

Aspectos de segurança na conectividade da rede acadêmica



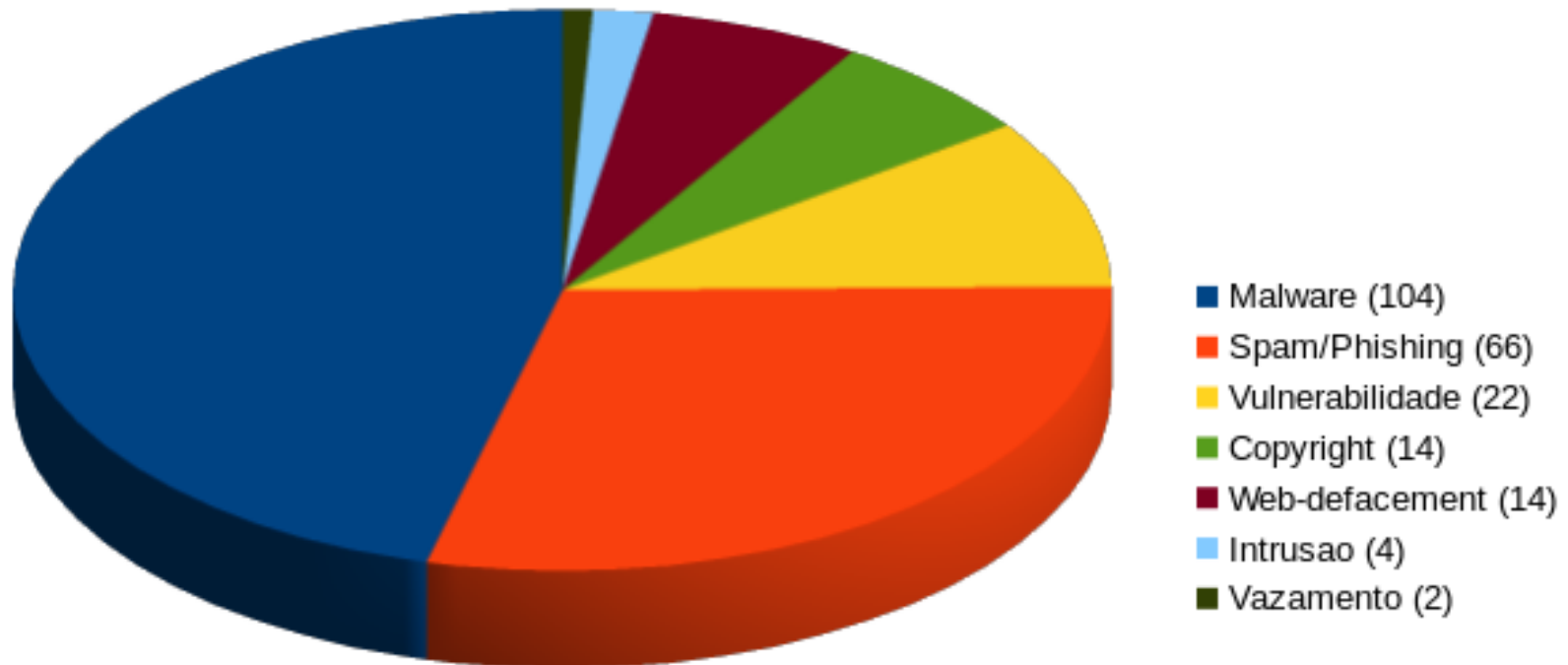
Italo Valcy <italovalcy@ufba.br>
25/Set/2017, VII WTR do PoP-BA

Cenário atual

- Boa conectividade de rede na região metropolitana, links melhores mas ainda não suficientes
 - Links de 4, 8, 10, 20, 100 Mbps... 1 Gbps, ...
- Grande volume de ataques de códigos maliciosos
 - Vírus, Botnet, Ransomware
- Algumas situações de má utilização da banda
- Serviços Federados, potencializando os danos causados por contas comprometidas

Incidentes de Segurança por Tipo na UFBA

Dados até Ago/2017



- Muitos incidentes de malware
- Phishing/Spam mais problemático que malware
- Alto consumo de banda com torrent/copyright
- Necessidade de processos de gestão de vuln.

