ATAQUE CIBERNÉTICO

que virou notícia no mundo

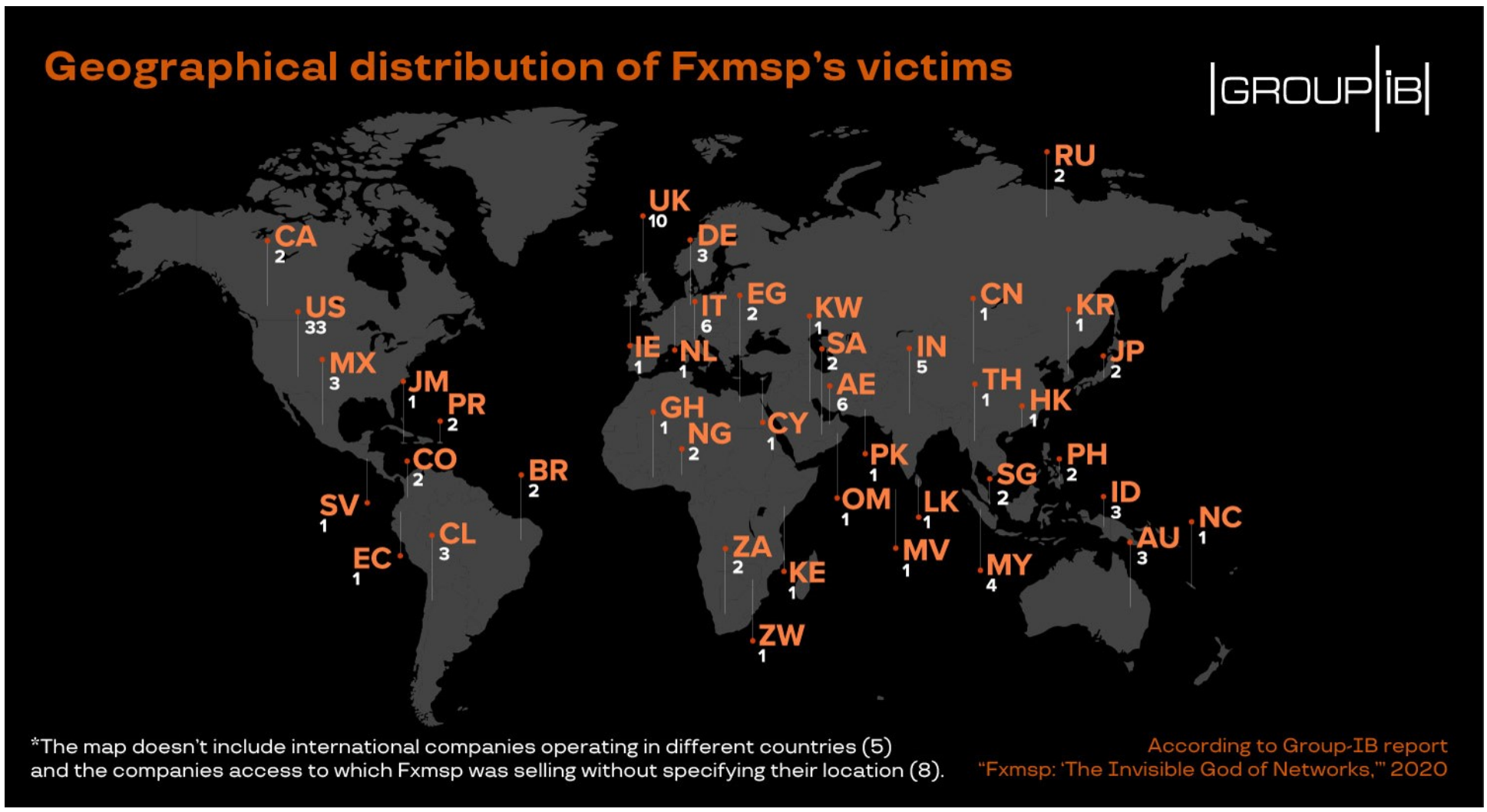
Vamos explorar o mundo dos ataques cibernéticos que tanto afetam as empresas. Nosso objetivo é que você compreenda melhor o mercado de trabalho de segurança da informação, que sofre transformações constantes com os novos negócios, novas tecnologias e com a evolução dos ataques cibernéticos.

FXMSP, O "DEUS INVISÍVEL"

Em 2020, um *hacker* ganhou notoriedade. É o caso de Fxmsp, o "Deus invisível", um cidadão de Cazaquistão de 37 anos de idade na data. O nome real dele é Andrey Turchin; ele ainda não foi preso, sendo acusado de conspiração, fraude eletrônica, fraude por acesso ilícito a dispositivos e abuso do uso do computador (*hacking*).

