Governo do Estado de
RONDÔNIA
SETIC

Coordenadoria de Segurança
RELATÓRIO MENSAL
Março/2021

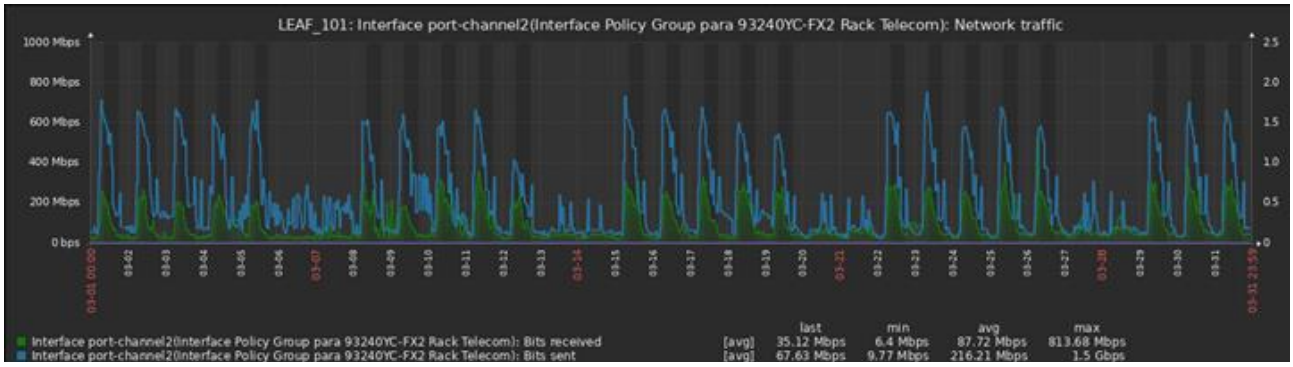
2021

Relatório Mensal - Março/2021

Sumário

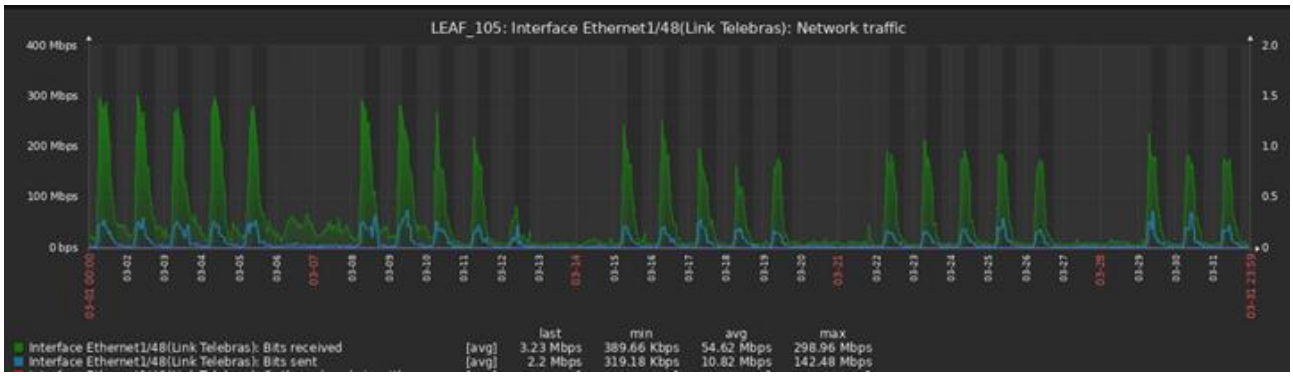
1. Tráfego de Rede

Considerando os dados de tráfego de rede transferidos via Cores de Comunicação de Dados da DETIC, entre estações de trabalho do Palácio Rio Madeira, INFOVIA e serviços hospedados, aferimos o Volume Total de **101 TB** de informação trafegada no mês deste relatório.

