Monitoramento e Caracterização de Botnets Bashlite em Dispositivos IoT

Artur Marzano[1], David Alexander[1], Elverton Fazzion[21], Osvaldo Fonseca[1], Ítalo Cunha[1], Cristine Hoepers[3], Klaus Steding-Jessen[3], Marcelo H. P. C. Chaves[3], Dorgival Guedes[1], Wagner Meira Jr.[1]

[1]Departamento de Ciência da Computação
Universidade Federal de Minas Gerais (UFMG)

[2]Departamento de Computação
Universidade Federal de São João del-Rei (UFSJ)

[3]CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança
NIC.br - Núcleo de Informação e Coordenação do ponto BR

{artur.marzano,david,osvaldo.morais,cunha,dorgival,meira}@dcc.ufmg.br

{cristine,jessen,mhp}@cert.br fazzion@ufsj.edu.br

Abstract. *The use of botnets, networks composed of malware-infected devices, for malicious activities, such as denial-of-service attacks and spam/phishing distribution, causes billion-dollar losses every year. The growth of the Internet of Things, combined with the low security of its devices, has provided invaders with a rich environment for the creation of botnets. To combat such networks, it is essential to understand their behavior. In this work we monitor widespread IoT-based Bashlite botnets using a network of low-interactivity honeypots. We analyzed both the scanning and infection of vulnerable devices as well as the command flow sent to infected devices by their controllers. Our results suggest that botnets rely on infrastructure providers, that most of the infections use unmodified publicly-available source code, and that there is a concentration of attacks on specific targets.*

Resumo. *O uso de botnets, redes formadas por dispositivos infectados por malware, para atividades maliciosas como ataques de negação de serviço e phishing gera prejuízos da ordem de bilhões de dólares todo ano. O crescimento da Internet das Coisas, combinado aos baixos níveis de segurança de seus dispositivos, tem proporcionado a invasores um ambiente favorável à criação de botnets. Entender o comportamento dessas redes é essencial para combatê-las. Neste trabalho, monitoramos várias redes Bashlite executando em dispositivos IoT utilizando uma rede de honeypots de baixa interatividade. Analisamos tanto o processo de ataque e infecção de dispositivos vulneráveis quanto o fluxo de comandos enviados a dispositivos infectados pelos seus controladores. Nossos resultados sugerem que botnets usam serviços de provedores de infraestrutura, que a maioria dos ataques de infecção utilizam ferramentas com código publicamente acessível sem modificações significativas, e que existe uma concentração de ataques em alvos específicos.*

1. Introdução

Ataques distribuídos de negação de serviço (DDoS, *Distributed Denial of Service*) buscam consumir recursos (como CPU, memória, ou banda) de um servidor ou de um componente no trajeto para o mesmo, a fim de degradar a qualidade dos serviços oferecidos ou até mesmo torná-los indisponíveis. Por exemplo, um ataque DDoS pode enviar requisições a um servidor alvo a uma taxa maior que sua capacidade de atendimento, resultando no descarte de conexões legítimas [Zargar et al. 2013]. Estima-se que ataques DDoS causem prejuízos da ordem de 2 bilhões de dólares ao ano [Neustar 2017]. Ataques realizados a partir de infraestruturas distribuídas são mais efetivos pois conseguem empenhar mais recursos computacionais para envio de requisições na tentativa de sobrecarregar o serviço alvo, e requerem mecanismos de mitigação avançados capazes de lidar com atacantes geograficamente e topologicamente distribuídos.

Ataques DDoS são comumente realizados a partir de *botnets*, redes formadas por dispositivos infectados por *malware*, também chamados de *bots* ou zumbis, e utilizados na prática de atividades maliciosas. Os *bots* pertencentes a uma *botnet* são controlados através de um servidor de Comando e Controle (C&C) responsável por coordenar os dispositivos infectados. Bots podem realizar tarefas diversas como varredura de rede à procura de dispositivos vulneráveis, infecção de dispositivos vulneráveis, envio de mensagens de spam ou *phishing*, e realização de ataques DDoS [Silva et al. 2013]. Para realizar tais ataques, o C&C envia para os dispositivos infectados pertencentes à *botnet* comandos para que enviem requisições maliciosas aos serviços alvo do ataque.

O crescimento da Internet das Coisas (IoT), combinado aos baixos níveis de segurança dos dispositivos que a compõem, atraiu o interesse de agentes maliciosos. Hoje, dispositivos IoT servem de plataforma para construção de botnets de grande escala e com significativo poder computacional. Ataques DDoS realizados a partir dessas botnets IoT podem alcançar 1,2 Tbps, como o ataque de 21 de outubro de 2016 realizado contra o DynDNS [Symantec 2017]. O nítido risco que estas botnets representam para a Internet e seus serviços, aliado à constante evolução das práticas e malwares utilizados pelos seus operadores, motivam estudos para melhor entendê-las e informar o desenvolvimento de contramedidas [Kolias et al. 2017]. Entretanto, botnets IoT podem ser bastante diferentes de outras plataformas e ainda não está claro como elas podem ser caracterizadas e entendidas. A metodologia aqui proposta é uma primeira contribuição deste trabalho, pois define critérios e métricas específicos para as botnets IoT que permitem entender melhor o seu funcionamento.

Neste artigo estudamos botnets da família Bashlite (seção 2), que infecta dispositivos IoT vulneráveis a acesso remoto. Utilizando 47 *honeypots* de baixa interatividade instalados no Brasil, coletamos por quase um ano dados sobre infecção de dispositivos por botnets e sobre a comunicação de operadores através dos seus C&C (seção 3). Utilizamos os dados coletados para caracterizar a infra-estrutura computacional que suporta a operação das botnets existentes (seção 4); as interações de operadores com essas botnets e os ataques disparados (seção 5); e o processo de infecção de dispositivos IoT vulneráveis (seção 6).

