MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA

INSTITUTO MILITAR DE ENGENHARIA

SEÇÃO DE ENGENHARIA DE COMPUTAÇÃO

ALAN FERREIRA BORBA

WILSON CAMARA MARRIEL

HONEYPOTS DE ALTA E BAIXA INTERATIVIDADE PARA COLETA DE MALWARES

RIO DE JANEIRO

2013

INSTITUTO MILITAR DE ENGENHARIA

ALAN FERREIRA BORBA

WILSON CAMARA MARRIEL

HONEYPOTS DE ALTA E BAIXA INTERATIVIDADE PARA COLETA DE MALWARES

Iniciação à Pesquisa apresentada ao Curso de Graduação em Engenharia de Computação do Instituto Militar de Engenharia.

Orientador: Prof. Claudio Gomes de Mello - D.C.

RIO DE JANEIRO

2013

INSTITUTO MILITAR DE ENGENHARIA

ALAN FERREIRA BORBA

WILSON CAMARA MARRIEL

HONEYPOTS DE ALTA E BAIXA INTERATIVIDADE PARA COLETA DE MALWARES

Relatório referente à VF de IP apresentado ao Curso de Engenharia de Computação do Instituto Militar de Engenharia (IME), como parte das exigências do IME.

Aprovado em 21 de junho de 2013 pela seguinte Banca Examinadora:

Orientador: Prof. Claudio Gomes de Mello - D.C., do IME

Sergio Dos Santos Cardoso Silva- D.C., do IME

Julio Cesar Duarte - D.C., do IME

RIO DE JANEIRO

2013

“ O homem é o lobo do próprio homem”.

THOMAS HOBBES

SUMÁRIO

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS

API	Application Programming Interface
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CTI	Centro de Tecnologia da Informação Renato Archer
DNS	Domain Name System
DoS	Denial-of-Service
FTP	File Transfer Protocol
HIDS	Host Intrusion Detection System
HTTP	HyperText Transfer Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
ISP	Internet Service Providers
NIDS	Network Intrusion Detection System
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol

RESUMO

A coleta de malwares é importante para entender como eles agem, como funcionam e para indentificá-los com o intuito de criar mecanismos de defesa cada vez mais eficazes. Prover segurança tornou-se essencial e esse fato causou um aumento nas pesquisas de malwares com o objetivo de criar ferramentas e procedimentos que possam ser usados no combate a estes artefatos maliciosos. Neste trabalho apresentamos alguns tipos de malwares e ferramentas de coleta. O trabalho se baseia na coleta de malware através de honeypots e nos permitirá identicar os recursos e entenderas funcionalidades e técnicas utilizadas por esse tipo de ferramenta.

Palavras-Chave: Honeypot, Malware, Vírus.

ABSTRACT

Collecting malware is important to understand how they act, how they work and identify them with the intention of creating defense mechanisms increasingly effective. Providing security has become essential and this fact has caused an increase in malware research with the goal of creating tools and procedures that can be used to combat these malicious artifacts. We present some types of malware and collection tools. The work is based on the collection of malware through honeypots and will indicate its resources and explain the features and techniques used for this type of tool.

1 INTRODUÇÃO

Hoje em dia uma das maiores ameaças aos usuários de computadores na Internet são os malwares (malicious software). Esses malwares afetam computadores pessoais, redes empresariais e servidores. São softwares que têm como objetivo se infiltrar e causar algum dano ou roubo de informações sem o conhecimento e consentimento do usuário. A falta de informação do usuário e o aumento do uso da Internet faz com que esses malwares se disseminem rapidamente, utilizando-se de falhas e vulnerabilidades nos sistemas para causar danos. Existem diversos malwares espalhados pela Internet e com isso os usuários estão constantemente expostos a essas ameaças, o que torna necessária a criação de ferramentas de proteção como antivírus, firewalls e outros programas capazes de identificar e remover esses malwares. A coleta de malwares, sua identificação e a criação de repositórios é importante para a criação de defesas contra essas ameaças, para que os mecanismos de defesa sejam cada vez mais eficazes e rápidos na identificação e remoção dos malwares.

1.1 OBJETIVO

Esse trabalho possui como objetivo o estudo de alguns tipos de malware e métodos de coleta de malware, focando nos honeypots como ferramenta de coleta.

O objetivo específico é implantar o Dionaea para participar da rede de coleta de malwares do Centro de Tecnologia da Informação (CTI) Renato Archer.

1.2 JUSTIFICATIVA

O honeypot foi escolhido devido à facilidade, rapidez e baixa necessidade de recursos para sua instalação.