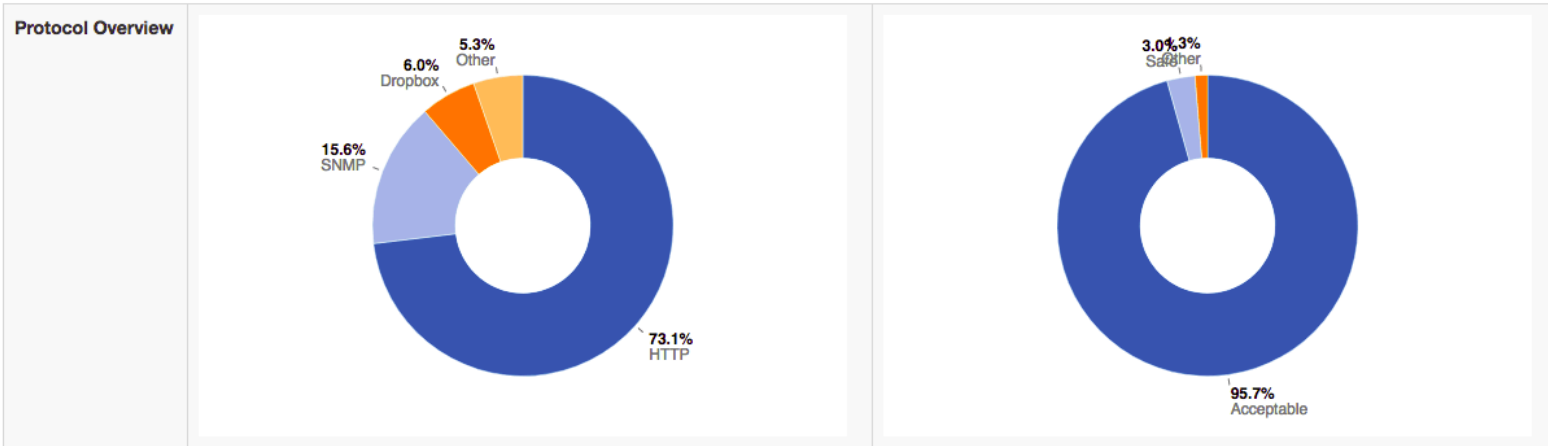
Estimar Perfil de Tráfego da rede

- Qual o perfil de tráfego total ao longo do dia, semana, mês? (bps, pps, con/sec)
- Tráfego broadcast, tcp, udp, icmp, tcp-syn
- Portas mais acessadas
- Aplicações mais utilizadas
- Provedores mais acessados

Ferramenta ntop-ng

ntop Home Alerts Flows **Hosts** Devices Interfaces Settings Power

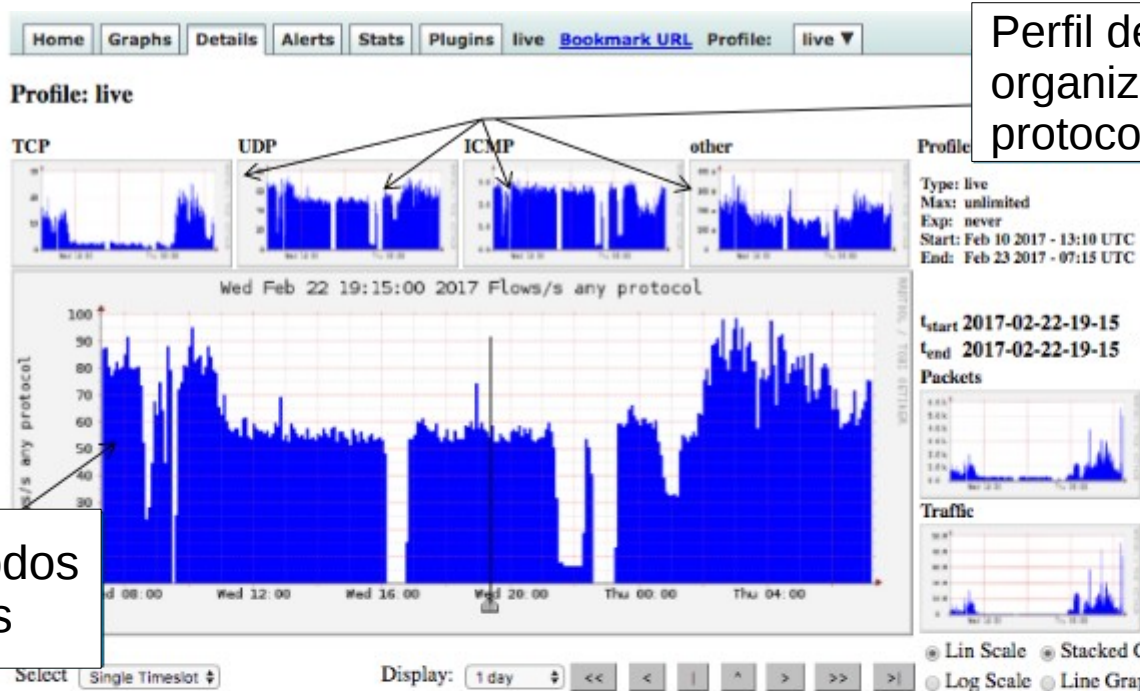
Host: 192.168.1.11 Home Traffic Packets Ports Peers ICMP **Protocols** Activity DNS HTTP Flows SNMP Talkers Alerts



Direction ▾

Application Protocol	Duration	Sent	Received	Breakdown	Total
Total	2 h, 10 min, 15 sec	31.02 MB	14.13 MB	Sent Rcvd	45.15 MB
Amazon	5 sec	66 Bytes	60 Bytes	Sent Rcvd	126 Bytes 0 %
DHCP	30 sec	2 KB	2 KB	Sent Rcvd	4.01 KB 0.01 %
DNS	10 min, 35 sec	27.32 KB	57.11 KB	Sent Rcvd	84.43 KB 0.18 %
Dropbox	39 min, 5 sec	2.22 MB	492.97 KB	Sent Rcvd	2.7 MB 5.99 %
Facebook	15 sec	456 Bytes	1.46 KB	Sent Rcvd	1.91 KB 0 %
Github	23 min, 55 sec	23 KB	31.53 KB	Sent Rcvd	54.53 KB 0.12 %