Nossos resultados mostram (i) uma concentração de C&C e servidores de malware em poucos provedores de computação em nuvem ou redes de distribuição de conteúdo, (ii) uma concentração de ataques contra provedores de conteúdo e de proteção

contra ataques, provedores de acesso a internet e serviços relacionados a jogos, e (iii) diferentes padrões de comportamento entre diferentes componentes de uma botnet, o que pode ser utilizado para monitorar e diferenciar botnets.

Nossos resultados ampliam e quantificam o entendimento sobre botnets Bashlite e derivativos. Nossos resultados podem ser utilizados para subsidiar novas políticas contra botnets, bem como para auxiliar no desenvolvimento de novos mecanismos de defesa. No primeiro caso, podemos citar a implantação de políticas para desincentivar ou impor retaliações a provedores de serviços de hospedagem que suportam uso malicioso; no segundo, essas informações podem ser usadas para desenvolver mecanismos de detecção de padrões de comunicação de botnets para serem aplicados na filtragem de tráfego.

2. *Bashlite*

Botnets Bashlite são organizadas em seis módulos lógicos descritos a seguir e ilustrados na figura 1. Esses módulos podem ser executados simultaneamente em múltiplos dispositivos para fins de redundância ou escalabilidade.

Servidores C&C são a interface de controle utilizada pelos operadores da botnet. São responsáveis por receber conexões e notificações dos bots, bem como por disseminar comandos a serem executados.

Servidores de malware hospedam e servem recursos utilizados pela botnet, como *shell scripts* e binários a serem carregados e executados por dispositivos infectados.

Varredores de rede sondam dispositivos conectados à Internet em busca de dispositivos executando servidores telnet e outras vulnerabilidades conhecidas.

Invasores tentam acessar dispositivos identificados pelos varredores e infectá-los com malware (obtido dos servidores de malware).

Bots são dispositivos infectados pelos invasores. Eles reportam seu estado aos servidores C&C e deles recebem e executam quaisquer comandos disseminados.

Base de dados (potencialmente distribuída) armazena informações coletadas pela botnet, p.ex., bots ativos, resultados de varredura ou tentativas de infecção.

Nas botnets Bashlite, bots são capazes de executar o módulo de varredura bem como realizar ataques de negação de serviço via inundação de pacotes (UDP e TCP SYN) ou de requisições HTTP. Durante o processo de infecção, invasores Bashlite desabilitam o servidor telnet, usado para acessar o dispositivo infectado, para impedir a reinfecção por outras botnets.

Uma botnet é construída e operada por um *atacante*, que pode vender seus serviços (p.ex., negação de serviço). O atacante pode disponibilizar uma interface Web que os *clientes* podem usar para contratar os serviços [Santanna et al. 2015]. A execução de varreduras é ativada e desativada sob demanda pelo operador via comandos específicos. Os invasores funcionam permanentemente e não permitem interação.

3. Conjunto de Dados

Os dados utilizados neste trabalho foram coletados por duas infraestruturas de monitoramento do projeto Honeypots Distribuídos do CERT.br em parceria com empresas e instituições de ensino.[1] Os dados nos possibilitam estudar o processo de infecção de dispositivos vulneráveis (seção 3.1) bem como o comportamento de atacantes e servidores

[1] `https://honeytarg.cert.br/honeypots/`

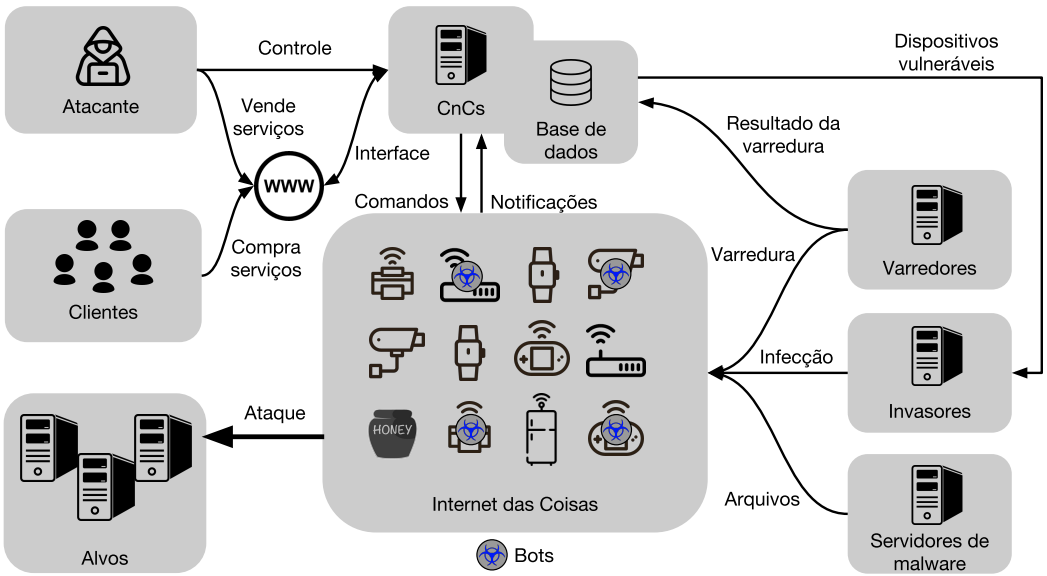

Figura 1. Visão geral do ecossistema de botnets IoT.

C&C (seção 3.2). Os resultados apresentados são associados a dados coletados entre 1 de janeiro e 13 de novembro de 2017.

3.1. Monitoramento dos Processos de Varredura e Infecção

Monitoramos o processo de infecção de dispositivos utilizando 47 honeypots de baixa interatividade (que não executam malware) distribuídos em 15 estados brasileiros. Os honeypots emulam serviços SSH e telnet acessíveis por um conjunto de credenciais vulneráveis utilizadas por fabricantes de dispositivos IoT. Com isso, capturam dois momentos do processo de infecção: (i) a varredura pelos varredores e (ii) a instalação do bot pelos invasores.

