Uso de Flows no Tratamento de Incidentes da Unicamp

Daniela Barbetti
daniela@unicamp.br

GTS-26
11 de dezembro de 2015
São Paulo, SP

Agenda:

✔ CSIRT Unicamp

✔ Rede de dados da Unicamp

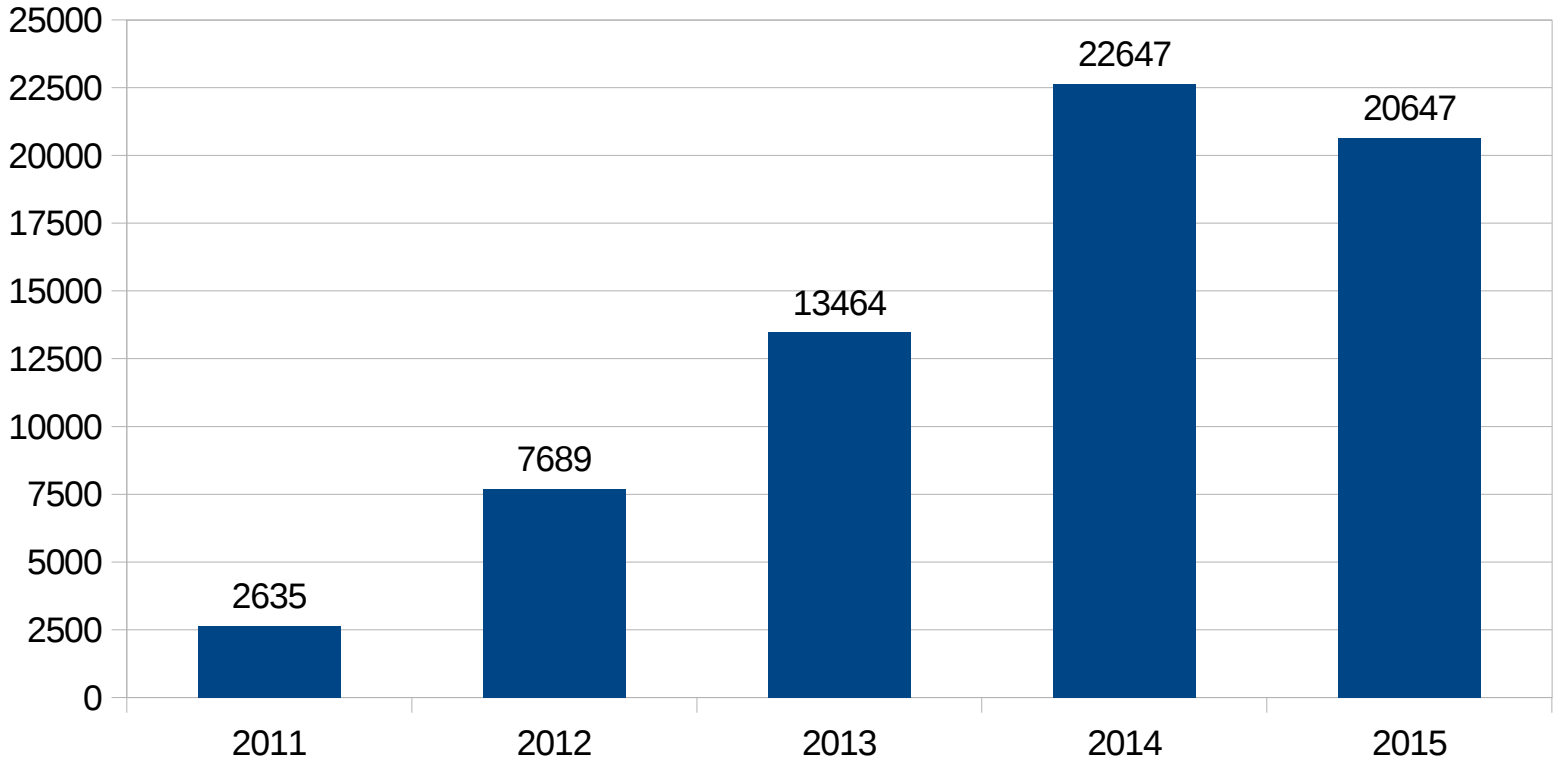
✔ Uso de flows no tratamento de incidentes
- Histórico do trabalho
- Estudos de casos
- Estatísticas