1.3 METODOLOGIA

Primeiramente, foram estudados os tipos de malware para um maior entendimento das ameaças existentes. Então, passou-se ao entendimento dos principais tipos de coletas de malware. Com isto foi feito um estudo mais aprofundado nos serviços dos honeypots e em seguida começou-se a implantação do Dionaea e do Valhala Honeypot em um computador pessoal, depois disso foram realizados testes de invasão em nossos honeypots instalados.

1.4 ESTRUTURA

O trabalho está estruturado da seguinte forma: na seção 2, são apresentados os tipos de malwares mais comuns. Na seção 3, são descritos os métodos de detecção de malware. Na seção 4, são introduzidos os principais métodos de coleta de malware. Na seção 5, define-se o honeypot, suas classificações e variações, além de serem detalhadas suas funcionalidades mais comuns. Na seção 6, são apresentados os softwares de coleta implementados. Na seção 7, tem-se as conclusões sobre os resultados da implementação do honeypot, e nas seções subsequentes, são apresentados o cronograma de atividades executadas e as referências do trabalho.

2 MALWARE

Os malwares são programas que modificam um computador sem o consentimento do usuário, com o objetivo de causar danos ou de utilizar recursos do computador. Quando um computador é infectado, o malware pode executar ações em nome do usuário ou acessar suas informações pessoais gravadas no computador.

De acordo com [1], os principais motivos que levam um atacante a desenvolver e a propagar códigos maliciosos são a obtenção de vantagens financeiras, a coleta de informações confidenciais, e vandalismo. Com o sistema operacional, firewall e antivírus sempre atualizados é possível minimizar as ameaças dos malware conhecidos.

2.1 TIPOS DE MALWARE

Os malwares podem ser classificados em diversas categorias, e segundo [4] as principais são vírus, worm, trojan, spyware e rootkit.

2.1.1 VÍRUS

Vírus é um programa ou um código anexado a uma parte de um software, que em seguida se reproduz quando o software é executado[4]. Os vírus se espalham reproduzindo-se e se inserindo em programas, documentos ou anexos de e-mails. Podem ser transmitidos por e-mail ou baixados por arquivos previamente infectados, podem estar em CDs, DVDs, pendrives ou qualquer outro tipo de mídia.

Um vírus normalmente requer uma ação para ser ativado e infectar a vítima. Os efeitos dos vírus podem ser desde simples brincadeiras até a destruição completa de programas e dados do computador.

2.1.2 WORM

É similar ao vírus, porém diferente do vírus ele não precisa de um arquivo ou programa hospedeiro, ele pode se espalhar e criar cópia dele mesmo, de um computador para o outro, sem ter sido ativado pelo usuário.

Os Worms procuram vulnerabilidades nos sistemas operacionais e se espalham por e-mail e outros programas de transmissão de arquivos. Eles normalmente se escondem no sistema operacional, se tornando invisíveis ao usuário. É comum perceber a presença do worm quando suas cópias começam a consumir recursos consideráveis do sistema e o deixando lento. Seus efeitos são similares aos dos vírus.

2.1.3 SPYWARE

Spyware é um programa que coleta informações sobre o usuário infectado[4]. Os tipos de informações roubadas pelos spywares variam de acordo com o objetivo de quem o criou, dentre os tipos de informações podemos citar dados de login de contas de e-mail, endereços IP e DNS dos computadores, hábitos de navegação e dados de conta bancárias.

Alguns softwares contêm spywares e avisam que ele está presente no Termo de Serviço do software, porém nem todo software que possui um spyware está mal intencionado. Alguns softwares utilizam spywares para fornecer propaganda de acordo com seus hábitos e gostos.

2.1.4 ROOTKIT

Um rootkit é um programa com código mal intencionado que busca se esconder de softwares de segurança e do usuário utilizando diversas técnicas avançadas de programação[4].

Rootkits são criados para permitir que os outros tipos de malwares se escondam dos softwares de segurança e do usuário. Portanto, eles não aparecem nos processos de execução do gerenciador de tarefas e muitos antivírus não conseguem encontrá-los.

Eles operam de maneira furtiva escondendo seus arquivos, processos e chaves de registros. Também podem criar diretórios e pastas ocultas destinadas a mantê-los ocultos do sistema operacional e softwares de segurança.

2.1.5 TROJAN

Um trojan é um programa malicioso que se mascara como uma aplicação benigna [4]. Diferente dos vírus, os trojans não se replicam, mas podem ser tão destrutivos quanto. O trojan pode executar quase todo o tipo de ação que um outro malware pode executar, por isso são classificados em diversas categorias e representam a maior parte dos tipos de malware que ameaçam os computadores.

