(32) 3696-4750
www.consulplan.net
atendimento@consulplan.com

Muriaé, 16 de novembro de 2020.

PROTOCOLO-CFC
Número : 2020/002034
Nome : CONSULPLAN
Data : 17/11/2020 15:23

Ofício n.º 010/2020/GDC

Ao Ilmo. Dr. Zulmir Breda

Presidente do Conselho Federal de Contabilidade

Resposta Ofício n.º 1979/2020 CFC-Direx

Assunto: Prazo para apresentação de relatório analítico relativo à indisponibilidade do sistema, que impossibilitou a aplicação da 2ª edição do Exame de Suficiência.

A CONSULPLAN - Consultoria e Planejamento em Administração Pública Eireli, responsável técnica pela operacionalização do Exame de Suficiência do Conselho Federal de Contabilidade, em atendimento à Notificação Extrajudicial supramencionada, vem tempestiva e respeitosamente à presença de V. Sª. prestar esclarecimentos sobre os tópicos solicitados, conforme adiante expendido:

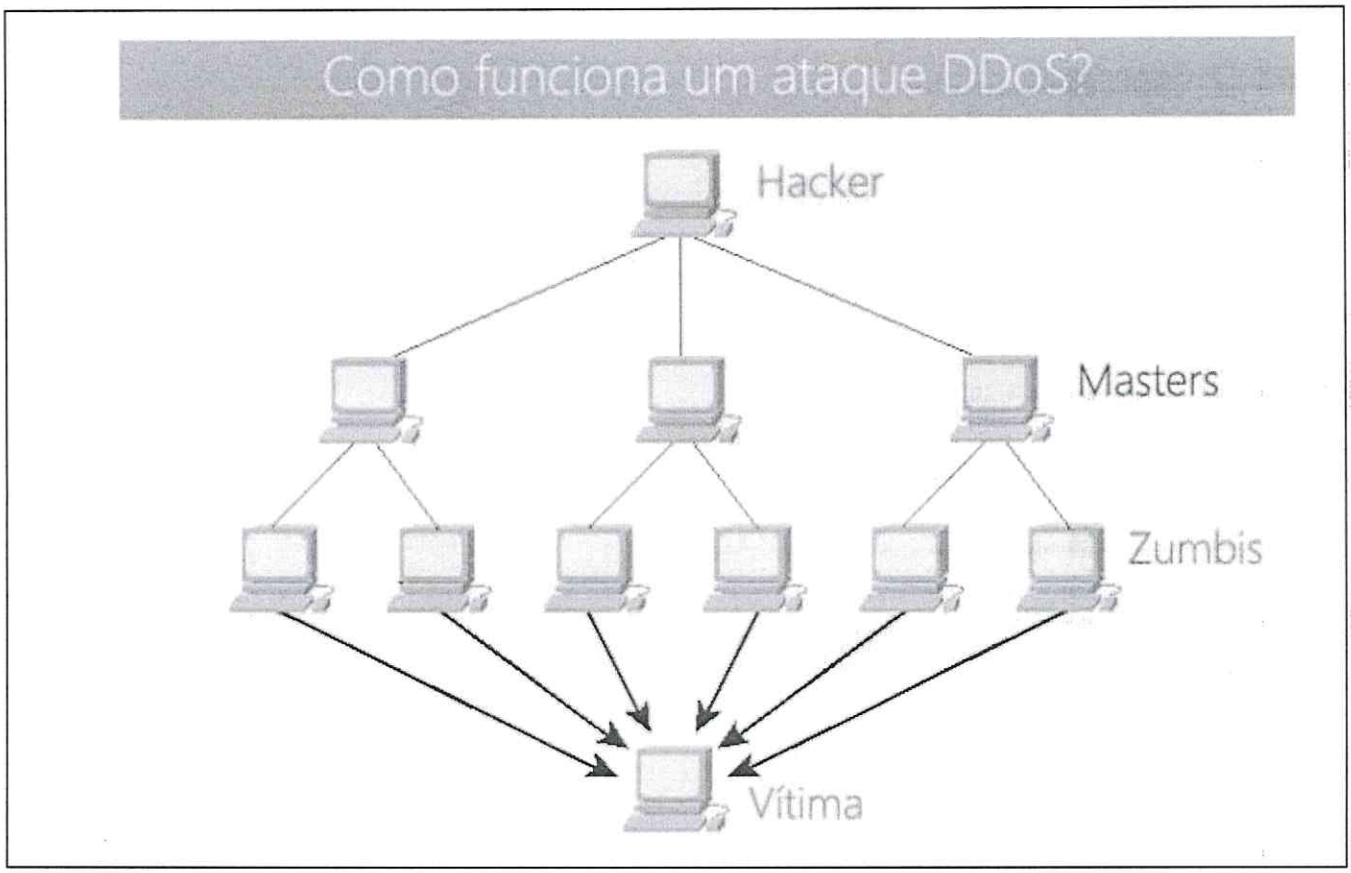
a) Relatório pormenorizado quanto aos problemas apresentados;

Conforme narrado nas primeiras tratativas, havia o indício de que a instabilidade no site da Consulplan – www.consulplan.net – derivava de ataque cibernético, sendo categorizado como DDoS – *Distributed Denial of Service* ou Ataque Distribuido de Negação de Serviço. Esse tipo de ataque explora o pilar da segurança da informação de disponibilidade, e tem como objetivo deixar o serviço indisponível.

No ataque distribuído de negação de serviço, um computador mestre pode gerenciar até milhões de computadores, chamados de zumbis.

Por meio do DDoS, o computador mestre escraviza várias máquinas e as fazem acessar um determinado recurso em um determinado servidor todos ao mesmo tempo. Assim, todos os zumbis acessam juntamente e de maneira ininterrupta o mesmo recurso de um servidor, geralmente um site. Levando em consideração que os servidores web possuem um número limitado de recursos, e consequentemente de usuários que eles conseguem atender ao mesmo tempo, esse grande número de tráfego impossibilita que o servidor seja capaz de atender a qualquer pedido, tornado o servidor indisponível. Desta forma, o servidor começa a exibir a mensagem *503 - Service Unavaliable* ou serviço indisponível.

