Ataques DDoS por reflexão:

Visão de um honeypot multiprotocolo

Tiago Heinrich e Rafael Obelheiro

UFPR e UDESC

Introdução

- Ataques distribuídos de negação de serviço (DDoS) estão presente na Internet há mais de 20 anos;
- Disponibilidade de recursos para realizar a **amplificação** do tráfego, como a praticidade de aplicar *IP spoofing*.

Sumário

1 **Introdução**

- Atualidade
- DRDoS

2 **Honeypot**

- Mecanismos de contenção
- Coleta de dados
- Definições

3 **Observações**

4 **Conclusão**

Atualidade

- NETSCOUT:
  - Aumento de 9% nos ataques DRDoS entre o segundo semestre de 2017 e o mesmo período de 2018;
  - e 15% de 2019 a 2020;
  - 25% durante o período de lockdown devido à pandemia COVID-19;
  - 70% dos ataques DDoS usando reflexão em 2019.
- Considerando que o nosso período de coleta teve início em 2018, algumas observações sobre especificações de ataques coletadas pelo nosso *honeypot* podem ser elencadas.

DRDoS

- *Distributed Reflection Denial of Service* (DRDoS), visa explorar recursos que tenham uma taxa de amplificação alta (menor quantidade de *bots*);
- Vantagens:
  - Difícil identificar a origem dos ataques;
  - Tráfego refletido é **maior** que o tráfego enviado pelo atacante;
  - Uso simultâneo de **múltiplos refletores** (diversos protocolos podem ser explorados).

Tendências recentes em ataques DRDoS

- *Ataques multiprotocolo*: vários protocolos usados simultaneamente contra uma mesma vítima.

Tendências recentes em ataques DRDoS

- *Ataques de carpet bombing*: visam múltiplos endereços de um sub-rede em vez de um endereço único;
  - Objetivo é saturar a rede, dificultando detecção/mitigação.

Honeypot

- Para observar e coletar o tráfego DRDoS, desenvolvemos o MP-H, um honeypot multiprotocolo que suporta nove diferentes protocolos (UDP-based);
  - Emulação: Chargen, CoAP, CLDAP, NTP, QOTD, SSDP e Steam;
  - Proxy: DNS e Memcached.

Mecanismos de contenção

- Limite diário de requisições por IP de origem: reduz o tráfego enviado pelo MP-H quando usado como refletor;
  - Requisições excedentes são registradas, mas não respondidas;
  - Limite fixado em 5 requisições/dia por IP.
- Blacklist de endereços IP: suprime respostas a varreduras por refletores abertos;
  - Compilada de diversas fontes na Internet;
  - Notificações recebidas.

Implementação e coleta de dados

- MP-H foi implementado em Python/Linux, usando SQLite para o BD, Unbound e Memcached para os servidores locais;
  - AMD Phenom II (4 núcleos), 4 GB RAM, Ethernet 100 Mbps.
- Implantado na rede da UDESC, com IP globalmente roteável exposto diretamente à Internet (sem FW/NAT);
- Coleta de dados iniciada no final de setembro/2018, com breves interrupções por problemas de infraestrutura (elétrica/rede);
- Análise de 731 dias de tráfego DRDoS coletado pelo honeypot.

Definições usadas na análise

- É preciso identificar **ataques** e **vítimas**, mas...
  - não há consenso na literatura sobre definição de ataque DRDoS (do ponto de observação de um refletor)
    - adaptou-se definição usada em trabalhos anteriores do grupo (estabelecida empiricamente)
  - ataques de carpet bombing complicam a noção de vítima
    - endereço IP único ou sub-rede?
    - difícil precisar a sub-rede a que pertence um endereço IP

Ataque DRDoS

Um ataque DRDoS é formado por um conjunto com no mínimo 5 requisições com endereço IP de origem referente a uma mesma vítima e com espaçamento máximo de 60 segundos entre requisições consecutivas

Vítima

Uma vítima é definida pelos três primeiros octetos do endereço IP de origem (i.e., bloco CIDR /24)

- Geolocalização das vítimas estabelecida usando dados do WHOIS
  - possível imprecisão para clientes de nuvens e CDNs

Observações

Grupo de ataque	requisições	%	vítimas	%	ataques	%
Monoprotocolo	20,203,393,971	**97.50**	1,079,210	97.08	1,432,775	99.05
Multiprotocolo	518,684,765	2.50	32,369	2.91	13,798	0.95
Total	20,722,078,736	100	1,111,579	100	1,446,573	100

- Volume total de tráfego processado: 1.8 TB;
- Total de 20,7 B requisições processadas (média de 28,3 M/dia);
  - Apenas 0,034% foram respondidas pelo honeypot;
- Mais de 1,4 M ataques DRDoS observados;
- 1,1 M vítimas (/24) em 226 países:
  - Com maior presença nos: Estados Unidos, China e Reino Unido.