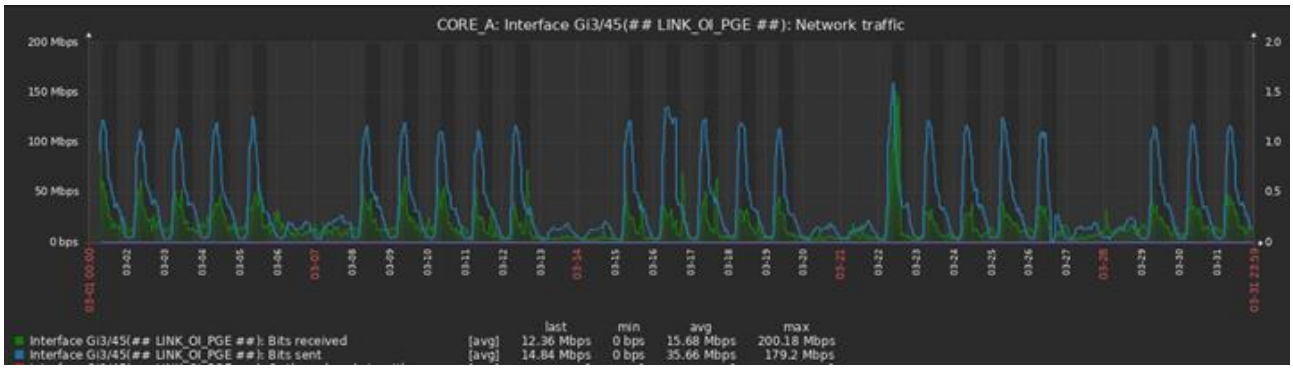


Monitoramento de tráfego Cores DETIC

Além disso, foram consumidos **39 TB** de tráfego da Internet, considerando acesso dos usuários à aplicações de Governo expostas na Internet e acesso a serviços pelo público geral.



Monitoramento de tráfego Link Telebrás



Monitoramento de tráfego Link Oi

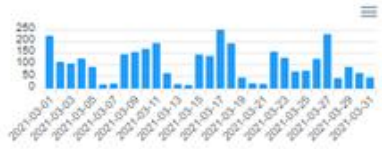
2. Ataques

Vale à pena frisar que ainda não possuímos uma infraestrutura que nos garanta a segurança de dados, no que tange às tecnologias de proteção topo de linha no mercado de TI. Porém a ferramenta que utilizamos hoje registrou um total de **74.172** Ataques Registrados durante o mês do presente relatório.

Como contramedida para resolver o problema acima relatado, estamos aguardando a entrega de novos appliances de Firewall, adquiridos via comodato em nosso novo contrato de link's. Com os novos dispositivos, de um fabricante líder de mercado em segurança da informação, teremos uma proteção ativa de maior qualidade frente aos nossos serviços.

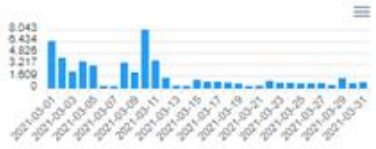
GOVERNO DO ESTADO DE RONDÔNIA
SUPERINTENDÊNCIA ESTADUAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
DIRETORIA TÉCNICA

Risco - Alto



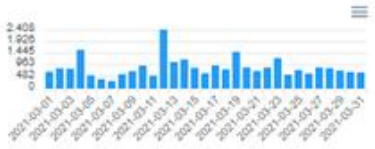
#	Ataque	Hits
1	png file attachment without matchin...	2.527
2	SMTP relaying denied	816
3	malicious file download attempt	13

Risco - Médio



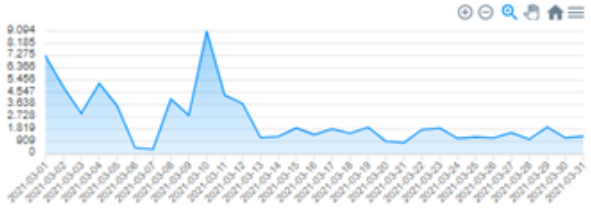
#	Ataque	Hits
1	Mambo upload.php access	32.001
2	Poison Null Byte	5.172
3	named version attempt	2.425
4	http GET request smuggling attempt	2.320
5	HTTP POST invalid method case	1.427
6	403 Forbidden	1.414
7	robots.txt access	1.129
8	Apache mod_proxy reverse proxy inf...	828
9	XML entity parsing information disclo...	252
10	Apache Tomcat Web Application Man...	212