(32) 3696-4750
www.consulplan.net
atendimento@consulplan.com



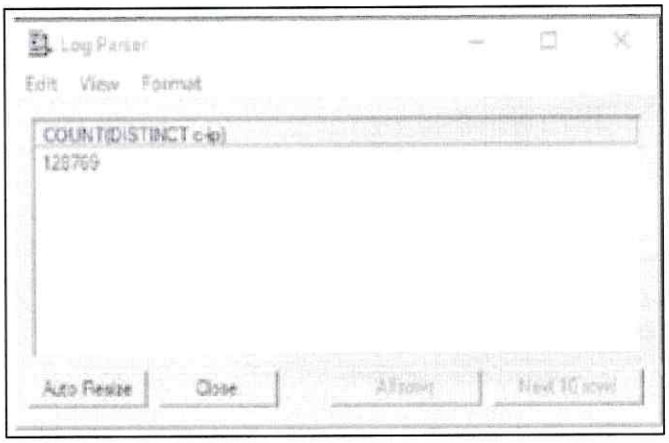
É preciso ressaltar que esse ataque não causa nenhum vazamento de dados, e sim a indisponibilidade do serviço web.

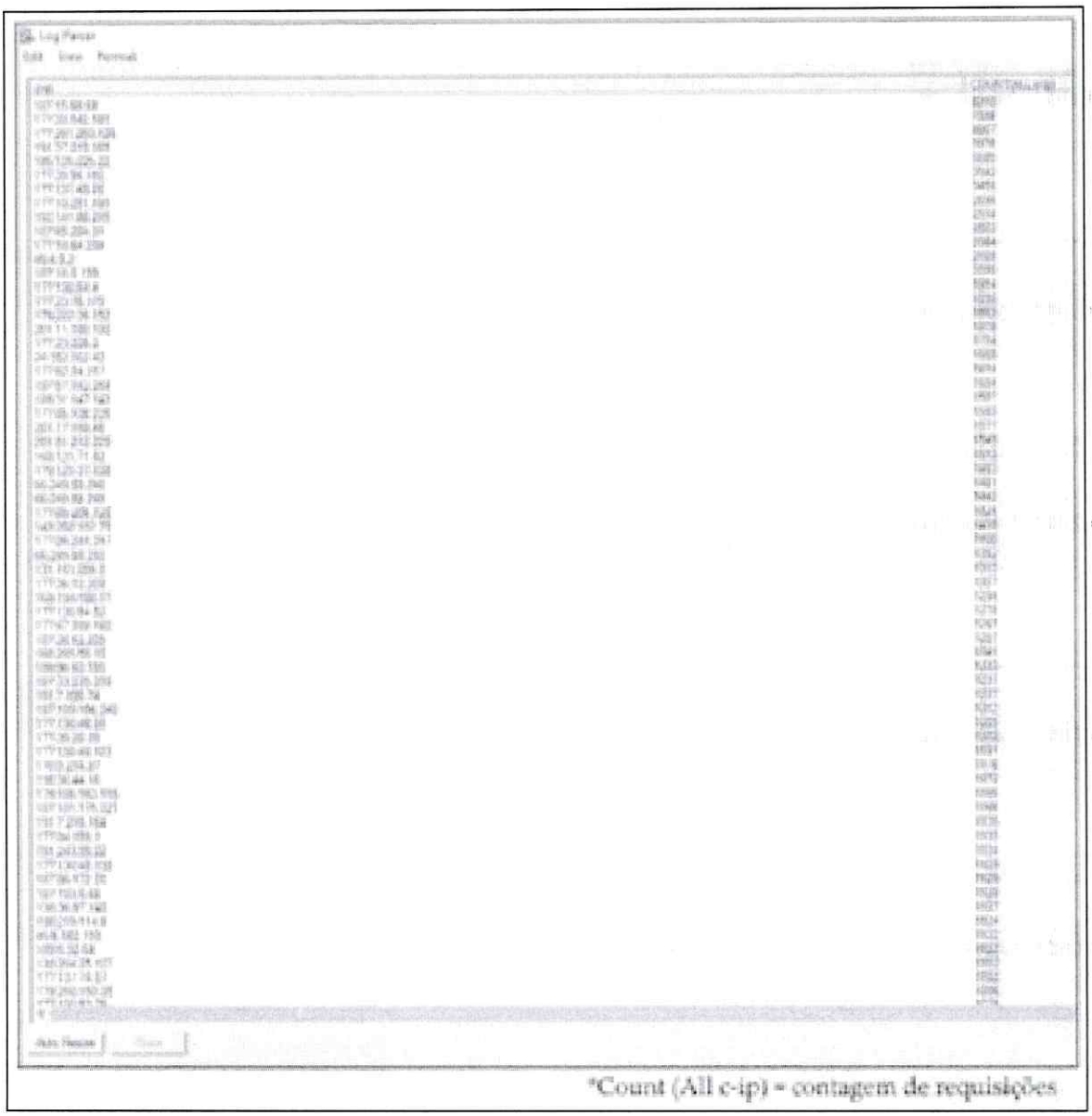
Conforme já esclarecido em documento anterior, o site da Consulplan está hospedado na *Amazon Web Services ou AWS* - https://aws.amazon.com/pt/, que é considerado o maior provedor de Cloud Computing do mundo. A AWS hospeda serviços como a Netflix, Amazon Prime Vídeo e a Amazon.com, que é a maior loja virtual do mundo, ou seja, o nosso site está dentro de uma infraestrutura robusta e segura.

O site está hospedado em uma máquina virtual dentro da AWS, conhecidas como EC2 ou *Elastic Cloud Computing* - https://aws.amazon.com/pt/ec2/features/. Essa tecnologia nos permite aumentar os recursos da máquina de acordo com a demanda.

A página da Consulplan obteve a partir dos minutos antecedentes ao horário agendado (8h50) e durante o período de indisponibilidade (até 10h30), 128.770 diferentes IPs em acesso, sendo certo que após o mapeamento realizado constatou-se que, a página recebeu 11.843.593 requisições, ou seja, foram quase 12 milhões de sessões, que: 1) comprovam a existência de um ataque externo; 2) superam a capacidade técnica do site, tornando-o indisponível ou inconsistente para acesso dos usuários. A título de exemplo, apenas um único IP realizou mais de 8 mil requisições, fato humanamente impossível, ainda que considerado todo o tempo de inatividade do site; e outros milhares de IPs também fizeram requisições humanamente impossíveis.

