Honeypots distribuídos para ataques distribuídos de negação de serviço: pesquisa bibliográfica sistemática tradicional

Rafael Tenfen[1], **Rafael R. Obelheiro**[1]

[1]Programa de Pós-Graduação em Computação Aplicada (PPGCAP)
Centro de Ciências Tecnológicas (CCT)
Universidade do Estado de Santa Catarina (UDESC)
Joinville - SC - Brasil

rafaeltenfen.rt@gmail.com

rafael.obelheiro@udesc.br

Resumo. *Ataques distribuídos de negação de serviço por reflexão (distributed reflection denial of service, DRDoS), Esses ataques são uma forma eficaz de provocar a indisponibilidade de hosts. Para detectar, e conhecer mais sobre esses ataques, honeypots são utilizados como isca para atacantes utilizarem o dispositivo como refletor, sendo possível registrar as atividades dos atacantes e salvar os dados de vários honeypots para analisar e correlacionar esses dados. Esse estudo apresenta uma pesquisa bibliográfica sistemática tradicional para trazer estudos e conhecimentos relativos a como os dados de múltiplos honeypots distribuídos são extraídos, armazenados e correlacionados. A pesquisa busca apresentar os trabalhos que já utilizam honeypots para recolher informações sobre atacantes, e assim responder onde os logs gerados dos honeypots distribuídos são armazenados, qual o processo de busca utilizado e como a correlação de dados entre múltiplos honeypots acontecem. Todos os trabalhos apresentados passaram pelos critérios de inclusão e exclusão, e receberam uma pontuação de acordo com perguntas de quantificação de qualidade. Nesse trabalho, foram abrangidas 171 pesquisas, das quais 26 se enquadram em todos os critérios de inclusão e exclusão. Desses 26 selecionados, apenas 8 trabalhos passaram de 1,5 pontos (inclusive) de acordo com a quantificação de qualidade.*

1. Introdução

A negação de serviço, ou DoS *(Denial of Service)*, é uma técnica em que um atacante retira de operação um serviço, um computador ou uma rede conectada à Internet, utilizando um equipamento conectado à rede. Quando um ataque é realizado de forma coordenada e distribuída, ou seja, quando um conjunto de equipamentos é utilizado no ataque, recebe o nome de ataque distribuído de negação de serviço DDoS *(Distributed Denial of Service)*. Um ataque DDoS não tem por objetivo direto invadir ou coletar informações, mas sim de exaurir recursos e causar indisponibilidade de serviço do alvo [CERT.br 2016].

Ao ser atacado, o alvo de um ataque DDoS não consegue diferenciar os acessos legítimos ao sistema dos maliciosos e pode ficar sobrecarregado ao tentar tratar todas as requisições recebidas [CERT.br 2016]. Uma maneira comum de iniciar ataques DDoS são *botnets* DDoS, ou seja, redes infectadas por *malware* e computadores controlados remotamente para participar dos ataques. Quanto maior a quantidade de agentes em uma

botnet, maior o impacto para exaurir os recursos do alvo, assim como aumenta a dificuldade de distinguir o acesso dos atacantes dos acessos legítimos ao sistema em termos de endereços de IP *(Internet Protocol)* [Welzel et al. 2014].

Os atacantes podem melhorar ainda mais os seus ataques estruturando-os para utilizar refletores. Para um atacante, um refletor é qualquer nó na rede que envia dados para um IP em resposta a uma requisição recebida anteriormente. Refletores podem amplificar a quantidade de dados enviados, ou seja, sua resposta produz mais bytes ou pacotes, ou ambos, do que a requisição recebida. Assim, refletores potencializam o tráfego gerado por um atacante [Gondim et al. 2020]. Esse tipo particular de ataque distribuídos de negação de serviço por reflexão DRDoS *(Distributed Reflection Denial of Service)* tem como objetivo esgotar a largura de banda da vítima [Rossow 2014].

Qualquer *host* na rede pode ser abusado como refletor, como por exemplo: servidor, *workstation* ou *honeypot*. *Honeypots*, por sua natureza, não são criados para serem acessados por usuário legítimos e sim com o objetivo de serem sondados, atacados ou até mesmo comprometidos [Hoepers et al. 2007]. Dessa forma, *honeypots* são extensivamente monitorados para possibilitar o estudo do comportamento e das atividades dos atacantes, levando à descoberta de novos ataques e de como ataques já conhecidos na teoria são realizados na prática [Heinrich 2019b].