O honeypot não executa nenhum comando fornecido pelo invasor, apenas interpreta comandos recebidos e retorna para o invasor a resposta esperada, emulando progresso da infecção e elicitando comandos adicionais. Isso é possível por que o processo de infecção é automatizado, utiliza sequências de comandos pré-definidas e o progresso da infecção é verificado apenas através da saída dos comandos.

Os comandos executados em tentativas de infecção são transferidos para um servidor que identifica comandos que buscam acessar arquivos e informações (p.ex., usando wget, curl, ou scp) para identificar servidores de malware (figura 1). O servidor então acessa e armazena os arquivos em um ambiente isolado para análise posterior.

No período da coleta foram registrados 342.001.071 comandos, realizados por varredores e invasores originados de 2.385.460 endereços IP pertencentes a 780.138 subredes /24 controladas por 12.842 sistemas autônomos.

3.2. Monitoramento de Servidores de Comando e Controle (C&C)

Para monitorar atividade nos C&Cs e os ataques realizados, utilizamos um monitor que emula um dispositivo infectado e se conecta a C&Cs para observar comandos enviados aos bots. O protocolo utilizado pelos C&Cs Bashlite também é usado para comunicação

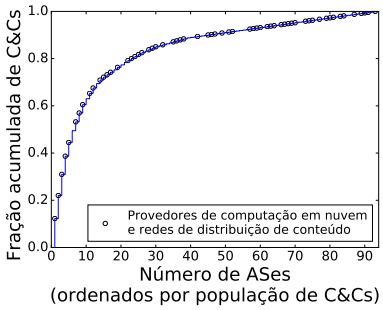

Figura 2. Distribuição acumulada dos C&Cs entre ASes.

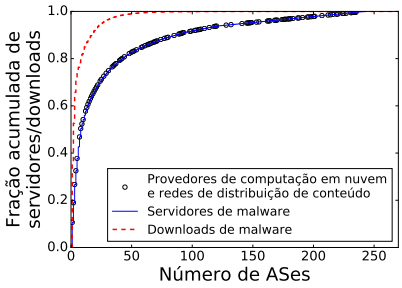

Figura 3. Distribuição dos servidores de download entre ASes.

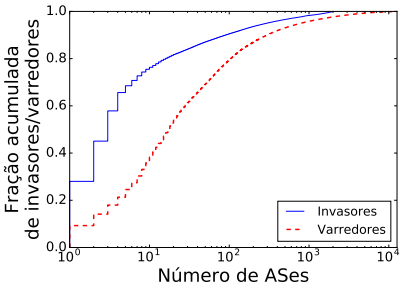

Figura 4. Distribuição de varredores e invasores entre ASes.

entre os operadores (como um canal IRC de bate-papo), assim como é capturada pelo monitor. Seguindo o princípio de baixa interatividade, o monitor nunca executa os comandos recebidos; apenas notificações falsas e respostas pré-programadas são enviadas ao C&C a fim de emular um bot, manter a comunicação ativa e coletar comandos.

Identificamos endereços IP de C&Cs realizando engenharia reversa dos binários baixados dos servidores de malware (seção 3.1). No período de coleta identificamos e monitoramos atividade em C&Cs hospedados em 486 endereços IP. Esses C&Cs dispararam 83.101 ataques a 29.428 alvos distintos, distribuídos em 25.575 subredes /24.

4. Caracterização da Infraestrutura de Suporte a Botnets

Nesta seção caracterizamos onde estão hospedados os C&Cs (seção 4.1) e servidores de malware (seção 4.2) que permitem o controle e expansão de botnets IoT para identificar redes particularmente vulneráveis ou potencialmente lenientes. Avaliamos também a localização dos varredores e invasores, que completam a infraestrutura de botnets (seção 4.3).

4.1. Localização de Servidores de Comando e Controle (C&C)

Nós mapeamos endereços IP para sistemas autônomos (AS) e *country codes* usando a base de dados do Team Cymru.[2] Conseguimos realizar o mapeamento de 99% dos 486 C&Cs e verificamos que eles estão em 93 ASes, distribuídos em 32 *country codes*.[3] A figura 2 mostra a distribuição acumulada dos C&Cs em função dos ASes onde estão hospedados. Observamos uma concentração de C&Cs em poucas redes; em particular, aproximadamente 80% dos C&Cs estão localizados em apenas 20% dos ASes observados.

Para entender melhor essa concentração, aplicamos a classificação de ASes da CAIDA[4] para avaliar o tipo de cada rede. Verificamos que 65% dos ASes hospedando C&Cs são classificados como provedores de computação em nuvem ou redes de distribuição de conteúdo e estão identificados na figura 2 com círculos. Estes ASes são seguidos por redes de trânsito ou acesso (31%) e redes empresariais (4%). Verificamos

[2]http://www.team-cymru.org/

[3]Para os endereços IP que foram mapeados para mais de um AS, verificamos que em todos os casos os ASes eram controlados pela empresa DigitalOcean e utilizamos o mapeamento mais frequente (AS14061) para consolidar a identificação.

[4]The CAIDA UCSD AS Classification Dataset.

ainda que 80% dos C&Cs são hospedados em provedores de computação em nuvem ou redes de distribuição de conteúdo. Por último, notamos que há uma concentração de provedores de computação em nuvem e redes de distribuição de conteúdo entre os ASes que hospedam o maior número de C&Cs (lado esquerdo da figura 2).

4.2. Localização de Servidores de Malware

Repetimos a análise anterior para os 1.955 endereços IP e 136 nomes de domínio utilizados por servidores de malware em nosso conjunto de dados. Dos 136 nomes de domínio, conseguimos resolver 42,7% deles em 18 de dezembro de 2017 e ignoramos os 57,3% restantes. Os nomes de domínio ignorados receberam apenas 0,1% das tentativas de acesso a servidores de malware feitas durante tentativas de infecção em nosso conjunto de dados.