(32) 3696-4750
www.consulplan.net
atendimento@consulplan.com





*Count (All c-ip) = contagem de requisições

(32) 3696-4750
www.consulplan.net
atendimento@consulplan.com

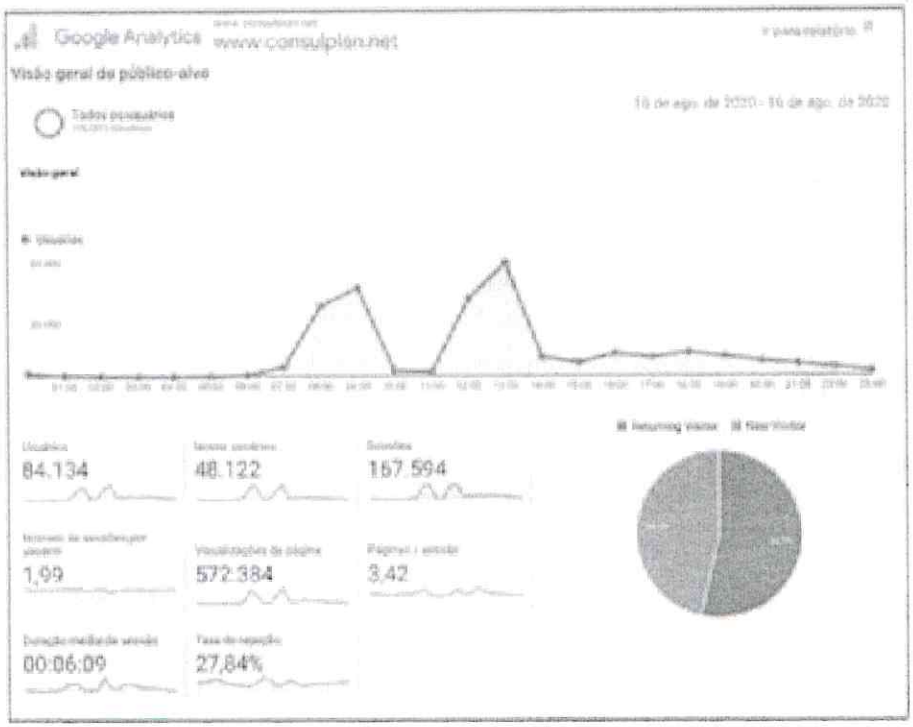
Durante o período de indisponibilidade, como medida imediata para solução, houve a majoração destes recursos em proporção três vezes superior. Iniciando-se com instância de c4.2xlarge, houve a ampliação para c4.8xlarge. Esta majoração, em termos normais de uma possível instabilidade decorrente de volume de acessos humanos, seria suficiente a solucionar a situação.

Instância	vCPU*	Mem (GiB)	Armazenamento	Largura de banda dedicada do EBS (Mbps)	Performance de rede
c4.large	2	3,75	Somente EBS	500	Moderada
c4.xlarge	4	7,5	Somente EBS	750	Alta
c4.2xlarge	8	15	Somente EBS	1.000	Alta
c4.4xlarge	16	30	Somente EBS	2.000	Alta
c4.8xlarge	36	60	Somente EBS	4.000	10 Gigabit

O servidor possui Firewall e Antivírus instalados, e só são habilitadas no servidor as entradas (portas) necessárias para o funcionamento do site. O servidor virtual também fica alocado dentro de um *Security group* - grupo de segurança da AWS, onde só são liberadas as permissões necessárias para que o site possa ser acessado.

Além disso, a Consulplan possui contratado o AWS Shield, um serviço gerenciado que fornece proteção contra ataques distribuídos de negação de serviço (DDoS) para os aplicativos executados na AWS.

Inclusive, de forma a demonstrar a segurança e estabilidade do servidor, destaca-se que esta estrutura foi utilizada na aplicação do 1º Exame de Suficiência, no dia 16 de agosto de 2020, quando houve resistência a ataque de mesma categorização, porém com menor exigência de recursos de banco.



No caso presente, o poder de ataque foi em proporções exponenciais, superior, onde nem mesmo as ferramentas de bloqueio e proteção do servidor foram capazes de suportar, ou seja, foi um ataque premeditado e arquitetado, visando ao prejuízo não apenas da Consulplan, mas de toda a comunidade envolvida, especialmente dos candidatos e do CFC.

Estas foram as constatações preliminares da equipe de T.I da Consulplan. Contudo, a fim de assegurar total imparcialidade e garantir total transparência e boa-fé, a Consulplan fez contratação de uma Auditoria Forense, com total autonomia e independência, para que pudesse analisar os dados do sistema, a fim de emitir parecer conclusivo sobre o ocorrido.

Foi feita a contratação da ZR2 Perícias Forenses tem sólida experiência nas áreas: Administrativa, Cível, Criminal, Trabalhista e Militar. Seus profissionais são membros da HTCIA – International High Technology Crime Investigation Association e habilitados pelo BJA – Bureau of Justice Assistance (Estados Unidos).

Assim, segue anexo o laudo emitido, dando conta que *"é seguro determinar que a indisponibilidade do site www.consulplan.net em 08/11/2020 se deu por ataque cibernético denominado DDoS (Distributed Denial-of-Service) de tipo SYN Flood, conforme já exposto, o tipo de ataque, ainda que com a proteção AWS Shield Standard, não permite a restauração da disponibilidade com o aumento de recursos do servidor sob ataque. "*

Isto é dizer que, apesar do site institucional da Consulplan contasse com ferramentas de segurança, essas não foram capazes de conseguir impedir o sucesso no ataque.

Não são raras os sites e instituições que veem sofrendo ataques cibernéticos nos últimos tempos, imperativo destacar que recentemente o site do Superior Tribunal de Justiça – STJ detectou uma invasão na rede de informática do tribunal na tarde de terça-feira, 03/11/2020, notícia confirmada pelo próprio órgão, disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/04112020-Em-razao-de-ataque-cibernetico--STJ-funcionara-em-regime-de-plantao-ate-o-dia-9.aspx

O Tribunal de Justiça do Rio Grande do Sul passou por situação semelhante, disponível em: https://www.tjrs.jus.br/novo/noticia/nota-de-esclarecimento-3/

E a mais recente empreita foi nas eleições municipais de 2020, onde o site do Tribunal Superior Eleitoral – TSE passou por momentos de instabilidades, disponível em: https://www.tse.jus.br/imprensa/noticias-tse/2020/Novembro/ministro-da-justica-afirma-que-tentativa-de-ataque-ao-sistema-do-tse-nao-afetou-lisura-da-eleicao

Apesar de ser uma situação totalmente previsível, sempre há a possibilidade de vulnerabilidades, pois assim como os softwares de segurança são aprimorados os ataques de hackers também evoluem, as vezes até de forma mais rápida.

