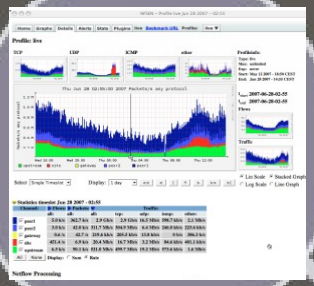
Monitoramento com foco em Segurança

Italo Valcy – UFBA



Network Flows

MONITORA-MENTO

Wi-Fi

FONTES ABERTAS

QoS / QoE

SEGURANÇA

REDES SOCIAIS

```
Dentry cache hash table entries: 131072 (order: 7, 524288 bytes)
Inode-cache hash table entries: 65536 (order: 6, 262144 bytes)
Memory: 902096k/917504k available (1499k kernel code, 14828k reserved, 599k da
, 256k init, 0k highmem)
Checking if this processor honours the WP bit even in supervisor mode... Ok.
Calibrating delay using timer specific routine.. 3584.98 BogoMIPS (lpj=716996
Security Framework v1.0.0 initialized
SELinux:  Disabled at boot.
Capability LSM initialized
Mount-cache hash table entries: 512
CPU: After generic identify, caps: 078bfbff e1d3fbff 00000000 00000000 0000000
00000000 00000000
CPU: After vendor identify, caps: 078bfbff e1d3fbff 00000000 00000000 0000000
0000000 00000000
CPU: L1 I Cache: 64K (64 bytes/line), D cache 64K (64 bytes/line)
CPU: L2 Cache: 1024K (64 bytes/line)
CPU: After all inits, caps: 078bfbff e1d3fbff 00000000 00000410 00000000 0000
0 00000000
Compat vDSO mapped to ffffe000.
CPU: AMD Opteron(tm) Processor 244 stepping 0a
Checking 'hlt' instruction... OK.
ACPI: Core revision 20060707
```

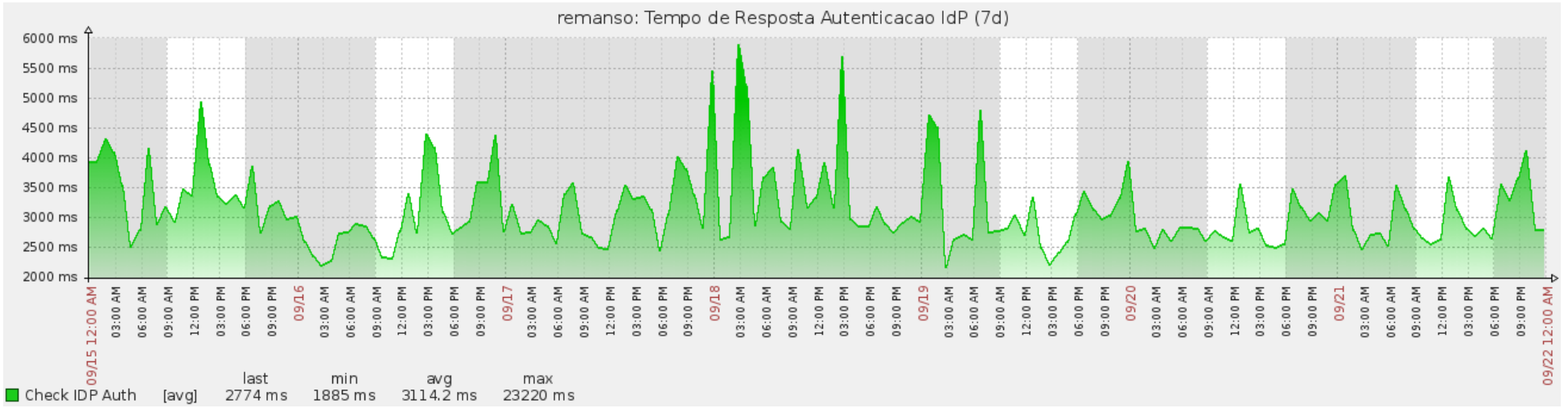
Logs

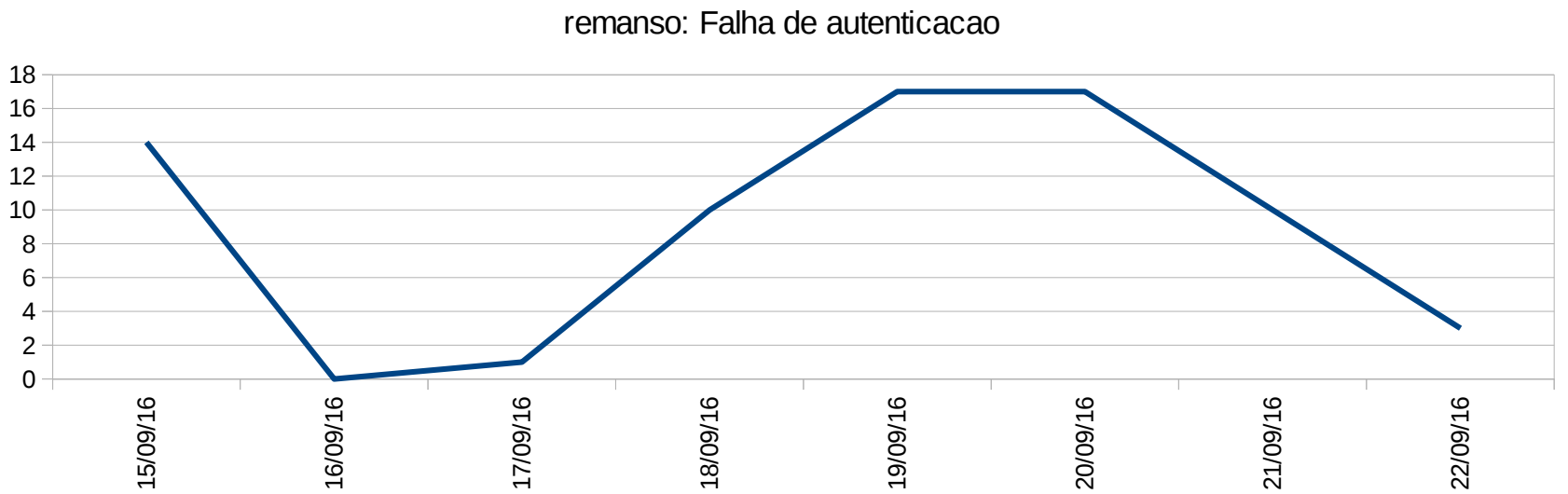
Disponibilidade

- A disponibilidade é um princípio básico da Segurança da Informação
  - *"Uma informação estará disponível para uso no momento desejado"*
- Monitoramento básico: checagem porta do serviço
- O que mais pode ser monitorado?
  - Emular um cliente (phantomjs, monitoring-plugins etc)
  - Tempo de resposta
  - Conteúdo da resposta
  - Não-Escopo