O mapa das vítimas de Fxmsp mostra a abrangência global de seus ataques. São 300 empresas de 44 países. As revelações são do Group-IB, após pagar US$ 1,5 milhões por todas as informações roubadas e os segredos para as invasões.

Distribuição geográfica das vítimas de Fxmsp



Fonte: Volkov (2020).

QUIZ

1 Com relação a ataques cibernéticos, considere as afirmativas a seguir:

I. Ataques cibernéticos podem ser feitos a partir de qualquer localidade pela internet.

II. Ataques cibernéticos podem ser realizados a partir da exploração de uma única vulnerabilidade.

III. É um desafio a proteção contra ataques cibernéticos, porque todas as vulnerabilidades devem ser tratadas; para o criminoso, basta encontrar um ponto fraco.

IV. Em um ataque cibernético, o agente de ameaça explora vulnerabilidades utilizando técnicas de ataques, incluindo ferramentas.

É correto o que se afirma em:

a. I e II, apenas.

 Tente novamente...

Esta alternativa está incorreta. Leia novamente a questão e reflita sobre o conteúdo para tentar novamente.

b. I, II e III, apenas.

 Tente novamente...

Esta alternativa está incorreta. Leia novamente a questão e reflita sobre o conteúdo para tentar novamente.

c. I, III e IV, apenas.

 Tente novamente...

Esta alternativa está incorreta. Leia novamente a questão e reflita sobre o conteúdo para tentar novamente.

d. I e IV, apenas.

 Tente novamente...

Esta alternativa está incorreta. Leia novamente a questão e reflita sobre o conteúdo para tentar novamente.

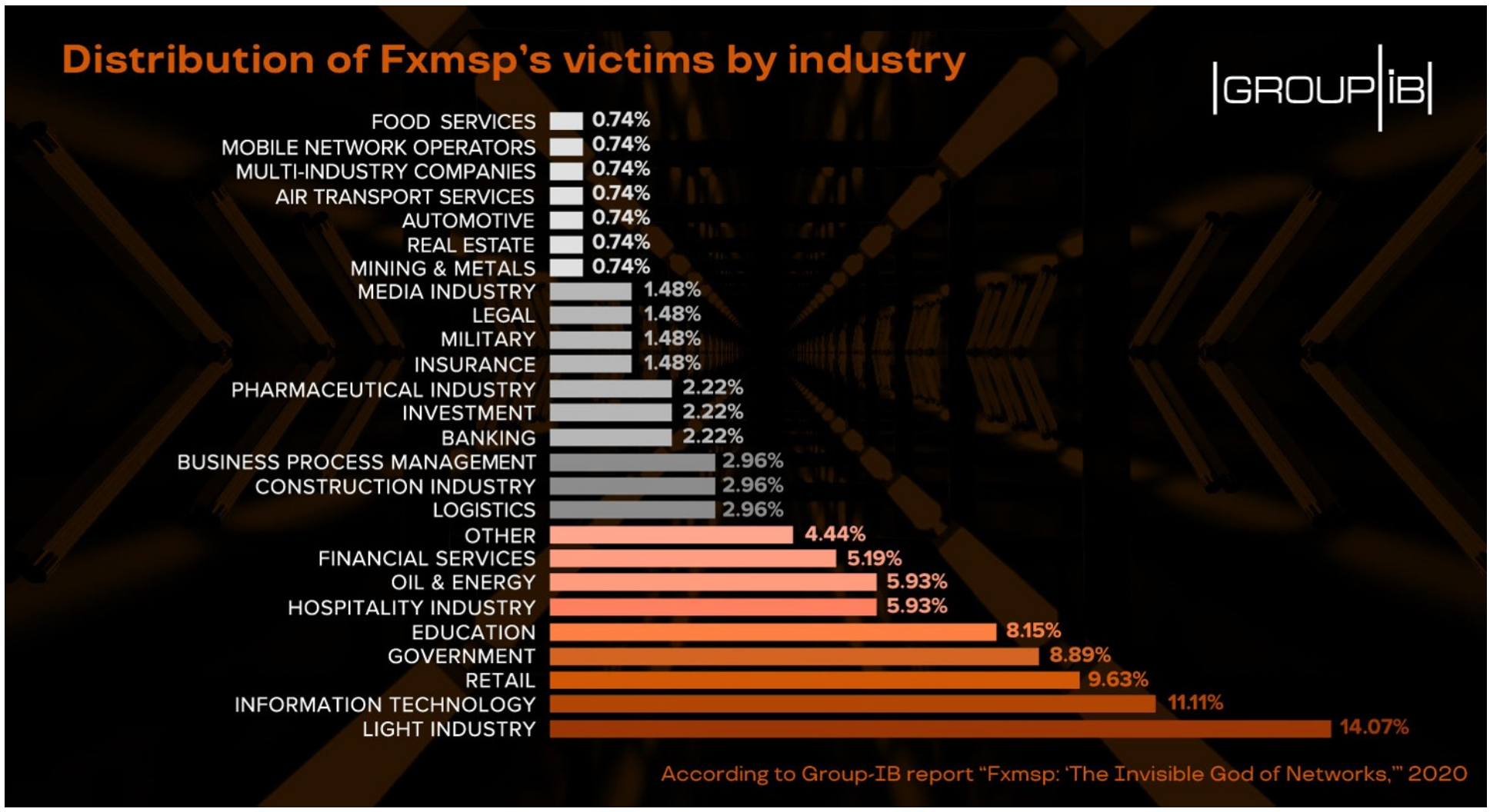
e. I, II, III e IV.