Sobre o CSIRT Unicamp:

- Recebe, analisa, processa e responde os incidentes de segurança da Universidade
- Analisa flows
- Realiza testes de detecção de vulnerabilidades
- Ministra palestras de conscientização para usuários finais
- Mantém o site e o ambiente computacional do CSIRT
- Emite certificados digitais (projeto ICPedu/RNP)

Sobre o CSIRT Unicamp:

Atendimentos entre 2011 e 09/12/2015:



Rede de dados da Unicamp

- AS próprio = 53187
- 3 blocos de rede IPv4: /16, /17 e /20
- 1 bloco de rede IPv6: /32
- Link agregado de internet: 20 Gbits/s
- Aproximadamente 70 mil usuários
- Média de 280 mil pacotes/segundo

Administração da Rede de dados da Unicamp

- Administração de TI é descentralizada: cada Unidade/ Órgão tem sua própria equipe de TI
- O CSIRT Unicamp interage com 90 equipes de TI
- Diversidade de conhecimento técnico, softwares e sistemas operacionais
- O CSIRT não tem atuação técnica na rede. É um CSIRT de coordenação.

Uso de flows no tratamento de incidentes:

Como tudo começou?

- Incentivo partiu no 2º Fórum de CSIRTs organizado pelo CERT.br em set/2013

Flows para CSIRT?
Flows não é para engenheiros ou analistas de redes?

- Os mesmos dados podem ser utilizados pelas duas equipes com objetivos diferentes
- A convivência é possível e saudável para a rede da Instituição

Uso de flows no tratamento de incidentes:

O que são flows de rede?

- 1 flow é um sumário com vários pacotes de rede

Para que serve?

- Analisar os pacotes que estão saindo da rede
- Detectar anomalias e tentativas de intrusão na rede de modo mais eficiente

Uso de flows no tratamento de incidentes:

Por que flows?

- Histórico do que passa pela rede (não existe a guarda do conteúdo mas sabe-se que a conexão existiu)
- Ferramenta de suporte para fazer a correlação de problemas de segurança
- Aumentar a eficiência do tratamento de incidentes identificando: computadores infectados, servidores comprometidos, envio de spam, erros de configuração, dentre outros

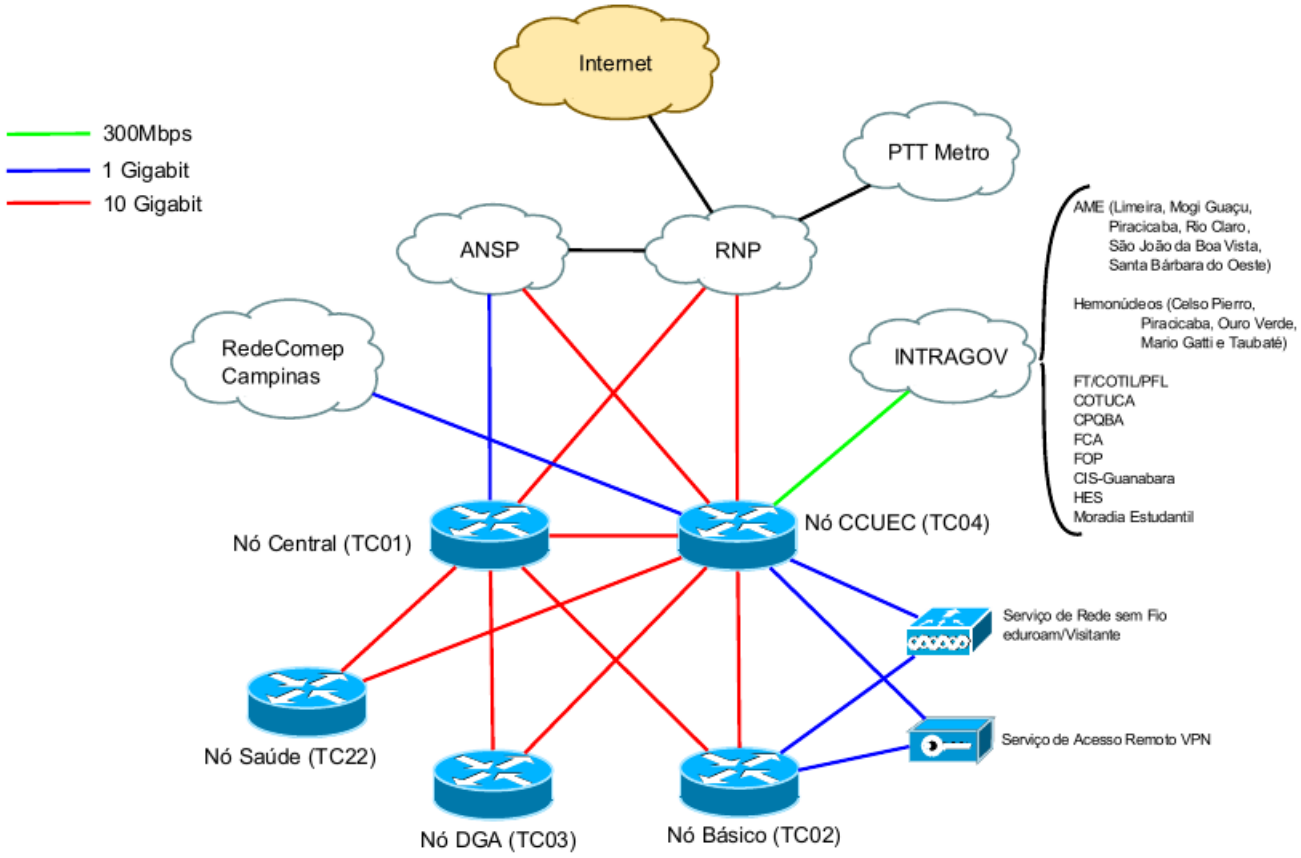
Uso de flows no tratamento de incidentes:

1º passo:

➔Coletar o tráfego nos roteadores de borda

- Protocolo utilizado: sflow (coleta por amostragem)
- A liberação foi feita de forma gradual: por roteadores e controlando a quantidade de amostras (1/2048, 1/1024, 1/512) → ajustes no ambiente: aprox. 3 meses
- Preocupações:
  - Impacto na performance dos roteadores e do computador que estava recebendo os dados

Rede de dados da Unicamp:



Uso de flows no tratamento de incidentes:

2º passo:

➔Analisar os dados gerados

- Desafios:
  - Interpretar o conjunto de dados
  - Buscar o conhecimento no assunto
  - Não gerar falso positivo → credibilidade

A análise de flows indica uma “possibilidade” de problema → não é concreto

Uso de flows no tratamento de incidentes:

2º passo:

➔Analisar os dados gerados

- Que ferramenta utilizar?

  1º opção: sflowtool + assinaturas do snort → Problema: começou a gerar muito falso positivo

  Início da parceria com o CERT.br:

  2ª opção: nfdump + nfsen + shell scripts → Relatórios diários com evidências de possíveis problemas

Uso de flows no tratamento de incidentes:

3º passo:

➔Tratar o possível problema junto ao responsável

- Maior dificuldade: temos a evidência do problema mas a certeza quem pode dar é o responsável pela rede

- Incluímos no processo de tratamento de incidentes: criamos templates, cadastro e categorização

Uso de flows no tratamento de incidentes:

Relatórios diários:

- Computadores da Unicamp que trocaram tráfego com C&C de botnets (regras de snort da Emerging Threats)

```
Date first seen          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Packets    Bytes Flows
2015-11-02 16:35:16.283     0.000 TCP     143.106.xxx.90:26944 ->    158.yyy.39.163:6667       512    29696     1
2015-11-02 17:11:43.955     0.000 TCP     143.106.xxx.90:26944 ->    158.yyy.39.163:6667       512    39424     1
2015-11-02 17:54:59.782     0.000 TCP     143.106.xxx.90:26944 ->    158.yyy.39.163:6667       512    29696     1

Summary: total flows: 3, total bytes: 98816, total packets: 1536, avg bps: 165, avg pps: 0, avg bpp: 64
Time window: 2015-11-02 15:00:00 - 2015-11-03 06:59:59
Total flows processed: 5360141, Blocks skipped: 0, Bytes read: 365835476
Sys: 3.007s flows/second: 1782233.1  Wall: 3.003s flows/second: 1784693.4
```

➔ Códigos maliciosos, servidores comprometidos e acessos a IRC

Uso de flows no tratamento de incidentes:

Relatórios diários:

- Computadores da Unicamp que mais enviaram dados (acima de 20 Gbytes)

```
Byte limit: > 20000000000 bytes
Top 20 Src IP Addr ordered by bytes:
Date first seen          Duration Proto         Src IP Addr    Flows(%)     Packets(%)       Bytes(%)         pps      bps   bpp
2015-10-31 15:00:00.134 57599.787 any   2801:8a:xxx:20::189   436402(33.5)  223.4 M(28.1)  294.1 G(47.3)     3879   40.8 M  1316
2015-10-31 15:00:00.108 57599.055 any       143.106.xxx.118    74382( 5.7)   38.1 M( 4.8)   56.2 G( 9.0)      661    7.8 M  1475
2015-10-31 15:52:46.644 51644.655 any        143.106.xxx.75    74186( 5.7)   38.0 M( 4.8)   55.3 G( 8.9)      735    8.6 M  1456
2015-10-31 15:12:31.427 56847.919 any       143.106.xxx.229    65883( 5.1)   33.7 M( 4.2)   36.3 G( 5.8)      593    5.1 M  1075
```

➔Códigos maliciosos, computadores participando de ataque DoS, servidores comprometidos e uso de P2P

Uso de flows no tratamento de incidentes:

Relatórios diários:

- Computadores da Unicamp que trocaram tráfego com destino à porta TCP/25 e que não são servidores de e-mail

Top 20 Src IP Addr ordered by bytes:

Date first seen	Duration	Proto	Src IP Addr	Flows(%)	Packets(%)	Bytes(%)	pps	bps	bpp
2015-08-19 13:35:59.100	2453.797	any	143.106.xxx.164	65(27.3)	133120(58.8)	9.5 M(29.4)	54	30974	71
2015-08-19 11:54:50.393	5005.321	any	143.106.xxx.86	158(66.4)	80896(35.7)	8.6 M(26.5)	16	13683	105
2015-08-19 09:17:55.775	19419.307	any	143.106.xxx.36	11(4.6)	5632(2.5)	7.8 M(24.2)	0	3216	1386
2015-08-19 09:52:21.543	3375.767	any	143.106.xxx.200	3(1.3)	6144(2.7)	6.4 M(19.7)	1	15074	1035
2015-08-19 08:36:34.789	0.000	any	143.106.xxx.10	1(0.4)	512(0.2)	53760(0.2)	0	0	105

➔Códigos maliciosos, abuso de formulários web, servidores comprometidos, bug de desenvolvimento de site, servidores antigos e troca de servidor

Uso de flows no tratamento de incidentes:

Relatórios diários:

- Correlação de IPs potencialmente maliciosos que acessaram os honeypots e que trocaram tráfego com algum IP da Unicamp → **análise de tendência**

Date first seen	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2015-11-23 14:01:49.242	2440.282	TCP	61.xxx.139.11:0	->	143.106.xxx.151:22	9728	1.1 M	19
2015-11-23 09:13:37.083	618.332	TCP	177.xxx.72.4:0	->	143.106.xxx.229:3389	8192	600576	16
2015-11-23 09:14:07.919	523.554	TCP	177.xxx.72.4:0	->	143.106.xxx.67:3389	5632	376832	11
2015-11-23 09:14:45.643	587.974	TCP	177.xxx.72.4:0	->	143.106.xxx.68:3389	3584	249856	7
2015-11-23 09:07:00.007	76.250	TCP	177.xxx.72.4:0	->	143.106.xxx.148:3391	1536	286720	3
2015-11-23 09:07:29.254	12.910	TCP	177.xxx.72.4:0	->	143.106.xxx.148:3389	1024	75776	2
2015-11-23 08:59:24.177	198.624	TCP	177.xxx.72.4:0	->	143.106.xxx.108:3389	1024	63488	2
2015-11-23 12:07:39.277	0.000	TCP	111.xxx.119.224:0	->	143.106.xxx.79:5363	512	29696	1
2015-11-23 10:41:07.639	0.000	TCP	117.xxx.35.25:0	->	177.8.xxx.139:23	512	39936	1
2015-11-23 14:53:09.026	0.000	TCP	78.xxx.152.94:0	->	143.106.xxx.95:21680	512	29696	1
2015-11-23 07:47:53.827	0.000	TCP	46.xxx.207.18:0	->	143.106.xxx.141:5946	512	29696	1
2015-11-23 09:52:32.708	0.000	TCP	219.xxx.180.236:0	->	143.106.xxx.41:8086	512	29696	1

