Honeypots no estudo do comportamento de ameaças e contenção de códigos maliciosos no contexto da internet brasileira

Anderson Silva Lima (Universidade Nove de Julho - UNINOVE) ls-anderson@uninove.edu.br
Adelia Greice dos Santos Altran (Universidade Nove de Julho - UNINOVE) adelia.s@uni9.pro.br
Leandro Vilella Fernandes (Universidade Nove de Julho - UNINOVE) lekovf@uninove.edu.br
Rosana Cordovil da Silva (Universidade Nove de Julho - UNINOVE) rosanacordovil@uni9.pro.br
Renato José Sassi (Universidade Nove de Julho - UNINOVE) sassi@uni9.pro.br

Resumo:
Programas maliciosos são utilizados como vetores de ataques para comprometer sistemas computacionais. A infecção por meio deste tipo de agente pode trazer prejuízos para a organização, o que pode levar a paralização dos seus sistemas ou até a inutilização de todas as informações. Assim, empresas adotam o uso de *honeypots* como medida preventiva às infecções. *Honeypots* são ambientes independentes da rede de computadores utilizados para atrair agentes maliciosos onde as ameaças ficam contidas em ambiente controlado e seguro. O objetivo deste trabalho foi abordar a utilização de *honeypot* na internet brasileira como forma de estudo do comportamento de ameaças e contenção de códigos maliciosos. Como metodologia foi adotada a pesquisa bibliográfica e a pesquisa documental na análise de estatísticas diárias geradas pelo Consórcio Brasileiro de *Honeypots*. Os resultados apontam que o maior fluxo de ataques que tem como alvo o Brasil tem origem nos Estados Unidos e que existe uma concentração de ataques buscando a exploração da porta 23 TCP, associada ao protocolo de rede TELNET.
Palavras chave: Comportamento de Ameaças, *Honeypots*, *Malwares*, Segurança da Informação.

Honeypots to study behavior of threats and contention of malware in Brazilian Internet

Abstract
Malwares are used as attack vectors to compromise computer systems. The infection by this kind of agent can damage the organization, which may lead to the downtime of its systems or even the destruction of all information. Therefore, companies adopt the use of honeypots as a preventive measure to infections. Honeypots are independent environments of the computer network used to attract malware in which the threats stay contained in a controlled and safe environment. The purpose of this study was to approach the use of honeypot in Brazilian internet as a way to study the behavior of threats and containment of malicious codes. The adopted methodology was bibliographic and documentary research in the analysis of the daily statistics generated by Consórcio Brasileiro de Honeypots. The results point that the majority of the attacks aiming Brazil are originated in the United States and that there is a concentration of attacks searching the exploration of the door 23 TCP, associated to the net protocol TELNET.
Key-words: Behavior of Threats, Information Security, Honeypots, Malwares.

1. Introdução

Atualmente a quantidade de ataques por *malware* na internet tem crescido de forma acelerada, segundo levantamento realizado pela Kaspersky Lab (2017), nos primeiros 8 meses do ano de 2016 foram registrados 398 milhões de ataques desse tipo na américa latina, nesse mesmo período em 2017 esse número aumentou em 59%, registrando 677.216.773 ataques.

Tendo em vista a quantidade de ameaças existentes, as empresas precisam adotar medidas que protejam sua rede desse vetor de ataque e que mantenham suas informações seguras, com esse propósito muitas delas adotam o uso de *honeypot*, atraindo os invasores para um ambiente controlado e que não comprometa o restante dos computadores na rede (SPITZNER, 2003).

A problemática que norteou a pesquisa foi: como o uso de *honeypot* é adotado para detecção de ataques e registro de comportamento de *malwares*? Foi adotada como metodologia a pesquisa bibliográfica em artigos científicos e pesquisa documental, analisando as estatísticas diárias geradas pelo Consórcio Brasileiro de *Honeypots*. Nesse sentido o objetivo deste trabalho foi abordar a utilização de *honeypot* na internet brasileira como forma de estudo do comportamento de ameaças e contenção de códigos maliciosos.