Nfsen



Perfil de tráfego organizado por protocolo

Período de tempo dos fluxos observados

Gráfico de todos os protocolos

Statistics timeslot Feb 22 2017 - 19:15

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
gw	56.0 /s	2.2 /s	51.0 /s	2.6 /s	0.2 /s	282.6 /s	107.8 /s	124.6 /s	47.9 /s	2.3 /s	284.3 kb/s	116.0 kb/s	133.1 kb/s	34.0 kb/s	1.1 kb/s
TOTAL	56.0 /s	2.2 /s	51.0 /s	2.6 /s	0.2 /s	282.6 /s	107.8 /s	124.6 /s	47.9 /s	2.3 /s	284.3 kb/s	116.0 kb/s	133.1 kb/s	34.0 kb/s	1.1 kb/s

Equipamentos monitorados

Opções estendidas Visualização dos fluxos

Processing

Filter: gw

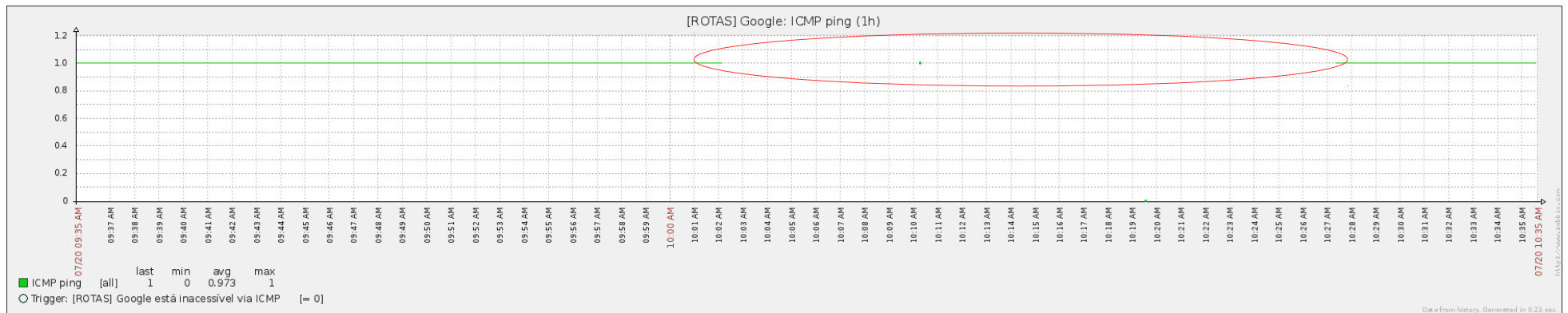
Options:

- List Flows Stat TopN
- Top: 10
- Stat: Any IP Address order by flows
- Limit: Packets > 0 -
- Output: /IPv6 long

Clear Form process

Estudo de caso 1

- Tráfego de syn-flood que provocou negação de serviço em alguns equipamentos de rede

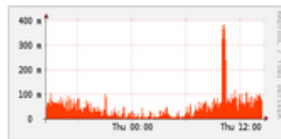


Estudo de caso 1

- Tráfego de syn-flood que provocou negação de serviço em alguns equipamentos de rede

Profile: live

TCP



UDP



ICMP



other



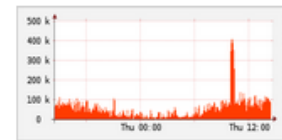
Profileinfo:

Type: live
Max: unlimited
Exp: never
Start: Nov 01 2015 - 01:00 -03
End: Jul 20 2017 - 14:30 -03

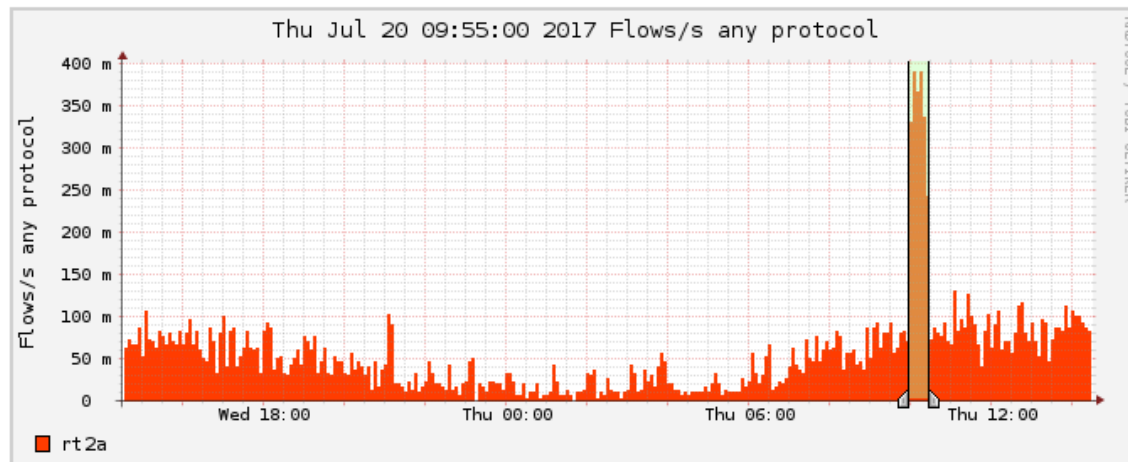
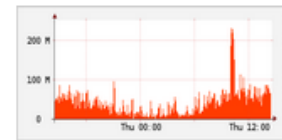
tstart 2017-07-20-09-55

tend 2017-07-20-10-25

Packets



Traffic



Select Time Window Display: 1 day

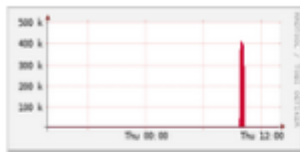
Lin Scale Stacked Graph
 Log Scale Line Graph

