rapidamente

Desvantagens

- Possui um ponto único de falha. Caso o C&C central for bloqueado ou desabilitado, toda a botnet é neutralizada

2.1.2 MULTI-SERVIDOR

Uma extensão lógica da topologia estrela, na qual vários servidores são utilizados para prover instruções de C&C para os bots agentes. Esses servidores comunicam entre si enquanto gerenciam a botnet. Essa topologia de C&C é mais refinada e por isso exige um maior esforço para ser implementada, porém por ter seu C&C descentralizado torna-se possível a manutenção da botnet mesmo caso um dos servidores de C&C forem derrubados.

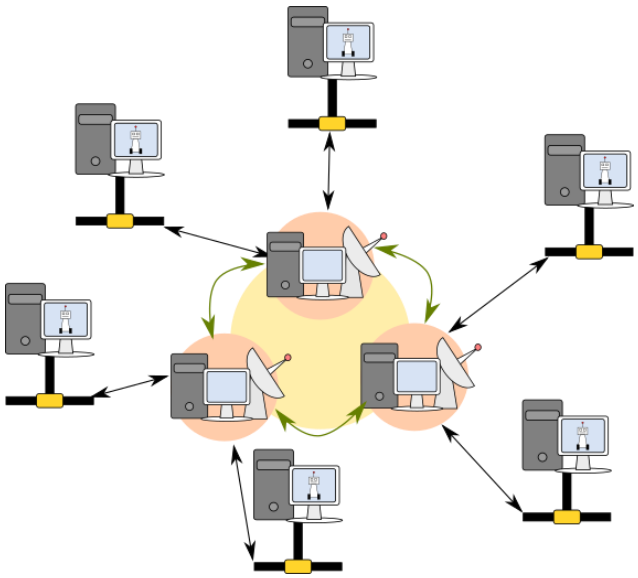


Figura 002.: Topologia Multi-Servidor de botnets

Vantagens

- Não possui um ponto único de falha. Caso um dos servidores C&C forem bloqueados ou desabilitados os remanescentes ainda são capazes de manter o controle de todos os demais bots agentes da botnet.
- Torna possível a realização de otimizações geográficas por meio da distribuição adequada dos servidores de C&C aumentando a velocidade da comunicação entre os elementos da botnet.

Desvantagens

- Exige mais esforço e conhecimento para a construção da infraestrutura de um C&C multi-servidor.

2.1.3 HIERÁRQUICA

Reflete a dinâmica dos métodos utilizados na contaminação e na posterior propagação dos bots. Os bots agentes tem a habilidade de transmitir novas instruções de C&C para bots agentes propagados anteriormente. A utilização desse método de propagação geralmente gera problemas com latência tornando difícil para o operador da botnet utilizar a botnet para atividades de tempo real.

Nessa topologia nenhum bot tem conhecimento da localização da botnet como um todo. Essa característica dificulta a determinação o tamanho de uma botnet. Essa estrutura também favorece a escalabilidade da botnet.

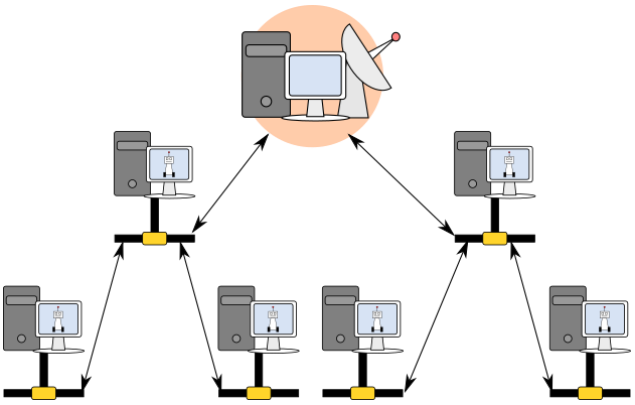


Figura 003.: Topologia Hierárquica de botnets

Vantagens

- A interceptação ou tomada de controle dos bots agentes não enumerará todos os membros da botnet nem o servidor de C&C.
- Maior escalabilidade da botnet.