Segundo Peotta e Amaral (2006), *honeypots* são amplamente ultilizados como ferramentas de detecção de trafego malicioso ou indesejável, para análise de vulnerabilidades em uma rede ou para adquirir conhecimento dos metódos de invasão que estão sendo adotados na internet, portanto a realização desse estudo é importante, uma vez que contribui para divulgação dos padrões encontrados no comportamento dos agentes maliciosos que têm como interesse o cenário nacional, apresentando um agregado dos dados recolhidos pelo Consórcio Brasileiro de *Honeypots*.

2. Revisão da literatura

2.1. Segurança da Informação

Atualmente a informação tornou-se o ativo de maior importância em uma organização independentemente do seu ramo de atividade, por esse motivo são adotadas medidas que visam mantê-la protegida de agentes que buscam comprometer sua segurança.

> O valor da informação vai além das palavras escritas, números e imagens: conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações geram informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requer proteção contra vários riscos (ABNT NBR ISO/IEC 27002, 2013).

Nesse sentido a segurança da informação tem como objetivo implantar os controles necessários para que seja mantido a proteção do ativo informacional em todo seu ciclo de vida, mantendo três itens principais: sua confidencialidade, integridade e disponibilidade, que juntos formam os pilares da segurança da informação que são apresentados na norma ISO/IEC 27000 (2014). Entende-se como Confidencialidade a necessidade que haja controles que garantam que a informação esteja acessível apenas para pessoas com autorização. A Integridade deve garantir que a informação não seja modificada de maneira não autorizada durante o seu manuseio, armazenamento, transporte e descarte e a Disponibilidade deve sempre que necessário garantir que a informação esteja acessível e utilizável.

2.2. *Malwares*

Segundo o CERT.br existem diversos tipos de *malwares*, cada um deles com propósitos diferentes, por isso é importante o estudo de seus comportamentos individuais, com o objetivo de catalogá-los e ter a possibilidade de criar defesas contra esse vetor de ataque.

Códigos maliciosos (*Malwares*), são programas desenvolvidos com o objetivo de comprometer computadores e dispositivos para que estes executem tarefas sob comando de alguém mal intencionado. As infecções geralmente são feitas a partir de exploração de vulnerabilidades em programas, auto execução de mídias removíveis infectadas, acesso a páginas web maliciosas, execução de arquivos ou programas infectados, etc. Alguns dos tipos mais comuns de *malwares* apresentados na cartilha de segurança para internet do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) são descritos a seguir:

a) vírus: necessitam da execução de um arquivo ou programa infectado para agir, portanto, é dependente da interação do usuário do sistema para executar suas ações, esse tipo de *malware* propaga cópias de si mesmo e torna-se parte de outros arquivos e programas;

b) *worms*: diferentemente dos vírus, *worms* se propagam entre computadores automaticamente através da rede, por isso costumam consumir muitos recursos e podem afetar negativamente o desempenho da rede e a utilização dos computadores;

c) *Bots*: são programas que se propagam pela rede de forma semelhante ao *worm*, porém, esse tipo de *malware* tem como função se comunicar com o invasor fazendo com que ele possa enviar instruções que serão executadas no dispositivo infectado. Um grupo de computadores infectados obedecendo a um invasor são denominados como *botnets*;

d) *Spywares* (programas espiões): têm a função de fazer o monitoramento das atividades realizadas em um computador, após as informações serem coletadas elas são enviadas para o invasor. Existem diferentes tipos de *spywares* categorizados conforme seus objetivos e funcionamento, são eles: *keyloggers*, *screenloggers* e *adwares*;

e) *Backdoors*: podem ser partes de um código malicioso ou programa que possibilita o retorno de um invasor por uma brecha criada propositalmente pelo *malware*, geralmente criando um serviço ou modificando um já existente no computador comprometido;

f) *Trojan* (cavalo de Tróia): é um tipo de malware que fica escondido em programas legítimos modificados para que além de executarem as funções que aparentemente foram projetados para fazer executam funções maliciosas.