Uso de flows no tratamento de incidentes:

Relatórios diários:

- Correlação de dados da Spamhaus sobre redes sequestradas, alugadas ou controladas por spammers e que trocaram tráfego com algum IP da Unicamp → **análise de tendência**

Date first seen	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2015-11-07 15:00:06.013	29901.198	TCP	185.xxx.187.10:0	->	143.106.xxx.188:3389	259072	21.8 M	506
2015-11-07 15:51:05.121	2233.557	TCP	185.xxx.187.58:0	->	143.106.xxx.148:3389	23040	1.7 M	45
2015-11-07 15:10:39.357	1485.579	TCP	185.xxx.187.10:0	->	143.106.xxx.148:3389	18944	1.2 M	37
2015-11-07 20:58:58.570	598.914	TCP	193.xxx.117.12:0	->	143.106.xxx.188:3389	4096	276992	8
2015-11-08 04:26:21.846	344.912	TCP	5.xxx.243.178:0	->	143.106.xx.166:25	3072	190464	6
2015-11-07 16:55:15.338	50260.023	TCP	193.xxx.117.207:0	->	143.106.xxx.130:5900	3072	227328	6
2015-11-07 17:29:08.960	40478.961	TCP	193.xxx.117.207:0	->	143.106.xxx.140:5900	1536	119808	3
2015-11-07 22:44:40.739	0.000	TCP	91.xxx.75.4:0	->	143.106.xxx.132:8080	512	29696	1
2015-11-07 16:53:54.362	0.000	TCP	193.xxx.116.72:0	->	143.106.xxx.37:2222	512	33792	1
2015-11-07 17:54:35.037	0.000	TCP	193.xxx.117.207:0	->	143.106.xxx.148:5900	512	35840	1
2015-11-07 16:53:53.920	0.000	TCP	193.xxx.116.72:0	->	143.106.xxx.141:2222	512	33792	1
2015-11-07 16:53:53.212	0.000	TCP	193.xxx.116.72:0	->	143.106.xxx.207:2222	512	33792	1
2015-11-08 02:35:58.862	0.000	TCP	91.xxx.75.4:0	->	143.106.xx.237:8080	512	29696	1

Estudo de caso 1) servidor comprometido

Relatório: Top Talkers

Date first seen	Duration	Proto	Src IP Addr	Flows(%)	Packets(%)	Bytes(%)	pps	bps	bpp
2015-05-23 16:08:14.231	53472.691	any	143.106.xxx.82	42335(5.7)	86.7 M(16.8)	48.5 G(16.4)	1621	7.3 M	559
2015-05-21 15:00:00.103	55550.134	any	143.106.xxx.82	31641(1.2)	64.8 M(3.6)	35.2 G(5.6)	1166	5.1 M	542
2015-05-20 15:09:25.170	57034.764	any	143.106.xxx.82	27219(1.0)	55.7 M(3.1)	29.8 G(4.5)	977	4.2 M	533
2015-05-19 15:03:04.233	57406.101	any	143.106.xxx.82	10605(0.4)	21.7 M(1.3)	10.0 G(1.8)	378	1.4 M	462

Trafego encontrado:

Date first seen	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2015-05-20 01:45:34.759	0.000	UDP	143.106.xxx.82:42826	->	67.196.xxx.108:9090	2048	1.9 M	1
2015-05-20 01:45:36.304	0.000	UDP	143.106.xxx.82:42826	->	67.196.xxx.108:9090	2048	1.9 M	1
2015-05-20 01:45:36.304	0.000	UDP	143.106.xxx.82:42826	->	67.196.xxx.108:9090	2048	1.9 M	1
2015-05-20 01:56:34.600	0.000	UDP	143.106.xxx.82:56050	->	138.128.xxx.2:9091	2048	1.1 M	1
2015-05-20 01:56:34.600	0.000	UDP	143.106.xxx.82:56050	->	138.128.xxx.2:9091	2048	1.1 M	1
2015-05-20 01:56:34.965	0.000	UDP	143.106.xxx.82:56050	->	138.128.xxx.2:9091	2048	1.1 M	1