Estudo de caso 1

- Tráfego de syn-flood que provocou negação de serviço em alguns equipamentos de rede

Profile: live-synflood

TCP



UDP



ICMP

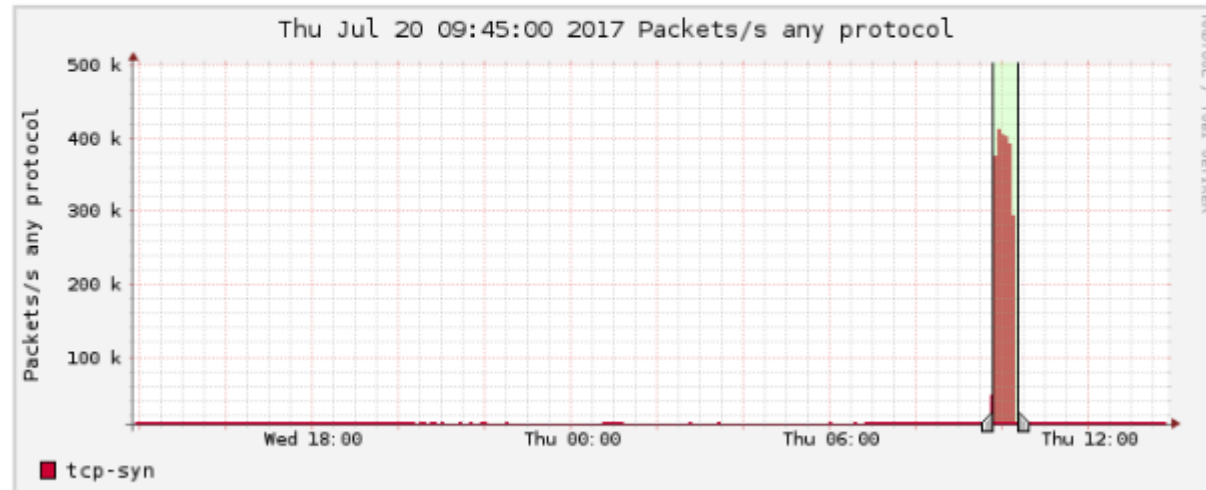


other



Profileinfo:

Type: continuous / shadow
Max: unlimited
Exp: never
Start: Sep 01 2016 - 00:00 BRT
End: Jul 20 2017 - 13:50 BRT



t_{start} 2017-07-20-09-45
t_{end} 2017-07-20-10-20

Flows



Traffic



Select Time Window Display: 1 day << < | ^ > >> >|

Lin Scale Stacked Graph
 Log Scale Line Graph

Estudo de caso 1

- Tráfego de syn-flood que provocou negação de serviço em alguns equipamentos de rede

```
** nfdump -M /var/lib/sflow/ [redacted] fba -T -R 2017/07/20/nfcpad.201707200945:2017/07/20/nfcpad.2017072010
nfdump filter:
(( ipnet [redacted] ) and (
proto tcp and flags S and not flags AFRPU
))
```

Top 10 IP Addr ordered by flows:

Date first seen	Duration	Proto	IP Addr	Flows(%)	Packets(%)	Bytes(%)	pps	bps	bpp
2017-07-20 09:46:30.555	1926.102	any	10. [redacted] 7	701399(68.3)	179.6 M(25.5)	12.2 G(26.5)	93223	50.7 M	68
2017-07-20 09:45:51.363	2074.257	any	200.12 [redacted] 2	283121(27.6)	506.2 M(72.0)	32.4 G(70.5)	244048	125.1 M	64
2017-07-20 09:45:00.043	2399.936	any	200.12 [redacted] 7	18262(1.8)	4.7 M(0.7)	382.3 M(0.8)	1947	1.3 M	81
2017-07-20 09:45:00.043	2399.936	any	190.210 [redacted] 1	17971(1.8)	4.6 M(0.7)	377.2 M(0.8)	1916	1.3 M	82
2017-07-20 09:45:00.312	2395.238	any	200.128 [redacted] 5	2206(0.2)	582656(0.1)	46.1 M(0.1)	243	154107	79
2017-07-20 09:45:04.421	2278.820	any	2801:86.. [redacted] 0	1326(0.1)	838656(0.1)	66.1 M(0.1)	368	231978	78
2017-07-20 09:47:06.765	2189.254	any	200.12 [redacted] 8	1100(0.1)	1.7 M(0.2)	108.0 M(0.2)	768	394779	64
2017-07-20 09:50:28.308	1685.303	any	200.128 [redacted] 5	1069(0.1)	1.6 M(0.2)	104.3 M(0.2)	964	495159	64
2017-07-20 09:50:27.628	1896.962	any	200.12 [redacted] 8	1063(0.1)	1.6 M(0.2)	103.8 M(0.2)	851	437553	64
2017-07-20 09:50:29.735	1686.130	any	200.12 [redacted] 9	1063(0.1)	1.6 M(0.2)	104.5 M(0.2)	965	496039	64