2.3. *Honeypot*

Honeypot é um recurso de segurança da informação que simula sistemas operacionais e vulnerabilidades em serviços, funcionando de forma independente do ambiente de rede em produção. Esse recurso computacional tem o intuito de ser sondado, atacado ou comprometido, tornando-se propositadamente o alvo dos possíveis agentes maliciosos (CERT.br, 2007).

A partir da exploração das vulnerabilidades implantadas no *honeypot*, uma vez invadido são coletadas informações sobre as ameaças existentes, para que sejam estudadas as formas de ataques utilizadas pelo invasor e consequentemente criar estratégias para saná-las (SPITZNER, 2003). Outro recurso é a possibilidade de detectar e coletar informações sobre tráfego indesejado em redes TCP/IP, um fluxo de rede que foge do padrão de utilização pode

caracterizar a presença de algum tipo de *malware* propagando-se, enviando informações ou recebendo instruções de um invasor (PUSKA, SANTOS e NOGUEIRA, 2014).

Os *honeypots* são classificados em, de baixa interatividade e de alta interatividade, conforme apresentada a comparação na Tabela 1.

Baixa Interatividade	Alta Interatividade
Fácil de instalar e configurar	Pode ser complexo de instalar e configurar (versões comerciais são mais simples)
Riscos controlados com serviços emulados limitando as opções do que o invasor pode ou não fazer	Riscos são aumentados, pois os invasores interagem com um sistema operacional real
Captura limitada de informações devido a limitação de interatividade	Pode capturar mais informações, incluindo novas ferramentas, dados de comunicação e o que foi digitado durante a interação com o *honeypot*

Fonte: Peotta e Amaral (2006)

Tabela 1 – *Honeypots* de baixa interatividade comparado ao de alta interatividade

Um *honeypot* de baixa interatividade emula sistemas operacionais e serviços, o agente mal-intencionado interage com esse ambiente evitando o comprometimento dos demais computadores na rede. Quando o *honeypot* utilizado é de alta interatividade os sistemas operacionais, aplicações e serviços são reais, instalados em uma máquina que deve ser protegida e monitorada constantemente para que a partir da exploração de suas vulnerabilidades não seja possível comprometer o restante da rede.

3. Metodologia

Para a realização deste trabalho foi adotada como metodologia a pesquisa bibliográfica e a pesquisa documental. A pesquisa foi desenvolvida em duas etapas:

Na primeira etapa foi feito o levantamento de artigos científicos que tratavam do uso de *honeypots* no estudo do comportamento de ameaças e contenção de códigos maliciosos, na segunda etapa foi feita a análise das estatísticas diárias geradas pelo Consórcio Brasileiro de *Honeypots* afim de verificar os fluxos de dados nos *honeypots* do projeto durante o período de 1 de Julho a 15 de Setembro de 2018.

O Projeto de *Honeypots* Distribuídos mantido pelo CERT.br faz parte do *honeyTARG Honeynet Project*, e tem o objetivo de coletar informações sobre o abuso da infraestrutura da Internet por atacantes e *spammers* (pessoas que enviam diversos e-mails ou mensagens sem autorização dos receptores), para isso foi criado o Consórcio Brasileiro de *Honeypots* (CBH) que mantêm ambientes simulados em diversas instituições pelo Brasil coletando diariamente informações relacionadas aos ataques sofridos. A partir do resumo diário e estatísticas públicas disponibilizados pelo CERT.br, será contabilizado o total do fluxo de rede nos últimos três meses catalogando os países que mais atacaram esses ambientes, também será feita a listagem das 10 portas mais visadas pelos agentes maliciosos.

Buscou-se no estudo avaliar o comportamento mais recente até o momento da pesquisa, por este motivo decidiu-se catalogar os países de origem dos ataques e portas acessadas nos três

últimos meses. Por fim, foi realizada uma amostragem com os dados disponíveis durante a pesquisa, identificando o país que mais interagiu com os *honeypot,s* baseando-se na quantidade em Gigabytes de fluxo de dados, bem como as portas de serviços TCP mais requisitadas nesse mesmo período.