Desvantagens

- Devido a necessidade de transmissão de comandos por meio de múltiplos canais de comunicação há latência.

2.1.4 RANDÔMICA

Não possui uma estrutura de C&C centralizada. Os comandos são introduzidos na botnet por meio de qualquer bot agente. Esses comandos geralmente fazem com que o bot agente propague automaticamente os comandos para todos os demais bots agentes presentes na botnet.

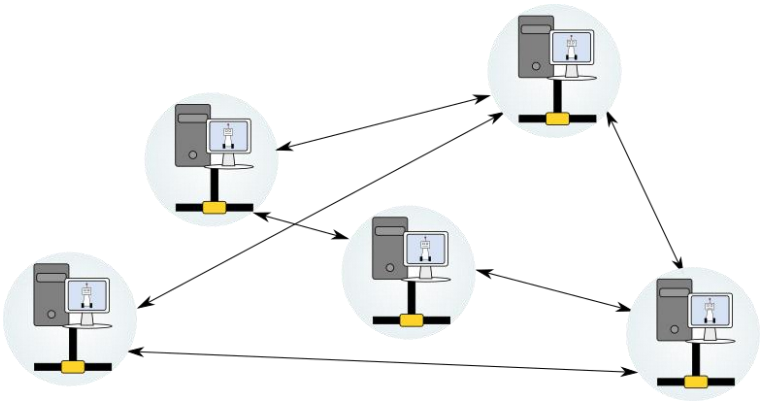


Figura 004.: Topologia Randômica de botnets

Vantagens

- A ausência de uma infraestrutura de C&C centralizada e o modelo de comunicação empregado torna muito difícil de derrubar a botnet.

Desvantagens

- A latência gerada pela natureza randômica dos links utilizados para a realização da comunicação de C&C.
- É possível a identificação de bots agentes por meio do monitoramento das comunicações de um dado bot agente.

2.2 COMO IDENTIFICAR UMA INFECÇÃO

Dimitry Betuzhey, diretor de pesquisa e análise da equipe da Kaspersky Lab. na América Latina, tem algumas dicas importantes para saber se o seu PC ou dispositivo móvel está infectado:

- A CPU do seu computador está trabalhando em alto consumo;
- Quando você usa a memória USB, o sistema diz que ela está infectada;

- São criados atalhos ou arquivos em drivers removíveis (pen drivers);
- Algumas pastas são ocultas do computador;
- Você não pode acessar as configurações do Windows, que estão bloqueadas;
- O tráfego de rede é alto;
- Você envia e-mails, mas não recebe;
- Não são feitos seus pagamentos de conta em celular;
- A bateria do dispositivo acaba mais rápido do que o normal e muitas vezes permanece aquecida;
- Entre os serviços do computador aparecem usuários ou administradores desconhecidos.

2.3 ATIVIDADES DESEMPENHADAS POR UM COMPUTADOR INFECTADO.

Caso seu dispositivo esteja mesmo infectado, ele pode realizar uma série de tarefas que você com certeza não permitiu

- Spam: seu computador pode enviar milhares de mensagens de spam sobre medicamentos ou outros produtos falsificados, enquanto você trabalha ou se diverte on-line;
- Fraude: você pode estar clicando em anúncios on-line, mesmo com o seu navegador fechado, para inflar de maneira fraudulenta os lucros de agências que anunciam com o sistema pay-per-click.
- Distributed Denial of Servisse (DDoS) seus dispositivos podem estar entre milhares de outros, bombardeando com pedidos de servidores de um site até fazê-lo cair e ficar offline.
- Ganhar dinheiro; literalmente, bitcoins, criptomoeda corrente da internet, são produzidos utilizando cálculos da sua CPU. É preciso muito tempo para gerar uma bitcoin e hackers usam computadores para acelerar esse processo. Bitcoins são aceitos como pagamento legítimo por bens legais e ilegais, e podem facilmente ser trocados em moeda real.
- Distribuir malware: os cibercriminosos tentam criar redes de computadores zumbis cada vez menos vulneráveis, à medida em que as