Summary: total flows: 1026490, total bytes: 46.0 G, total packets: 703.0 M, avg bps: 153.3 M, avg pps: 292926, avg bpp: 65

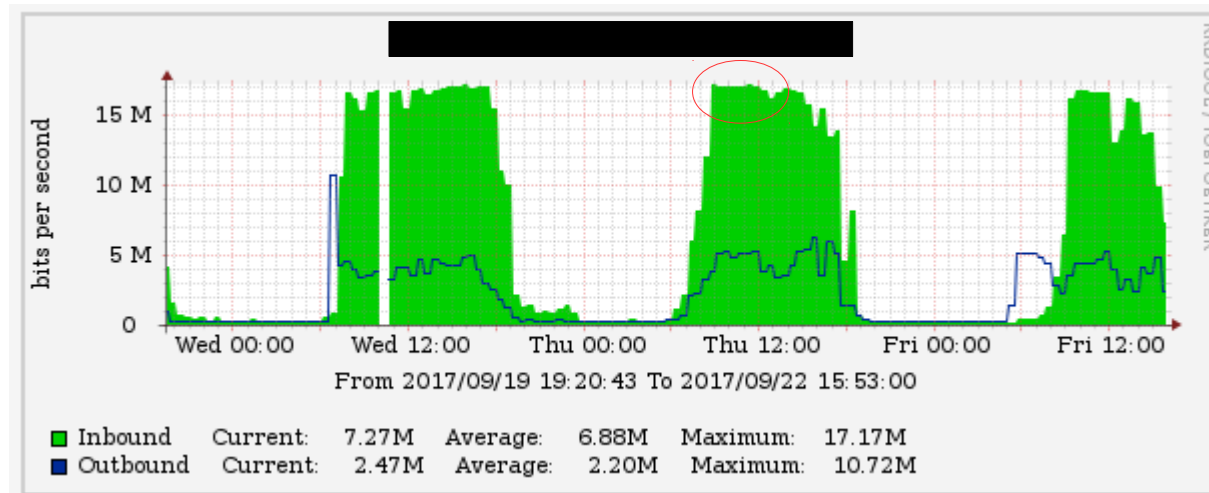
Time window: 2017-07-20 09:45:00 - 2017-07-20 10:24:59

Total flows processed: 2517615, Blocks skipped: 0, Bytes read: 242367548

Sys: 0.508s flows/second: 4955632.6 Wall: 0.509s flows/second: 4940723.8

Estudo de caso 2

- Download de conteúdo protegido por direitos autorais com alto consumo de banda



Estudo de caso 3

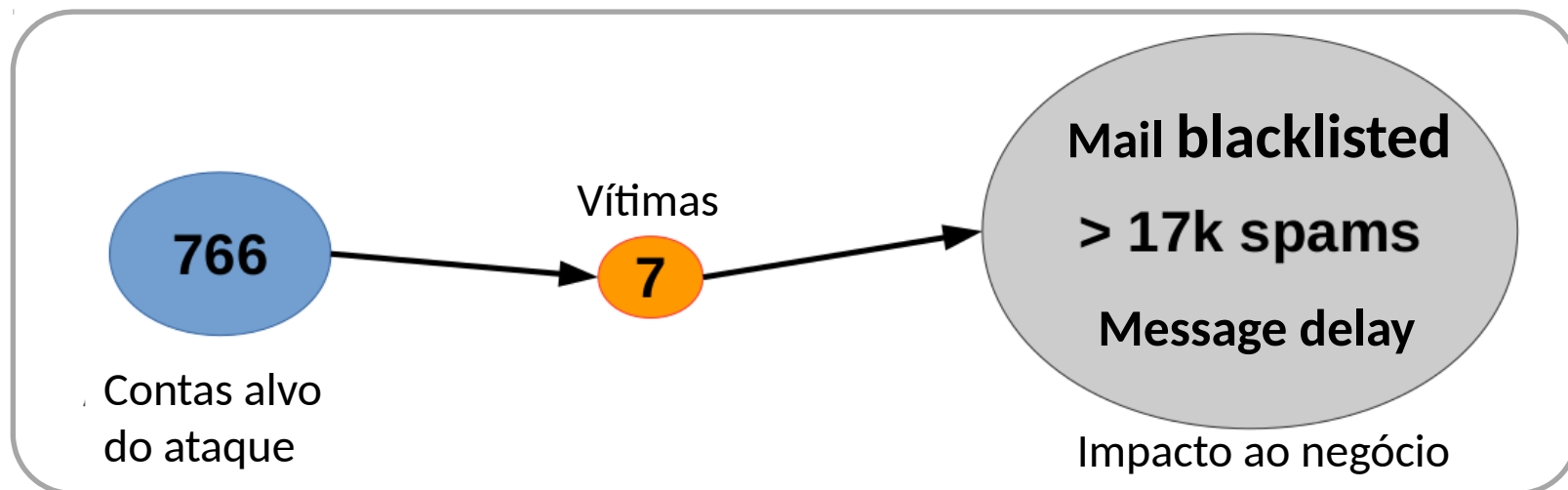
- Consumo de banda para atualização de sistemas ou ferramentas administrativas

Top 50 Most Visited Sites

#	Website	Category	Requests
1	a2f6a41 [REDACTED].e.com.	Information Technology	1,077,149
2	a2f6a41 [REDACTED].e.com.	Information Technology	1,038,046
3	au.download.windowsupdate.com	Information Technology	717,826
4	clients3.google.com	Search Engines and Portals	217,973