O projeto do CERT.br utiliza o *software* Honeyd como *honeypot* de baixa interatividade e a partir dele coleta informações relacionadas ao fluxo de rede, durante este estudo para a análise dos dados foi utilizado o Excel, editor de planilhas da Microsoft.

4. Apresentação dos Resultados

Com a utilização de uma rede distribuída de *honeypots* de baixa interatividade foram coletados dados relacionados aos ataques sofridos nesses ambientes, aumentando a capacidade de detecção de incidentes, correlação de eventos e determinação de tendências de ataques disparados no espaço da Internet brasileira.

Na Tabela 2 são identificadas as localizações dos *honeypots* que fazem parte do CBH.

#	Cidade	Instituições
1	São José dos Campos	INPE, CTA
2	Rio de Janeiro	CBPF, Eletrobras, Eletronuclear, Embratel, Fiocruz, Furnas, PUC-RIO, RedeRio, UFRJ, VIVO
3	São Paulo	ANSP, CERT.br, Durand, LOCAWEB, PRODESP, TIVIT, UNESP, UOL, USP
4	Campinas	ITAL, SEFAZ-SP, UNICAMP
5	São José do Rio Preto	UNESP
6	Piracicaba	USP
7	Petrópolis	---
8	Brasília	CTIR Gov, Eletronorte, UnB
9	Porto Alegre	CERT-RS, Commcorp, PROCERGS, TRI
10	Ribeirão Preto	USP
11	São Carlos	USP
12	Florianópolis	POP-SC, UFSC DAS
13	Uberlândia	Algar Telecom
14	Lins	---
15	Passo Fundo	UPF
16	Curitiba	CELEPAR, Onda, PoP-PR
17	Belém	---
18	São Leopoldo	Unisinos
19	Belo Horizonte	CSIRT, PoP-MG, CEMIG
20	Recife	Chesf, EMPREL, Nlink
21	Salvador	TELETALK, UFBA
22	Vitória	PoP-ES
23	Americana	---
24	Bebedouro	MD Brasil
25	Porto Velho	PoP-RO
26	Rio Claro	TALKLINK
27	Fortaleza	MORPHUS
28	Natal	PoP-RN

Fonte: https://honeytarg.cert.br/honeypots/

Tabela 2 – Localização dos *Honeypots* por cidades e instituições

Os espaços simbolizados com "---" indicam cidades onde haviam instituições participantes do Consórcio Brasileiro de *honeypots* que deixaram o projeto.

Na Figura 1 é apresentado o mapa do Brasil com a distribuição geográfica dos *honeypots* relacionados na Tabela 2.

Figura 1 – Localização dos Honeypots

Fonte: https://honeytarg.cert.br/honeypots/index-po.html

A partir das estatísticas que podem ser acompanhadas no Projeto de *Honeypots* Distribuídos mantido pelo CERT.br, foi possível analisar o comportamento real dos agentes maliciosos, uma vez que estes não têm conhecimento de que estão interagindo com ambientes simulados. Portanto, adotam técnicas reais de exploração de falhas, conexões as portas de serviços e tentativa de obtenção de acesso, fazendo com que seja possível o estudo de padrões de comportamento das ameaças existentes.

Para este estudo foram analisadas as estatísticas de fluxos diários direcionados aos *honeypots* monitorados no projeto do CERT.br, mais especificamente, foi realizada a coleta de dados desde o dia 1 de Julho até 15 de Setembro de 2018, totalizando uma amostragem de 77 dias corridos.

A Tabela 3 apresenta a origem do acesso associada pelo código do país (CC), o nome do país e a quantidade de fluxo de rede nesse período. O código do país simbolizado como "XX" representa uma origem que não pôde ser associada a nenhum dos códigos conhecidos.

