UNICAMP

nic.br | cert.br

4º Fórum Brasileiro de CSIRTs

17 e 18 de setembro de 2015

São Paulo, SP

Uso de Flows no Tratamento de Incidentes - Estudo de Caso do CSIRT Unicamp

Daniela Barbetti
daniela@unicamp.br

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:

Criado em 1.999:

- Ser o ponto de contato para notificação de incidentes.
- Responder e tratar os incidentes de segurança da informação do domínio “unicamp.br”
- Estabelecer parceria com os Administradores de Redes e Sistemas das Unidades/Órgãos
- Conscientizar a comunidade universitária sobre a importância da segurança da informação

Sobre o CSIRT Unicamp:

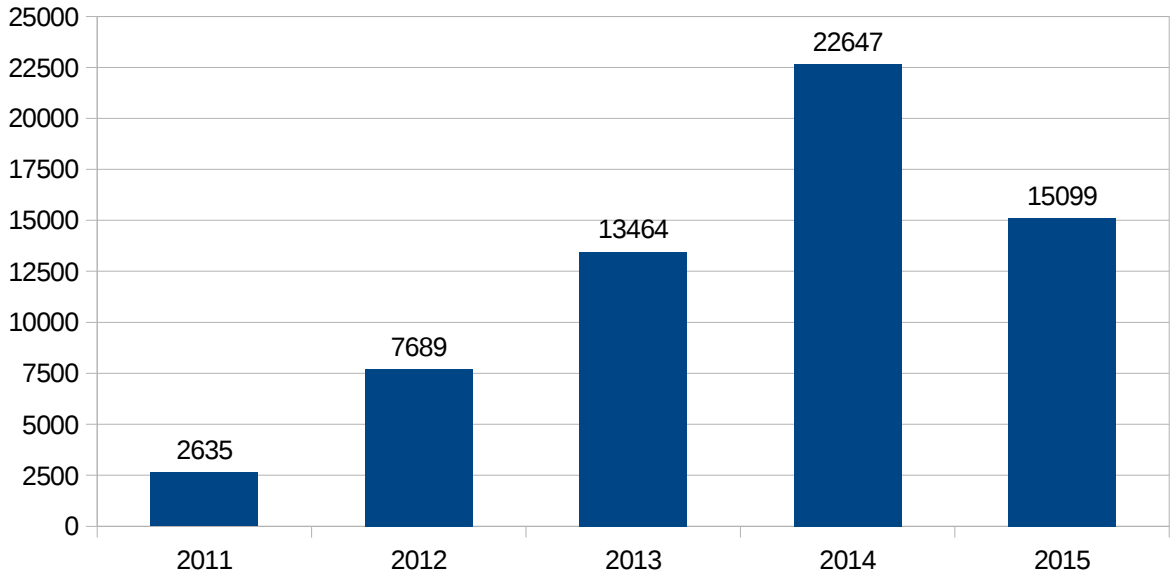
Atividades atuais:

- Resposta e tratamento de incidentes de segurança
- Análise de flows
- Testes de detecção de vulnerabilidades
- Palestras de conscientização para usuários finais
- Site e ambiente computacional do CSIRT
- Certificados digitais (projeto ICPedu/RNP)

Sobre o CSIRT Unicamp:

Atividades atuais:

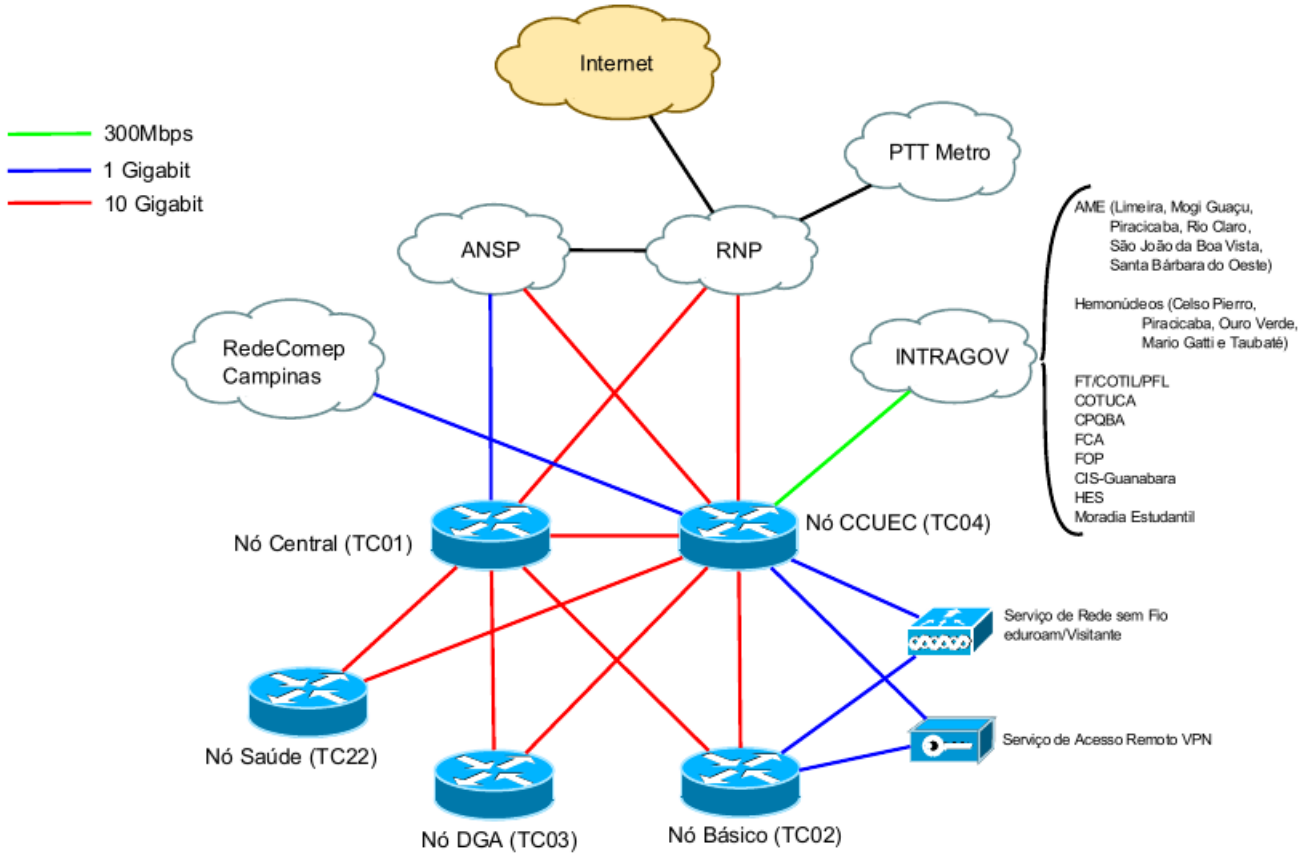
- Atendimentos entre 2011 e 14/09/2015:



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

Rede de dados da Unicamp:



Uso de flows no tratamento de incidentes:

Como tudo começou?

- Incentivo partiu do 2º Fórum de CSIRTs em set/2013

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

- Os mesmos dados podem ser utilizados pelas duas equipes 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?

- Flow é uma sumarização de pacotes de rede
- 1 flow = 1 sumário com vários pacotes de rede

Para que serve?

- 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

Voce sabe o que está saindo da sua rede?

Uso de flows no tratamento de incidentes:

1º passo:

➔Coletar o tráfego nos roteadores de borda (Brocade)

- 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

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:

➔Notificar os adms de TI das Unidades

- Maior dificuldade: temos a evidência do problema mas a certeza quem pode dar é o responsável na Unidade
- Divulgação do serviço explicando o propósito e pedindo a colaboração para identificação se o tráfego era legítimo, malicioso ou erro de configuração
- Incluímos no processo de tratamento de incidentes: criamos templates, cadastro e categorização

Uso de flows no tratamento de incidentes:

Relatórios diários:

- Correlação de IPs potencialmente maliciosos que acessaram os nossos honeypots e que trocaram tráfego com algum IP da Unicamp

- Correlação de redes sequestradas, alugadas para spam ou controladas por spammers ou cyber-crime listadas pela Spamhaus e que trocaram tráfego com algum IP da Unicamp

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
- Computadores que trocaram tráfego com C&C de botnets
- Computadores que mais trafegam dados (acima de 10 Gbytes)

O tráfego deve ser analisado pois os relatórios indicam a possibilidade de problema.