Desta forma, entende-se que não houve dolo, culpa ou negligência no caso em tela, mas sim um fato que talvez fosse impossível de ser rechaçado ou se fosse, fatalmente traria prejuízo aos examinandos, como lentidão no sistema ou até mesmo dificuldade de logar no sistema.

b) Relatório de aplicação apresentado pela The Perfect Link, mencionado no item 5 do ofício;

Segue em anexo o relatório do teste de estresse feito pela Consulplan com a consultoria contratada Júlio de Lima – Consultoria em Tecnologia: "Relatório Consulplan.pdf".

Destacamos que a Consulplan não teve acesso ao relatório do teste de estresse feito pela The Perfect Link, o referido teste apenas foi mencionado pela própria Auditoria no parecer de auditoria elaborado em 09 de novembro de 2020, cujo trecho foi transcrito para o ofício em comento.

c) Relatório dos testes e processos que foram realizados pelas empresas de consultoria referenciadas no item 6 do ofício;

Segue em anexo o relatório apresentado pela consultoria contratada: "Relatório consultoria BrazilianDev.pdf".

Segue também em anexo os currículos dos consultores, "Currículo Júlio de Lima - JL Consultoria.pdf" e "Currículo Rafael dos Santos - BrazilianDev.pdf". Os currículos também podem ser consultados publicamente através do Linkedin - https://www.linkedin.com, em https://www.linkedin.com/in/juliodelimas e https://www.linkedin.com/in/rsantosdev.

d) Comprovante das informações apresentadas nos itens 9, 11 e 13 do ofício;

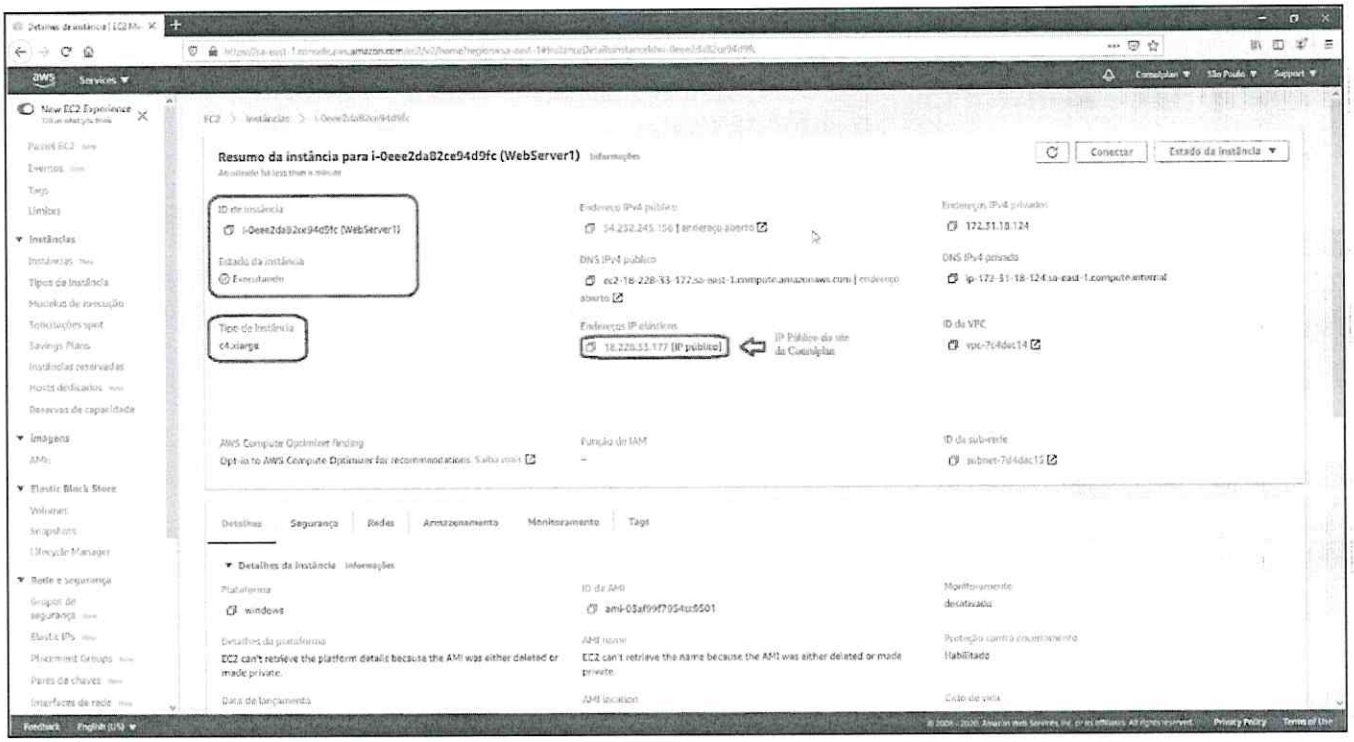
Item 9:

O arquivo de log do servidor que comprova os quase **12 Milhões de requisições** no site da Consulplan – www.consulplan.net, está disponível no link https://d3du0p87blxrg0.cloudfront.net/u_ex201108.zip, o arquivo está compactado e protegido por senha que será enviada por e-mail.