Estudo de caso 2) computador de usuário participando de ataque DoS

```
Relatorio: Top Talkers

Date first seen          Duration Proto       Src IP Addr    Flows(%)     Packets(%)       Bytes(%)
2015-04-04 10:27:16.509 16363.468 any      143.106.xxx.yyy   612386(44.5)  313.5 M(43.2)   18.2 G(13.5)
2015-04-04 07:01:54.763 28685.213 any      143.106.xxx.zzz   443369(32.2)  227.0 M(31.3)   13.2 G( 9.8)
2015-04-04 15:00:00.035 19516.899 any      143.106.xxx.yyy    1.3 M(43.4)  686.8 M(42.0)   39.8 G(16.3)
2015-04-04 15:00:00.035 19516.749 any      143.106.xxx.zzz    1.3 M(40.8)  645.8 M(39.5)   37.5 G(15.3)
2015-04-09 07:00:00.023 28799.941 any      143.106.xxx.yyy    2.5 M(45.0)    1.3 G(40.7)    1.4 T(73.6)

Trafego encontrado:

Date first seen          Duration Proto      Src IP Addr:Port           Dst IP Addr:Port   Packets    Bytes Flows
2015-04-04 12:46:08.613     0.000 UDP     143.106.xxx.yyy:45719 ->      58.50.zzz.43:80         512    29696     1
2015-04-04 12:46:08.613     0.000 UDP     143.106.xxx.yyy:45719 ->      58.50.zzz.43:80         512    29696     1
(...)
2015-04-04 20:25:16.601     0.000 UDP     143.106.xxx.yyy:42423 ->      58.50.zzz.43:80         512    29696     1
2015-04-04 20:25:16.934     0.000 UDP     143.106.xxx.yyy:53760 ->      58.50.zzz.43:80         512    29696     1

2015-04-04 12:46:09.589     0.000 UDP     143.106.xxx.zzz:54413 ->      58.50.zzz.43:80         512    29696     1
2015-04-04 12:46:09.800     0.000 UDP     143.106.xxx.zzz:48522 ->      58.50.zzz.43:80         512    29696     1
(...)
2015-04-04 20:25:16.601     0.000 UDP     143.106.xxx.zzz:43631 ->      58.50.zzz.43:80         512    29696     1
2015-04-04 20:25:16.601     0.000 UDP     143.106.xxx.zzz:53385 ->      58.50.zzz.43:80         512    29696     1
```

Estudo de caso 3) servidor web comprometido

```
Relatorio: Top Talkers

Date first seen          Duration Proto       Src IP Addr    Flows(%)     Packets(%)       Bytes(%)
2015-02-03 15:56:25.880 35760.242 any      143.106.xxx.yyy   518368(22.7)  265.4 M(19.8)   12.5 G( 3.0)


Relatorio: CnC Botnets

Date first seen          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Packets    Bytes Flows
2015-02-09 20:20:06.262     0.000 TCP     143.106.xxx.yyy:15435 ->   154.35.zzz.201:6667       512    35840     1
2015-02-09 23:15:23.460     0.000 TCP     143.106.xxx.yyy:54870 ->   94.125.zzz.255:6667       512    41472     1
2015-02-10 00:25:00.926     0.000 TCP     143.106.xxx.yyy:54870 ->   94.125.zzz.255:6667       512    35840     1
2015-02-10 01:06:19.209     0.000 TCP     143.106.xxx.yyy:15435 ->   154.35.zzz.201:6667       512    41472     1
2015-02-10 02:32:41.375     0.000 TCP     143.106.xxx.yyy:15435 ->   154.35.zzz.201:6667       512    35840     1


A primeira conexão com o IP suspeito ocorreu em 15/11/2014:
Date first seen           Duration Proto Src IP Addr:Port        Dst IP Addr:Port   Packets  Bytes
2014-11-15 17:32:59.444 196512.120 TCP   143.106.xxx.112:60173 -> 64.32.zzz.127:80       5120  3.4 M
```

Estudo de caso 4) computador de usuário infectado com código malicioso e enviando spam