Os principais tipos de trojans são:

- Remote Access Trojans: São feitos para permitir total controle ao sistema da vítima. São normalmente escondidos em jogos e outros programas que usuários executam em seus computadores.

- Data Sending Trojans: São feitos para fornecer ao atacante informações sobre senhas, cartões de credito, log files, endereço de e-mail ou outro tipo de informação. Esses trojans podem procurar por informações específicas ou instalar um keylogger que envia tudo que é digitado pelo teclado para o atacante.

- Proxy Trojans: Esse tipo de trojan faz com que o computador da vítima se torne um servidor proxy. Isso permite que o atacante possa utilizar seu computador para fraudes de cartão de crédito ou outras atividades ilegais, além de usar o sistema da vítima para lançar ataques contra outras redes e computadores.

- FTP Trojans: Esses trojans abrem a porta 21 (porta para transferência por FTP) e permite que o atacante utilize essa porta para se conectar ao computador da vítima.

- Security Software disabler Trojans: Esses trojans param ou destroem os softwares de segurança do computador da vítima, softwares como antivírus e firewalls, e fazem isso sem o usuário tomar conhecimento. É utilizado em combinação com outros tipos de trojans.

- Denial-of-service attack (DoS) Trojans: É utilizado para sobrecarregar uma rede, inundando a rede com tráfego inútil. A maioria dos ataques DoS exploram limitações do protocolo TCP/IP.

3 SISTEMAS DE DETECÇÃO DE MALWARE

São programas ou dispositivos que detectam ameaças de segurança a um sistema e podem ser utilizados para bloquear tais ameaças ou direcionar o ataque a um software de coleta.

3.1 FIREWALL

Segundo [5] os firewalls são dispositivos ou programas que controlam o fluxo de tráfego da rede. Eles realizam esse controle baseado em um conjunto de regras ou instruções previamente estabelecidas. Com base nas regras o firewall determina quais transmissões e recepções de dados podem ser executadas. O firewall pode ser utilizado para transferir o tráfego bloqueado para um sistema de coleta como o honeypot para análise da detecção.

3.2 ANTIVÍRUS

Segundo [1] os antivírus são programas criados para prevenir, detectar e eliminar malwares, é a principal ferramenta no combate dos malwares nos computadores. Seu método de detecção é principalmente baseado em:

1. **Assinatura:** Os antivírus possuem uma base de dados com uma assinatura para cada malware conhecido, e a utiliza para detectá-los no sistema.
2. **Heurística:** Neste método o antivírus procura por anomalias nos programas executados, porém nem sempre tais anomalias são maliciosas, gerando falso positivos.
3. **Integridade:** Na detecção por integridade o antivírus cria um hash para cada programa do sistema e o verifica a cada execução, caso o hash tenha sido modificado, o antivírus alerta uma possível ameaça.

3.3 SISTEMA DE DETECÇÃO DE INTRUSOS

Segundo [2], um sistema de detecção de intruso ou IDS (Intrusion Detection System) é um programa que age para impedir que uma invasão aconteça baseado no comportamento de um sistema e na assinatura de programas maliciosos de um banco de dados. O IDS pode ser utilizado como detecção direta de malware ou como um complemento a outro sistema de defesa. Um IDS pode ser classificado de várias formas como descrito a seguir.

3.3.1 NETWORK INTRUSION DETECTION SYSTEM

É um IDS que monitora todo o tráfego da rede para identificar tentativas de ataque, como exposto em [2]. A vantagem desse tipo de IDS é que eles conseguem detectar os ataques de forma abrangente através de duas metodologias, uma baseada no comportamento da rede (detecção de anomalias) e a outra baseada em um conhecimento prévio (detecção por assinatura). A principal desvantagem é que ele não monitora as aplicações de cada máquina da rede, apenas os pacotes que passam pela rede.

A detecção por assinatura envolve a procura em tráfego de rede de bytes ou sequências de pacotes conhecidos como maliciosos. Esse tipo de NIDS é mais eficiente que os de detecção por anomalia, pois gera um número menor de falso positivos.

A detecção por anomalia envolve o conhecimento de como o tráfego da rede se comporta durante o dia, ou seja, se em algum momento do dia o comportamento da rede sair do que foi definido como padrão o NIDS irá acusar a anomalia. A desvantagem desse tipo de IDS é que gera muitos falso positivos, pois nem tudo que sai do padrão estabelecido é um ataque, e é necessária uma atualização frequente no banco de dados das assinaturas.