 Correto!

Todas as afirmações representam características de ataques cibernéticos: qualquer localidade onde haja acesso à internet, exploração de uma única vulnerabilidade, necessidade de proteger contra todas as vulnerabilidades e uso de ferramentas e técnicas de ataques que levam ao incidente de segurança.

As atividades criminosas de Fxmsp eram conhecidas desde 2016. Suas vítimas eram de todos os setores, como mostra a figura a seguir.

Distribuição por indústria das vítimas de Fxmsp



Fonte: Volkov (2020).

Chama a atenção a lista de vítimas de Fxmsp, que inclui empresas de cibersegurança, como McAfee, Symantec, Trend Micro.

Além das atividades criminosas, Turchin foi inovador: vendia as informações obtidas oferecendo uma experimentação, com acesso prévio limitado para potenciais compradores, a fim de que pudessem verificar a qualidade e a confiabilidade de seus produtos.

Além disso, Turchin sabia como monetizar suas façanhas, tendo contratado um gerente comercial, um "laranja", que negociava as informações com potenciais compradores. Ele vendia não somente as informações, mas também o acesso à empresa e ainda códigos-fonte.

E como era o *modus operandi* de Fxmsp?

Ele realizava os ataques focando um serviço em especial, o *Remote Desktop Protocol* (RDP), na porta TCP 3389.

QUIZ

2 Qual dos ataques citados a seguir possibilitou a descoberta de serviços específicos, como o RDP?

b. *Ransomware*.

Tente novamente...

Esta alternativa está incorreta. Leia novamente a questão e reflita sobre o conteúdo para tentar novamente.

c. *Scan*.

 Correto!

O *scan* de portas possibilita o mapeamento dos serviços existentes na empresa ou em determinada faixa de endereços IP.

d. Ataque do Homem do meio ou *Man-In-The-Middle* (MITM).

 Tente novamente...

Esta alternativa está incorreta. Leia novamente a questão e reflita sobre o conteúdo para tentar novamente.

e. Negação de serviço ou *Denial-of-Service* (DoS).

 Tente novamente...

Esta alternativa está incorreta. Leia novamente a questão e reflita sobre o conteúdo para tentar novamente.

RDP é o serviço disponibilizado pelo Windows para acesso remoto, o Microsoft Terminal Services. O acesso remoto possibilita que acessos externos sejam feitos a equipamentos, que, muitas vezes, estão na rede interna da empresa. Isso facilita atividades como administração remota ou suporte remoto, porém abre uma brecha significativa que pode ser explorada em ataques. O *firewall* tem que liberar a porta TCP 3389 para que o RDP funcione, e, já que o *firewall* possibilita essas conexões, os ataques passam diretamente pelo *firewall*.

O *firewall* bloqueia tráfegos baseado em suas regras, que são basicamente as origens, os destinos e os serviços/portas liberadas pela empresa. No caso do RDP (porta TCP 3389), a regra deve definir quem pode fazer o acesso remoto a quais equipamentos da empresa. Uma vez liberado o tráfego desse protocolo, o suporte técnico, por exemplo, pode acessar os equipamentos via Microsoft Terminal Services, em que uma senha de acesso é solicitada. O *hacker* também pode explorar esse acesso ao serviço para realizar os ataques.

QUIZ

3 No caso do RDP, uma vez que Fxmsp conseguiu o acesso ao serviço, qual é o passo posterior do ataque, considerando que há a necessidade de senha para acessar o equipamento?

a. Não é necessário o passo posterior.

 Tente novamente...

Esta alternativa está incorreta. Leia novamente a questão e reflita sobre o conteúdo para tentar novamente.

b. Força bruta para descobrir a senha.

 Correto!

Uma vez obtida a conexão no equipamento via RDP, o *hacker* precisa acessar o serviço com a senha. Um ataque para descobrir a senha é o ataque de força bruta, em que diferentes combinações são testadas até o sucesso.

c. *Ransomware*.

 Tente novamente...