Geralmente um *honeypot* é um *host* que possui um endereço público na Internet, o qual não é anunciado. Por consequência o *host* precisa ser descoberto para a realização de qualquer tipo de interação com o sistema, o que exige algum tipo de mapeamento realizado pelos atacantes. Desta forma, é possível afirmar que qualquer interação realizada com o *honeypot* é considerada suspeita [Heinrich 2019b].

Quanto mais funcionalidades um *honeypot* implementa e quanto mais possibilidades de interação ele oferece, maior e mais detalhado é o comportamento dos atacantes que esse *honeypot* pode observar e coletar. Um *honeypot* de baixa interatividade basicamente emula algumas funcionalidades de um sistema vulnerável, permitindo uma observação mais restrita do comportamento dos atacantes mas oferecendo um risco menor. • Um honeypot de alta interatividade, por outro lado, permite que atacantes interajam com aplicações e serviços reais, o que oferece uma visão mais detalhada de suas atividades mas introduz um nível maior de risco [Heinrich 2019a].

O objetivo de expor o *honeypot* como um endereço público aberto é receber os ataques, e armazenar informações sobre eles, como quantidade de dados enviados e retornados, qual o endereço de IP (*Internet Protocol*) que enviou a requisição, entre várias outras informações que possam ser recolhidas através da requisição suspeita recebida, para após o recolher dessas informações ser possível analisar e tirar conclusões sobre o conjunto de dados.

As informações recolhidas pelos *honeypots* podem ser salvas de inúmeras formas, como salvar localmente no servidor, enviar os dados para um banco de dados centralizado ou enviadas para um fila para depois ser processada. Dessa forma, o foco desse estudo é recolher informações sobre a estrutura utilizada para capturar, analisar os dados gerados pelos *honeypots*, além de como é feita a correlação de dados entre *honeypots* distribuídos.

2. Trabalhos Relacionados

O gerenciamento eficaz da segurança de uma rede depende em grande parte da compreensão das ameaças existentes e emergentes na Internet [Nawrocki et al. 2016]. Os *honeypots* são capazes de detectar ataques no momento em que eles ocorrem gerar *logs* e fornecer informações sobre as ações e possíveis motivações dos invasores para assim agrupar e analisar essas informações e extrair conclusões como a caracterização desses ataques e assim auxiliar no processo de mitigação desses ataques.

Os *honeypots* evoluíram em diversas frentes para lidar com várias novas ameaças de segurança, não apenas contra os defensores da segurança, mas também contra usuários novatos em toda a Internet [Bringer et al. 2012]. Além disso, com a mudança do mundo para o foco em descentralização e servidores distribuídos, ataques distribuídos de negação de serviço podem explorar ainda mais servidores com falhas de configurações de *firewall*.

Como pode ser observado pelo trabalho de [Bringer et al. 2012], os estudos foram separados em 5 grandes áreas: novos tipos de *honeypots* para compatibilidade com novas ameaças de segurança, a utilização dos dados extraídos pelos *honeypots* para promover a detecção de novas ameaças, a configuração dos *honeypots* para reduzir o custo de manutenção assim como aumentar a exatidão em detecção de ameaças, como neutralizar as detecções de *honeypot* por invasores e questões legais e éticas no uso de *honeypots*.

Outro estudo mais recente, como de [Nawrocki et al. 2016], apresenta uma visão mais atualizada e próxima do tópico desse estudo com foco nas diferentes técnicas de análise utilizadas sobre os dados recolhidos de *honeypots*, além de uma visão extensa sobre o funcionamento, arquitetura e desenvolvimento do software do *honeypot*, também uma breve discussão sobre questões legais e éticas envolvidas ao uso e desenvolvimento de *honeypots*, assim como a metodologia da análise de dados utilizada.

Acima de todas essas contribuições como [Bringer et al. 2012] e [Nawrocki et al. 2016], a presente pesquisa bibliográfica sistemática tem um objetivo diferente das demais, com o foco de prover e organizar uma visão de recente estudos para os tópicos de como e onde os *honeypots* distribuídos salvam as informações das requisições, como os dados salvos são recolhidos e agrupados para realizar a análise, como esses dados são analisados e como é feita a correlação entre os mesmos.