3.3.2 HOST INTRUSION DETECTION SYSTEM

Diferente dos NIDS os HIDS não monitoram a rede e sim são instalados em cada máquina

dela. Os HIDS tem como função detectar anomalias nas máquinas como utilização indevida ou excessiva da memória, conexão de rede suspeitas, utilização da CPU, processos estranhos ou suspeitos e outros. Portanto um HIDS é uma defesa que detecta ataques que cheguem à máquina, e assim como os NIDS ele também gera falso positivos e necessitam de atualização frequente[2].

4 MÉTODOS DE COLETA DE MALWARE

São médodos que detectam malwares ou ameaças de segurança e coletam os dados extraídos destes.

4.1 PARCERIA COM EMPRESAS

É o método onde o interessado na coleta estabelece uma parceria com uma empresa que coleta malware para ter acesso às ameaças capturadas pela empresa.

Assim como neste trabalho os malwares coletados pelo honeypot são diretamente enviados para o banco de dados do CTI Renato Archer com o objetivo ter acesso ao seu banco de dados de malwares.

4.2 SPAM TRAPS

É um e-mail criado sem filtro de spam, ele considera todos os e-mails recebidos como spam, pois o e-mail criado não é usado por ninguém e nem se cadastra para receber e-mails de qualquer site. Portanto todo e-mail que chega a este e-mail é uma mensagem não solicitada, o que pode ser potencialmente um spam.Esta técnica é usada em conjunto à lista negra, onde os e-mails que são coletados nas spam traps são adicionados nas lista negras. Além de incluir o endereço de e-mail para lista negra, os arquivos e links no e-mail podem ser também coletados.

4.3 ANTIVIRUS ONLINE

Este método provê um serviço de análise de arquivo a um usuário, ele utiliza vários antivírus para fazer a análise do arquivo e mostra o resultado ao usuário, caso o arquivo esteja infectado ele coleta o malware. Exemplos desse tipo de serviço são o Vírus Total (www.virustotal.com) e o Vírus Lab (www.viruslab.com.br).

4.4 HONEYPOT

É um sistema que simula serviços e falhas de segurança reais ou virtuais, com o objetivo de ser infectado por um malware e então estudar a fonte e a natureza do ataque, ou apenas para isolar um ataque do restante de uma rede que deve ser protegida, de acordo com [2].

5 HONEYPOT

Segundo [4] um honeypot simula vários serviços de um computador. Ele escuta as portas dos serviços mais comuns, aceita qualquer pedido de comunicação requisitado, e simula a comunicação com o invasor através de diversos protocolos como TCP, UDP, FTP, VoIP entre outros.

Após receber uma tentativa de conexão em algum módulo do simulador, o Honeypot detecta e analisa o Shellcode recebido. Devido ao processo não ser instantâneo ele normalmente é feito em threads para não bloquear a execução de outras tarefas. A detecção e análise do Shellcode muitas vezes são feitas executando o Shellcode em uma máquina virtual e gravando os argumentos e comunicações API para extrair informações do ataque.

Para cada tipo de ataque detectado o honeypot se comporta de forma diferente, e armazena o arquivo ou o conjunto de comandos executados durante o ataque junto ao restante das informações coletadas, como IP de origem, data do ataque, protocolo utilizado, porta de comunicação e outros dados que variam de acordo com cada honeypot.

5.1 CLASSIFICAÇÃO

Segundo [2], os honeypots podem ser classificados em duas categorias: Honeypots de Baixa Interatividade e Honeypots de Alta Interatividade.

5.1.1 HONEYPOTS DE ALTA INTERATIVIDADE

Oferece serviços reais que possam atrair invasores. Esses serviços podem ser programas que funcionem como servidores de e-mail ou de transferência de arquivos ou acesso a um shell de comando.

A grande vantagem dos honeypots de alta interatividade, é que dificilmente o invasor perceberá que está caindo em uma armadilha, pois são serviços reais que o sistema está operando. No entanto é muito perigoso, pois por se tratar de um sistema real o atacante

pode conseguir controle total da máquina e comprometer a rede em que o honeypot está instalado.

É usado para investigar as ameaças que as organizações enfrentam e aprender a melhor forma de se proteger contra elas, são usados principalmente por pesquisadores, militares e organizações governamentais. Como o nível de interação com o atacante é muito grande a quantidade de dados obtidos sobre o ataque é maior do que no de baixa interatividade, porém são mais difíceis de manter e implementar.