Comprometimento de contas

- Ocasionam diversos tipos de ataques na organização, mais comuns: phishing/spam
 - Serviços Federados (CAFe, Edugain)
- Estudo de caso: phishing ocorrido no início desse ano



Código malicioso

← ⓘ 🔒 | https://ip.team-cymru.org

TEAM CYMRU Our Insight Our Initiatives Dragon News Who We Are

YOUR IP: 177.██████████202

Information about your IP address

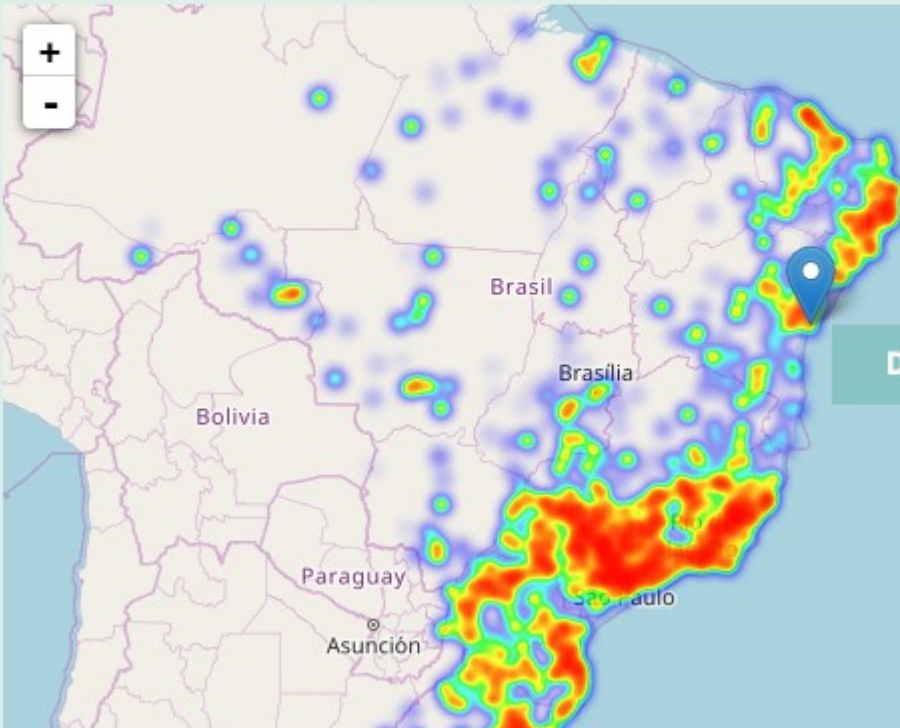
Status	No malware reported on your IP	
PTR	1██████████	mic.adslgvt.net.br
AS	18881	
As Name	TELEFÔNICA BRASIL S.A, BR	
Country	Brazil	
Netblock	177.99.32.0/19	

Country ranking based on malicious IP addresses reported

Rank	Country	Change since 30 days
1	China	↓ -15%
2	Brazil	↓ -20%
3	Russian Federation	↓ -30%
4	United States of America	↑ 2%

Possible malware infection? Click [here](#) for more help

Heatmap showing infected IPs in Brazil



Código malicioso

Segurança

Brasil é um dos países mais suscetíveis a ataques da botnet Mirai

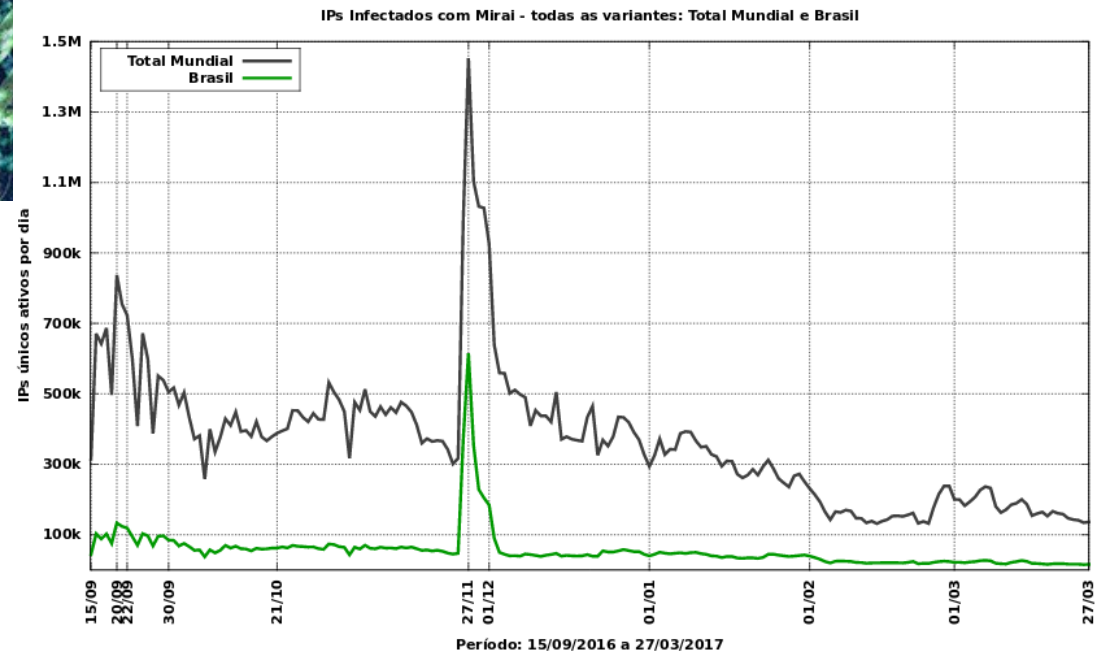
Da CIO Brasil

24/02/2017 - 10h05

Tweet 18 Share 57 G+ Flip Imprima Mais +

Dados da Kaspersky Lab mostram cerca de 500 ataques DDoS à sistemas únicos agora em 2017. Mercados emergentes estão particularmente em risco