3. Metodologia

O processo de realizar uma pesquisa bibliográfica sistemática tem particular importância para um estudo ou pesquisa. Revisões de outros trabalhos podem servir para a atualização do pesquisador sobre determinado tema, ou até para visualizar como os demais trabalhos lidaram com as perguntas de pesquisas, apresentadas na Seção 3.1. Além disso, pode-se utilizar uma PBS como ponto de partida de um estudo em um assunto em que não se possui total proficiência. Dada a importância das revisões sistemáticas, tornou-se uma ferramenta para pesquisadores realizarem uma comparação de diversos estudos sobre determinado tema.

Diversas iniciativas se apresentaram, principalmente na área de medicina, mas também chegando na área de engenharia, para padronizar pesquisas bibliográficas. Para a área das engenharias [Kitchenham 2004] sugeriu que pesquisadores de engenharia de software adotem Engenharia de Software baseado em evidências - EBSE (Evidence-

based Software Engineering). EBSE tem por objetivo aplicar uma abordagem baseada em evidências para a pesquisa e prática de engenharia de software [Kitchenham et al. 2009].

3.1. Perguntas de Pesquisa

A definição do protocolo deve ser a pergunta principal que irá definir o escopo da pesquisa e também as demais perguntas associadas a pesquisa. Nesse trabalho, tem-se como pergunta principal: *Quais são os modelos de funcionamento de honeypots em relação aos dados capturados, armazenados e correlacionados entre múltiplos honeypots*. Já, as perguntas de pesquisa associadas a esse estudo são:

1. Onde os dados ou *logs* dos *honeypots* distribuídos são armazenados?
2. Como acontece o processo de armazenamento?
3. A análise e correlação dos dados é realizada com qual propósito?

A respeito das perguntas de pesquisa 1 e 2, foi reconhecido que os *honeypots* armazenam dados sobre o comportamento de ataque observado, contudo a forma, o local e nem os dados armazenados seguem um padrão, então foi levantado a questão de como e onde esses dados são armazenados, e qual o impacto que a forma de armazenamento afeta o *honeypot*.

Já para abordar a pergunta 3, será identificado como os dados de múltiplos *honeypots* distribuídos têm os seus dados agrupados, como esses dados se relacionam entre si e por fim se o seu propósito tem foco na caracterização de ataques para futuras pesquisas e mitigações, ou a análise é realizada praticamente em tempo de coleta para que ocorra um alerta ao alvo do ataque.

3.2. Processo de busca

A construção da frase de busca foi realizada com foco em inglês, pois a maioria das pesquisas relacionadas ao tema, estão escritas em inglês, mas também foi adicionado a frase de busca a sua correspondência em português, como: (”attack?” OR ”ataque?”) ou (”analyse” OR ”analysis” OR ”analise” OR ”análise”). Além disso, foi utilizada a combinação de palavras chaves associadas as perguntas de pesquisa e ao tema relacionado, como DDoS (ataque distribuído de negação de serviço) ou sua variação DRDoS (ataque de negação de serviço de reflexão distribuída) e por fim a associação de que a pesquisa possui algum *honeypot*, da seguinte forma: (”distributed honeypot?” OR ”multiple honeypot?” OR ”honeypot? distribuído?” OR ”honeypot? distribuido?” OR ”múltiplo? honeypot?”).

Assim, a frase de busca formada pode ser expressa da seguinte forma: ’(”DDoS” OR ”DRDoS”) AND (”attack?” OR ”ataque?”) AND (”distributed honeypot?” OR ”multiple honeypot?” OR ”honeypot? distribuído?” OR ”honeypot? distribuido?” OR ”multiplo? honeypot?”) AND (”analyse” OR ”analysis” OR ”analise” OR ”análise”)’. A execução da frase de busca foi realizada em paralelo para que cada um dos autores execute a frase de busca em diferentes MBA (Mecanismos de Busca Acadêmica), como: Springer Link, IEEE Xplore e Google Scholar. Os mecanismos de buscas Springer Link e IEEE Xplore foram selecionados por conhecimento do autor o terceiro mecanismo de busca acadêmica Google Scholar foi indicação de orientador. Além dos mecanismos de buscas, o orientador aconselhou incluir um estudo também para a pesquisa bibliográfica sistemática [Leita et al. 2008].