5.1.2 HONEYPOTS DE BAIXA INTERATIVIDADE

Diferente dos honeypots de alta interatividade os de baixa tem todos os serviços simulados, ou seja, o atacante nunca terá acesso ao sistema real. São instaladas ferramentas para emular partes de sistemas operacionais e serviços com os quais o invasor irá interagir.

Como o atacante não interage com o sistema real, é muito vantajoso em relação à segurança, pois como se trata de simulações o atacante não terá como comprometer o computador e a rede que ele se encontra. Porém atacantes com mais habilidade conseguem perceber que se trata de uma armadilha, o que fará com que não se consiga obter muitas informações sobre o ataque, mas mesmo assim o ataque será registrado.

O objetivo destes honeypots é detectar o ataque e tomar as providências para impedir que algum dano seja causado. É utilizado basicamente como proteção. Como o nível de interação é baixo as informações capturadas são limitadas e, portanto é usado principalmente por empresas ou corporações para diminuir os riscos de segurança.

5.1.3 COMPARATIVO ENTRE OS TIPOS DE HONEYPOTS

Cada honeypot tem a sua função sendo os de baixa interatividade para proteção e os de alta para estudo e coleta de informação. Em TAB. 5.1.1 resume-se as principais diferenças entre eles.

Características	Baixa Interatividade	Alta Interatividade
Instalação	simples	complexa
Manutenção	simples	complexa
Risco de comprometimento	baixo	alto
Informações	essenciais	detalhadas
Invasor tem acesso ao Sistema Operacional real	não	sim
Aplicações e serviços oferecidos	emulados	reais

TAB. 5.1.1: Comparação entre honeypots de alta e baixa interatividade

5.2 VANTAGENS DOS HONEYPOTS

Todo o tráfego direcionado ao honeypot provém de uma ação mal intencionada, pois o honeypot não interage com o exterior espontaneamente o que reduz a ocorrência de falso positivos.

Os honeypots capturam apenas dados importantes para o administrador, não perdendo pacotes importantes para a análise como uma ferramenta de IDS perderia se começassem a chegar muitos pacotes da rede em um determinado momento. Utilizando os honeypots é possível visualizar como o atacante se infiltrou no sistema, que ferramentas foram utilizadas e como se proteger delas.

Como só analisam o tráfego direcionado a eles, utilizam pouca banda da rede e como são softwares bem leves, exigem o mínimo do hardware.

5.3 DESVANTAGENS DOS HONEYPOTS

Honeypots só conseguem analisar os dados direcionados a eles. Se nenhum pacote chegar para ele analisar, não será gerado nenhum dado.

O honeypot corre o risco de ser invadido por alguém e ser utilizado para lançar ataques a outros locais.

5.4 HONEYNET

Um Honeynet é uma rede com vulnerabilidade intencional que consiste em um ou mais Honeypots, e tem o objetivo de se tornar mais atrativa a ataques, por concentrar uma maior quantidade de sistemas aparentemente vulneráveis, de acordo com [2].

5.4.1 TIPOS DE HONEYNET

De acordo com [2] as honeynets podem ser classificadas em duas categorias: Honeynets Virtuais e Honeynets Reais.

Uma honeynet real é a honeynet em que seus componentes são físicos, o que torna a honeynet mais difícil de ser detectada como armadilha por usuários avançados, e mais tolerante a falhas, porém possui um custo de manutenção elevado.

Uma honeynet virtual é a implementação dos componentes da honeynet em um número reduzido de dispositivos físicos, utilizando máquinas virtuais.

5.5 HONEYTOKENS

Os honeytokens são informações criadas com objetivo de atrair a curiosidade do invasor [2]. Por exemplo, um arquivo falso com nome password.txt ou um registro falso inserido no banco de dados que caso sejam utilizados alertam a tentativa de ataque. Podem ser criadas regras nos IDS a fim de monitorar de perto as honeytokens criadas.

6 HONEYPOTS IMPLANTADOS

O Dionaea foi nossa primeira opção para implementação pois o CTI Renato Archer o utiliza e tínhamos a intenção de participar de sua honeynet, portanto nossa instalação do Dionaea foi configurada para enviar os dados coletados para este banco de dados.

O Valhala Honeypot foi escolhido devido a sua facilidade de instalação e configuração e por simular os principais serviços de comunicação entre máquinas.