Dados dos sensores do CERT.br: IPs únicos infectados com Mirai, por dia

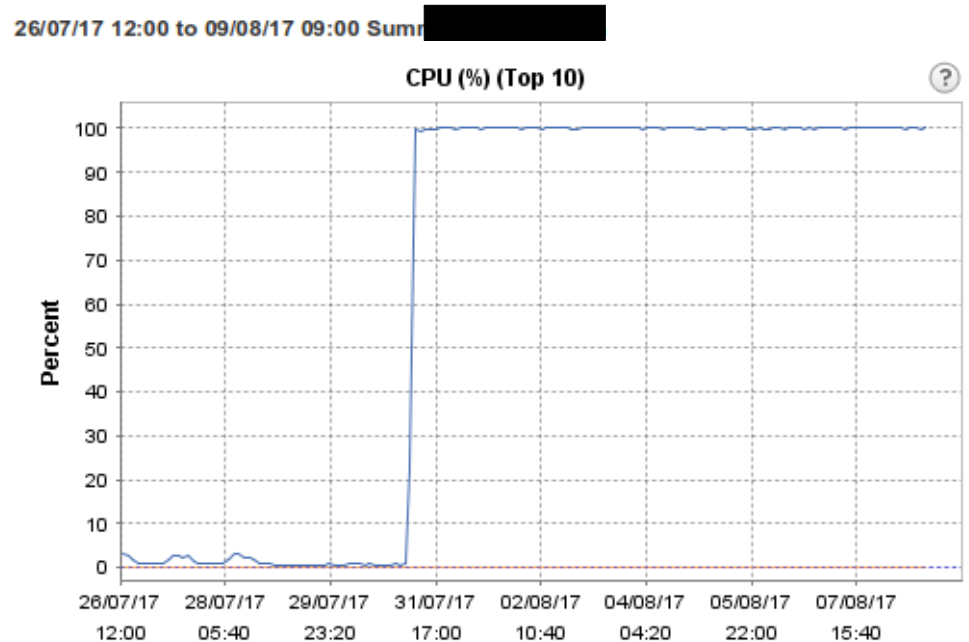
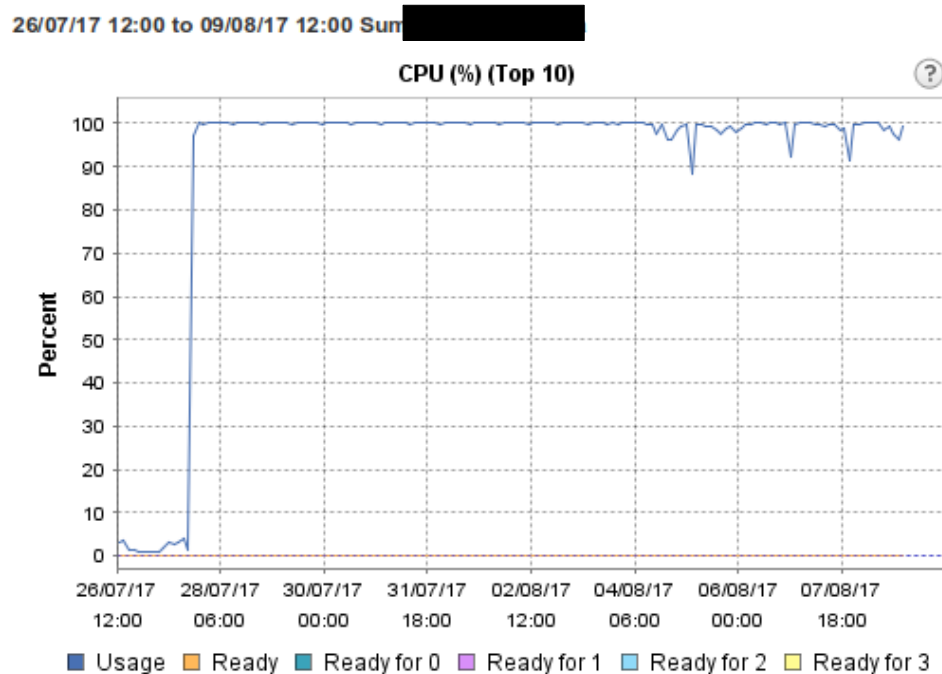


Código malicioso

- Casos de botnets em IoT tem se tornado frequentes
 - Infectam DVRs, CCTVs, roteadores domésticos
- Malware se propaga geralmente via Telnet
- Exploram senhas fracas ou padrões do fabricante
- Foco em dispositivos com versões padrões
- Temos acompanhado as atividades maliciosas em dispositivos IoT, porém sem casos de exploração