autoridades policiais se aprimoram em derrubar botnets. As botnets P2P (peer-to-peer) são um exemplo, onde cada computador infectado é usado para fazer downloads maliciosos em outros computadores e emitir comandos para escravizar PCs.

- Vender Warez. Programas comuns são capturados para que funcionem em número de série. Desta forma os criminosos podem vende-los a partir de lojas secretas e ilegais em seu PC
- Haccking: cibercriminosos assumem remotamente o controle de diferentes PCs para esconder os rastros e atacar seu alvo real. Se a atividade for rastreada será atribuída a você.
- Baixar ou assistir o conteúdo ilegal. Como alguns países desenvolvidos criaram punições para quem faz downloads piratas, usar outros computadores para baixar ou acessar conteúdos ilegais começou a fazer sentido. Como se isso não fosse preocupação suficiente, conselhos desse tipo são publicados em fóruns de hackers: Use RPD para navegar. Se você assistir conteúdos ilegais através de um RPD e acontecer algum problema, o verdadeiro dono é que será pego em seu lugar RPD significa Remote Desktop Protocol, um protocolo de rede usado para controlar remotamente outro computador, nesse caso ferramenta para crimes cibernéticos.
- Decifrar senhas: Hackers podem usar a capacidade de processamento de seu computador para tentar todas as senhas únicas, quando tentam obter informações valiosas de alguém.

2.4 COMO SE PREVINIR DE UMA POSSÍVEL ATAQUE/INFECÇÃO

- Reforce as defesas do seu computador
- Não seja dissuadido a baixar malware instale programas antivírus e antispyware de uma forma confiável. Os programas antimalwares verificam e monitoram o computador em busca de vírus e spywares conhecidos.
- Mantenha todos os softwares atualizados. Instale regularmente as atualizações de todos os seus softwares.

- Use senhas fortes e nunca as revele. Use um verificador de senha para determinar a força da senha;
- Nunca desinstale seu Firewall. O firewall coloca uma barreira protetora entre seu computador e a internet. Desativa-lo mesmo que em um minuto, aumenta o risco de seu PC ser infectado por um malware.
- Use unidades flash com cautela colocar uma unidade de flash. (pen drive) em um
- Computador infectado pode corromper

Invasores podem incluir o seu computador em uma botnet:

Inserindo malware em downloads que parecem ser imagens ou filmes, ou por meio de links clicados em e-mails ou mensagens instantânea (IM), ou em redes sociais, assustando você e induzindo-o a clicar em um botão falsos ou avisos de que seu computador tem vírus.

3. ESTATÍSTICAS

Para analisar de maneira prática e eficaz a disseminação de uma infecção de botnet, foi utilizado um ambiente simulado e controlado.

O ambiente consistiu na criação de uma página na internet, onde o tema principal do link de acesso era relacionado a área da saúde, tendo em vista a alta taxa de procura por esse tema devido a pandemia de COVID-19. Após a criação, foi divulgado via grupos de aplicativo de mensagens instantâneas (WhatsApp) o link da página (https://saudecerta.rf.gd/) com a frase *“Israel cria remédio natural 100% eficaz contra casos graves da Covid-19”*, com uma imagem de comprimidos de remédio, conforme imagem abaixo.

Imagem 001.: Link divulgado no WhatsApp

Fonte: O próprio autor

Após uma semana de divulgação, foram coletados os dados através da plataforma Google Analytics que estava vinculada a página para levantamento dos dados.