A figura 3 mostra que aproximadamente 80% servidores de malware também estão concentrados em 20% dos ASes. Ao analisar o número de requisições aos servidores de malware em cada AS, verificamos que essa concentração é ainda maior (linha pontilhada). Também analisamos o tipo de ASes onde servidores de malware são hospedados e encontramos que estão concentrados em provedores de computação em nuvem ou redes de distribuição de conteúdo (círculos na figura 3). Por fim, verificamos que há uma interseção de 80% entre os 20 ASes que mais hospedam C&Cs e os 20 ASes que mais hospedam servidores de malware.

Discussão das seções 4.1 e 4.2: Uma possível explicação para a concentração de C&Cs em redes de conteúdo é a existência de serviços de hospedagem "à prova de balas" (*bullet-proof*) ou com políticas de uso aceitável permissivas. Estes serviços permitem a hospedagem de serviços maliciosos e não identificam os clientes hospedando C&Cs, mesmo após receberem notificações de autoridades [Goncharov 2015, Konte et al. 2015]. Nossas observações sugerem que esse tipo de rede não somente continua existindo, apesar de esforços da comunidade em contrário, mas que continua contribuindo para sustentar a infraestrutura de ataques DDoS na Internet conforme observado em trabalhos anteriores [Sood and Enbody 2013].

4.3. Localização de Varredores e Invasores

Por último, repetimos a análise de localização para varredores e invasores observados tentando infectar os 47 honeypots. Como nosso conjunto de dados não permite identificar os bots nas botnets, a caracterização de varredores é a única forma que temos de caracterizar o tamanho e espalhamento das botnets estudadas.

Nós classificamos os endereços IP observados nos honeypots como invasores se eles executam uma sequência de comandos que inclui algum comando para baixar arquivos de servidores de malware (wget, curl, ftp e tftp). Todos os demais endereços IP, i.e., os que não conseguiram autenticar-se ou que não tentaram baixar malware, são classificados como varredores.

No geral, identificamos que 96,1% dos endereços IP que se conectam aos honeypots como varredores e 2,5% como invasores. A figura 4 mostra que, apesar dos varredores estarem espalhados em 12.681 redes, mais de 90% deles estão concentrados em 300 ASes (2,4%). A figura 4 também mostra a localização dos invasores entre ASes e permite observar que estão ainda mais concentrados.

Para classificar os ASes dos varredores e invasores, utilizamos a metodologia aplicada na seção 4.1. Conseguimos rotular a maioria das redes que hospedam varredores (84,8%) e invasores (92,7%). Encontramos, em ambos os casos, que mais de 80% de varredores e invasores são hospedados em redes de trânsito ou acesso (diferente dos C&Cs e servidores de malware, que estão hospedados em provedores de computação em nuvem). Essa observação vai de encontro à expectativa de que dispositivos IoT estão frequentemente conectados a redes na ponta da Internet, como redes empresariais e domésticas.

5. Caracterização do Uso de Botnets

Nesta seção analisamos o fluxo de comandos observado na monitoração dos servidores de C&C. Discutimos os comandos utilizados pelos operadores, os alvos identificados para os diversos comandos e os padrões de comportamento associados aos operadores.

5.1. Comandos Observados

Nesta seção analisamos os comandos mais comuns para entender as capacidades e uso dessas redes. Um comando é uma mensagem de texto começando com os caracteres `!*`, seguidos pelo nome do comando e os parâmetros que o comando recebe. Observarmos 583 nomes de comandos diferentes. Apesar desse número ser aparentemente grande, muitos nomes de comandos aparecem uma ou poucas vezes, e podem ser resultado de erros de digitação por parte do operador da botnet. Além disso, diversas botnets utilizam variações do software original [Kolias et al. 2017], frequentemente modificando o nome de um comando. Para permitir uma análise mais detalhada, consideramos apenas os 80 nomes de comandos mais frequentes, que representam 98,9% dos comandos. A figura 5 mostra a popularidade dos comandos.

Para entender a semântica de cada comando, coletamos e estudamos o código-fonte de 39 clientes da família Bashlite disponíveis em diretórios abertos indexados por máquinas de busca. Analisamos manualmente os 80 nomes de comandos e determinamos a semântica de 72 deles: 48 nomes estão presentes nos códigos-fonte coletados, 17 nomes possuem significado equivalente aos 48 nomes anteriores, e 7 nomes de comandos estão descritos em mensagens de *banners* de C&Cs monitorados. Assim, agrupamos os 80 nomes de comandos em seis classes:

Ataque (25,0%): comandam os bots a atacar uma porta específica em um endereço IP alvo a fim de realizar um ataque de negação de serviço. Ataques comuns incluem inundação usando pacotes UDP, inundação de pacotes TCP SYN, ou inundações de requisições HTTP. Exemplo:
`!* TCPFLOOD 192.168.0.1 80 120 32 syn`

Controle (15,0%): administram a botnet, p.ex., para atualizar o binário do malware, terminar processos de malwares concorrentes, ou remover bots da botnet. Exemplo:
`!* UPDATE` e `!* BOTKILL`

Informação (10,0%): informam ao operador dados sobre a botnet como a lista de comandos disponíveis e quantidade de bots. Exemplo:
`!* HELP` e `!* STATUS`

Interrupção (15,0%): terminam a execução de ataques. Exemplo:
`!* KILLATTK`

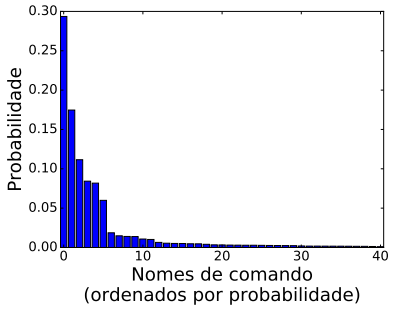

Figura 5. Popularidade de nomes de comandos.