O Dionaea se mostrou mais eficiente e completo do que o Valhala principalmente na quantidade de informações que ele armazena e na possibilidade de criação de scripts em python que permitem estruturar as informações adquiridas de maneira personalizada. Os dois cumpriram o papel de redirecionar as tentativas de ataque por FTP para uma simulação e assim protegendo o sistema real, o que mostra que os honeypots não servem apenas como uma armadilha para malwares, mas também uma forma a mais de proteção.

6.1 DIONAEA

Ele utiliza a máquina virtual libemu para executar e detectar shell code e suporta IPv6, TLS. Ele copia qualquer malware que tente violar suas vulnerabilidades utilizando os serviços SMB, HTTP, FTP e TFTP, e pode trabalar em conjunto com outros honeypots como o Kippo.

Fizemos alguns ataques ao nosso honeypot que armazenou os arquivos relacionados ao ataque, expostos em FIG. 6.1.1. Para cada ataque o Dionaea armazena um log que contém as ações do invasor, em FIG. 6.1.2 é exibida a pasta com os ataques do dia 5 de junho de 2013 e em FIG. 6.1.3 um log onde podemos visualizar as mensagens trocadas entre o invasor e o Dionaea, em que o atacante faz upload do arquivo FAKEscreenLogger.exe para o sistema via FTP.

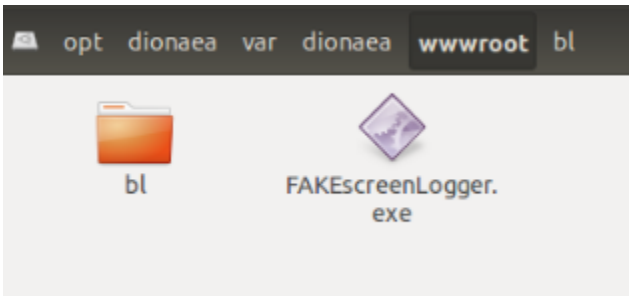

FIG. 6.1.1: Downloads realizados pelo Dionaea

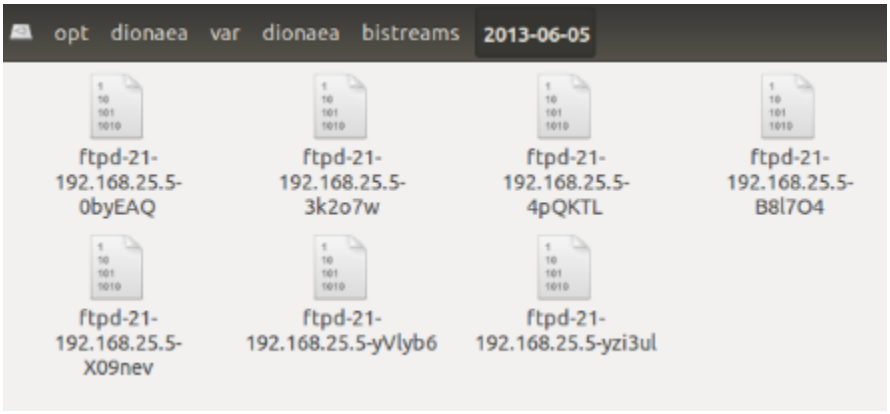

FIG. 6.1.2: Sistema de pastas que armazena os logs de cada ataque

```
stream = [('out', b'220 Welcome to the ftp service\x0d\x0a'),
('in', b'USER qualquer\x0d\x0a'),
('out', b'331 Password required for qualquer.\x0d\x0a'),
('in', b'PASS coisa\x0d\x0a'),
('out', b'230 User logged in, proceed\x0d\x0a'),
('in', b'SYST\x0d\x0a'),
('out', b'215 UNIX Type: L8\x0d\x0a'),
('in', b'FEAT\x0d\x0a'),
('out', b'211-Features:\x0d\x0a PASV\x0d\x0a PORT\x0d\x0a211 End\x0d\x0a'),
('in', b'TYPE I\x0d\x0a'),
('out', b'200 Type set to I.\x0d\x0a'),
('in', b'REST 0\x0d\x0a'),
('out', b'502 Command \x27REST\x27 not implemented\x0d\x0a'),
('in', b'PWD\x0d\x0a'),
('out', b'257 "/"\x0d\x0a'),
('in', b'SIZE FAKEscreenLogger.exe\x0d\x0a'),
('out', b'550 FAKEscreenLogger.exe: No such file or directory.\x0d\x0a'),
('in', b'PASV\x0d\x0a'),
('out', b'227 Entering Passive Mode (192,168,25,18,163,164).\x0d\x0a'),
('in', b'STOR FAKEscreenLogger.exe\x0d\x0a'),
('out', b'150 File status okay; about to open data connection.\x0d\x0a226 Transfer Complete.\x0d\x0a'),
('in', b'SIZE FAKEscreenLogger.exe\x0d\x0a'),
('out', b'213 8144640\x0d\x0a'),
('in', b'NOOP\x0d\x0a'),
('out', b'502 Command \x27NOOP\x27 not implemented\x0d\x0a'),
('in', b'NOOP\x0d\x0a'),
('out', b'502 Command \x27NOOP\x27 not implemented\x0d\x0a'),
('in', b'NOOP\x0d\x0a'),
('out', b'502 Command \x27NOOP\x27 not implemented\x0d\x0a')]
```