#	CCs	Nome	Fluxo de rede (GB)
1	US	Estados Unidos da América	194,32
2	RU	Federação Russa	27,90
3	IT	Itália	24,82
4	NL	Países Baixos	23,15
5	BR	Brasil	14,27
6	CN	China	11,93
7	FR	França	7,65
8	EU	União Europeia	3,52
9	XX	N/A	3,29
10	CA	Canadá	1,76

Fonte: Elaborado pelos autores

Tabela 3 – Fluxo de rede considerando o período de 1 de julho a 15 de setembro de 2018

Na tabela 3 foi possível identificar o fluxo de dados dos 10 países que mais interagiram com os *honeypots* brasileiros no período de estudo considerado neste trabalho. Os Estados Unidos da América assumiram a primeira posição por gerarem uma quantidade de 194,32 GB de fluxo na rede, esse valor corresponde a 62,16% do fluxo total de dados analisados e representa um fluxo de rede 6,96 vezes maior do que o gerado pela Federação Russa, país que assumiu a segunda posição.

Na Tabela 4 foram identificadas as portas TCP que nesse período tiveram maior tentativa de acessos, seguido dos serviços geralmente associados a elas. Foi possível observar que os serviços de TELNET, SSH e Microsoft-DS apresentaram maior tentativa de exploração. Portanto são os serviços mais visados pelos atacantes, sendo que 91,47% do fluxo total gerado por agentes maliciosos têm como alvo o protocolo de rede TELNET, isso corresponde a 12,87 vezes mais acessos do que o protocolo *Secure Shell*.

#	Portas	Nome	Fluxo de rede
1	23	TELNET	263,07 GB
2	22	SSH (*Secure Shell*)	20,44 GB
3	445	Microsoft-DS *Active Directory*	1,75 GB
4	80	HTTP (*Hypertext Transfer Protocol*)	1,09 GB
5	110	POP3 (*Post Office Protocol – version 3*)	344,45 MB
6	8080	HTTP Proxy	305,83 MB
7	8291	Milrotik Winbox	220,82 MB
8	7547	Mirai/IoT botnets	190,69 MB
9	8000	N/A	105,78 MB
10	3372	N/A	71,09 MB

Fonte: Elaborado pelos autores

Tabela 4 – Portas TCP mais acessadas

Com base nos resultados apresentados na tabela 4, pode-se observar um comportamento padrão em relação as portas e serviços que um agente malicioso procura para obtenção de acesso ao testar os serviços existentes na máquina e uma possível vulnerabilidade que garanta seu comprometimento.

Assim, foi possível observar portas altas que tiveram uma grande quantidade de fluxo de dados, como é o caso das portas 8000 e 3372, que não estão associadas a serviço identificado na lista de portas da IANA (*Internet Assigned Numbers Authority*), por esse motivo a identificação do serviço aparece como não disponível (N/A).

Foi possível identificar a ocorrência comum de acessos à porta TCP 7547, utilizada pelo *malware* Mirai, que visa infectar dispositivos IoT (Internet of Things) ou Internet das Coisas para uso em *botnets.* Mesmo esse *malware* tendo sido encontrado pela primeira vez em 2016 os dados apontam uma grande atividade ainda nos dias de hoje no contexto da Internet brasileira. Portanto, através dos *honeypots* de baixa interatividade utilizados no Projeto de *Honeypots* Distribuidos pode ser estudado a quantidade de fluxo de rede relacionado ao seu comportamento enquanto o *malware* permanece contido em ambiente simulado e protegido.

5. Conclusão

Baseando-se na situação problema que originou a pesquisa, o objetivo deste trabalho foi abordar a utilização de *honeypot* na Internet brasileira como forma de estudo do comportamento de ameaças e contenção de códigos maliciosos.

Com o levantamento diário dos dados disponibilizados pelo Consórcio Brasileiro de *Honeypots* foram analisadas as informações recolhidas durante os meses de Julho, Agosto e Setembro de 2018, totalizando uma amostragem de 77 dias, o que tornou possível a identificação de padrões no comportamento das ameaças que interagiram com os *honeypots* durante esse período.