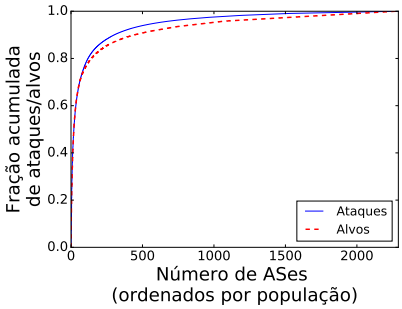

Figura 6. Distribuição dos alvos entre ASes.

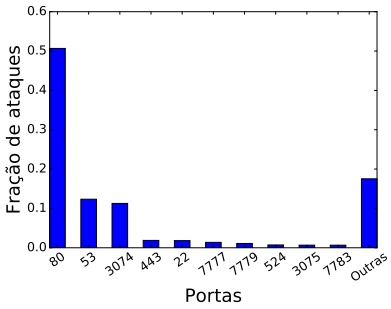

Figura 7. Popularidade de portas atacadas.

Varredura (22,5%): iniciam ou terminam a execução de varreduras em diferentes portas e faixas de endereços IP. Exemplo:

```
!* SCAN ON
```

Outros (12,5%): comandos utilitários do C&C que não encaixam nas classes anteriores e comandos não categorizados. Exemplo:

```
!* CLEAR
```

5.2. Alvos de Ataques

Comandos de ataque podem especificar alvos por endereço IP ou por nome de domínio. A maioria dos ataques (94,9%) especificam alvo por endereço IP diretamente, possivelmente para evitar que bots geograficamente distribuídos resolvam nomes de domínios para endereços IP diferentes. Conseguimos resolver 90,3% dos alvos especificados por nome de domínio em 18 de dezembro de 2017. Os domínios que não conseguimos resolver estavam presentes em apenas 0,4% dos ataques observados.

Como na seção 4, mapeamos endereços IP para ASes para identificar os ASes mais atacados. Os ataques observados tiveram como alvos 29.286 endereços IP em 2.289 ASes. A figura 6 mostra que 80% dos alvos estão concentrados em 6% dos ASes. A figura 6 também mostra que a concentração de ataques em ASes é ainda maior, visto que alguns alvos são mais populares e recebem vários ataques.

Inspecionamos manualmente os 25 alvos mais atacados, que receberam 13,2% de todos os ataques, e constatamos que podem ser classificados entre provedores de conteúdo e de proteção contra ataques de negação de serviço como Akamai e Cloudflare (11 alvos), provedores de acesso à Internet (7 alvos) e servidores e sítios relacionados a jogos (6 alvos). Um dos 25 alvos mais populares foi o endereço IP 1.1.1.1, provavelmente utilizado para testes. Esses resultados reforçam análises anteriores que mostram que servidores de jogos e empresas que oferecem serviços de proteção a ataques DDoS são alvos frequentes [Antonakakis et al. 2017].

A figura 7 mostra a popularidade das portas atacadas. A porta 80 (HTTP) é a mais atacada, recebendo 50,7% dos ataques. Esse resultado é intuitivo, uma vez que ataques têm como objetivo tornar uma página ou serviço Web indisponível. Além da porta 80, as portas 53 (DNS) e 3074 (Xbox Live) recebem uma quantidade significativa de ataques (12,4% e 11,3%, respectivamente). Os ataques na porta 53 são justificados

pela criticidade do serviço de DNS para o funcionamento da Internet e o impacto negativo sobre usuários dos servidores atacados. Por fim, os ataques à porta 3074 indicam a existência de motivação de parte de *gamers* na utilização de ataques DDoS como um serviço [Karami and McCoy 2013]. Esta constatação é reforçada pela observação de servidores de jogos (p.ex., Minecraft e Counter Strike) entre os servidores atacados.

5.3. Sessões de Operação das Botnets

Para entender o processo de operação das botnets e sua utilização, nesta seção caracterizamos as interações dos operadores com seus bots. Definimos uma *sessão de operação* como sequências de comandos ou mensagens de bate-papo consecutivos enviados a um C&C separadas de outras sequências por um intervalo de duração configurável δ. Para configurar a duração do intervalo, relacionamos o valor de δ com o número de sessões resultantes e escolhemos o ponto de inflexão da curva (o ponto a partir do qual aumentar o valor de δ tem impacto pequeno na quantidade de sessões). No restante desta seção utilizamos $\delta = 900$ segundos.

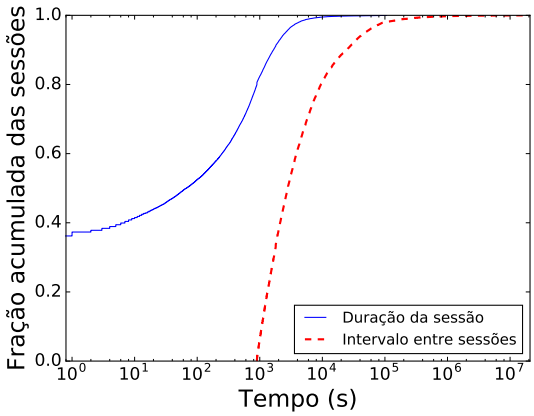

Figura 8. Distribuição da duração da sessão e do intervalo entre sessões.

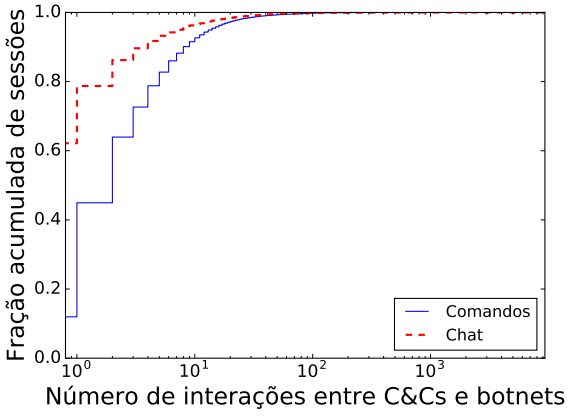

Figura 9. Distribuição do número de mensagens de bate-papo e comandos em sessões de operação.