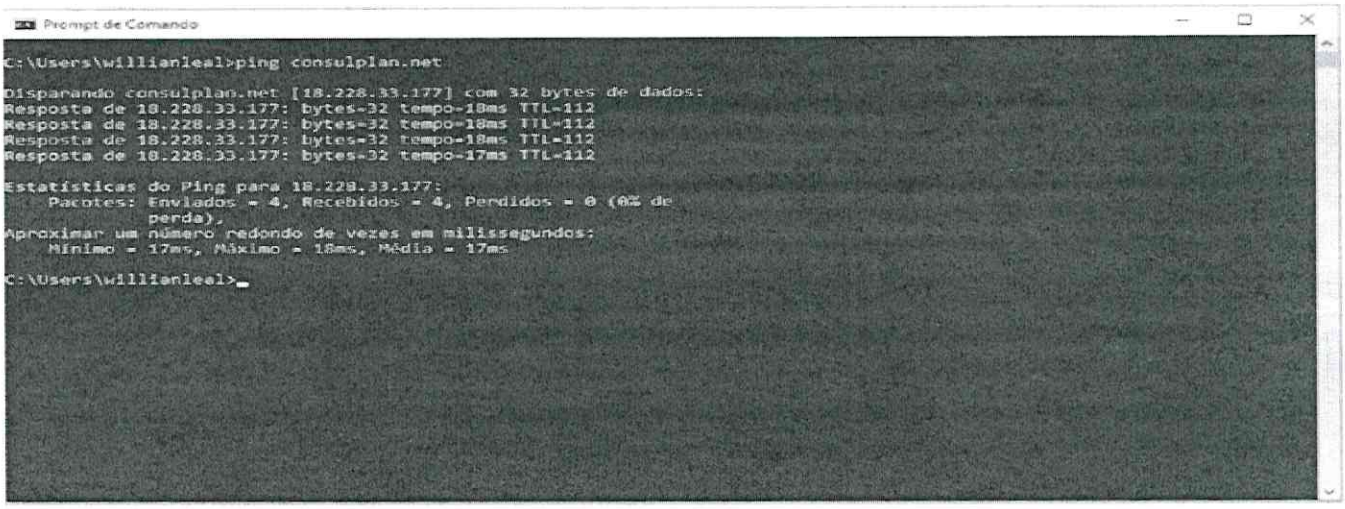
As leituras dos arquivos de log, assim como os respectivos quantitativos apresentados, foram extraídos utilizando o programa *Microsoft Log Parser 2.2* https://www.microsoft.com/en-us/download/details.aspx?id=24659.

Item 11: Hospedagem Consulplan AWS EC2 – Elastic Cloud Computing

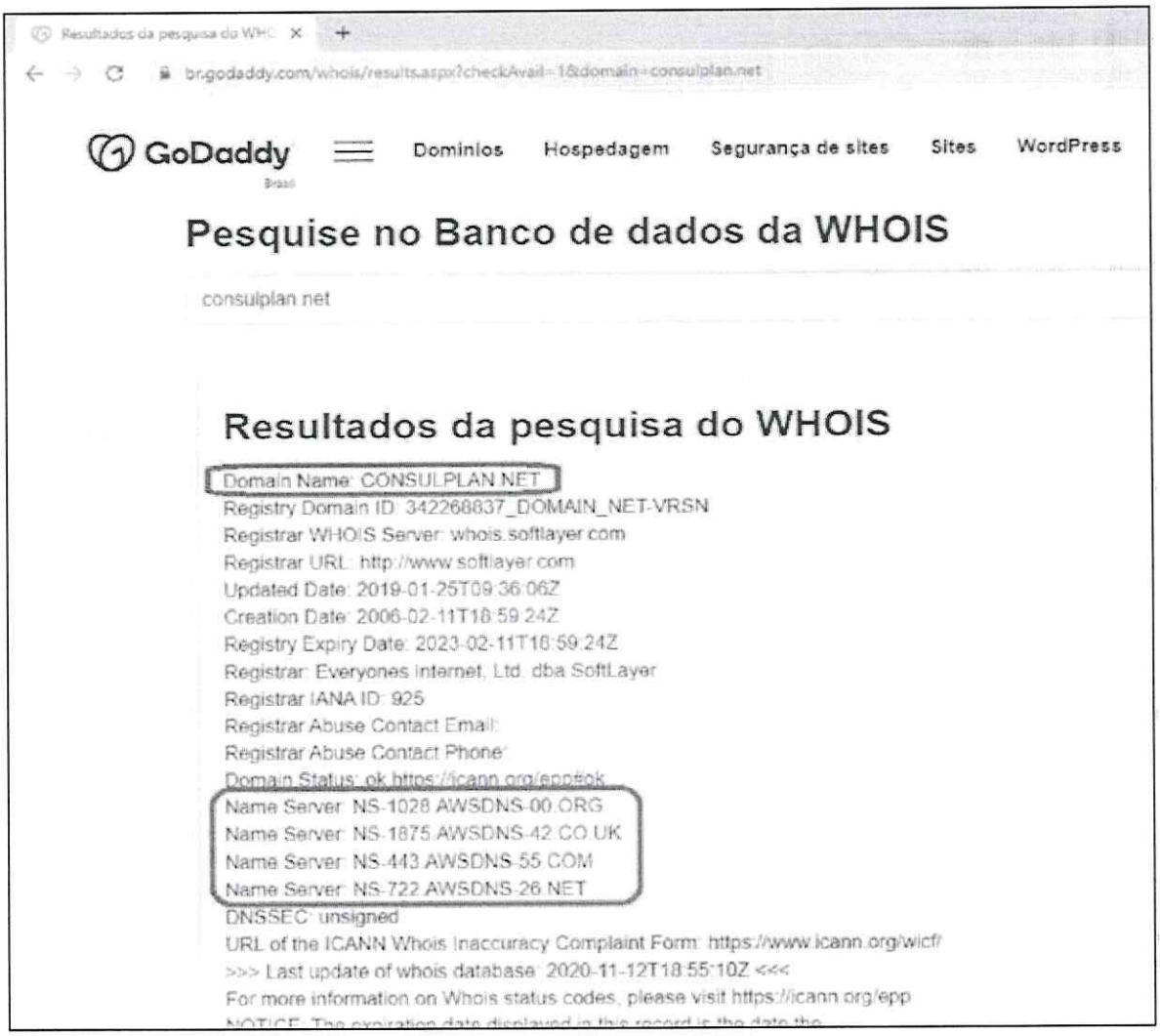
Máquina virtual EC2 alocada na AWS e que hospeda o site da Consulplan – www.consulplan.net



A comprovação de que o IP do servidor pertence ao site da Consulplan pode ser verificado publicamente executando a seguinte linha comando no prompt do Windows, ***ping consulplan.net***, imediatamente o servidor irá responder com o IP pertencente ao site.