Com os acessos acontecendo diariamente, foi possível mapear diversas informações conforme imagens abaixo, como cidade de acesso, tipo de dispositivo, tempo médio de permanência na página, tipo de navegador utilizado, tipo de sistema operacional etc. Essas informações são importantes, pois em um caso real de infecção, seria possível explorar falhas de segurança e coletar dados em celulares, sistemas operacionais e navegadores de internet.

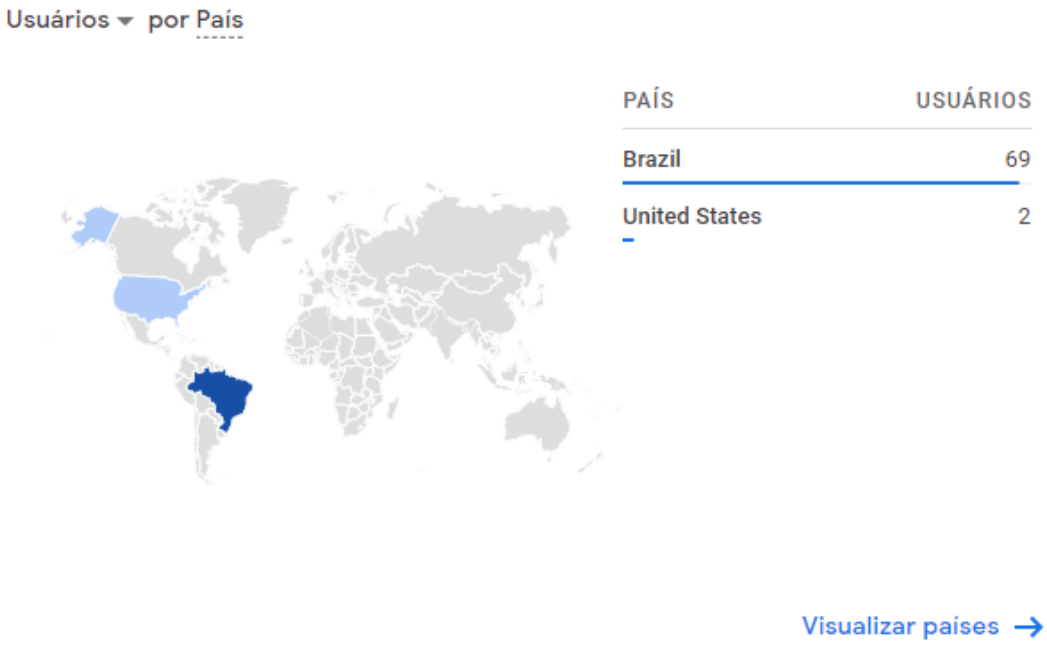


Imagem 003.: Mapa de acessos no Mundo

Fonte: Google Analytics

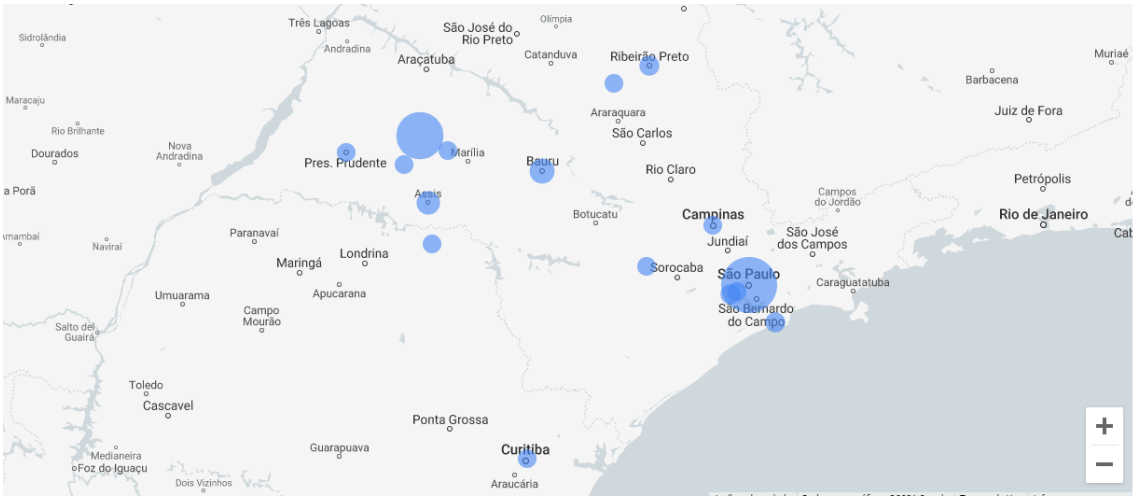
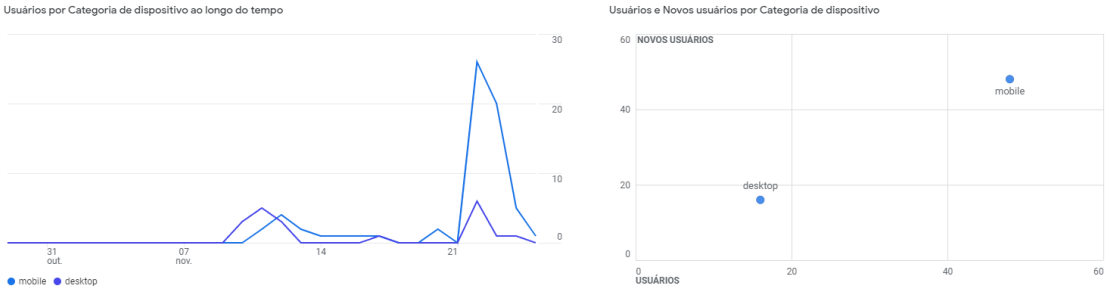


Imagem 003.: Mapa de acessos no Brasil
Fonte: Google Analytics

Cidade	↓Usuários	Novos usuários	Sessões engajadas	Taxa de engajamento	Sessões engajadas por usuário	Tempo médio de engajamento	Contagem de eventos Todos os eventos