A figura 8 mostra as distribuições acumuladas da duração da sessão e do intervalo entre sessões. Notamos que o intervalo entre sessões (linha pontilhada) começa de $x = 900$, de acordo com o valor de δ. O tempo entre sessões é em geral longo (note a escala logarítmica no eixo x), e aproximadamente 80% dos tempos entre sessões é superior a 30 minutos. Observamos ainda que cerca de 40% das sessões têm duração menor que 10 segundos, e que a maioria das sessões (80%) duram 15 minutos ou menos (linha azul). Esse comportamento sugere que os operadores de botnets, em geral, trabalham em rajadas, isto é, disparam comandos para os bots e esperam por seus efeitos. Investigamos esse comportamento analisando o tempo utilizado pelos atacantes em três comandos de ataque listados entre os dez comandos mais frequentes. Constatamos que, em média, 96% das execuções desses comandos são configuradas para durarem cerca de 30 minutos.

A figura 9 mostra as distribuições acumuladas do número de mensagens de bate-papo e do número de comandos em sessões de operação de botnets. A figura mostra que

muitas sessões possuem poucos comandos, o que explica as sessões com curta duração na figura 8.

Para entender melhor a semântica da sequência de comandos em uma sessão de operação, a figura 10 mostra um grafo de transição de comandos geral para todos os C&Cs. Os nós do grafo correspondem às seis classes de comandos descritas na seção 5.1 e ao início de uma nova seção. As arestas representam sequências de comandos. Calculamos o peso das arestas direcionadas do nó u para o nó v como a probabilidade de um comando da classe u ser sucedido por um comando da classe v. Arestas saindo do estado inicial indicam os primeiros comandos de uma sessão. Na construção do grafo ignoramos as mensagens de chat. Omitimos arestas com peso inferior a 0,10 para melhorar legibilidade e para focarmos nas transições mais importantes.

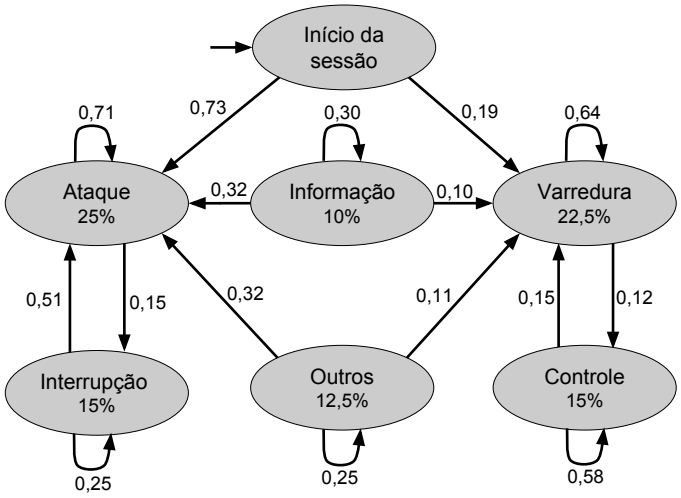

Figura 10. Grafo de transições entre comandos em sessões de operação.

O grafo mostra que 92% das sessões iniciam com um comando de ataque ou de varredura, indicando que esses são os motivos mais comuns para iniciar interação com a botnet. Observamos também que não há um comando específico para terminar sessões. De forma geral, a classe mais comum antes do término de sessões é interrupção de ataques, totalizando apenas 19,7% das sessões (não mostrado).

Constatamos que operadores realizam uma sequência de comandos de ataque (71% dos comandos de ataque sucedidos de outro comando de ataque). Constatamos por inspeção manual que essas sequências objetivam realizar ataques a alvos em diferentes redes ou estender a duração dos ataques disparando comandos a alvos repetidos. A aresta com peso 0,51 de comandos de interrupção seguidos de comandos de ataque indica que operadores frequentemente interrompem ataques antes de começar novos ataques.

Comandos de controle da botnet, em geral, também são encadeados. Através de inspeção manual, verificamos que operadores realizam diversos comandos para acessar arquivos dos servidores de malware para atualizar o malware executado nos bots. Notamos que comandos de varredura têm comportamento análogo, o que pode ser explicado pela necessidade de varreduras e infecções para a manutenção ou expansão da população de bots. Por fim, operadores frequentemente disparam novos ataques após obter informações sobre o estado corrente da botnet.

6. Correlação de Varredores e Invasores entre Honeypots

Nesta seção investigamos indiretamente as características dos varredores e invasores utilizados pelas botnets monitoradas. Nesta seção, identificamos varredores e invasores como descrito na seção 4.3.

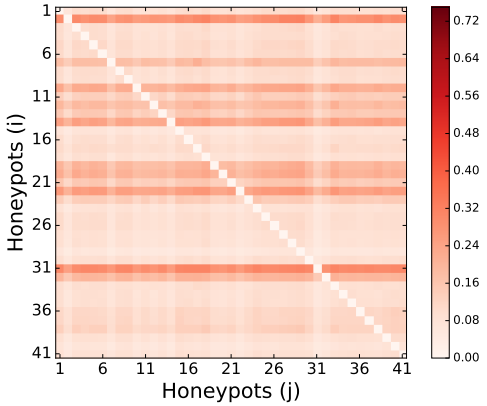

Figura 11. Mapa de calor da co-ocorrência de varredores entre honeypots.