A frase de busca não precisou ser modificada, pois os 3 mecanismos de buscas acadêmicas contemplam operadores *booleanos* "OR" e "AND", priorização de parênteses "()" e a *wildcard* "?" que representa, algum ou nenhum caractere.

3.3. Critérios de inclusão e exclusão

Devem ser incluídos os estudos que se caracterizam verdadeiro para todos os seguintes tópicos:

- Publicados partir de primeiro de janeiro de 2002, pois a partir dai os termos de *honeypots* e ataques de negação de serviço distribuídos começaram a se conectar.
- Apresentam o processo de armazenamento dos dados gerados pelo *honeypot*
- Explicam claramente os resultados obtidos a partir da análise dos dados.

Devem ser excluídos os estudos que se caracterizam verdadeiro para algum dos seguintes tópicos:

- Pesquisas que não apresentam a análise dos dados obtidos pelos *honeypots*.
- Estudos duplicados (para o caso em que um estudo esteja no resultado de busca de diferentes mecanismos de busca).

3.4. Quantificação da qualidade

O critério de qualidade das pesquisas foi determinado em 3 questões construídas de acordo com o foco do estudo:

Q1 O nível de interação dos *honeypots* é alto?
Q2 Os dados são armazenados de forma fácil para a análise e mineração de dados?
Q3 É realizada a correlação de dados entre múltiplos *honeypots*?

- Q1: Atende, quando o nível de interação de alta interatividade, parcialmente para *honeypot* de média interatividade ou híbrido e não atende quando é baixo o nível de interatividade.
- Q2: Atende, quando os dados são armazenados em um banco relacional, parcialmente para dados salvos em banco não relacional ou banco de dados de chave valor e não atende quando os dados são salvos em arquivos textos, CSV (Comma-Separated Values) ou outro tipo de arquivo que não seja trivial a consulta de dados.
- Q3: Atende, quando a correlação de dados ocorre e é explícita na pesquisa, parcialmente para quando ocorre a correlação dos dados, mas não está descrita de forma explícita no estudo e não atende quando não ocorre a correlação entre os dados gerados pelos *honeypots* distribuídos.

A pontuação foi baseada em [Kitchenham et al. 2009], então os pontos de cada qualificação são: atende = 1, parcialmente = 0.5, não atende = 0 ou desconhecido, quando a informação não é especificada. No caso de que a informação não foi encontrada ou não foi especificada, deve ser contatado os autores para esclarecer a avaliar novamente o critério de qualidade.

O processo de quantificação de qualidade deve ser analisado pelos dois autores, e quando ocorrer divergência da qualificação entre os autores, os mesmos devem debater e entrar em um acordo para redefinir a pontuação do critério de qualidade do estudo divergido.

3.5. Coleta de dados

A coleta de dados foi realizada apenas para os estudos que se caracterizam verdadeiros por todos os critérios de inclusão e se caracterizam falsos para todos os critérios de exclusão. Somando todos os resultados na execução da frase de busca nos mecanismos de buscas acadêmicas resultam em 171 estudos. Desses 171 estudos (IEEE Xplore: 10 resultados, Google Scholar: 137 resultados e Springer Link: 23 resultados e 1 inclusão por indicação do orientador), 26 passaram em todos os critérios de inclusão e exclusão.

Os seguintes dados foram coletados dos estudos 26 selecionados: o nível de interação (Q1), como os dados gerados pelos *honeypots* são armazenados (Q2), qual o processo de armazenamento, se os dados são enviados para um outro servidor ou armazenados localmente, a conclusão sobre os dados analisados, como é feita a correlação entre vários dados de *honeypots* distribuídos (Q3), qual o objetivo principal do estudo, qual o país em que os autores e instituições estão situados, quais os resultados obtidos do estudo, quantos *honeypots* distribuídos foram implementados, quais os protocolos atendidos pelos *honeypots*, como é feita a análise dos dados obtidos, qual o propósito da correlação e análise dos dados.