Disponibilidade

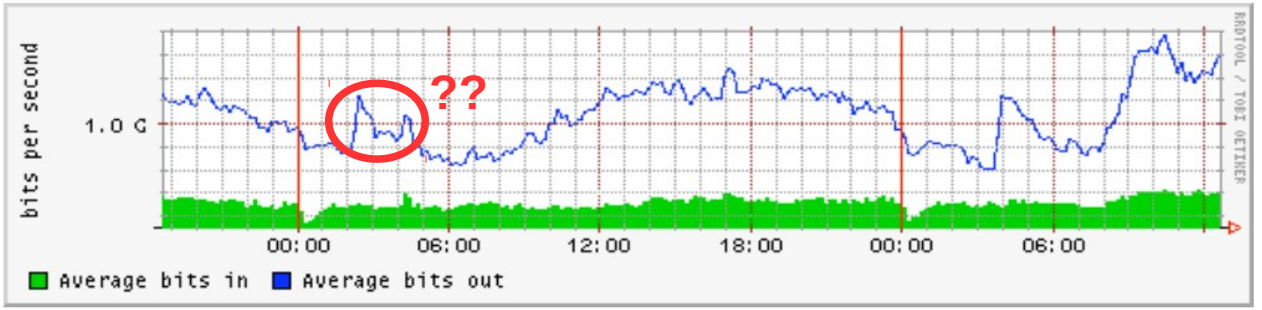
- Exemplo: tempo de resposta e falhas no login CAFe





Monitoramento de Flows

- Monitoramento tradicional não fornece os detalhes suficientes para área de redes ou segurança



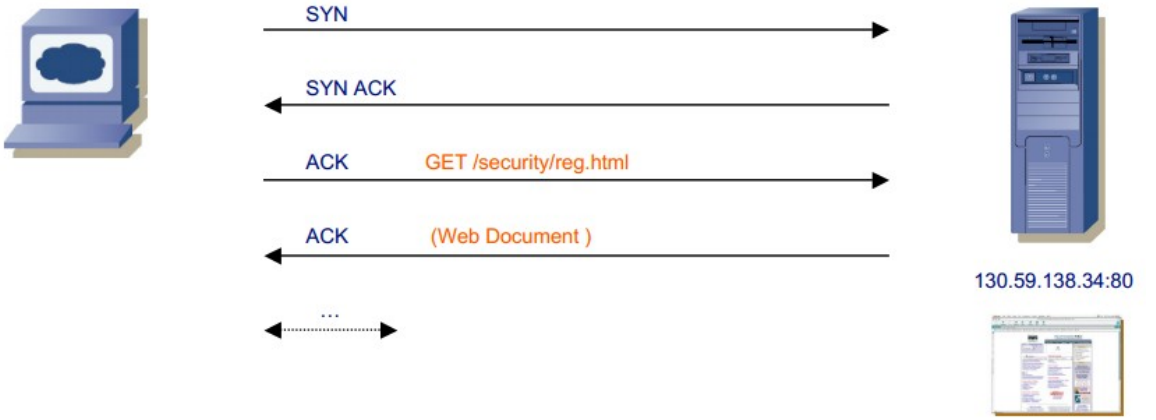
- O que causou esse pico no gráfico?
- Quais são os top talkers da sua rede?
- Quais os hosts envolvidos naquele ataque XYZ?
- Existem máquinas acessando hosts maliciosos?

Monitoramento de Flows

- O que são fluxos de rede?
  - 1 flow é um sumário com vários pacotes de rede
  - Apenas o cabeçalho é coletado, por amostragem
- Para que serve?
  - Apoiar o tratamento de incidentes de segurança
  - Detectar anomalias e tentativas de intrusão
  - Identificar computadores infectados, servidores comprometidos, envio de spam etc.

Monitoramento de Flows

- O equipamento deve fornecer suporte para sflow, netflow ou ipfix
- Importante dimensionar a taxa de amostragem
- Software de Análise (nfsen, ntop, silk etc.)




```
Date flow start          Duration Proto     Src IP Addr:Port          Dst IP Addr:Port   Packets    Bytes
2007-10-01 10:00:57.308    20.113 TCP    172.16.250.225:1582 ->    130.59.138.34:80          10      848
2007-10-01 10:00:57.311    16.685 TCP    130.59.138.34:80    ->    172.16.250.225:1582       13    14176
```

Monitoramento de Flows

- Estudo de caso 1) máquina possivelmente infectada

```
Date flow start          Duration Proto   Src IP Addr:Port       Dst IP Addr:Port
2016-03-17 14:42:32.802     0.000 TCP     200.128.xxx.2:60272 -> 83.xxx.xxx.47:6667
2016-03-17 14:42:32.802     0.000 TCP     200.128.xxx.2:60272 -> 83.xxx.xxx.47:6667
(..)
2016-03-17 16:31:10.342     0.000 TCP     200.128.xxx.2:60272 -> 83.xxx.xxx.47:6667
```

- A equipe responsável pela rede não conseguiu identificar o host interno que originou essa conexão
  - Necessidade de monitoramento do Firewall/NAT!

Monitoramento de Flows

- Estudo de caso 2) violação de copyright
  - Os dados da notificação não casavam com os logs
  - O dispositivo não suportava gerar logs de NAT

Date flow start	Duration	Proto	Src IP Add:Prort		Dst IP Add:Prort	Bytes
2016-08-31 16:33:32.459	0.000	TCP	200.128.xxx.24:23637	->	192.168.xxx.11:51036	17.0 G
2016-08-31 15:10:54.282	0.000	TCP	200.128.xxx.24:23637	->	104.xxx.xxx.139:80	227584
2016-08-31 15:10:54.282	0.000	TCP	200.128.xxx.24:23637	->	104.xxx.xxx.139:80	227584
2016-08-31 15:10:54.282	0.000	TCP	200.128.xxx.24:23637	->	104.xxx.xxx.139:80	227584
2016-08-31 15:47:33.153	0.000	TCP	200.128.xxx.24:23637	->	186.xxx.xxx.40:80	17408
2016-08-31 15:47:33.153	0.000	TCP	200.128.xxx.24:23637	->	186.xxx.xxx.40:80	17408
2016-08-31 15:47:33.153	0.000	TCP	200.128.xxx.24:23637	->	186.xxx.xxx.40:80	17408