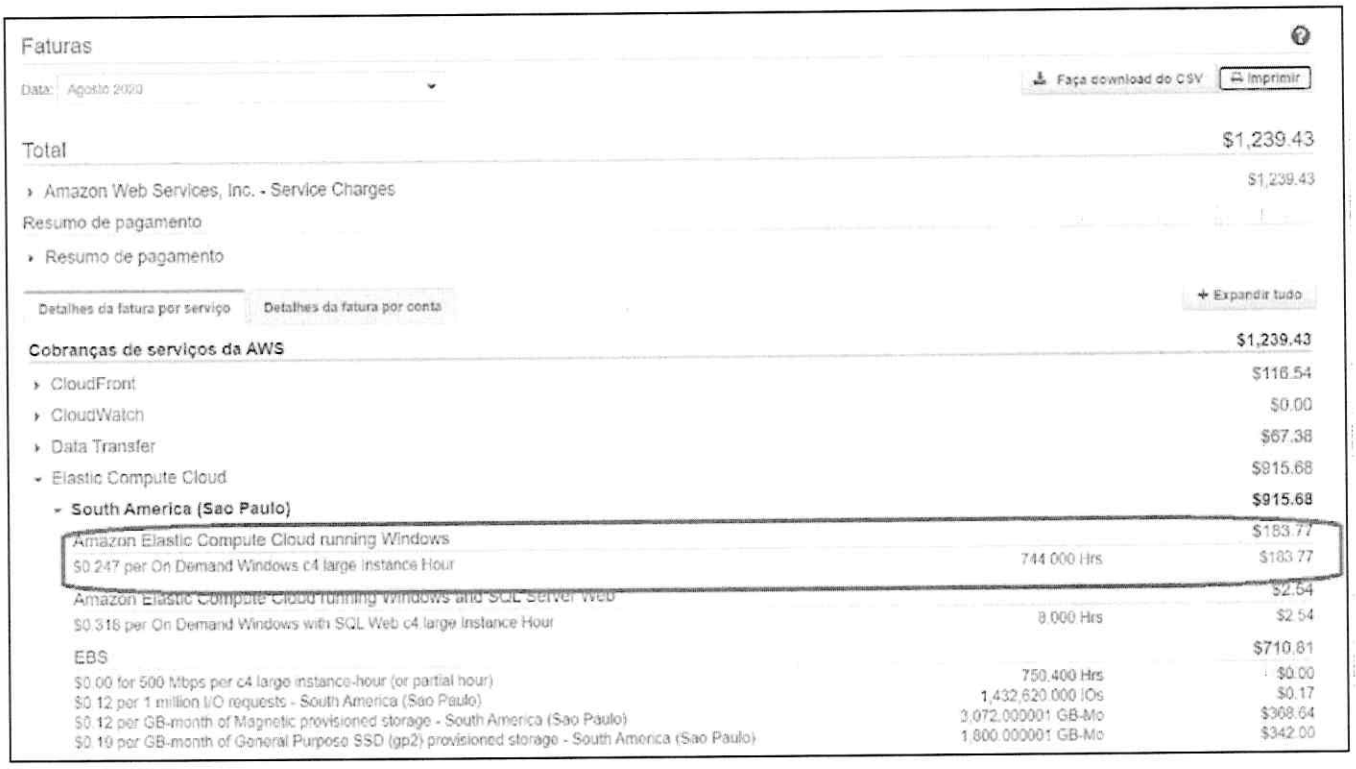
A consulta do DNS do endereço www.consulplan.net que está hospedado no serviço AWS Route 53 também pode ser feita publicamente através do endereço: https://br.godaddy.com/whois/results.aspx?checkAvail=1&domain=consulplan.net.



Item 13:

O serviço de hospedagem utilizado é o mesmo utilizado no EXAME DE SUFICIÊNCIA 1/2020 como pode ser comprovado através do *print* da fatura de pagamento de agosto de 2020.

(32) 3696-4750
www.consulplan.net
atendimento@consulplan.com



Faturas

Data: Agosto 2020

Faça download do CSV | Imprimir

Total	$1,239.43
› Amazon Web Services, Inc. - Service Charges	$1,239.43

Resumo de pagamento

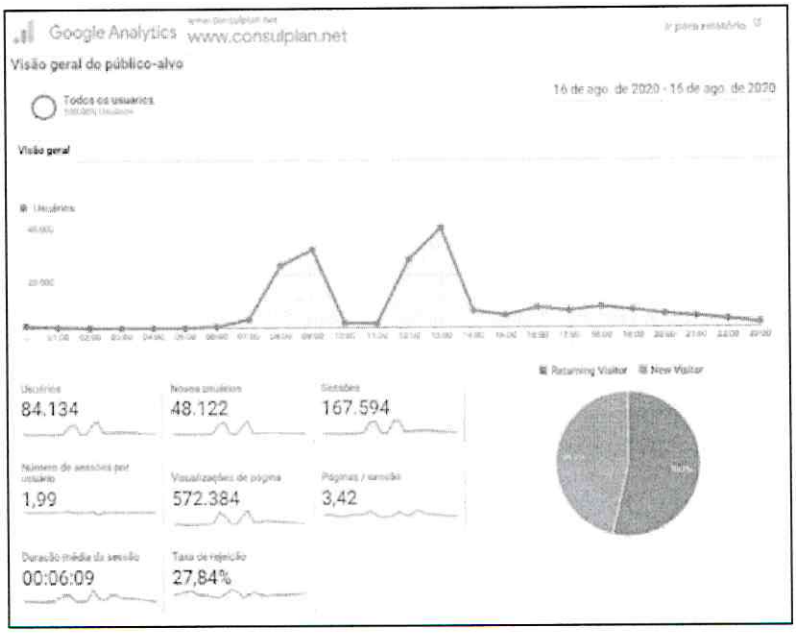
› Resumo de pagamento

Detalhes da fatura por serviço | Detalhes da fatura por conta | + Expandir tudo

Cobranças de serviços da AWS		$1,239.43
› CloudFront		$116.54
› CloudWatch		$0.00
› Data Transfer		$67.38
› Elastic Compute Cloud		$915.68
▾ **South America (Sao Paulo)**		**$915.68**
Amazon Elastic Compute Cloud running Windows		$183.77
$0.247 per On Demand Windows c4 large instance Hour	744.000 Hrs	$183.77
Amazon Elastic Compute Cloud running Windows and SQL Server Web		$2.54
$0.318 per On Demand Windows with SQL Web c4 large instance Hour	8.000 Hrs	$2.54
EBS		$710.81
$0.00 for 500 Mbps per c4 large instance-hour (or partial hour)	750.400 Hrs	$0.00
$0.12 per 1 million I/O requests - South America (Sao Paulo)	1,432,620.000 IOs	$0.17
$0.12 per GB-month of Magnetic provisioned storage - South America (Sao Paulo)	3,072.000001 GB-Mo	$368.64
$0.19 per GB-month of General Purpose SSD (gp2) provisioned storage - South America (Sao Paulo)	1,800.000001 GB-Mo	$342.00

A fatura original segue em anexo com o nome "Fatura AWS agosto 2020.pdf", e a informação acima pode ser vista no final da página 6 da fatura.