Esta alternativa está incorreta. Leia novamente a questão e reflita sobre o conteúdo para tentar novamente.

d. Ataque do Homem do meio ou *Man-In-The-Middle* (MITM).

Tente novamente...

Esta alternativa está incorreta. Leia novamente a questão e reflita sobre o conteúdo para tentar novamente.

e. Negação de serviço ou *Denial-of-Service* (DoS).

Tente novamente...

Esta alternativa está incorreta. Leia novamente a questão e reflita sobre o conteúdo para tentar novamente.

Uma vez descoberta a senha de acesso ao equipamento via RDP, Fxmsp passa para o passo posterior, que visa ao domínio do equipamento ou servidor. Ele desabilita o antivírus e o *firewall*, além de criar contas adicionais e descobrir outras credenciais da rede. Outra medida dele é a instalação de *backdoor*, que abre uma porta no servidor para que acessos posteriores possam ser feitos diretamente pelo atacante.

Metasploit é uma ferramenta para criação de *exploits*, que são utilizados por profissionais de segurança da informação para explorar vulnerabilidades e testar a segurança de diferentes serviços e aplicações.

O *meterpreter* utiliza o *metasploit* para criar um *backdoor* que funciona na memória da vítima, sem persistência e uso de criptografia na comunicação com o servidor de comando e controle. Informações podem vazar via esse *backdoor*.

QUIZ

4 Fxmsp utilizava esse *backdoor* a cada 15 dias para evitar a sua detecção. Qual controle de segurança é capaz de detectar uma comunicação de *backdoor*, da rede interna, para o servidor de comando e controle na internet?

a. IDS / IPS.

Correto!

IDS / IPS monitora o tráfego em busca de padrões que indicam ataques em andamento. O ataque de Fxmsp, que acionava o *backdoor* a cada 15 dias, mostra que IDS / IPS podem ser evadidos. *Firewall* bloqueia, antivírus detecta vírus em equipamentos, autenticação faz parte do controle de acesso e a criptografia protege a mensagem.

b. *Firewall*.

Tente novamente...

Esta alternativa está incorreta. Leia novamente a questão e reflita sobre o conteúdo para tentar novamente.

c. Antivírus.

Tente novamente...

Esta alternativa está incorreta. Leia novamente a questão e reflita sobre o conteúdo para tentar novamente.

d. Autenticação.

Tente novamente...

Esta alternativa está incorreta. Leia novamente a questão e reflita sobre o conteúdo para tentar novamente.

e. Criptografia.

Tente novamente...

Esta alternativa está incorreta. Leia novamente a questão e reflita sobre o conteúdo para tentar novamente.

As informações das empresas eram roubadas com a movimentação lateral a partir do acesso obtido via RDP, explorando-se, ainda, as relações de confiança existentes na rede. Para finalizar, Fxmsp fazia com que mudanças de senhas ou restauração de *backups*, que poderiam ser feitas pelas empresas em caso de desconfiança de um ataque, não resolvessem o comprometimento do equipamento e servidor, já que os *backups* também continham o *backdoor*.

QUIZ

5 Qual seria a sua recomendação para que sua empresa não tenha o serviço RDP explorado, como ocorreu com cerca de 300 empresas de 44 países que foram vítimas de Fxmsp?

a. Uso de *firewall* e IDS / IPS.

Tente novamente...

Esta alternativa está incorreta. Leia novamente a questão e reflita sobre o conteúdo para tentar novamente.

b. Uso de antivírus.

Tente novamente...

Esta alternativa está incorreta. Leia novamente a questão e reflita sobre o conteúdo para tentar novamente.

c. Uso de criptografia.

Tente novamente...

Esta alternativa está incorreta. Leia novamente a questão e reflita sobre o conteúdo para tentar novamente.

d. Uso de portas alternativas TCP para o RDP e controles de autenticação.

Correto!

Caso a empresa precise utilizar o RDP, é recomendável que a porta padrão seja alterada. Porém, isso apenas minimiza a possibilidade de ataque. Outra medida importante é habilitar controles de autenticação, como o travamento em caso de tentativa de ataque de força bruta.

e. Não é possível fazer nada.

Tente novamente...

Esta alternativa está incorreta. Leia novamente a questão e reflita sobre o conteúdo para tentar novamente.

REFERÊNCIAS

BBC NEWS. 'Deus invisível': quem é o hacker acusado de roubar informações de 300 empresas em 44 países. BBC News, 2020. Disponível em: https://www.bbc.com/portuguese/internacional-53604079. Acesso em: 1 dez. 2020.

VOLKOV, D. Fxmsp: the untold story of infamous seller of access to corporate networks who made at least USD 1.5 mln. Group-IB, 2020. Disponível em: https://www.group-ib.com/media/fxmsp/. Acesso em: 1 dez. 2020.