Intensidade dos ataques

- 1.9 k (mono) e 60 (multi) com 1 M de solicitações ou mais (correspondem $0,1\%$ e $0,4\%$ dos ataques);
- O maior ataque (mono) teve duração de 15h com 221,9 M;
- Já para (multi) teve uma duração de 11h com 7,8 M, envolvendo três protocolos;
- 87% de todos os ataques foram mais curtos que 15 minutos e 95.9% duraram até 1 hora
- Considerando mono e multiprotocolo:

	monoprotocolo	multiprotocolo
ataques $\geq$ 1 hora	39.886 (2,7%)	1.737 (12,5%)
ataque mais longo	178,6 h (7,4 dias)	180 h (7,5 dias)

Evolução Temporal

Lockdown e Eleição

- Eleição presidencial (2018):
  - A taxa de pacotes dobrou durante o mês da eleição em comparação com o mês anterior;
  - no dia do segundo turno o número de ataques teve um aumento de 227%.
- Lockdown (2020):
  - Comparamos o período de quatro meses de *lockdown* (março - junho) com o mesmo período de 2019 e aos quatro meses anteriores;
  - Observamos um crescimento de $4\times$ na taxa de pacotes;
  - Surgimento de novas vítimas em organizações de saúde, comércio eletrônico e instituições acadêmicas.

Tráfego por protocolo

Protocolo	Chargen	CLDAP	CoAP	DNS	Memcached	NTP	QOTD	SSDP	Steam
Ataques (%)	21.5	9.2	0.01	25.0	30.5	5.3	2.0	5.8	0.05
Requisições (%)	60.9	12.6	0.0002	0.9	23.3	0.01	1.5	0.5	0.000004

- Chargen e Memcached estão presentes em 52.1% dos ataques e 84.2% das requisições;
- Esses protocolos oferecem grandes fatores de amplificação que ajudam a explicar sua prevalência;
- CLDAP, que foi implantado em julho de 2020, já subiu para o número três em solicitações e número quatro em ataques.

Fatores de amplificação

Protocol	MP-H	Literature
Chargen	60	556.9 [7]
CLDAP	62	46–70 [1, 5]
CoAP	25	34–46 [2, 6]
DNS	50	28.7–64.1 [7]

Protocol	MP-H	Literature
Memcached	262	51,200 [4]
NTP	42	556.9 [7]
QOTD	78	140.3 [7]
SSDP	97	20–75.9 [3, 7]

- Memcached teve o maior fator de amplificação, 262;
- A maioria dos protocolos exibiu fatores de amplificação mais baixos do que relatado antes;
- A resposta sintetizada para o SSDP era maior do que a usada em outros trabalhos;
  - reduzida na versão atual.

.

Protocolos em ataques multiprotocolo

Protocol	CG:DNS	CG:CLDAP	CG:SSDP	CG:Memcached	Others
Attacks (%)	8.2	65.4	8.6	5.6	12.2
Requests (%)	27.9	16.7	19.5	9.2	26.7

- Os protocolos mais usados foram Chargen, DNS, CLDAP e SSDP
- Ataques com Chargen e um dos outros três respondem por 82,2 % dos ataques e 64,1 % das solicitações

Payload

- Para protocolos onde as respostas não dependem do conteúdo da solicitação;
  - Atacantes podem maximizar o fator de amplificação, minimizando o tamanho da carga útil;
  - 100% das solicitações Chargen observadas tinham apenas um byte de carga útil e 98% das solicitações QOTD tinham dois bytes ou menos.
- Quando a amplificação depende do conteúdo da mensagem;
  - SSDP tinha 99,9% das solicitações `M-SEARCH`;
  - O NTP tinha 99,9% de solicitações `MONLIST`;
  - 99,5% das solicitações CoAP continham um URI nulo;
  - 99,1% das solicitações CLDAP continham um `searchRequest <ROOT>|operation.`

Payload: DNS

Table: consultas DNS

Resource Record	%	Size
`isc.org ANY`	22.1	2701
`067.cz ANY`	4.0	388
`access-board.gov ANY`	3.6	N/A
`irs.gov ANY`	2.1	4302
`1x1.cz ANY`	1.6	1501
`pbgc.gov ANY`	1.1	4223
Others	65.5	–

Table: tipos de consultas

QTYPE	%
ANY	91.9
TXT	7.9
A	0.035
CNAME	0.014
NS	0.009
Others	0.14

- 115,9 k RRs distintos foram observados
- Os seis mais utilizados respondem por 34,5% das consultas

Payload: Memcached

- Memcached é abusado para amplificação de duas maneiras:
  1. Solicitar estatísticas do servidor, que fornece um fator de amplificação de 32 em média;
  2. Usar `set` para armazenar um grande pedaço de dados no banco de dados na memória e, posteriormente, recuperar esses dados repetidamente com solicitações `get` para a chave associada (99% dos casos).
- Principalmente com dados aleatórios.