O relatório original do Google Analytics que foi apresentado na imagem abaixo segue em anexo com o nome "Analytics www.consulplan.net 16-08-2016.pdf"



Obs: Caso seja necessário, um técnico do CFC pode auditar as informações diretamente no portal da AWS, juntamente com um técnico da Consulplan.

(32) 3696-4750
www.consulplan.net
atendimento@consulplan.com

Segue também em anexo o relatório atualizado da Braziline "RELATORIO V2 SECURITY CONSULPLAN - BRASILINE.pdf", informando que o servidor SRVWEB01 está totalmente atualizado e protegido contra ameaças de acordo com as melhores práticas do fabricante F-Secure. Com todos os updates relacionados a segurança aplicadas neste servidor, firewall ativado do Windows, atualizações e vacinas de antivírus e agente de detecção e resposta ativados.

e) Participação de integrante da TI do CFC na reunião que será realizada com a Amazon Web Service (AWS), empresa responsável pela hospedagem do site da Consulplan, agendada para 13/11/2020.

Reunião foi realizada na sexta-feira, dia 13/11/2020, às 13:00h. O link da reunião foi enviado para que a TI do CFC e o Auditoria, The Perfect Link, pudessem participar. Assim, na referida reunião estiveram presentes o Sr. Rogério e Edson, por parte do CFC, e o Sr. Fernando, representando a The Perfect Link.

Sem mais para o momento, apresentamos votos de elevada estima e consideração, ficando sempre à disposição para fornecimento de dados e participação de reuniões para discutirmos a melhor solução para o caso em tela.

Atenciosamente,

Elder José Dala Paula Abreu
Diretor Presidente – Consulplan

PARECER TÉCNICO DE INFORMÁTICA FORENSE
RESPOSTA INCIDENTE

Ofício: 001640 em Resp. ao Ofício n.º 1979/2020 CFC-Direx
Consulente: CONSULPLAN CONSULTORIA E PLAN. EM ADM. PÚBLICA EIRELI

Responde a este parecer, **ANTONIO RODRIGUES FILHO**, brasileiro, casado, perito forense, portador da C.I. nº 9.730.506-4, inscrito sob nº de CPF/MF 054.167.939-29, com Telefone 041 3117-7676, e escritório profissional situado à Rua Marcos Andreatta, 284, Ecoville, Curitiba, Estado do Paraná, CEP 81.200-120, onde recebe processos, intimações e materiais para perícia.

DO PROFISSIONAL:

Analista de sistemas;
Tecnólogo em redes de computadores;
Especialista em Computação Forense
Especialista em Direito Digital;
Especialista em segurança da informação;
Especialista em documentoscopia avançada com uso de quimiometria;
Certificado MCP e MCSE Microsoft;
OSCP – Offensive Security Certified Professional;
CCSE – Certified Security Expert;
Membro Consultor da Comissão de Direito Eletrônico OAB/PR portaria 06/2011;
Membro da HTCIA (International High Technology Crime Investigation Association);
Atua como Perito Oficial nos 26 Estados brasileiros;
Habilitado pelo Conselho da Justiça Federal – AJG
Tribunal de Justiça do Paraná – CAJU-PR
Tribunal Regional do Trabalho 9ª Região – Registro nº 1340
Tribunal de Justiça de Santa Catarina
Tribunal Regional do Trabalho 12ª Região
Tribunal de Justiça de São Paulo – Registro nº 16.173
Habilitado pejo BJA – Bureau of Justice Assistance (Estados Unidos);

Rua Marcos Andreatta, 284 | Ecoville | Curitiba - PR | CEP 81.200-120
www.zr2.com.br | E-mail atendimento@zr2.com.br | Fone/Whatsapp +55 41 3117-7676 | 11 3500-8092

Para o presente trabalho e para fins de declaração de impedimento ou suspeição em processos judiciais deve ser considerado a atuação como Perito Oficial no Tribunal da Justiça Federal da 4ª Região - TRF4, assim como nos Tribunais de Justiça do Paraná, São Paulo e Santa Catarina.

OBJETO DO PARECER

Portal eletrônico da consulente (www.consulplan.net) onde seria divulgado endereço eletrônica para realização de Exame de Suficiência 2/2020 do Conselho Federal de Contabilidade (CFC).

OBJETIVO DO PARECER

Determinar a origem da indisponibilidade do portal eletrônico da consulente na data de 08 de novembro de 2020 durante a aplicação de Exame de Suficiência 2/2020 do Conselho Federal de Contabilidade (CFC).

ATAQUE DDoS SYN Flood

Um dos tipos mais comuns de ataque DDoS e também um dos mais efetivos é o SYN Flood. Este tipo de ataque consiste em enviar um grande volume de pacotes SYN até o alvo, sem nunca efetivamente abrir a conexão. Como os pacotes SYN possuem alguns poucos bytes, o ataque pode ser feito mesmo a partir de uma conexão doméstica, em especial por computadores contaminados e então escravizados por um servidor, dessa forma os tornando zumbis para este tipo de ataque.

SYN flood ou ataque SYN é uma forma de ataque de negação de serviço na qual o atacante envia uma sequência de requisições SYN para um sistema-alvo visando uma sobrecarga direta na camada de transporte e indireta na camada de aplicação do modelo OSI (Open System Interconnection).

Quando um cliente tenta iniciar uma conexão TCP com um servidor, o cliente e o servidor trocam um série de mensagens, que normalmente são assim:

- O cliente requisita uma conexão enviando um SYN (*synchronize*) ao servidor.
- O servidor confirma esta requisição mandando um SYN-ACK(acknowledge) de volta ao cliente.
- O cliente por sua vez responde com um ACK, e a conexão está estabelecida.

Isto é o chamado aperto de mão em três etapas (Three-Way Handshake).

Um cliente malicioso, que implemente intencionalmente um protocolo TCP errado e incompleto, pode não mandar esta última mensagem ACK. O servidor

Rua Marcos Andreatta, 284 | Ecoville | Curitiba - PR | CEP 81.200-120
www.zr2.com.br | E-mail atendimento@zr2.com.br | Fone/Whatsapp +55 41 3117-7676 | 11 3500-8092

irá esperar por isso por um tempo, já que um simples congestionamento de rede pode ser a causa do ACK em falta.