Relatório: Top SMTP Talkers

Date first seen	Duration	Proto	Src IP Addr	Flows(%)	Packets(%)	Bytes(%)	pps	bps	bpp
2015-08-19 11:54:50.393	5005.321	any	143.106.xxx.86	158(66.4)	80896(35.7)	8.6 M(26.5)	16	13683	105
2015-08-20 09:23:56.323	20162.817	any	143.106.xxx.86	612(98.1)	313344(97.1)	24.0 M(75.0)	15	9541	76
2015-08-20 15:00:18.975	721.661	any	143.106.xxx.86	29(96.7)	14848(96.7)	1.0 M(92.7)	20	11243	68
2015-09-09 09:12:57.984	20802.595	any	143.106.xxx.86	884(97.1)	452608(95.6)	37.1 M(75.6)	21	14285	82
2015-09-09 15:00:11.530	1124.480	any	143.106.xxx.86	90(77.6)	46080(65.7)	3.6 M(26.9)	40	25461	77

Tráfego encontrado:

2015-09-09 15:15:21.030	0.000	TCP	143.106.xxx.86:3433	->	173.194.yyy.26:25	512	130048	1
2015-09-09 15:15:22.325	0.000	TCP	143.106.xxx.86:3446	->	64.233.yyy.26:25	512	124928	1
2015-09-09 15:16:42.498	0.000	TCP	143.106.xxx.86:4958	->	210.152.yyy.55:25	512	29696	1
2015-09-09 15:16:49.759	0.000	TCP	143.106.xxx.86:1142	->	173.194.yyy.26:25	512	29696	1
2015-09-09 15:17:06.182	0.000	TCP	143.106.xxx.86:1448	->	98.136.yyy.26:25	512	29696	1
2015-09-09 15:18:56.010	0.000	TCP	143.106.xxx.86:2669	->	65.54.yyy.126:25	512	49152	1
2015-09-09 15:19:10.075	0.000	TCP	143.106.xxx.86:2761	->	64.233.yyy.27:25	512	32768	1

Estudo de caso 5) servidor comprometido

Relatório: Cnc Botnets

Date first seen	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2015-11-07 19:58:42.212	0.000	TCP	143.106.xxx.54:51777	->	158.xxx.39.163:6667	2048	118784	1
2015-11-07 20:28:09.113	0.000	TCP	143.106.xxx.54:51777	->	158.xxx.39.163:6667	2048	165888	1
2015-11-07 21:06:36.796	0.000	TCP	143.106.xxx.54:52955	->	158.xxx.39.163:6667	2048	118784	1

Relatório: Top SMTP Talkers

Date first seen	Duration	Proto	Src IP Addr	Flows(%)	Packets(%)	Bytes(%)	pps	bps	bpp
2015-12-04 12:03:58.182	10541.397	any	143.106.xxx.54	884(99.4)	1.8 M(99.9)	136.8 M(99.3)	171	103797	75
2015-12-04 15:00:12.379	3477.309	any	143.106.xxx.54	412(94.7)	843776(98.4)	56.0 M(91.9)	242	128949	66

Estudo de caso 6) servidor comprometido

Evidencia do problema:

```
Jun 19 07:20:20.793954 143.106.xxx.12.37975 > xxx.xxx.xxx.231.22
Jun 19 07:20:20.794012 143.106.xxx.12.56113 > xxx.xxx.xxx.242.22
Jun 19 07:20:20.794055 143.106.xxx.12.46680 > xxx.xxx.xxx.236.22
Jun 19 07:20:20.794117 143.106.xxx.12.35264 > xxx.xxx.xxx.204.22
Jun 19 07:20:20.794159 143.106.xxx.12.59225 > xxx.xxx.xxx.208.22
```

Investigação:

- Esse servidor só aceitava conexão de IPs da rede da Unicamp
- Invasor tinha a senha de uma conta com privilégio de root
- Todos os logs de auditoria foram apagados

Estudo de caso 6) servidor comprometido

Correlação de dados:

Date first seen	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2015-06-19 04:06:03.899	0.000	TCP	143.106.yyy.222:33002	->	143.106.xxx.12:22	512	35840	1
2015-06-19 04:07:36.193	0.000	TCP	143.106.yyy.222:33002	->	143.106.xxx.12:22	512	35840	1
2015-06-19 04:07:57.028	0.000	TCP	143.106.yyy.222:33002	->	143.106.xxx.12:22	512	35840	1
(...)								
2015-06-19 05:54:44.273	0.000	TCP	143.106.yyy.222:33235	->	143.106.xxx.12:22	512	35840	1
2015-06-19 06:00:55.121	0.000	TCP	143.106.yyy.222:33235	->	143.106.xxx.12:22	512	35840	1
2015-06-19 06:01:54.022	0.000	TCP	143.106.yyy.222:33235	->	143.106.xxx.12:22	512	60416	1