Monitoramento de Flows

- Estudo de caso 3) intrusão em servidor
  - Invasor tinha a senha de uma conta com acesso remoto
  - Todos os logs de auditoria foram apagados
  - Identificação do IP do atacante via sflow

```
Date flow start          Duration Proto Src IP Addr:Port          Dst IP Addr:Port      Packets Bytes
(...)
2016-xx-xx xx:21:05.239  3924.373 GRE   192.xxx.xxx.4:0       => 177.yyy.yyy.yyy:0     21504   13.1 M
2016-xx-xx xx:24:47.110  3720.248 GRE   177.yyy.yyy.yyy:2257  => 192.xxx.xxx.4:1500    9216    1.0 M
2016-xx-xx xx:24:59.906  3249.059 GRE   192.xxx.xxx.4:4942    => 177.yyy.yyy.yyy:1500  3072    1.5 M
(...)
2016-xx-xx xx:36:19.701  2932.059 GRE   192.xxx.xxx.4:1500    => 177.yyy.yyy.yyy:54603 6912    1.6 M
2016-xx-xx xx:35:54.223  3043.441 GRE   177.yyy.yyy.yyy:54603 => 192.xxx.xxx.4:1500    35328   3.5 M
2016-xx-xx xx:35:09.464  3034.701 GRE   192.xxx.xxx.4:54603   => 177.yyy.yyy.yyy:1500  20736   5.7 M
```

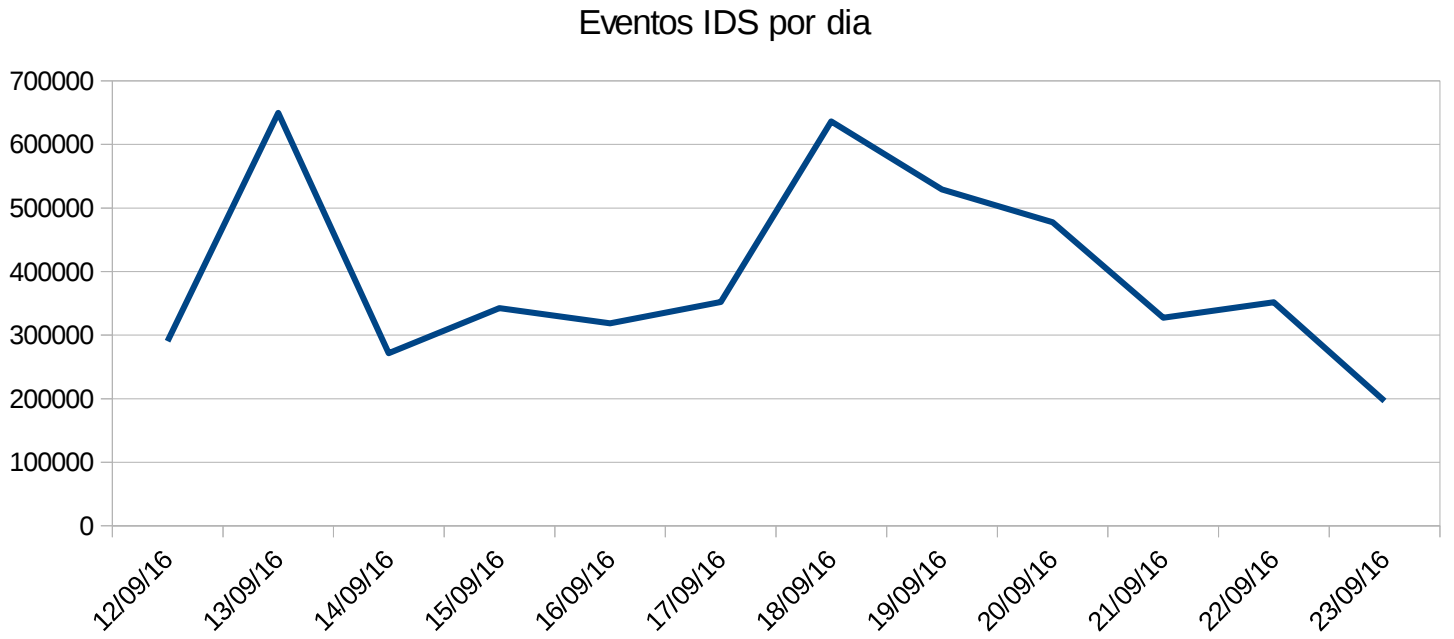
  - Foi possível também fazer correlação com outros eventos anteriores

Sistema de Detecção de Intrusão

- São sistemas de detecção de comportamento malicioso com base em:
  - Assinaturas de ataques
  - Análise de comportamento (ex: redes neurais etc.)
- Monitoramento inline, mirror ou baseado em flows
- Tipos:
  - Baseado em host (Tripware, OSSEC, Samhain etc.)
  - Baseado em rede (Snort, Suricata, Bro etc.)