Esta chamada conexão semi-aberta explora a boa-fé do protocolo TCP que espera por um certo tempo e algumas tentativas de restabelecimento de um sinal ACK válido para retomar a comunicação. A resposta maliciosa ao comando SYN gerada pelo cliente pode ocupar recursos no servidor (memória e processamento). Pode ser possível ocupar todos os recursos da máquina, com pacotes SYN. Uma vez que todos os recursos estejam ocupados, nenhuma nova conexão (legítima ou não) pode ser feita, resultando em negação de serviço. Alguns podem funcionar mal ou até mesmo travar se ficarem sem recursos desta maneira.

Ao contrário do que muitos pensam, não se resolve negação de serviço por SYN Flood limitando conexões por minuto, pois as conexões excedentes seriam descartadas pelo firewall, sendo que desta forma o próprio firewall tiraria o serviço do ar, desta forma, se limitar as conexões SYN a 10/seg, um atacante precisa apenas manter uma taxa de SYNs superior a 10/s para que conexões legítimas sejam descartadas pelo firewall.

Um ataque de SYN Flood é feito com os IPs forjados (spoof), para que o atacante não receba os ACKs de suas falsas solicitações.

CONSIDERAÇÕES

Inicialmente devemos considerar que por parte da Consulplan foram realizados testes de desempenho e de segurança para realização do exame de Suficiência, assim como pelo Conselho Federal de Contabilidade fora contratada empresa especializada de auditoria, *THE PERFECT LINK*, para que previamente fosse aprovado a aplicação *online* do exame agendado para o dia 09/11/2020.

Com isto em mente, bem como que foi de conhecimento das partes que o link para realização do exame seria disponibilizado pelo site www.consulplan.net. ou seja, link https://exames.consulplan.net. O site institucional da Consulplan, apesar de possuir ferramentas de segurança disponibilizadas pelo serviço AWS Shield Standard[1] para impedir ataques DDoS, não foi suficiente para o ataque articulado, pois o tipo de ataque sofrido dependeria de proteção adicional. De modo a ser considerado como uma vulnerabilidade de nível médio, todavia, o impacto da indisponibilidade em serviço como do caso em tela, se devidamente avaliado pelas diretrizes da ISO 270005 seria de nível alto, especialmente se referenciado pela ISO 27034.

DAS ANÁLISES

De acordo com os relatórios já apresentados, seja pela *THE PERFECT LINK, BRASILINE* assim como a própria *CONSULPLAN,* é possível aferir que a aplicação disponibilizada para realização online do exame de suficiência é *tecnicamente* segura, escalável e estável, assim como permite monitoramento e auditoria ativa, porém, os sites cfc.org.br e consulplan.net embora escalável e

[1] https://docs.aws.amazon.com/pt_br/waf/latest/developerguide/ddos-overview.html

Rua Marcos Andreatta, 284 | Ecoville | Curitiba - PR | CEP 81.200-120
www.zr2.com.br | E-mail atendimento@zr2.com.br | Fone/Whatsapp +55 41 3117-7676 | 11 3500-8092

monitorável não tinham os controles de segurança necessários para evitar ou gerenciar riscos cibernéticos, como ataques DDoS (Distributed Denial of Service), desta forma, por meio dos logs do servidor que hospeda o site consulplan.net é possível identificar prontamente, fosse pela auditoria ativa ou posterior, 246 acessos suspeitos, ou seja, com mais de 899 requisições, característica de ataque DDoS do tipo SYN Flood, dos quais totalizaram 175.847 requisições, ou seja, uma média de 1426 requisições por IP.

Notadamente, podemos ver os IPs abaixo como principais suspeitos e indicativos iniciais de ataques:

N	IP	REQUISIÇÕES	PAÍS
1	187.15.68.69	8210	BR
2	177.33.142.181	7386	BR
3	177.201.203.126	4867	BR
4	191.37.219.169	3976	BR
5	185.125.225.22	3585	NL
6	177.39.96.180	3542	BR
7	177.131.49.26	3456	BR

----------Total **35.022** Requisições

Neste panorama temos o total de 128.770 IPs acessando o site, dos quais tiveram 11.843.593 requisições, sendo que na espectativa de 90 mil inscritos, cada IP deveria fazer no máximo 6 requisições, ou seja, era esperado 540.000 requisições, todavia, foi totalizado 21 vezes a mais o número de requisição esperado e ainda considerando que o servidor teve escalonamento de serviço ativo alterado conforme o número de acessos, o mesmo não se mostrou suficiente, pois de acordo com a disponibilização de recurso, mais requisições eram realizadas até o estouro de pool total de recursos.

DA SEGURANÇA DOS DADOS

De acordo com os registros de Logs de segurança, bem como a inspeção do servidor objeto de perícia, não há indicativos de técnicos de qualquer nível de vazamento de dados por meio do servidor afetado, assim como o mesmo mostra-se íntegro em relação aos seus sistemas de armazenamento de dados e gestão de acessos.

Adicionalmente a ferramenta de Windows Defender Firewall with Advanced Security não possuem registros de invasão ou intrusão por qualquer técnica reconhecida na atualidade que seja passível de vazamento de dados primários ou secundários.

CONCLUSÃO

De acordo com as análises preliminares realizadas, é seguro determinar que a indisponibilidade do site www.consulplan.net em 08/11/2020 se deu por ataque cibernético denominado *DDoS* (Distributed Denial-of-Service) de tipo *SYN Flood*, conforme já exposto, o tipo de ataque, ainda que com a proteção AWS Shield Standard, não permite a restauração da disponibilidade com o aumento

Rua Marcos Andreatta, 284 | Ecoville | Curitiba - PR | CEP 81.200-120
www.zr2.com.br | E-mail atendimento@zr2.com.br | Fone/Whatsapp +55 41 3117-7676 | 11 3500-8092

de recursos do servidor sob ataque.

Ainda, o referido ataque é possível a partir de vulnerabilidades não críticas.

Finalmente, é seguro declarar que por meio do ataque sofrido não há elementos técnicos que indiquem qualquer tipo de vazamento de dados, seja primário ou secundário, por ou em decorrência do ataque ora em comento.

O presente trabalho pericial dispensou 36 horas e vai assinado em 5 páginas timbradas.

Curitiba, 16 de novembro de 2020.

Antonio Rodrigues Filho
Perito Forense | CTO

Rua Marcos Andreatta, 284 | Ecoville | Curitiba - PR | CEP 81.200-120
www.zr2.com.br | E-mail atendimento@zr2.com.br | Fone/Whatsapp +55 41 3117-7676 | 11 3500-8092