3.6. Análise de dados

Todos os 26 estudos selecionados, tiveram os dados coletados e planilhados em um CSV (*Comma-separated values*), e ao realizar a quantificação de qualidade da pesquisa, verificou-se que cerca de 70% dos trabalhos não atingiram 1,5 pontos, o que representa metade do máximo possível a ser obtido de 1 ponto para cada questão da quantificação da qualidade, no total de 3 pontos. Os 70% dos trabalhos representam 18 pesquisas que pontuaram entre 0 e 1,5 pontos, essas 18 pesquisas foram excluídas da apresentação dos dados.

3.7. Apresentação dos dados

A apresentação dos dados contempla os 8 trabalhos que alcançaram no mínimo 1,5 pontos (inclusive), que são em ordem de pontos decrescente: Somente um trabalho com 3 pontos [Ceron et al. 2020], [Leita et al. 2008] e [Krämer et al. 2015] com 2,5 pontos, já com 2 pontos são 4 trabalhos [Serbanescu et al. 2015], [Briffaut et al. 2011], [Heinrich et al. 2021] e [Trajanovski and Zhang 2021], por fim o último trabalho com 1,5 pontos [Afeworki 2014]. Os trabalhos são originados de vários países como: Holanda, França, Alemanha, Suíça, França, Brasil, Reino Unido e Noruega respectivamente.

A apresentação dos dados será apresentada na próxima sessão, em uma tabela classificatória ordenada pelo critério de qualidade em pontos na ordem decrescente, apresentando o título da obra abreviado, em qual mecanismo de busca foi encontrado, qual o nível de interação dos *honeypots* e quantos pontos a pesquisa alcançou na quantificação de qualidade.

A Figura 1, apresenta as 8 obras ordenadas com apenas alguns dados mais genéricos, os demais dados definidos na seção 3.5, ficaram definidos em um arquivo CSV que pode ser disponibilizado para demais pesquisadores que se interessarem e entrarem em contato com qualquer um dos autores desse trabalho.

Figure 1. Obras selecionadas acima de 1,5 na Quantificação da Qualidade

Obra	MBA	Nível Interação	Pontos
MikroTik Devices Landscape, Realistic Honeypots and Automated Attack Classification	IEEE Xplore	Alto	3
The Leurre.com Project: Collecting Internet Threats Information using a Worldwide Distributed Honeynet	Incluído p/ orientador	Híbrido	2,5
AmpPot: Monitoring and Defending Against Amplification DDoS Attacks	Springer Link	Híbrido	2,5
A Scalable Honeynet Architecture for Industrial Control Systems	Springer Link	Baixo	2
New Kids on the DRDoS Block: Characterizing Multiprotocol and Carpet Bombing Attacks	Springer Link	Alto	2
From Manual Cyber Attacks Forensic to Automatic Characterization of Attackers' Profiles	Google Schollar	Híbrido	2
An Automated and Comprehensive Framework for IoT Botnet Detection and Analysis (IoT-BDA)	Google Schollar	Híbrido	2
Comparative Analysis of Network Attacks Against FQDN Using Honeynet	Google Schollar	Alto	1,5

4. Resultados

Em relação aos trabalhos apresentados na Figura 1, 6 das 8 pesquisas salvam os dados das requisições dos atacantes utilizando TCPDUMP, que é um programa de computador analisador de pacotes de rede de dados que é executado em uma interface de linha de comando. Ele permite que o usuário exiba e armazene o TCP / IP e outros pacotes sendo transmitidos ou recebidos em uma rede à qual o computador está conectado. Distribuído sob a licença BSD, o programa é um software livre.

Além disso, 7 dos 8 trabalhos os dados capturados pelo TCPDUMP são armazenados localmente nos *honeypots*. Periodicamente, os dados são buscados nos *honeypots* (de forma automática ou manual) e armazenados em um servidor central para posterior análise.

Por fim, todos os *honeypots* apresentados atendem três ou mais protocolos em sua implementação, desses *honeypots* 3 possuem o nível de interação altos, 4 híbridos e apenas 1 possui a sua interatividade baixa.

5. Conclusão

Esta pesquisa bibliográfica sistemática teve a abrangência de 171 trabalhos, com 26 estudos que passaram nos critérios de inclusão e exclusão, com apenas 30% dos trabalhos alcançando 1,5 ou mais pontos de acordo com as questões de quantificação da qualidade.