Código malicioso

- Estudo de caso: máquina infectada e usada para mineração de bitcoin



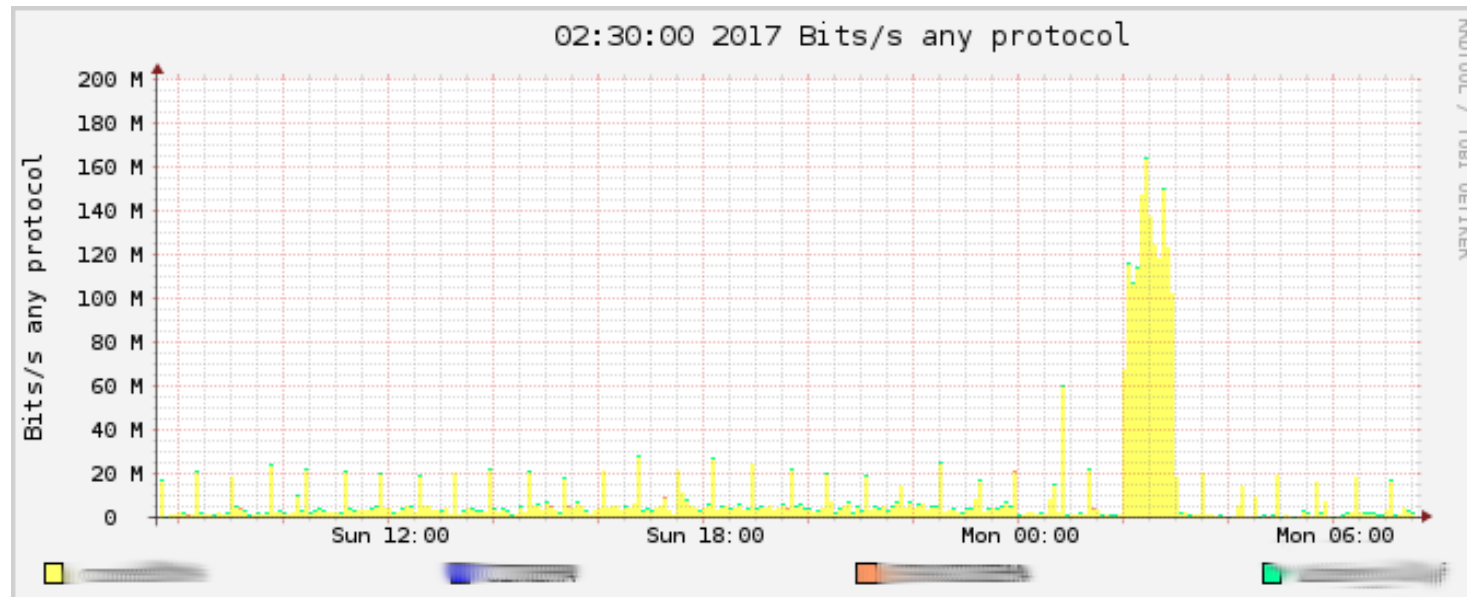
Vulnerabilidade equipamentos de VC

- Equipamentos de utilização eventual e configurados em redes sem proteção
- Configurações padrões permitindo diversos protocolos de gerencia
 - Telnet, SNMP, HTTP/HTTPS, ...

```
italovalcy@gonzaga ~/Desktop> snmpwalk -v2c -c public 200.128 )
iso.3.6.1.2.1.1.1.0 = STRING: "\"Videoconferencing Device\""
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.2684.1.1
iso.3.6.1.2.1.1.3.0 = Timeticks: (34160) 0:05:41.60
iso.3.6.1.2.1.1.4.0 = STRING: "\"IT Administrator\""
iso.3.6.1.2.1.1.5.0 = STRING:      UFBA"
iso.3.6.1.2.1.1.6.0 = STRING: "\"Location Name\""
```

Vulnerabilidade equipamentos de VC

- Estudo de caso: mais de 40 equipamentos vulneráveis e sendo explorados em “pequenos” ataques de DRDoS
 - Tivemos casos de exploração de ~120 Mbps



Ransomware

- Casos de ransomware afetando diversas organizações: WannaCry (May/17) e Petya (Jun/17)
 - WannaCry afetou mais de 300 mil computadores em mais de 150 países no mundo
 - Exploração da vulnerabilidade Microsoft MS 17-010
- Movimentação lateral, criptografia da MBR, solicitações de resgate, etc

Ransomware

- Intensificação de campanhas de conscientização e alertas
- Aplicação de patches de atualização
- Revisão de políticas de controle de acesso



Lições aprendidas

- Revisar periodicamente as políticas de firewall
- Utilizar cache e soluções de distribuição de conteúdo locais
- Levantamento do perfil de tráfego da organização
- Aplicar rate-limit para aplicações não prioritárias na organização
- Aplicar QoS para aplicações prioritárias

Normatização e conscientização

- Normas e política de uso aceitável da rede e dos serviços
- Ações de educação e conscientização dos usuários para bom uso dos recursos
 - Campanhas para usuários finais (diferentes perfis)
 - Campanhas para equipe de TI
- Implantação de processos e controles para identificação de usuários

Obrigado!!!
;-)

Perguntas?



Italo Valcy
italovalcy@ufba.br