Totais	64 100% do total	64 100% do total	61 100% do total	62,24% Média de 0%	0,95 Média de 0%	0 min 52 s Média de 0%	515 100% do total
1 Sao Paulo	23	20	18	58,06%	0,78	0 min 27 s	169
2 Tupa	18	14	15	62,5%	0,83	1 min 08 s	133
3 (not set)	14	12	10	62,5%	0,71	0 min 28 s	89
4 Bauru	4	4	4	66,67%	1,00	1 min 00 s	36
5 Assis	3	2	2	33,33%	0,67	1 min 15 s	20
6 Embu	2	2	2	100%	1,00	0 min 33 s	9
7 Santos	2	2	2	100%	1,00	2 min 25 s	8
8 Bandeirantes	1	1	1	100%	1,00	0 min 10 s	4
9 Campinas	1	1	1	100%	1,00	2 min 27 s	9
10 Curitiba	1	1	1	100%	1,00	0 min 56 s	5
11 Guariba	1	0	0	0%	0,00	0 min 00 s	2
12 Pompeia	1	1	0	0%	0,00	0 min 00 s	3
13 Presidente Prudente	1	1	1	100%	1,00	0 min 27 s	5
14 Quata	1	1	1	100%	1,00	0 min 16 s	8
15 Ribeirao Preto	1	1	2	100%	2,00	0 min 21 s	9
16 Taboao da Serra	1	1	1	100%	1,00	0 min 11 s	4
17 Tatui	1	0	0	0%	0,00	0 min 00 s	2