Foi possível observar o total de fluxo de dados direcionado aos *honeypots*, bem como a origem desse tráfego ao identificar os países onde mais se originaram ataques como os Estados Unidos da América, a Federação Russa, a Itália, os Países Baixos e o Brasil apresentando como fluxo de rede os seguintes valores: 194,32 GB, 27,90 GB, 24,82 GB, 23,15 GB e 14,27 GB, respectivamente.

Durante o estudo foram identificadas as portas TCP com maior requisição e fluxo de dados na rede, apontando que TELNET, SSH (*Secure Shell*), Microsoft-DS *Active Directory*, HTTP (*Hypertext Transfer Protocol*) e POP3 (*Post Office Protocol – version 3*) são os serviços associados às portas que foram mais visados pelos atacantes, sendo que 91,47% do fluxo total gerado por agentes maliciosos tiveram como alvo o protocolo de rede TELNET.

Portanto, concluiu-se que o objetivo desta pesquisa foi alcançado ao analisar os resultados e obter os padrões de comportamento de ameaças e de tendências de ataques, afim de desenvolver medidas de prevenção e detecção voltadas à segurança da informação e do seu auxílio na contenção de *malwares*.

Como continuidade da pesquisa, visualiza-se que novos estudos podem ser feitos analisando as estatísticas públicas do Projeto de *Honeypots* Distribuídos divulgadas durante todo o período do ano de 2018, buscando o levantamento detalhado das tendências e padrões que poderão ser encontrados durante os 365 dias de tráfego no Brasil. A continuidade pode ser considerada no desenvolvimento de um projeto distribuindo *honeypots* de alta interatividade em ambientes protegidos e monitorados no Brasil, para capturar informações mais detalhadas de como se comportam as ameaças durante a tentativa de invasão, incluindo novas ferramentas que estão sendo utilizadas, armazenamento de dados de comunicação e até a captura daquilo que foi digitado durante a interação com o *honeypot*.

Referências

KASPERSKY LAB. 33 ataques por segundo: Kaspersky Lab registra aumento de 59% nos ataques de malware na América Latina, 11 de setembro de 2017. Disponível em: <https://www.kaspersky.com.br/about/press-releases/2017_kaspersky-lab-registers-increase-in-malware-attacks-in-latin-america>. Acesso em: 18 set. 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002: Tecnologia da informação: Técnicas de segurança: Código de prática para a gestão da segurança da informação. 2013.

CERT.BR, Cartilha De Segurança Para Internet, 2017. Disponível em: <https://cartilha.cert.br/malware/>. Acesso em: 20 set. 2018.

HOEPERS, C.; STEDING-JESSEN, KLAUS; CHAVES H.P.C. M. Honeypots e Honeynets: Definições e Aplicações. **CERT.br**, 2007. Disponível em: <https://www.cert.br/docs/whitepapers/honeypots-honeynets/>. Acesso em: 20 set. 2018.

CERT.BR. HoneyTARG: *Distributed Honeypots Project*, 2018. Disponível em: <https://honeytarg.cert.br/stats/flows/>. Acesso em: 20 set. 2018.

INTERNATIONAL STANDARD. **ISO/IEC 27000:** *Information technology: Security techniques: Information security management systems: Overview and vocabulary*. 2014.

PEOTTA, L.; AMARAL, D. Estudo de taxonomia de ataques e atacantes em um honeypot de alta interação. *The First International Conference On Forensic Computer Science – ICoFCS 2006.*

PUSKA, A.; SANTOS, A.; NOGUEIRA, M. Caracterização de Tráfego Indesejado em Redes TCP/IP Usando um Honeypot de Baixa Interatividade. Anais do 4º Workshop de Redes de Acesso em Banda Larga – WRA 2014.

SPITZNER, L. *Honeypots: Catching the insider threat. In Computer Security Applications Conference, 2003. Proceedings. 19th Annual*, p. 1–3, 10, 2003.