FIG. 6.1.3: Log de um ataque realizado via FTP

Com os testes realizados, foi verificado que o Dionaea aceita qualquer requisição que o invasor faz e autentica quaisquer usuário e senha que o atacante informe, além de proteger a máquina dando privilégios diferentes para os invasores. A comunicação entre o honeypot e o malware, armazenamento, tratamento e envio de dados são controlados através de scripts em python, que podem ser configurados para qualquer funcionalidade nova que o host do Dionaea queira criar. Ao somar a isso os arquivos de configuração de serviços, concluímos que o Dionaea é seguro e facilmente customizável.

6.2 KIPPO

O Kippo é um honeypot que simula um serviço SSH com falhas. Tem como característica armazenar os logs de ataques de força bruta e toda interação do atacante com shell. Emula um sistema de arquivos falso, onde o atacante tem a possibilidade de criar e apagar arquivos e salva os arquivos baixados pelo atacante com o comando wget para uma análise futura. Como ele permite uma interação grande não é recomendado utilizar em servidores reais e sim

em máquinas virtuais.

6.3 VALHALA HONEYPOT

O Valhala Honeypot é um honeypot open source brasileiro que foi desenvolvido para Windows. Ele possui serviços de baixa interação e uma opção de alta interação, a qual não foi usada em nossos testes. Alguns dos serviços que ele simula são HTTP, Telnet, FTP e SMTP. Ele também faz cópia dos malwares envolvidos no ataque e guarda as mensagens trocadas na invasão.

Para realizar testes com o Valhala Honeypot utilizamos uma máquina executando o Valhala enquanto em outra máquina a tentávamos invadir por meio de FTP e Telnet, na invasão por FTP fizemos download, upload e deletamos arquivos, na invasão por Telnet executamos comandos na shell oferecida pelo honeypot e em ambos os casos todos os comandos enviados ao honeypot são gravados no log, exibido em FIG. 6.2.4.

```
(21:32:56) The IP 192.168.0.105 tried to invade by ftp (PORT 192,168,0,105,238,255)
(21:32:56) The IP 192.168.0.105 tried to invade by ftp (LIST )
(21:33:57) The IP 192.168.0.105 tried to invade by ftp (PORT 192,168,0,105,239,6)
(21:33:57) The IP 192.168.0.105 tried to invade by ftp (GET login.txt)
(21:34:10) The IP 192.168.0.105 tried to invade by ftp (DELETE login.txt)
(21:35:54) The IP 192.168.0.105 tried to invade by ftp (PORT 192,168,0,105,239,9)
(21:35:54) The IP 192.168.0.105 tried to invade by ftp (PUT Logins2.txt)
(21:36:43) The IP 192.168.0.105 tried to invade by ftp (PORT 192,168,0,105,239,10)
(21:36:43) The IP 192.168.0.105 tried to invade by ftp (PUT foto.exe)
(21:36:55) The IP 192.168.0.105 tried to invade by ftp (QUIT )
(21:36:55) The IP 192.168.0.105 tried to invade by ftp (disconnect)
(22:03:02) The IP 192.168.56.1 tried to invade by ftp (disconnect)
(23:30:46) The IP 192.168.56.1 tried to invade by telnet (connection)
(23:31:07) The IP 192.168.56.1 tried to invade by telnet (USER adminroot)
(23:31:23) The IP 192.168.56.1 tried to invade by telnet (PASSWORD qwerty)
(23:31:25) The IP 192.168.56.1 tried to invade by telnet (USER root)
(23:31:29) The IP 192.168.56.1 tried to invade by telnet (PASSWORD qwerty)
(23:31:32) The IP 192.168.56.1 tried to invade by telnet (dir )
(23:31:49) The IP 192.168.56.1 tried to invade by telnet (cd jogoaarchives )
(23:31:54) The IP 192.168.56.1 tried to invade by telnet (cd .. )
(23:32:06) The IP 192.168.56.1 tried to invade by telnet (cdcd fotos )
(23:32:13) The IP 192.168.56.1 tried to invade by telnet (cd jogos )
(23:32:20) The IP 192.168.56.1 tried to invade by telnet (dir )
(23:32:29) The IP 192.168.56.1 tried to invade by telnet (login.txt )
(23:32:50) The IP 192.168.56.1 tried to invade by telnet (jhelp )
(23:32:56) The IP 192.168.56.1 tried to invade by telnet (help )
(23:33:03) The IP 192.168.56.1 tried to invade by telnet (/help )
(23:33:09) The IP 192.168.56.1 tried to invade by telnet (bye )
(23:33:14) The IP 192.168.56.1 tried to invade by telnet (close )
(23:33:36) The IP 192.168.56.1 tried to invade by telnet (connection)
(23:37:47) The IP 192.168.0.105 tried to invade by telnet (connection)
(23:37:51) The IP 192.168.0.105 tried to invade by telnet (USER root)
(23:37:53) The IP 192.168.0.105 tried to invade by telnet (PASSWORD qwerty)
(23:38:02) The IP 192.168.0.105 tried to invade by telnet (ls )
(23:38:04) The IP 192.168.0.105 tried to invade by telnet (cd )
(23:38:05) The IP 192.168.0.105 tried to invade by telnet (dir )
(23:38:14) The IP 192.168.0.105 tried to invade by telnet (cd backup )
(23:38:37) The IP 192.168.0.105 tried to invade by telnet (cd jogos )
(23:38:39) The IP 192.168.0.105 tried to invade by telnet (dir )
(23:41:51) The IP 192.168.0.105 tried to invade by telnet (ls startlog logins.txt )
(23:42:11) The IP 192.168.0.105 tried to invade by telnet (startl loginclose )
(23:42:21) The IP 192.168.0.105 tried to invade by telnet (start login.tctxt )
(23:42:24) The IP 192.168.0.105 tried to invade by telnet (close )
(23:42:27) The IP 192.168.0.105 tried to invade by telnet (bye )
```