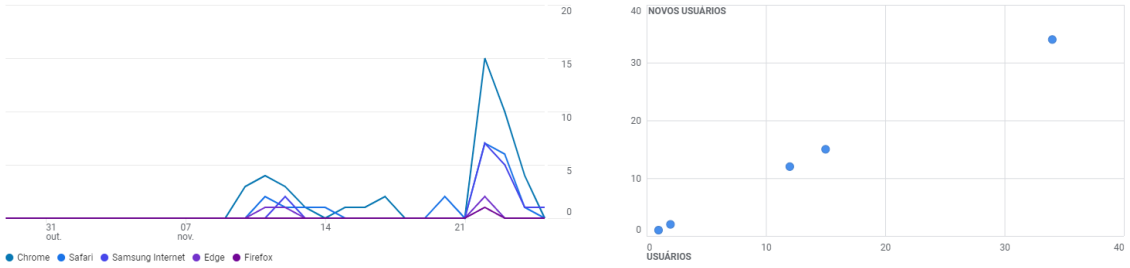
Imagem 004.: Tabela de acessos por cidades
Fonte: Google Analytics



Pesquisar... Linhas por página: 10 1–2 de 2

	Categoria de dispositivo	↓ Usuários	Novos usuários	Sessões engajadas	Taxa de engajamento	Sessões engajadas por usuário	Tempo médio de engajamento	Contagem de eventos Todos os eventos	Conversões Todos os eventos	Receita total
	Totais	**64** 100% do total	**64** 100% do total	**61** 100% do total	**62,24%** Média de 0%	**0,95** Média de 0%	**0 min 52 s** Média de 0%	**515** 100% do total	**0,00**	**R$ 0,00**
1	**mobile**	48	48	45	58,44%	0,94	0 min 55 s	339	0,00	R$ 0,00
2	**desktop**	16	16	16	76,19%	1,00	0 min 43 s	176	0,00	R$ 0,00

Imagem 005.: Tabela de acessos por tipo de dispositivo
Fonte: Google Analytics



Pesquisar... Linhas por página: 10 1–5 de 5

	Navegador	↓ Usuários	Novos usuários	Sessões engajadas	Taxa de engajamento	Sessões engajadas por usuário	Tempo médio de engajamento	Contagem de eventos Todos os eventos	Conversões Todos os eventos	Receita total
	Totais	**64** 100% do total	**64** 100% do total	**61** 100% do total	**62,24%** Média de 0%	**0,95** Média de 0%	**0 min 52 s** Média de 0%	**515** 100% do total	**0,00**	**R$ 0,00**
1	**Chrome**	34	34	30	62,5%	0,88	0 min 50 s	279	0,00	R$ 0,00
2	**Safari**	15	15	13	52%	0,87	0 min 48 s	99	0,00	R$ 0,00
3	**Samsung Internet**	12	12	13	68,42%	1,08	1 min 00 s	94	0,00	R$ 0,00
4	**Edge**	2	2	4	80%	2,00	1 min 21 s	34	0,00	R$ 0,00
5	**Firefox**	1	1	1	100%	1,00	0 min 35 s	9	0,00	R$ 0,00

Imagem 005.: Tabela de acessos por tipo de navegador
Fonte: Google Analytics

CONCLUSÃO

O objetivo desse trabalho foi abordar e conscientizar os usuários das redes de computadores sobre o risco de clicar em links suspeitos ou baixar arquivos de procedência desconhecida, podendo infectar o dispositivo com uma botnet. Esse objetivo foi alcançado de maneira eficaz, uma vez que após realizarmos a disseminação de um link falso via aplicativo de mensagem instantânea (WhatsApp), onde ao clicar na mensagem o usuário era redirecionado para uma página da internet, na qual havia informações pertinentes ao tema e com uma mensagem, informando que ele poderia ter sido infectado com uma botnet. Após a disseminação, muitos usuários reportaram que haviam clicado sem observar o que realmente estava no link, fazendo com que houvesse um pouco mais de conscientização em relação a essa situação. O objetivo de coletar informações e mapear a formação de uma possível rede através desses dispositivos foi atingido de forma parcial, pois conseguimos coletar informações relacionadas a mais de quinhentos acessos, contendo informações de localização, tipo de equipamento, sistema operacional, navegador etc. Quanto ao objetivo de melhorar o meio acadêmico Bano (2010, p. 1) diz que a maior parte da literatura no campo das botnets permanece de forma não estruturada, e, portanto, o presente trabalho contribui para o campo acadêmico na área das botnets, na forma pela qual apresenta o processo de desenvolvimento e de técnicas utilizadas por estas.