- Na análise dos artefatos foi identificado 1 IP que era do repositório dos códigos maliciosos do atacante

Correlação de dados:

Date first seen	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2015-06-23 16:39:32.924	0.000	TCP	5.231.zzz.150:80	->	143.106.xxx.59:52446	512	777216	1
2015-06-23 16:39:33.118	0.000	TCP	5.231.zzz.150:80	->	143.106.xxx.59:52446	512	777216	1
2015-06-23 16:39:33.144	0.000	TCP	5.231.zzz.150:80	->	143.106.xxx.59:52446	512	777216	1
2015-06-23 16:39:33.214	0.000	TCP	5.231.zzz.150:80	->	143.106.xxx.59:52446	512	777216	1
2015-06-23 16:39:33.398	0.000	TCP	5.231.zzz.150:80	->	143.106.xxx.59:52446	512	777216	1
2015-06-23 16:39:33.963	0.000	TCP	5.231.zzz.150:80	->	143.106.xxx.59:52446	512	777216	1

Estudo de caso 7) switches comprometidos

Evidência do problema:
Notificação da Spamhaus que 2 IPs estavam infectados e participando de uma botnet.

Correlação de dados:

Date first seen	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2015-10-05 05:43:26.887	0.000	TCP	14.xxx.167.157:30430	->	143.106.xxx.190:22	512	46592	1
2015-10-05 16:48:17.011	0.000	TCP	195.xxx.56.56:59151	->	143.106.xxx.190:22	512	70656	1
2015-10-05 23:36:57.826	0.000	TCP	189.xxx.148.161:42938	->	143.106.xxx.190:23	512	35840	1
2015-10-06 09:45:39.707	0.000	TCP	112.xxx.37.68:50677	->	143.106.xxx.190:22	512	62464	1
2015-10-06 11:43:52.193	0.000	TCP	93.xxx.126.206:53544	->	143.106.xxx.190:23	512	39936	1
2015-10-06 21:00:43.846	0.000	TCP	5.xxx.8.132:50659	->	143.106.xxx.190:22	512	35840	1
2015-10-05 00:46:54.776	0.000	TCP	119.xxx.197.196:49264	->	143.106.xxx.189:23	512	39936	1
2015-10-05 10:32:01.795	0.000	TCP	80.xxx.66.235:58690	->	143.106.xxx.189:23	512	39936	1
2015-10-06 18:27:16.612	0.000	TCP	178.xxx.134.197:41171	->	143.106.xxx.189:22	512	35840	1
2015-10-07 03:16:00.284	0.000	TCP	144.xxx.118.170:41896	->	143.106.xxx.189:22	512	101376	1
2015-10-07 09:06:16.070	0.000	TCP	123.xxx.116.66:40374	->	143.106.xxx.189:22	512	39936	1

Estatísticas de detecção por flows:

Total de tickets gerados até 30/11/2015: 212

155 – detecções corretas (73%)

57 – falso positivo (27%)

Com o tempo, o que mudou?

- Maior percepção do que era ou não um problema
- Ajustes nas configurações da ferramenta
- A eficácia da ferramenta aumenta com o tempo e com ajustes
- Melhor conhecimento do comportamento da rede
- Cautela

Sucesso do projeto:

- Todas as ferramentas são código livre
- Trabalho em equipe
- Perfil do técnico responsável pela análise dos dados
- A detecção é baseada no comportamento do tráfego e não em assinaturas

Uso de flows no tratamento de incidentes:

Vocês podem compartilhar os scripts?

➔ Sim

Como solicitar?

➔ E-mail para “security@unicamp.br”

Agradecimentos:

Alexandre Berto Nogueira
Diretoria de Redes e Segurança do Centro de Computação

Klaus Steding-Jessen
CERT.br

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

CCUEC

Perguntas?

http://www.security.unicamp.br
security@unicamp.br

Apoio:

AFPU
Agência para a Formação Profissional da Unicamp