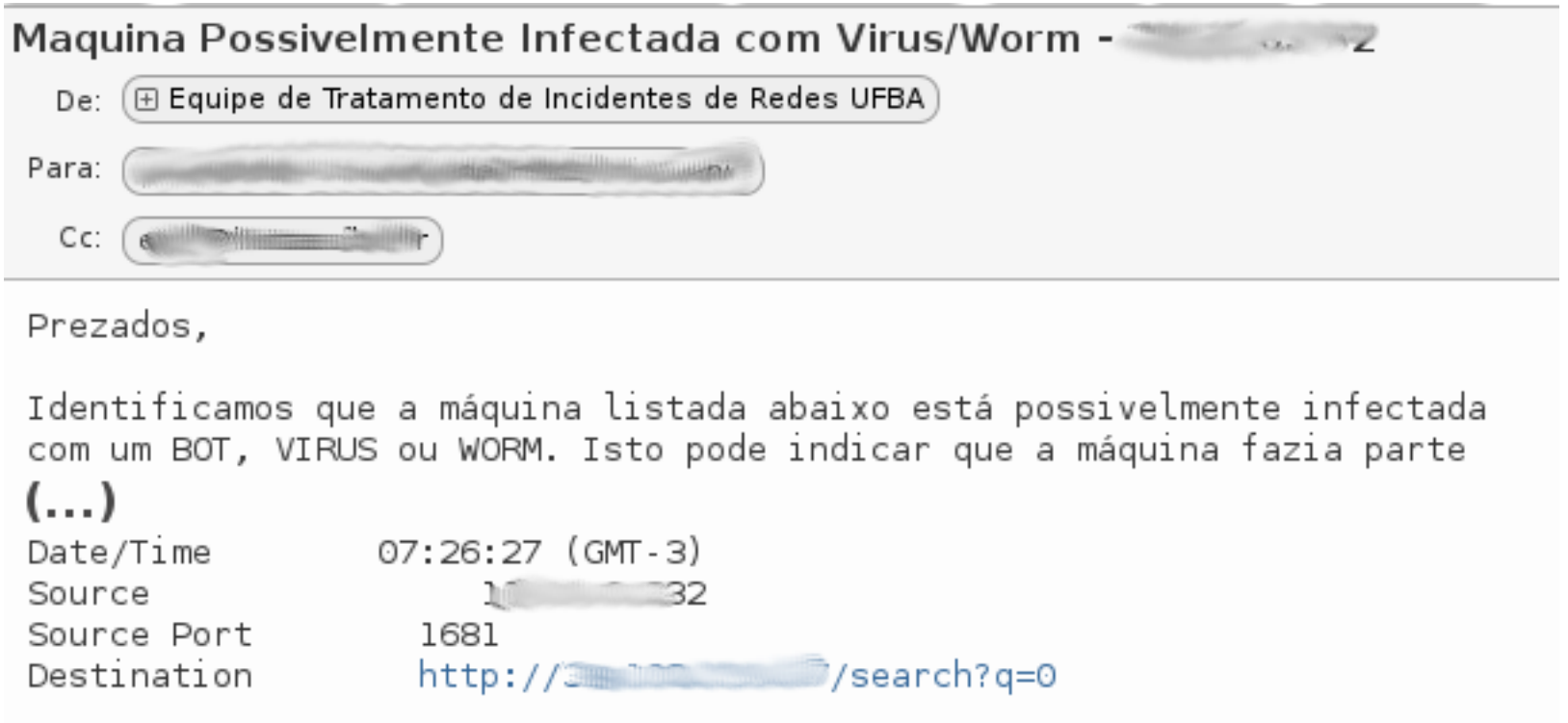
Sistema de Detecção de Intrusão

- Estudo de caso UFBA (Suricata)
  - Eventos observados por dia



Sistema de Detecção de Intrusão

- Estudo de caso 1) máquina infectada com vírus
  - Infecção com Conficker
  - Equipamento médico – sistema de raio X



Maquina Possivelmente Infectada com Virus/Worm -

De: Equipe de Tratamento de Incidentes de Redes UFBA

Para:

Cc:

Prezados,

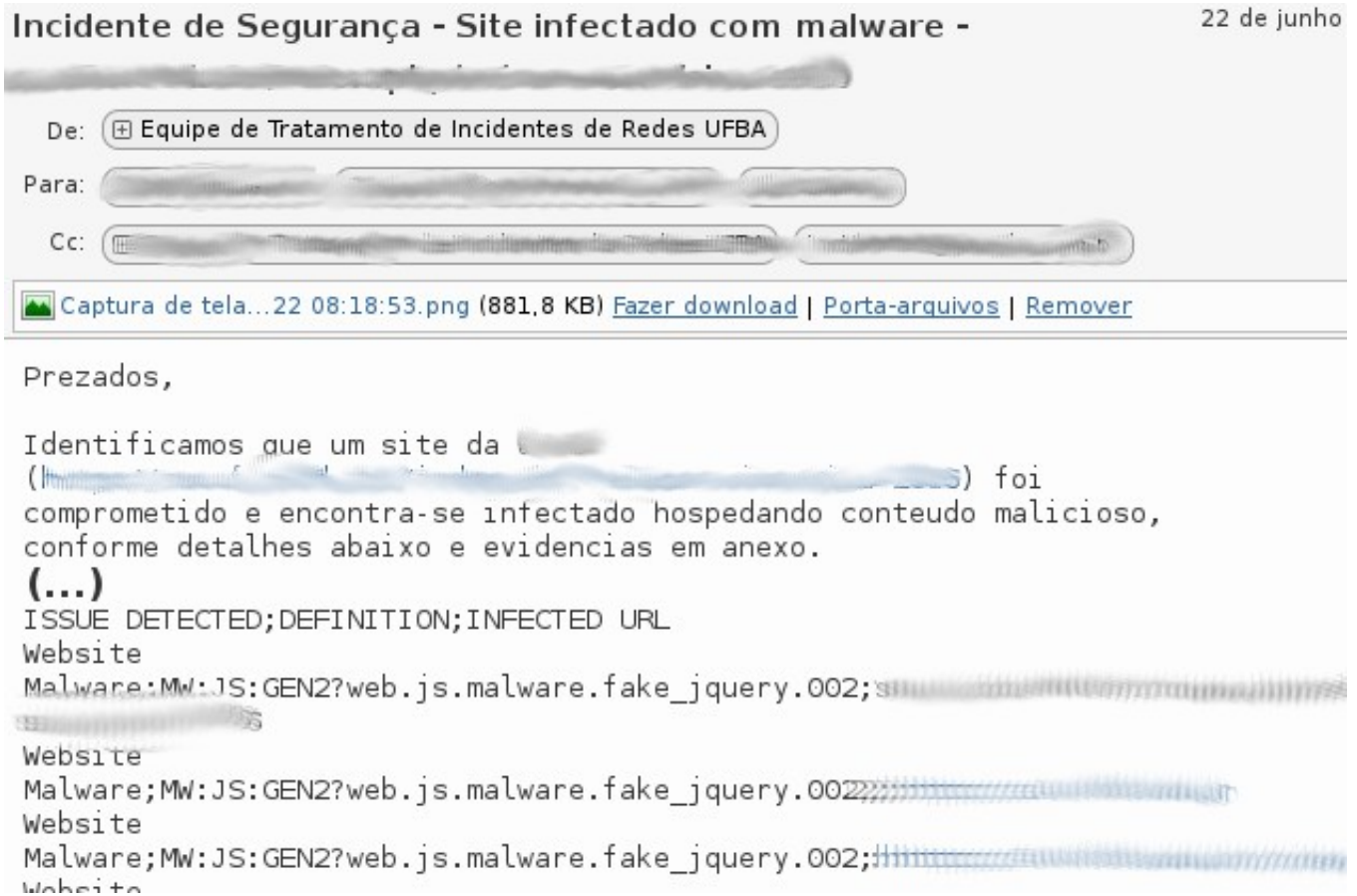
Identificamos que a máquina listada abaixo está possivelmente infectada com um BOT, VIRUS ou WORM. Isto pode indicar que a máquina fazia parte

(...)

Date/Time 07:26:27 (GMT-3)
Source
Source Port 1681
Destination http://[redacted]/search?q=0

Sistema de Detecção de Intrusão

- Estudo de caso 2) site propagando vírus
  - Vírus Fake JS / jQuery.php



Incidente de Segurança - Site infectado com malware - [redacted] 22 de junho

De: Equipe de Tratamento de Incidentes de Redes UFBA

Para: [redacted]

Cc: [redacted]

Captura de tela...22 08:18:53.png (881,8 KB) Fazer download | Porta-arquivos | Remover

Prezados,

Identificamos que um site da [redacted]
([redacted]) foi
comprometido e encontra-se infectado hospedando conteudo malicioso,
conforme detalhes abaixo e evidencias em anexo.