Os modelos de funcionamento de *honeypots* em relação aos dados capturados, armazenados e correlacionados, apresentam formas parecidas de lidar com as situações levantadas nas perguntas de pesquisa, caracterizando algo que já está funcionando corretamente e pode ser adotado por outros pesquisadores.

Além dos dados coletados, esse trabalho auxilia para o entendimento e como respostas para as questões levantadas ao planejar o desenvolvimento de múltiplos *honeypots* distribuídos, como o funcionamento para recolher os dados gerados pelos *honeypots* e como é realizada a correlação dos dados entre inúmeros *honeypots*.

References

Afeworki, S. F. (2014). Comparative analysis of network attacks against fqdn using honeynet. Master's thesis.

Briffaut, J., Clemente, P., Lalande, J., and Rouzaud-Cornabas, J. (2011). From manual cyber attacks forensic to automatic characterization of attackers' profiles. *Université d'Orléans*.

Bringer, M. L., Chelmecki, C. A., and Fujinoki, H. (2012). A survey: Recent advances and future trends in honeypot research. *International Journal of Computer Network and Information Security*, 4(10):63.

Ceron, J. M., Scholten, C., Pras, A., and Santanna, J. (2020). Mikrotik devices landscape, realistic honeypots, and automated attack classification. In *NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium*, pages 1–9. IEEE.

CERT.br (2016). Recomendações para melhorar o cenário de ataques distribuídos de negação de serviço (ddos). *https://www.cert.br/docs/whitepapers/ddos/*.

Gondim, J. J., de Oliveira Albuquerque, R., and Orozco, A. L. S. (2020). Mirror saturation in amplified reflection distributed denial of service: A case of study using snmp, ssdp, ntp and dns protocols. *Future Generation Computer Systems*, 108:68–81.

Heinrich, T. (2019a). *Caracterizaçao de Ataques DRDoS Usando Honeypot*. PhD thesis, Dissertaçao de mestrado em Computaçao Aplicada, UDESC, Joinville (SC).

Heinrich, T. (2019b). Caracterização de ataques drdos usando honeypot. Master's thesis, UNIVERSIDADE DO ESTADO DE SANTA CATARINA - UDESC.

Heinrich, T., Obelheiro, R. R., and Maziero, C. A. (2021). New kids on the drdos block: Characterizing multiprotocol and carpet bombing attacks. In *PAM*, pages 269–283.

Hoepers, C., Jessen, K. S., and Chaves, M. (2007). Honeypots e honeynets: Definições e aplicações. *Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, ver*.

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University*, 33(2004):1–26.

Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., and Linkman, S. (2009). Systematic literature reviews in software engineering–a systematic literature review. *Information and software technology*, 51(1):7–15.

Krämer, L., Krupp, J., Makita, D., Nishizoe, T., Koide, T., Yoshioka, K., and Rossow, C. (2015). Amppot: Monitoring and defending against amplification ddos attacks. In *International Symposium on Recent Advances in Intrusion Detection*, pages 615–636. Springer.

Leita, C., Pham, V., Thonnard, O., Ramirez-Silva, E., Pouget, F., Kirda, E., and Dacier, M. (2008). The leurre. com project: collecting internet threats information using a worldwide distributed honeynet. In *2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing*, pages 40–57. IEEE.

Nawrocki, M., Wählisch, M., Schmidt, T. C., Keil, C., and Schönfelder, J. (2016). A survey on honeypot software and data analysis. *arXiv preprint arXiv:1608.06249*.

Rossow, C. (2014). Amplification hell: Revisiting network protocols for ddos abuse. In *NDSS*.

Serbanescu, A. V., Obermeier, S., and Yu, D.-Y. (2015). A scalable honeynet architecture for industrial control systems. In *International Conference on E-business and Telecommunications*, pages 179–200. Springer.

Trajanovski, T. and Zhang, N. (2021). An automated and comprehensive framework for iot botnet detection and analysis (iot-bda). *arXiv preprint arXiv:2105.11061*.

Welzel, A., Rossow, C., and Bos, H. (2014). On measuring the impact of ddos botnets. In *Proceedings of the Seventh European Workshop on System Security*, pages 1–6.