Risco - Baixo



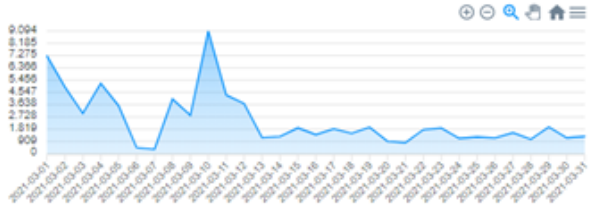
#	Ataque	Hits
1	external admin access attempt	14.733
2	password sent via URL parameter	3.665
3	base64 x86 NOOP	2.367
4	PHPUnit PHP remote code execution ...	908
5	password sent via POST parameter	607
6	PHP function CRLF injection attempt	368
7	PHP tag injection in http header atte...	352
8	PHP uri tag injection attempt	328
9	PHP tags in HTTP POST	304
10	Suspicious Chmod Usage in URI (Inb...	124

Top Categorias

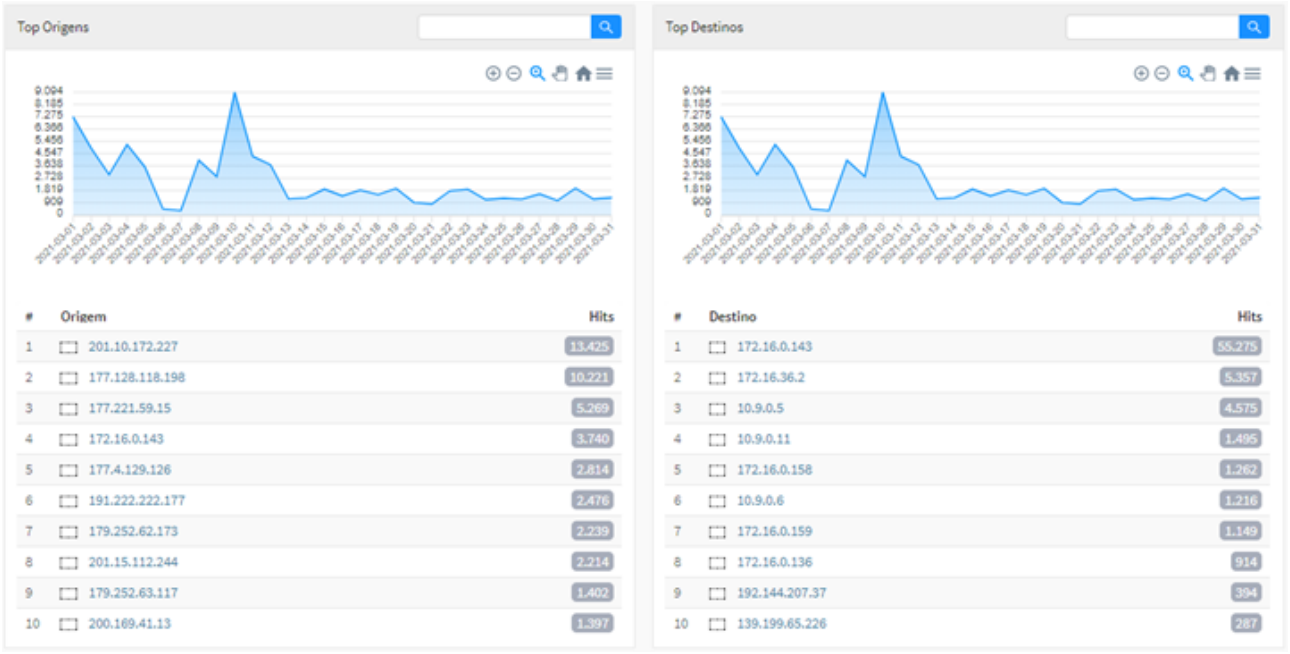


#	Categoria	Hits
1	SERVER-WEBAPP	39.470
2	POLICY-OTHER	15.427
3	WEB_SERVER	6.782
4	INDICATOR-COMPROMISE	5.375
5	INDICATOR-SHELLCODE	2.412
6	SCAN	1.427
7	PROTOCOL-DNS	1.372
8	SERVER-APACHE	1.290
9	DNS	1.053
10	SERVER-MAIL	466

Top Tipos de Classes



#	Tipo de Classe	Hits
1	Access to a Potentially Vulnerable Web Application	38.371
2	Attempted Administrator Privilege Gain	15.137
3	Attempted Information Leak	5.370
4	Potential Corporate Privacy Violation	4.381
5	Misc activity	3.156
6	Web Application Attack	2.762
7	Executable Code was Detected	2.452
8	Misc Attack	2.320
9	Potentially Bad Traffic	1.584
10	Attempted User Privilege Gain	306