(...)

ISSUE DETECTED;DEFINITION;INFECTED URL
Website
Malware;MW:JS:GEN2?web.js.malware.fake_jquery.002;[redacted]
Website
Malware;MW:JS:GEN2?web.js.malware.fake_jquery.002[redacted]
Website
Malware;MW:JS:GEN2?web.js.malware.fake_jquery.002;[redacted]

Firewall / NAT

- É fundamental monitorar o Firewall para viabilizar a GIS e identificar comportamento anormal
  - Hosts comprometidos
  - Tentativas de violação da política de Segurança
  - Tradução de Endereços de Rede (NAT/PAT)
- Monitoramento pode se dá de diversas maneiras:
  - Syslog
  - SNMP / Traps
  - Notificações por e-mail
  - Dashboards (top talkers, hits, app control, cpu, mem, sess)

Firewall / NAT

- Casos já identificados na UFBA:
  - Máquina com backdoor/rootkit
  - Máquina participando de botnet para spam
  - Máquina realizando scan de rede
  - Evidências de acesso de atacante (correlação com inc.)
  - Máquina com vírus e comunicação C&C

Firewall / NAT

- E com relação ao NAT, o que monitorar?
  - É importante monitorar as traduções de endereços de rede para tratamento de incidentes
  - No mínimo: IP/Porta originais e traduzidos, duração, protocolo
- Seu firewall suporta fazer logging do NAT?
  - Cisco, Fortinet, Checkpoint, PaloAlto, Juniper, etc: Sim
  - IPTables/Netfilter, PFSense: não nativamente

Firewall / NAT

- Logging de NAT no IPTables/Netfilter:
  - https://github.com/italovalcy/nfct-snatlog

- Logging de NAT no PFSense/PF
  - https://github.com/italovalcy/pfnattrack

Exemplo:

```
2016-06-19,21:44:34 proto=6 osrc=192.168.100.105:51496 tsrc=192.168.25.4:2474
odst=192.168.25.7:22 tdst=192.168.25.7:22 duration=117

2016-06-19,22:07:05 proto=17 osrc=192.168.100.105:37205 tsrc=192.168.25.4:22834
odst=8.8.8.8:53 tdst=8.8.8.8:53 duration=30
```

IPv4/IPv6 Host Address

- No tratamento de incidentes, nem sempre o IP é suficiente:
  - E se você utilizar DHCP?
  - E máquinas com IP estático?
  - E com IPv6 auto-configuration?
- Opção: L2M (Layer 2 manager)
  - https://certbahia.pop-ba.rnp.br/projects/l2m

L2M

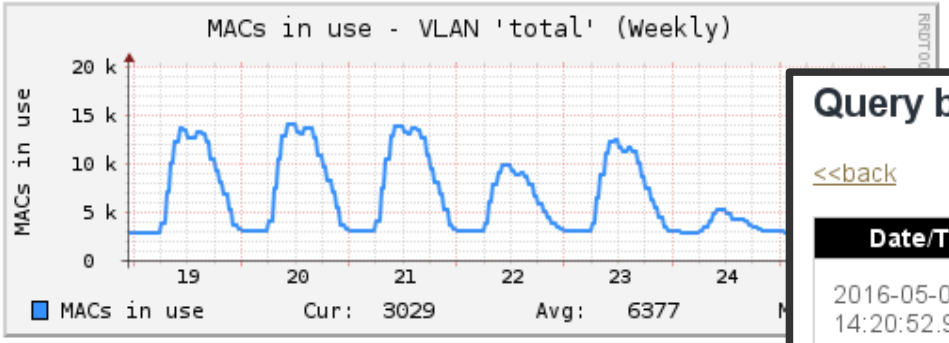
L2M :: LAYER 2 MANAGER

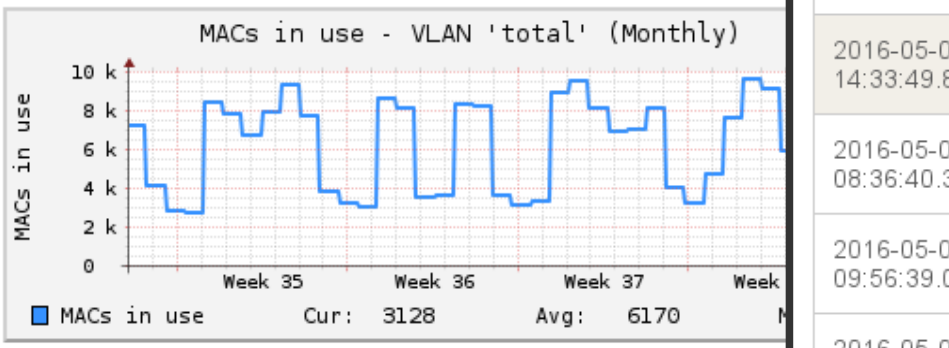
HOME | STATS | CONTAINMENT | SETTINGS | ABOUT

Statistics

VLAN: all

Stats by VLAN
Query by MAC/IP
List of MAC/IP by VLAN





Query by MAC/IP

<<back

Date/Time	Alive?	MAC	IP	VLAN
2016-05-06 14:20:52.999575	t	6c:f0:49:f8:ff:ee	192.168.137.20	Rede_QUI (VLAN 137)
2016-05-06 14:33:49.88518	f	6c:f0:49:f8:ff:ee	192.168.137.20	Rede_QUI (VLAN 137)
2016-05-07 08:36:40.302866	t	ac:87:a3:32:02:b1	192.168.137.20	Rede_QUI (VLAN 137)
2016-05-07 09:56:39.061157	f	ac:87:a3:32:02:b1	192.168.137.20	Rede_QUI (VLAN 137)
2016-05-09 07:10:34.546118	t	74:ea:3a:fe:1e:ff	192.168.137.20	Rede_QUI (VLAN 137)

Logs e correlação de logs

- Logs do sistema são fonte importante para verificação e alertas de segurança
  - Erros, alertas, mal funcionamento
  - Tentativas de ataque (brute-force, SQLi, DoS, ...)
  - APTs
  - Vazamento de dados
  - Bloqueios maliciosos
- Necessidade de ferramentas e scripts para automatizar o tratamento devido ao volume
  - Média da UFBA ~ 190M logs/dia