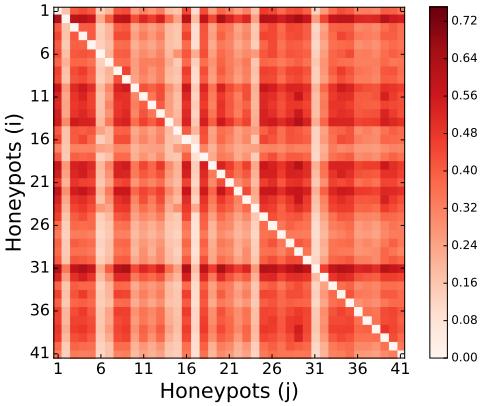

Figura 12. Mapa de calor da interseção de carregadores entre honeypots

Seja $\mathcal{V}_i$ o conjunto de varredores observados pelo honeypot i e $\mathcal{I}_i$ o conjunto de invasores observados pelo honeypot i, para todos os honeypots. Definimos a co-ocorrência de varredores em i e j como $f_{\mathcal{V}}(i,j) = |\mathcal{V}_i \cap \mathcal{V}_j|/|\mathcal{V}_i|$. Definimos a co-ocorrência de invasores $f_{\mathcal{I}}(i,j)$ de forma análoga. Note que a relação de co-ocorrência é assimétrica. Para evitar resultados tendenciosos devido a honeypots que ficaram ativos por um período reduzido de tempo, ignoramos 6 (entre 47) honeypots que ficaram ativos por menos do que 200 dias (entre 317 no dataset).

As figuras 11 e 12 mostram os valores de co-ocorrências de varredores e invasores para todos os pares de honeypots, respectivamente, usando mapas de calor. O valor máximo de $f_{\mathcal{V}}$ que observamos foi 0,34 e a média 0,11; o valor máximo de $f_{\mathcal{I}}$ foi 0,75 e a média 0,32.

Notamos que a co-ocorrência de varredores entre honeypots é muito menor que a de invasores. Como esperado, esse resultado confirma que botnets Bashlite usam mecanismos diferentes para execução de varredores e invasores. Em particular, varredores são executados por um grande número de bots (seção 4.3). Bots podem possuir banda de rede limitada e serem desconectados da rede (p.ex., desligados ou bloqueados em um firewall), o que pode levar a um processo de varredura lento e pouco confiável. Outra prática comum, motivada por questões de eficiência ou para evitar detecção, é que varreduras podem ser executadas em pequenos intervalos do espaço de endereçamento IP. Estes fatores levam a uma menor co-ocorrência de varredores entre honeypots. Uma consequência prática é que a quantificação do tamanho de botnets requer múltiplos pontos de observação distribuídos.

Notamos também que a co-ocorrência de invasores é maior; isso é esperado pois invasores são executados em servidores dedicados com banda e disponibilidade estáveis. Além disso, invasores não precisam operar por intervalos de espaço de endereçamento

IP já que iteram por uma base de dados com informações sobre dispositivos vulneráveis. Uma consequência da maior probabilidade de co-ocorrência é que identificar a infraestrutura de computação em nuvem utilizada por uma botnet pode ser feita a partir de um número menor de pontos de observação.

Além da diferença absoluta entre co-ocorrência de varredores e invasores, notamos que a co-ocorrência é variável entre honeypots. Este comportamento indica que alguns honeypots têm mais visibilidade do que outros, o que pode motivar mecanismos para atrair a atenção de botnets ou instalação de honeypots em redes mais visadas.

7. Trabalhos Relacionados

Problemas de segurança em IoT. Muitos dispositivos IoT executam sistemas operacionais de uso específico para os quais os fabricantes frequentemente não disponibilizam atualizações de software. Mesmo quando os fabricantes disponibilizam atualizações, a maior parte dos usuários finais não têm conhecimento técnico para instalá-las. Além disso, vários dispositivos IoT possuem senhas fracas que permitem acesso remoto à interface de configuração. Estes e outros fatores motivaram o desenvolvimento de malware para infectar estes dispositivos e construir botnets com grande poder de geração de tráfego [Pa et al. 2015, Kolias et al. 2017].

Caracterização de botnets e malware. Diversos trabalhos na literatura caracterizam o comportamento de botnets e propõem novos mecanismos de defesa contra seus ataques. Um desafio central é observar o comportamento de botnets IoT (frequentemente usando honeypots) sem contribuir com seu funcionamento ou ataques realizados [Kolias et al. 2017]. Exemplos de defesas resultantes de estudos sobre botnets incluem mecanismos paliativos acionados durante ataques para filtrá-los e impedir interrupção de serviços, bem como mecanismos para identificar bots participando de ataques e retardar o crescimento de botnets [Fabian and Terzis 2007, Silva et al. 2013]. Porém, com o crescimento da Internet das Coisas e proliferação de dispositivos vulneráveis conectados à Internet, muitas dessas medidas tornam-se inadequadas, p.ex., por que não conseguem acompanhar o dinamismo e diversidade dos dispositivos infectados e malware utilizados pelas botnets.

Mais relacionados ao nosso trabalho são artigos caracterizando o comportamento das redes Bashlite e de seu derivado Mirai. Estas redes tiveram seus códigos fonte disponibilizados publicamente e foram alvo de estudos sobre seu comportamento e sua evolução [Kolias et al. 2017, Antonakakis et al. 2017, Angrishi 2017], cujos resultados instruíram este artigo e sumarizamos na seção 2. Entretanto, diferente de trabalhos que apenas avaliam o ecossistema de botnets IoT [Kolias et al. 2017, Angrishi 2017], fizemos uma extensa coleta de dados para caracterizar a infraestrutura utilizada para infecção de dispositivos e operação de botnets. Nossos resultados, utilizando os dados coletados, complementam análises anteriores [Antonakakis et al. 2017], expandindo e atualizando nosso entendimento sobre o comportamento de botnets e seus operadores. Mais especificamente, utilizamos o conceito de sessão para melhorar o entendimento da interação entre C&Cs e botnets IoT, e identificamos indícios de redes coniventes correlacionando a localização dos servidores de malware com a localização dos C&Cs.