Vítimas: países

Table: Principais países-alvo em número de ataques

Mono	%	Multi	%
US	32.6	US	49.6
CN	7.2	CN	14.0
GB	3.6	GB	4.7
FR	2.6	CA	3.4
CA	2.2	BR	2.7
DE	2.1	AU	2.4
Outros	49.7	Outros	23.2

- Ataques monoprotocolo afetaram vítimas em 226 países, e 111 países tiveram vítimas de ataques multiprotocolo.

Vítimas: ASNs

Table: Principais ASNs alvo em número de vítimas

ASN	País	Vítimas (%)
7922	US	7.1
7018	US	3.3
20115	US	1.8
37963	CN	1.6
701	US	1.5
16276	FR	1.3
Outros	–	83.4

- ASNs: **pertencem a provedores de serviços de Internet**[1] e *pertencem a provedores de nuvem*[2].

[1] 7922 (Comcast), 7018 (ATT INTERNET), 20115 (Charter Communications), e 701 (UUNET).
[2] 37963 (HangzhouAlibaba Advertising Co), e 16276 (OVH).

Carpet bombing

- Ataques a múltiplos endereços em um bloco para saturar a rede;
  - mais difícil de detectar/mitigar.

Carpet Bombing	requisições	%	vítimas	%	ataques	%
Monoprotocolo	1,117,437,837	5.39	235,244	21.16	52,689	3.64
Multiprotocolo	78,018,641	0.37	22,825	2.05	949	0.07
Total	1,195,456,478	**5.76**	242,030	21.77	53,638	**3.71**

Carpet bombing

- Exemplo: um ataque que durou 14 minutos e usou dois protocolos, Chargen e Memcached, com 340 k solicitações que foram espalhadas por 43 diferentes endereços IP no mesmo bloco CIDR (média de 7,9 k);
- Ao observar a distribuição das requisições temos uma média de 9.6 k requisições por host;
- Quanto maior a utilização do bloco, menor o número de requisições (50%+ do bloco, média 41,5 k, por host 185);
- Mas geralmente um conjunto baixo do bloco é explorado (média 6,2% do CIDR);
- 1,7% dos ataques teve como alvo 90%+ endereços em um bloco CIDR.

Carpet bombing com antecedentes

- Ataque CB ocorre depois de alguns dias com ataques a endereços únicos.

Conclusão

- Refletores abertos **serão** encontrados e usados em ataques DRDoS;
- Descobrimos que protocolos frequentemente negligenciados, como Chargen e CLDAP, estão sendo empregados nesses ataques;
- Embora limitados a um único ponto de observação, podemos afirmar que ataques têm espaço para piorar
  - novos protocolos, fatores maiores de amplificação, intensificação do uso de ataques multiprotocolo/carpet bombing
- Futuro:
  - aumentar o número de honeypots e integrá-los em uma plataforma distribuída;
  - usar dados agregados para detectar ataques e suas origens.

Referências I

[1] J. Arteaga and W. Mejia.
CLDAP reflection DDoS, apr 2017.
https://bit.ly/3kqyIku.

[2] C. Cimpanu.
The CoAP protocol is the next big thing for DDoS attacks.
ZDNet, Dec. 2018.
https://zd.net/333hymy.

[3] M. Majkowski.
Stupidly simple DDoS protocol (SSDP) generates 100 Gbps DDoS, jun 2017.
https://bit.ly/35lq2W0.

[4] M. Majkowski.
Memcrashed – major amplification attacks from UDP port 11211, Feb. 2018.
https://bit.ly/2HvD4Ix.

Referências II

[5] C. McAuley.
Following the crumbs: Deconstructing the CLDAP DDoS reflection attack, nov 2016.
https://bit.ly/3mgR08h.

[6] NETSCOUT.
CoAP attacks in the wild, Jan. 2019.
ASERT blog, https://bit.ly/2HqNxou.

[7] C. Rossow.
Amplification hell: Revisiting network protocols for DDoS abuse.
In *Network and Distributed System Security Symposium (NDSS)*, 2014.

Muito obrigado!

Perguntas?

Contatos

heinrichtx at gmail.com
rafael.obelheiro at udesc.br