Logs e correlação de logs

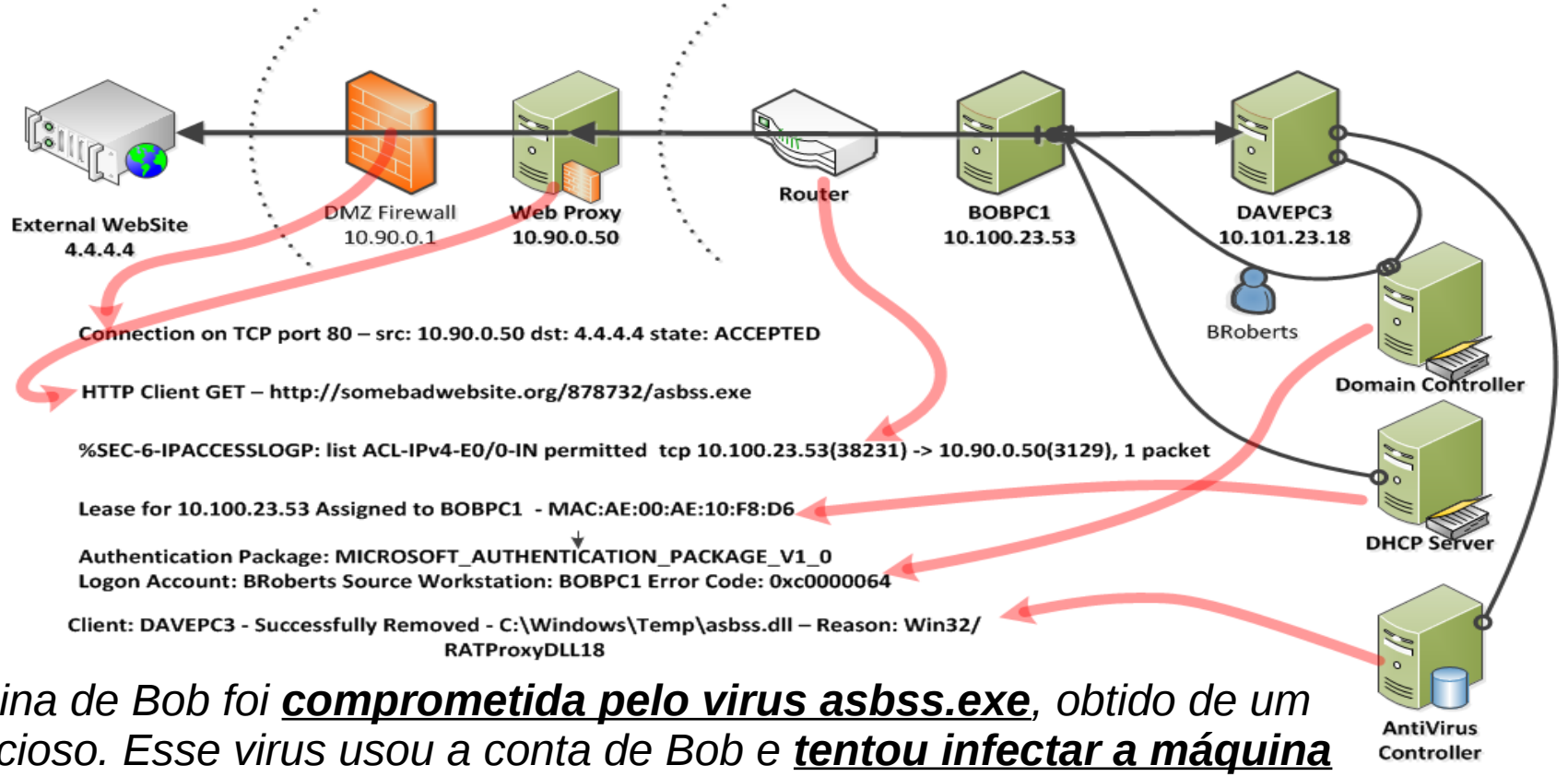
- Logs do sistema são fonte importante para verificação e alertas de segurança
  - Erros, alertas, mal funcionamento
  - Tentativas de ataque (brute-force, SQLi, DoS, ...)
  - APTs
  - Vazamento de dados
  - Bloqueios maliciosos
- Necessidade de ferramentas e scripts para automatizar o tratamento devido ao volume
  - Média da UFBA ~ 190M logs/dia

Logs e correlação de logs

- Exemplo: ELK

Logs e correlação de logs

- SIEM: Security Information and Event Management



*"A máquina de Bob foi **comprometida pelo virus asbss.exe**, obtido de um site malicioso. Esse virus usou a conta de Bob e **tentou infectar a máquina DAVEPC3**, mas o antivirus bloqueou. No entanto, a máquina de Bob, BOBPC1, provavelmente ainda esta comprometida. Devemos **bloquear o dominio malicioso** e limpar a máquina de Bob o quanto antes!"*

OSSIM – Open Source SIEM

- SIEM open source – GPL v3
- Monitoramento de ativos de rede
- Centralização de informações e gerenciamento
- Levantamento de vulnerabilidades e ricos
- Provê capacidade de detecção de ameaças
- Aprendizado colaborativo de APT

http://communities.alienvault.com/

Ferramentas integradas ao OSSIM

Mapeamento

- nmap
- prads

Detecção de Ameaças

- ossec
- snort
- suricata

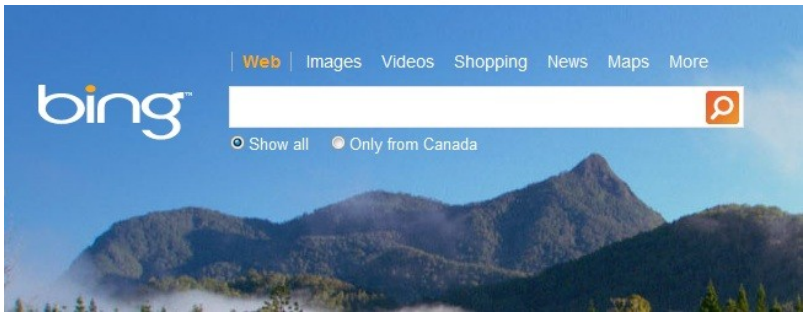
Monitoramento

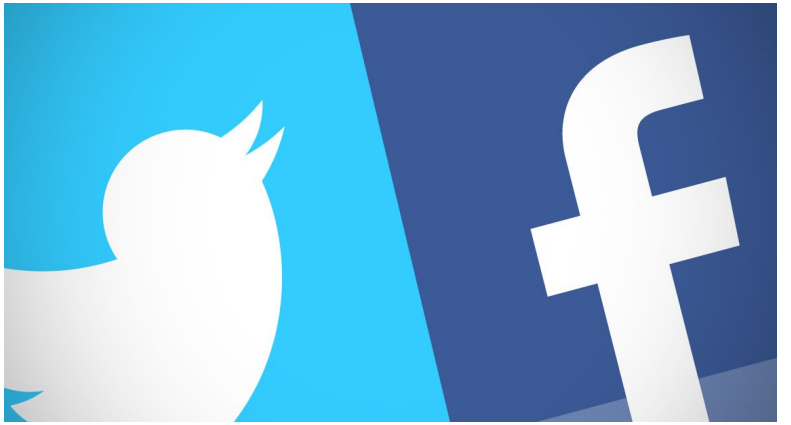
- fprobe
- nfdump
- ntop
- tcpdump
- nagios