REFERÊNCIAS BIBLIOGRÁFICAS

AMAYA, Camilo Gutiérrez. WeLiveSecurity, 2017. Por trás de uma botnet: entenda como um botmaster pode atuar. Disponível em: <https://www.welivesecurity.com/br/2017/07/05/por-tras-de-uma-botnet/>. Acesso em 06 novembro 2021.

BANO, Shehar. A Study of Botnets: Systemization of Knowledge and Correlation-based Detection. 2010. 117 f. Dissertação (Mestrado em Computação e comunicação segura) -, Universidade Nacional de Ciências e Tecnologia (NUST), Islamabad, Paquistão.

BANTIM, Rudolfh. TechTudo, 2012. O que é botnet?. Disponível em: <https://www.techtudo.com.br/artigos/noticia/2012/03/o-que-e-botnet.html>. Acesso em 25 maio 2021.

BOTNET: O que é uma botnet e como se proteger dela. **Avast.** 23, janeiro 2021. Disponível em: <https://www.avast.com/pt-br/c-botnet>. Acesso em 28 abril 2021.

BRASIL entre os 10 países que mais espalham spam. **Forbes**. 26, abril 2019. Disponível em: <https://forbes.com.br/listas/2019/04/10-paises-que-mais-espalham-spam/>. Acesso em 31 maio 2021.

COELHO, Beatriz. Blog do Mettzer, 2021. Metodologia científica: aprenda como delimitar na sua pesquisa. Disponível em: <https://blog.mettzer.com/metodologia-cientifica/>. Acesso em 29 abril 2021.

DUARTE, Otto Carlos Muniz Bandeira. Negação de Serviço e Botnets. Disponível em: <https://www.gta.ufrj.br/grad/15_1/dos/index.html> Acesso em 31 agosto 2021.

FIGUEIREDO, Iria Luppi. Oficina da Net, 2014. História das redes de computadores. Disponível em: <https://www.oficinadanet.com.br/post/10123-historia-das-redes-de-computadores/>. Acesso em 08 novembro 2021.

HISTÓRIA das Redes. **Comdados**. Disponível em: <https://analicia-comdados.webnode.pt/historia-das-redes/>. Acesso em 08 novembro 2021.

MACEDO, Joyce. Canaltech, 2013. Botnets: descubra se o seu computador faz parte de uma e saiba como se proteger. Disponível em: <https://canaltech.com.br/seguranca/Botnets-descubra-se-o-seu-computador-faz-parte-de-uma-e-saiba-como-se-proteger/>. Acesso em 03 novembro 2021.

RODRIGUES, Renato. Kaspersky Daily, 2016. Seu computador virou um zumbi?. Disponível em: <https://www.kaspersky.com.br/blog/botnets-explained/6782/>. Acesso em 26 maio 2021.

GLOSSÁRIO

Broadcast: Limite da rede

Comutação: Processo de interligar dois ou mais pontos entre sim

Cracker: Indivíduo com conhecimentos em códigos de computadores, utilizando para atividades criminosas.

Firewall: Aplicativos e equipamentos que ficam entre um link de comunicação e um computador filtrando todo o fluxo de dados.

Hacker: Indivíduo que elabora e modifica softwares e hardwares de computadores, desenvolvendo funcionalidades ou adaptando novas.

Hardware: Se refere a parte física do computador.

Malware: Softwares ou códigos maliciosos prejudiciais ao hardware ou software.