#	Origem	Hits
1	201.10.172.227	13.425
2	177.128.118.198	10.221
3	177.221.59.15	5.269
4	172.16.0.143	3.740
5	177.4.129.126	2.814
6	191.222.222.177	2.476
7	179.252.62.173	2.239
8	201.15.112.244	2.214
9	179.252.63.117	1.402
10	200.169.41.13	1.397

#	Destino	Hits
1	172.16.0.143	55.275
2	172.16.36.2	5.357
3	10.9.0.5	4.575
4	10.9.0.11	1.495
5	172.16.0.158	1.262
6	10.9.0.6	1.216
7	172.16.0.159	1.149
8	172.16.0.136	914
9	192.144.207.37	394
10	139.199.65.226	287

Visualização dos dados de ataques na ferramenta e impactos.

3. Vulnerabilidades

Trata-se das análises de vulnerabilidades realizadas em servidores de rede pertencentes ao Governo do Estado de Rondônia gerenciados ou hospedados pela SETIC, utilizando-se os softwares Nmap[1] e OpenVas[2].

Tais procedimentos se deram em decorrência das diretrizes da Coordenação de Segurança da Informação da SETIC, bem como da intenção de criar a Gerência de Prevenção e Respostas a Incidentes e a solicitação das equipes de Operações e DataCenter da Coordenação de Infraestrutura da SETIC.

O OpenVAS, ao analisar determinado alvo, classifica as vulnerabilidades encontradas em 3 (três) diferentes níveis de gravidade: alto, médio e baixo. Destaca-se ainda que apresenta também o nível denominado “log”, que objetiva trazer informações sobre o alvo, não sendo objeto de discussão neste relatório.

Ao todo, foram analisados 54 (cinquenta e quatro) servidores de rede, dos quais 14 (25,4%) apresentaram alto nível de gravidade, 28 (51,9%) apresentaram médio nível, 7 (13%) apresentaram baixo nível, conforme classificação do OpenVAS, destacando-se ainda que 5 (9,3%) servidores não apresentaram nenhuma vulnerabilidade, pelo fato de estarem com todas as portas fechadas.

Importante ressaltar que nas análises, alguns servidores que apresentaram alto nível de gravidade também apresentaram gravidades de nível médio e baixo, bem como alguns servidores que apresentaram médio nível de gravidade também apresentaram gravidades de nível baixo.

No decorrer das análises o OpenVAS detectou 319 notificações, sendo que cada uma dessas representa uma vulnerabilidade. Dentre as notificações apresentadas destacam-se: 27 (8,5%) de alto nível, 241 (75,5%) de médio nível e 51 (16%) de baixo nível.

Nos testes realizados foram identificadas diversas vulnerabilidades, entretanto não se descarta outras que porventura não foram detectadas ou que surjam futuramente.

3.1 - Gráficos

Utilizando-se do OpenVAS, considerando sua classificação das vulnerabilidades em 3 (três) diferentes níveis de gravidade (alto, médio e baixo) foi possível analisar 54 (cinquenta e quatro) servidores de rede, dos quais 14 (25,4%) apresentaram alto nível de gravidade, 28 (51,9%) apresentaram médio nível, 7 (13%) apresentaram baixo nível, conforme classificação do OpenVAS, destacando-se ainda que 5 (9,3%) servidores não apresentaram nenhuma vulnerabilidade, pelo fato de estarem com todas as portas fechadas, conforme "Gráfico 1 – Nível de gravidade" abaixo:

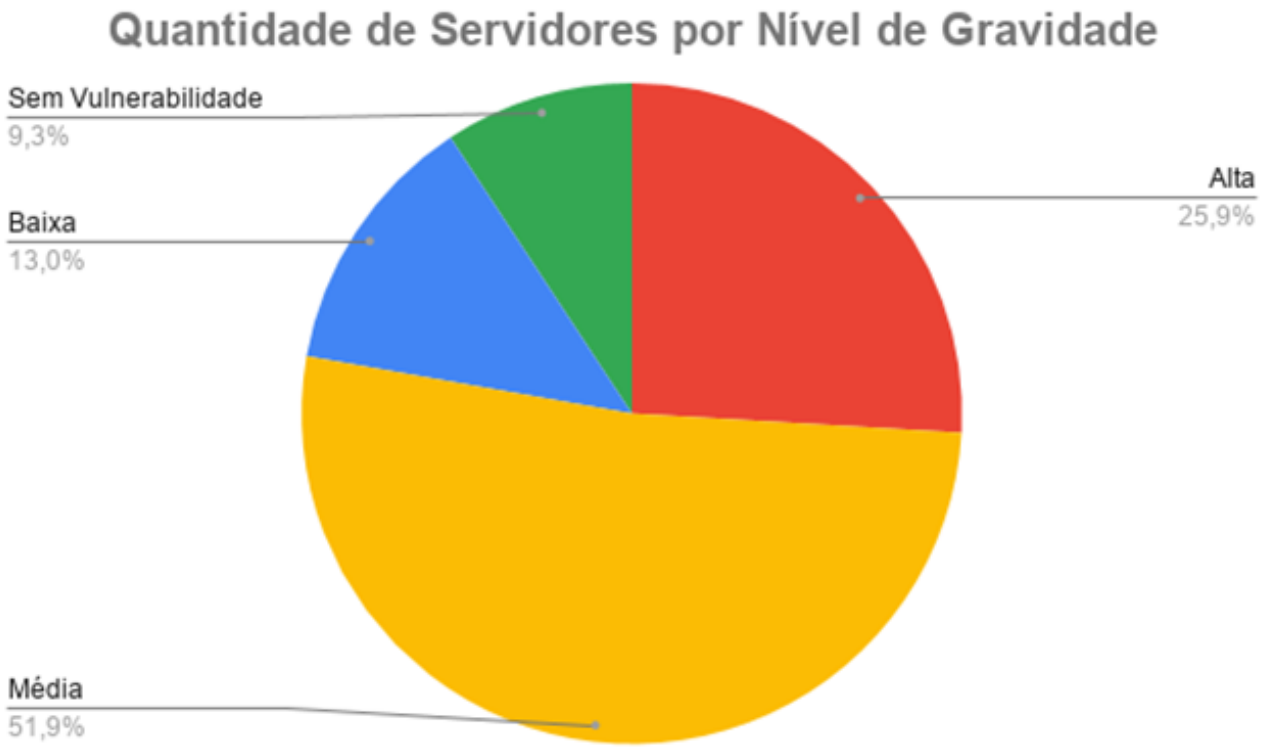


Gráfico 1 – Nível de Gravidade

No que diz respeito às notificações apresentadas pelo OpenVAS, destacam-se que foram detectadas 27 (8,5%) de alto nível, 241 (75,5%) de médio nível e 51 (16%) de baixo nível conforme “Gráfico 2 – Total de notificações” abaixo:

Gráfico 2 – Total de Notificação

Além disso, com base nos relatórios do OpenVAS, procurou-se categorizar as principais vulnerabilidades encontradas nos servidores de rede que foram analisados, criando as seguintes categorias: Web (PHP, HTTP, APACHE); Chaves de Segurança (SSL, TLS, OPENSSH); Acesso Remoto (RPC, FTP, DCE, TCP); Informações do Sistema (TCP TIMESTAMPS); Compartilhamento de Arquivos (SMB WINDOWS); Banco de Dados (MariaDB, SQL); Trojan horses; e Sistema Operacional.

Dessa forma, procurou-se destacar a vulnerabilidade mais crítica de cada servidor e classificá-la em uma dessas categorias, com objetivo de facilitar a identificação do seguimento que se encontra mais vulnerável na rede, exigindo atenção e adoção de políticas de correção e mitigação de falhas e problemas de segurança. Sendo assim, foi possível perceber que a maioria das vulnerabilidades encontradas estão vinculadas à Acesso Remoto (34 servidores) Chaves de Segurança (34 servidores) e Informações do Sistema (44 servidores), conforme observado no “Gráfico 3 – Categorias de vulnerabilidades” abaixo:

Gráfico 3 – Categorias de vulnerabilidades.

Gráfico 3 – Categoria de Vulnerabilidades

Superintendência do
Estado para Resultados

Governo do Estado de
RONDÔNIA

Wiki.DETIC

Plataforma de Documentação Operacional e Gerencial dos Serviços da EpR

Conheça: wiki.detic.ro.gov.br