Levantamento de vulnerabilidades

- osvdb
- openvas

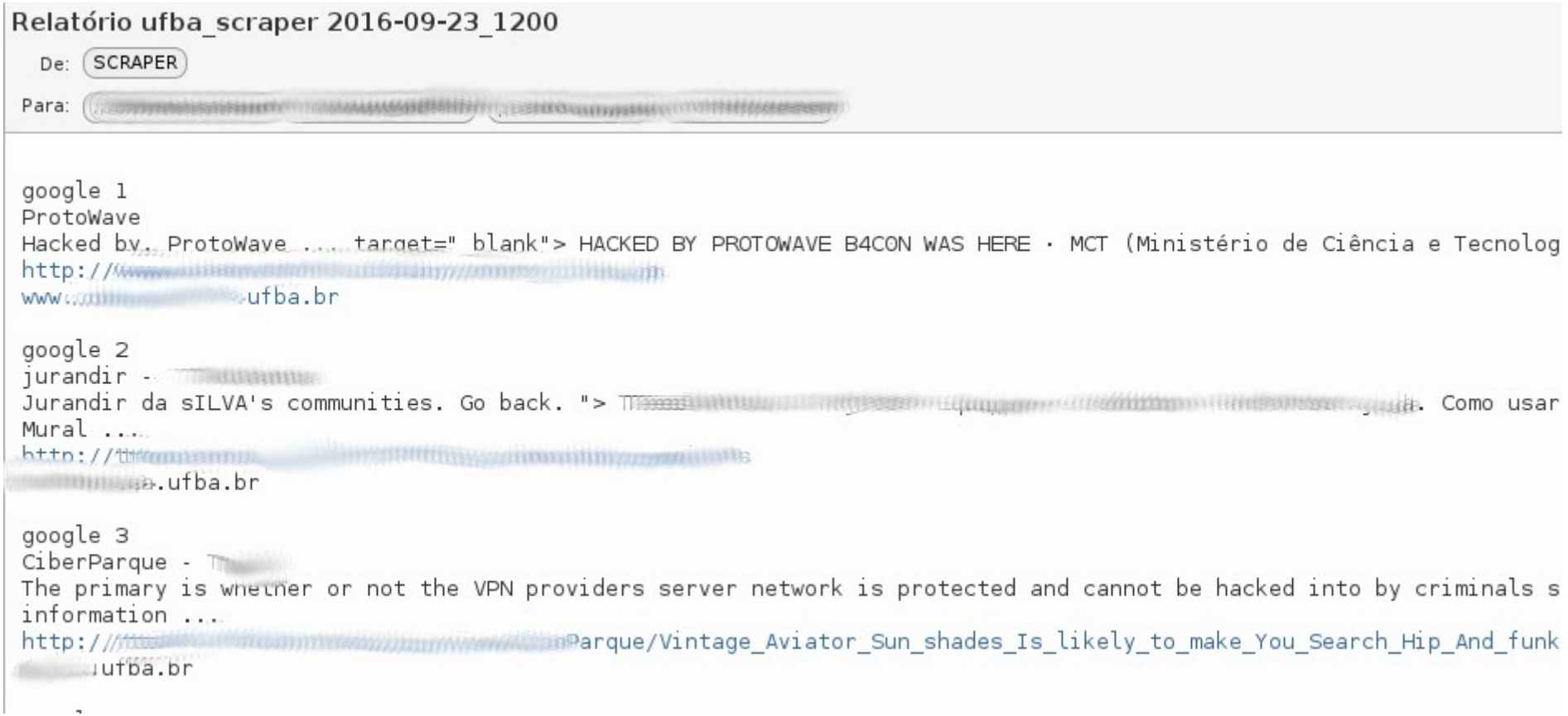
Fontes abertas





Buscador UFBA

- Script Python de busca em fontes abertas por sites hackeados


Relatório ufba_scraper 2016-09-23_1200

De: SCRAPER

Para: [redacted]

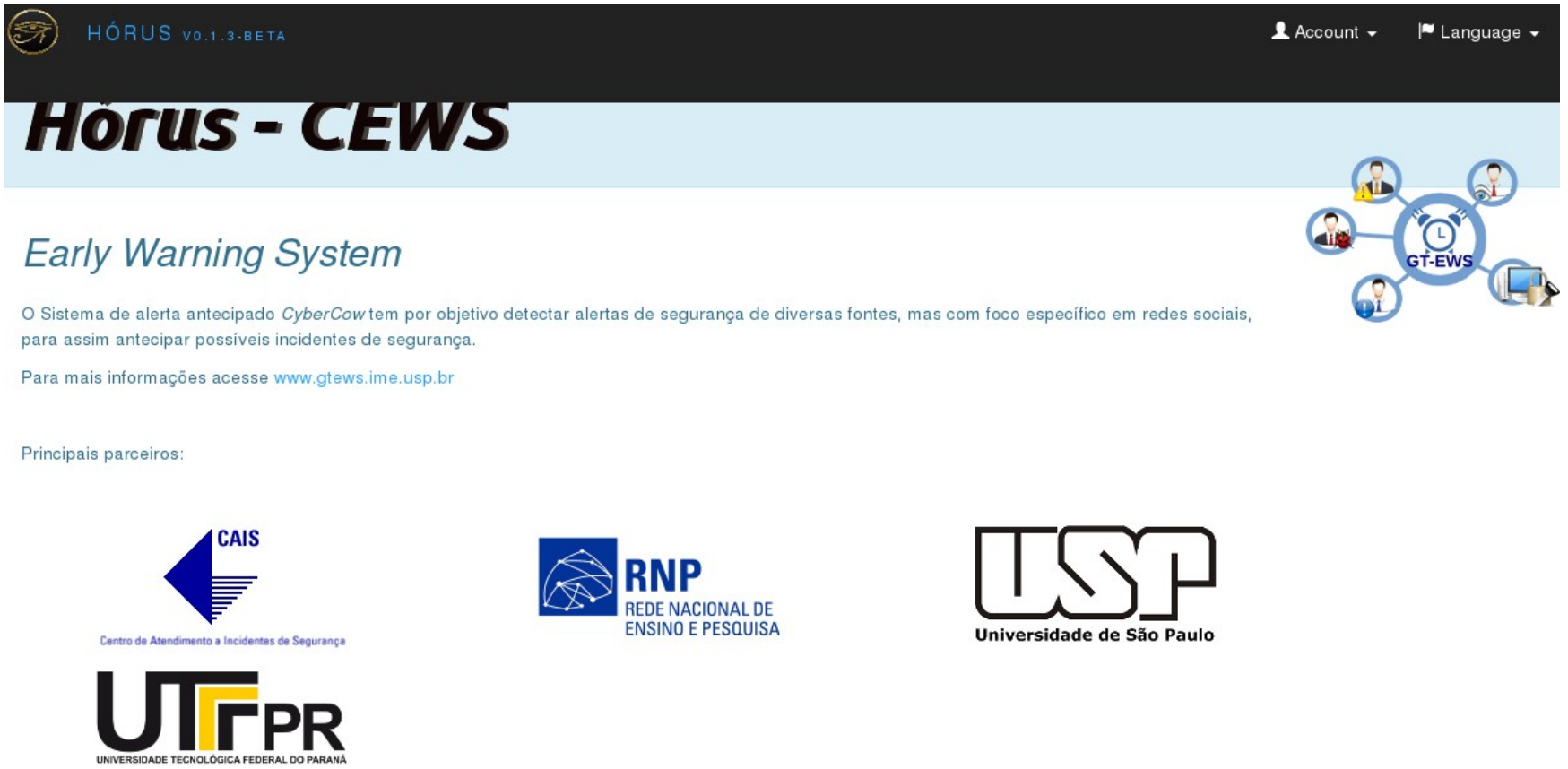
google 1
ProtoWave
Hacked by. ProtoWave .... target=" blank"> HACKED BY PROTOWAVE B4CON WAS HERE · MCT (Ministério de Ciência e Tecnolog
http://[redacted]
www.[redacted]ufba.br