1º estudo de caso: acessos a C&C botnets

Relatório: CnC Botnets

Date first seen	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2014-10-21 15:53:28.311	0.000	TCP	143.106.xxx.18:59214	->	83.170.zzz.249:6667	512	49152	1
2014-10-21 16:53:27.698	0.000	TCP	143.106.xxx.18:59214	->	83.170.zzz.249:6667	512	49152	1
2014-10-21 16:57:59.123	0.000	TCP	143.106.xxx.166:50973	->	91.217.zzz.44:6667	512	35840	1
2014-10-21 19:52:14.669	0.000	TCP	143.106.xxx.18:59214	->	83.170.zzz.249:6667	512	35840	1
2014-10-21 20:16:43.087	0.000	TCP	143.106.xxx.166:50973	->	91.217.zzz.44:6667	512	48640	1
2015-08-26 15:56:49.665	0.000	TCP	143.106.xxx.45:55229	->	158.69.yy.163:6667	512	29696	1
2015-08-27 06:52:36.423	0.000	TCP	143.106.xxx.45:57440	->	158.69.yy.163:6667	512	29696	1

Situações encontradas:

- IPs acessando IRC (falso positivo)
- Servidores web comprometidos
- Computadores infectados com trojan

2º estudo de caso: computador de usuário 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

3º estudo de caso: computador de usuário infectado com código malicioso

Relatorio: Spamhaus DROP

Date first seen	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2015-03-07 01:19:48.993	4785.756	TCP	91.236.zzz.174:0	->	143.106.xxx.yyy:3389	42496	3.8 M	83
2015-03-10 07:48:43.815	4884.242	TCP	91.236.zzz.17:0	->	143.106.xxx.yyy:3389	42496	3.4 M	83
2015-03-10 22:11:03.247	1323.547	TCP	91.236.zzz.174:0	->	143.106.xxx.yyy:3389	9728	761856	19
2015-03-17 20:52:48.539	3446.829	TCP	195.238.zzz.164:0	->	143.106.xxx.yyy:3389	22016	2.1 M	43
2015-03-18 14:45:13.503	843.160	TCP	77.91.zzz.102:0	->	143.106.xxx.yyy:3389	10240	1.2 M	20

Date first seen	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2015-03-10 22:28:49.091	0.000	TCP	91.236.zzz.174:57967	->	143.106.xxx.yyy:3389	512	29696	1
2015-03-10 22:30:10.386	0.000	TCP	91.236.zzz.174:65170	->	143.106.xxx.yyy:3389	512	29696	1
2015-03-10 22:30:33.614	0.000	TCP	91.236.zzz.174:51168	->	143.106.xxx.yyy:3389	512	29696	1
2015-03-10 22:30:48.537	0.000	TCP	91.236.zzz.174:52096	->	143.106.xxx.yyy:3389	512	29696	1
2015-03-10 22:32:40.563	0.000	TCP	91.236.zzz.174:61563	->	143.106.xxx.yyy:3389	512	29696	1
2015-03-10 22:33:06.794	0.000	TCP	91.236.zzz.174:64133	->	143.106.xxx.yyy:3389	512	29696	1

4º estudo de caso: 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
```

→ Ambiente apache alterado dentro de um /proc que inicializava um malware que fazia a conexão com o C&C

5º estudo de caso: 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
```

6º estudo de caso: DNS recursivo aberto

Evidencia do problema:

```
Jun 14 14:35:43.650604 143.106.xxx.yyy.53 > xxx.xxx.xxx.85.80: 31095 40/0/4 A 77.222.56.187,
NS ns3.spaceweb.pro., NS ns1.spaceweb.ru., NS ns2.spaceweb.ru., NS ns4.spaceweb.pro., SOA,
MX mx2.spaceweb.ru. 20, MX mx1.spaceweb.ru. 10,
TXT "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx25",
TXT "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx26",
TXT "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx27",
TXT "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx28",
TXT "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx29",
TXT[|domain]
```

Trafego encontrado:

Date first seen	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2015-06-15 11:11:58.661	166.328	UDP	143.106.xxx.82:53	->	92.53.yyy.85:80	7168	10.9 M	14
2015-06-15 11:12:02.627	158.354	UDP	92.53.yyy.85:80	->	143.106.xxx.82:53	6656	565760	13
2015-06-15 15:22:51.222	0.000	UDP	143.106.xxx.82:53	->	121.40.yyy.104:18652	512	138240	1
2015-06-15 23:37:19.689	0.000	UDP	182.254.yyy.155:25818	->	143.106.xxx.82:53	512	44032	1
2015-06-16 10:13:15.283	0.000	UDP	143.106.xxx.82:53	->	183.61.yyy.211:33670	512	123904	1
2015-06-15 12:59:27.008	0.000	UDP	143.106.xxx.82:49342	->	69.28.yy.170:53	512	41984	1
2015-06-16 08:55:07.804	0.000	UDP	143.106.xxx.82:53	->	101.71.yy.95:63418	512	123904	1

→ Admin afirmava que estava bloqueado no firewall

7º estudo de caso: ataque de amplificação de SSDP

Evidência do problema:

Horario: 2015-06-19 01:16:16
IP: 143.106.xx.137
Protocolo: UDP
Infeccao : ddos-participant-ssdp-amplifier
Aplicacao: ssdp_reflection

Trafego encontrado:

Date first seen	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2015-06-21 06:13:44.461	25852.174	UDP	143.106.xx.137:1900	->	117.27.yyy.15:80	258048	89.9 M	126
2015-06-22 00:18:36.164	22203.189	UDP	143.106.xx.137:1900	->	23.234.yy.217:80	247808	86.9 M	121
2015-06-21 00:45:54.773	18186.200	UDP	143.106.xx.137:1900	->	117.27.yyy.15:5988	149504	51.8 M	73
2015-06-20 01:04:07.975	179672.328	UDP	143.106.xx.137:1900	->	60.214.yyy.122:80	112640	39.5 M	55
2015-06-19 02:35:37.748	77761.932	UDP	143.106.xx.137:1900	->	183.60.yyy.226:27035	53248	18.7 M	26
2015-06-18 16:19:39.383	7870.728	UDP	143.106.xx.137:1900	->	184.154.yy.69:53	45056	15.7 M	22
2015-06-19 08:23:55.329	18372.637	UDP	143.106.xx.137:1900	->	58.221.yy.101:80	45056	16.0 M	22
2015-06-19 16:06:21.974	2343.972	UDP	143.106.xx.137:1900	->	189.79.yy.16:27019	38912	13.5 M	19

→ não tínhamos os logs do reclamante

8º estudo de caso: 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 IP só aceitava conexão de máquinas da rede da Unicamp
- Invasor tinha a senha de uma conta com privilégio de root
- Todos os logs do servidor foram apagados

8º Estudo de caso: 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

Outros problemas identificados:

- Servidores web enviando spam
- Servidores web comprometidos
- Computadores com alto tráfego indicando uso de P2P
- Vários erros de configuração

→ Abril/2015: primeiros alertas com tráfego IPv6

→ Quando os admins sabem que vai acontecer algum comportamento diferente na rede: avisam o CSIRT antecipadamente

Estatísticas de detecção por flows:

Mês	Total de detecções	Detecção Correta		Falso Positivo	
		Qtde	%	Qtde	%
out	20	8	40	12	60
nov	34	15	44	19	56
dez	20	5	25	15	75
jan	9	5	56	4	44
fev	12	12	100	0	0
mar	14	13	93	1	7
abr	15	15	100	0	0
mai	19	19	100	0	0
jun	8	7	88	1	12
jul	11	11	100	0	0
ago	15	15	100	0	0

Estatísticas de detecção por flows:

- A detecção por flows foi correta? Foi algo anormal?

- Qual a diferença a partir de fevereiro de 2015?

  - Maior percepção do que era ou não um problema
  - Ajustes nas configurações da ferramenta
  - Melhor conhecimento da rede
  - Cautela

Importante:

As 177 detecções foram "EXCLUSIVAMENTE" por flows !

Próximos passos:

- Incentivar a coleta de flows nos roteadores das Unidades/Órgãos
- Propor mudanças em algumas políticas do backbone

Lições aprendidas:

- Melhor conhecimento da rede e de seu comportamento
- Percepção que determinados comportamentos geram ações preventivas
- A eficácia aumenta com o tempo e com ajustes

Agradecimentos:

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

Klaus Steding-Jessen
CERT.br

Perguntas?

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

Apoio:
AFPU
Agência para a Formação Profissional da Unicamp