FIG. 6.3.4: Log de utilização do Valhala Honeypot

7 CONCLUSÃO

Neste trabalho apresentamos os principais tipos de malwares, softwares que têm como objetivo se infiltrar e causar algum dano ou roubo de informações sem o conhecimento e consentimento do usuário, e suas características com o objetivo de entender os tipos de ameaças existentes. Foram descritos os principais métodos de detecção e captura destes. O trabalho teve como tema principal a coleta de malware através de honeypots. Foi feita a instalação de dois tipos de honeypots, o Dionaea e o Valhala Honeypot. Foram analizados os relatórios de invasão e coleta e foi constatado que ambos direcionam o ataque para um ambiente seguro simulado e capturam os arquivos envolvidos.

Propomos como trabalhos futuros a implementação de um honeypot com mais opções de customização e facilidade de utilização para incentivar mais usuários a se interessarem por esse método de coleta e assim aumentar a quantidade de dados coletados por esse tipo de software.

8 REFERÊNCIAS

[1] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL, CERT.br. Cartilha de Segurança para Internet. São Paulo: Comitê Gestor da Internet no Brasil, 2012.

[2] ASSUNÇÃO, Marcos Flávio Araújo. HONEYPOTS E HONEYNETS: Aprenda a detectar e enganar invasores. Santa Catarina: Visual Books, 2009.

[3] LIGH, Michael Hale; ADAIR, Steven; HARTSTEIN, Blake; RICHARD, Matthew. Malware Analyst's Cookbook. Indiana: Indianopolis, 2011.

[4] SZOR, Peter. THE ART OF COMPUTER VIRUS RESEARCH. Addison Wesley Professional, 2005.

[5] SCARFONE, Karen; HOFFMAN, Paul. GUIDELINES ON FIREWALLS AND FIREWALL POLICY: Recommendations of the National Institute of Standards and Technology. Maryland: Gaithersburg, 2009.

[6] dionaea – catches bugs. Disponível em:< http://dionaea.carnivore.it/>.Acesso em: 17 nov. 2013.

[7] Valhala Honeypot | Free System Administration software downloads at SourceForge.net. Disponível em:< http://sourceforge.net/projects/valhalahoneypot/>.Acesso em: 17 nov. 2013.

[8] SPITZNER, Lance. HONEYPOTS: Tracking Hackers. Addison Wesley Professional, 2002.

[9] THE HONEYNET PROJECT. KNOW YOUR ENEMY: Learning about Security Threats. Addison-Wesley Professional: 2004.