google 2
jurandir - [redacted]
Jurandir da sILVA's communities. Go back. "> [redacted]. Como usar
Mural ...
http://[redacted]
[redacted].ufba.br

google 3
CiberParque - [redacted]
The primary is whether or not the VPN providers server network is protected and cannot be hacked into by criminals s
information ...
http://[redacted]Parque/Vintage_Aviator_Sun_shades_Is_likely_to_make_You_Search_Hip_And_funk
[redacted]ufba.br

Horus – GT-EWS

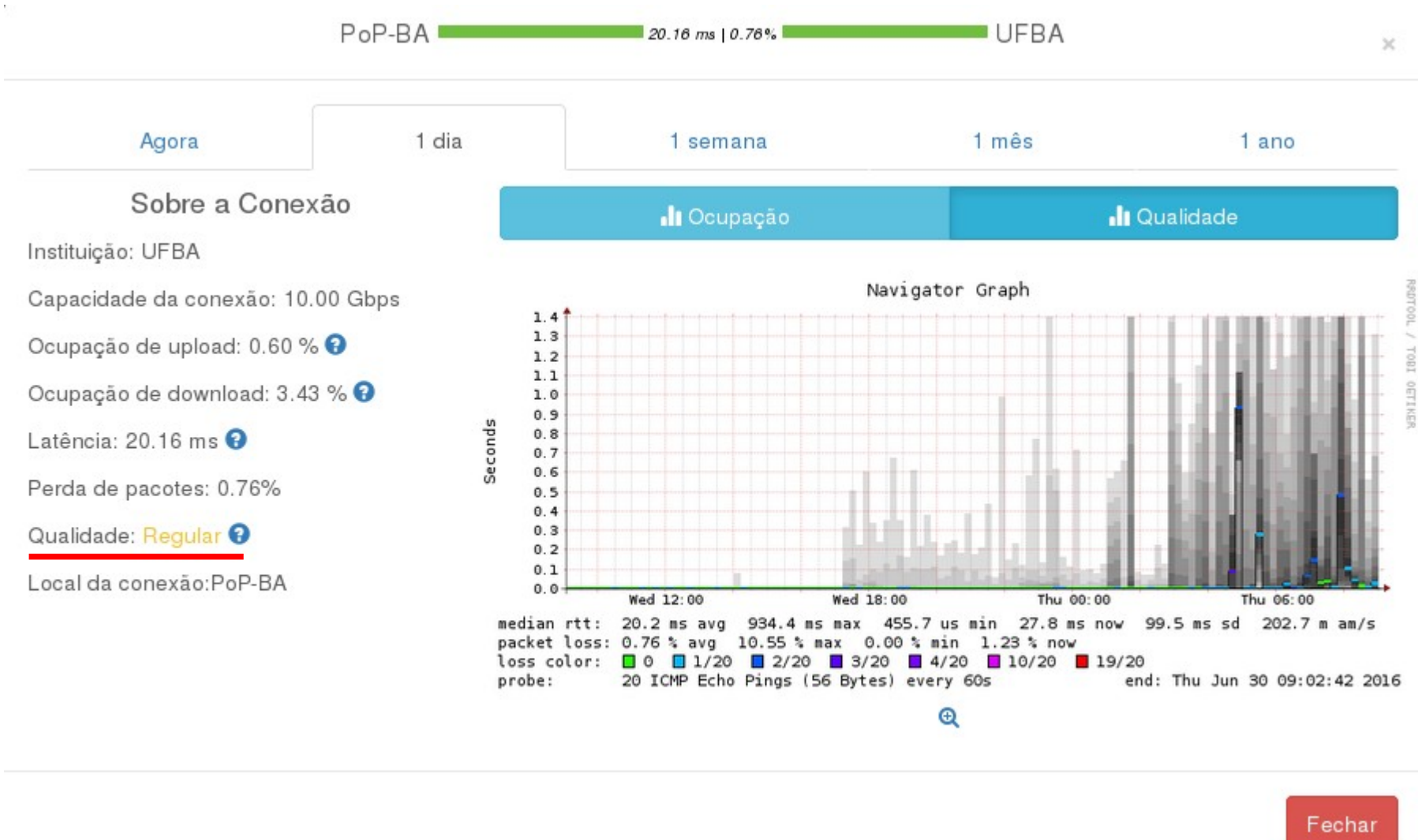
- GT-RNP *Cybersecurity Early Warning System*



Conclusão

- O monitoramento é essencial para Segurança da Informação
  - Não monitorar o ambiente é como dirigir à noite com os faróis apagados! Você pode se prejudicar ou prejudicar os outros...
- Comece pelo básico: monitore o desempenho dos serviços, logs locais e remotos, fluxos de rede, ferramentas de segurança, …
- Realize auditorias periódicas
- É difícil uma solução/ferramenta que se adeque a tudo
- Faça apresentações sobre o ambiente monitorado!
  - Estatísticas, Relatórios, Dashboards

Impacto na QoE



Fonte: http://viaipe.rnp.br

Obrigado! Perguntas?

Italo Valcy <italovalcy@ufba.br>