Ataques DDoS. Ataques DDoS são uma ameaça real, com exemplos recentes causando impacto significativo em diversos serviços na Internet e seus usuários

[Angrishi 2017]. Não surpreendentemente, pesquisadores estudam ataques DDoS há mais de uma década, classificando e criando taxonomias de diferentes ataques DDoS [Mirkovic and Reiher 2004, Cooke et al. 2005, Zargar et al. 2013]; caracterizando impacto [Behal and Kumar 2017, Wang et al. 2015]; e revelando o mercado de serviços de ataques DDoS utilizando botnets [Santanna et al. 2015, Kolias et al. 2017]. Neste artigo não caracterizamos ataques DDoS, mas nossos resultados podem instruir o desenvolvimento de futuros modelos e mecanismos de mitigação de ataques.

8. Conclusão

Neste trabalho, estudamos o comportamento de botnets IoT da família Bashlite utilizando dados coletados por 47 honeypots de baixa interatividade instalados em diversos pontos da rede brasileira. Nossos resultados mostram que C&Cs e servidores de malware, em geral, estão localizados em redes de conteúdo, o que indica que serviços de hospedagem "permissivos" podem estar contribuindo indiretamente para o problema. Além disso, verificamos que existe uma preferência por parte dos atacantes a servidores de jogos e empresas que oferecem serviços de proteção a ataques DDoS. Ataques DDoS de botnets se concentram em um número pequeno de redes. Também analisamos as sequências de comandos enviados pelos C&Cs, permitindo entender os comportamentos mais frequentes (p.ex., uma sequência de comandos de ataques pode ser utilizada pelos operadores para estender a duração dos ataques ou para realizar ataques a diferentes alvos). Por fim, encontramos que varredores e invasores estão, predominantemente, em redes de acesso que indica que essas redes hospedam dispositivos IoT vulneráveis e provavelmente não implementam políticas de proteção.

Como trabalho futuro pretendemos investigar a existência de comportamentos distintos para diferentes C&Cs (p.ex., *script kiddies*, botmasters, clientes); de forma a classificar os atacantes e entender melhor as motivações por trás de ataques DDoS que utilizam botnets IoT. Ainda, pretendemos estender a análise de sessões de operação botnet e avaliar as sessões nos honeypots, que podem definir o comportamento dos varredores e invasores. Esperamos identificar os comandos típicos utilizados em uma invasão e, dessa forma, criar mecanismos de defesa e prevenção de infecções. Por fim, pretendemos criar um sistema de tempo real que identifique dispositivos fazendo varreduras e realizando infecções, permitindo à comunidade utilizar essa informação na criação de mecanismos de defesa e formas de bloqueio.

Agradecimentos

Este trabalho foi parcialmente financiado pelo NIC.Br, Fapemig, CNPq, CAPES, RNP, e pelos projetos InWeb (MCT/CNPq 573871/2008-6), MASWeb (FAPEMIG-PRONEX APQ-01400-14), H2020-EUBR-2015 EUBra-BIGSEA, H2020-EUBR-2017 Atmosphere e INCT-Cyber.

Referências

Angrishi, K. (2017). Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV): IoT Botnets. *CoRR*, abs/1702.03681.

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z.,

Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., and Zhou, Y. (2017). Understanding the Mirai Botnet. In *Proc. of USENIX Security Symposium*.

Behal, S. and Kumar, K. (2017). Characterization and Comparison of DDoS Attack Tools and Traffic Generators: A Review. *IJ Network Security*, 19(3).

Cooke, E., Jahanian, F., and McPherson, D. (2005). The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets. *Proc. of the Steps to Reducing Unwanted Traffic on the Internet Workshop*.

Fabian, M. and Terzis, M. A. (2007). My Botnet is Bigger than Yours (Maybe, Better than Yours): Why Size Estimates Remain Challenging. In *Proc. of USENIX Workshop on Hot Topics in Understanding Botnets*.

Goncharov, M. (2015). Criminal hideouts for lease: Bulletproof hosting services.

Karami, M. and McCoy, D. (2013). Understanding the Emerging Threat of DDoS-as-a-Service. In *Proc. of USENIX Workshop on Large-Scale Exploits and Emergent Threats*.

Kolias, C., Kambourakis, G., Stavrou, A., and Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer*, 50(7):80–84.

Konte, M., Perdisci, R., and Feamster, N. (2015). ASwatch: An AS reputation system to expose bulletproof hosting ASes. *ACM SIGCOMM Computer Communication Review*, 45(4).

Mirkovic, J. and Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2).

Neustar (2017). Worldwide DDoS Attacks & Cyber Insights Research Report. Online.

Pa, Y. M. P., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T., and Rossow, C. (2015). IoTPOT: Analysing the Rise of IoT Compromises. In *Proc. of USENIX Workshop on Offensive Technologies*.

Santanna, J. J., van Rijswijk-Deij, R., Hofstede, R., Sperotto, A., Wierbosch, M., Granville, L. Z., and Pras, A. (2015). Booters: An analysis of DDoS-as-a-service attacks. In *Proc. of IEEE/IFIP International Symposium on Integrated Network Management (IM)*.

Silva, S. S., Silva, R. M., Pinto, R. C., and Salles, R. M. (2013). Botnets: A survey. *Computer Networks*, 57(2).

Sood, A. K. and Enbody, R. J. (2013). Crimeware-as-a-service—a survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection*, 6(1).

Symantec (2017). Internet Security Threat Report, Volume 22. Online.

Wang, A., Mohaisen, A., Chang, W., and Chen, S. (2015). Delving into Internet DDoS Attacks by Botnets: Characterization and Analysis. In *Proc. of IEEE/IFIP International Conference on Dependable Systems and Networks*.

Zargar, S. T., Joshi, J., and Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE communications surveys & tutorials*, 15(4).