Guerra Cibernética já chegou!

A guerra cibernética não tem limitações territoriais! É invisível, não tem rosto, não distingue governo de organizações privadas, não faz sanções, não dá trégua, mas existe e quanto mais a nação for informatizada, mais catastróficos serão os danos. Atualmente nos países desenvolvidos e em desenvolvimento, há sistemas financeiros interligados, sistema de fornecimento de energia, sistema de controle de tráfico, abastecimento de água e internet, todos podem ser alvos de ataques *hackers* que podem deixar estes serviços inoperantes e provocando desabastecimento, acidentes, dentre outras catástrofes e requer uma ação do governo para restabelecer esses serviços... e não estou nem falando num grupo treinado em *cyber* defesa que o país deveria ter.

Mesmo a guerra tradicional entre Rússia e Ucrânia esteja acontecendo a quilômetros de distância e a maioria das pessoas acompanharem pela TV e, muitas vezes ao vivo, a guerra cibernética é travada nos bastidores, às ocultas e num campo de batalha desconhecido pela maioria das pessoas.

A guerra cibernética, apesar de se manifestar com maior intensidade na Rússia e Ucrânia onde o conflito armado é intenso, esta provoca efeitos colaterais nas grandes potências como nos USA, países apoiadores da guerra, ou mesmo aqueles que se declararem neutros durante a guerra. Países que têm servidores de internet localizados em Data Centers nesses países, estão propensos ficarem sem serviços de internet em razão da guerra.

Nessa arena cibernética, os principais serviços a serem atacados são os dos governos, tais como o fornecimento de energia, água, notícias, transporte coletivo, trânsito, dentre outros. A seguir acontecimentos que marcaram a "guerra paralela" travada nos bastidores da guerra tradicional:

Em 2007, segundo o site Diário do Aço, com a reportagem: "*A guerra cibernética já é uma realidade, e as empresas precisam ser preparar*", hackers russos desativaram a internet da Estônia com ataques DDos (ataque de negação de serviços) contra os sites de governos e instituições financeiras, o motivo era que o país queria, simplesmente, mover um memorial da 2ª. Guerra Mundial. Em 2008, a Rússia lançou um ataque hacker na internet da Geórgia a fim de facilitar invasão física da Rússia. Em 2009, hackers russos derrubaram internet do Quirquistão com a finalidade de pressionar a evacuação de uma base militar dos USA, e em 2014, ataque cibernético contra sistema eleitoral na Rússia.

Resumindo, os ataques cibernéticos não são de hoje, já acontecem a muito tempo por motivos simplórios ou mesmo significativos, porém nunca até momento foi tão explícito para o mundo como na guerra entre Rússia e Ucrânia, tanto que a Ucrânia pediu ajuda de um "exército de Tecnologia da Informação (TI)" para fazer frente aos ataques cibernético russos... e foi atendida! Conforme a reportagem no site **G1**: "*Ucranianos mobilizam vale do silício na guerra contra a Rússia*".

Mas os ataques cibernéticos não param por aí! Um ataque se transformou em global através do malware NotPetya que começou o ataque no sistema de contabilidade da Ucrânia e se auto-propagou para o resto do mundo, ou seja, os sistemas foram contaminados em várias organizações espalhada pelo mundo.

Em 4/1/2022, de acordo com o **site SecurityWeek**, com a reportagem: "*BlackEnergy malware usado em ataques da rede elétrica da Ucrânia*" a empresa de segurança ESET descobriu um malware denominado BlackEnergy que tinha como alvo as empresas de mídias e energia elétrica

na Ucrânia e a iSIGHT Partners acredita que os hackers russos responsáveis pelos ataques fazem parte do grupo Sandworm Teams, esses ataques tiveram como alvos a concessionária de energia elétrica e empresas jornalísticas da Ucrânia.

No entanto, em 15/1/2022, a Microsoft relatou a ação de um malware denominado de WhisperGate que não sequestravam dados, mas simplesmente os destruíam! Esses hackers não estão querendo dinheiro para o sequestro de dados como acontece na maioria dos ataques, eles querem simplesmente apagar os dados e dessa forma provocar o caos, chamado também de "operação limpeza de dados". Em 23/2/2022, foi descoberto o malware HermeticWiper, que tinha o objetivo também de apagar os dados, ou seja, pura destruição.

Já em 4/2/2022, segundo o **site SecurityWeek**, com a reportagem: "*Microsoft, Symantec Share Notes on Russian Hacks Hitting Ukraine*", especialistas da Microsoft compartilharam observações sobre uma "enxurrada" de novos ataques de espionagem cibernética da agência de espionagem da Rússia nas organizações ucranianas. O grupo responsável foi o Gamerodon do grupo do governo russo, este grupo tem atuando desde 2013 através de ataques de intrusão e são considerados audaciosos. Conforme os relatórios da Microsoft, os ataques de *phishing* por e-mail são os primeiros estágios de contaminação nesse tipo ataques. De acordo com os dados oficiais do governo ucraniano, os grupos russos foram responsáveis por mais de 5.000 ataques contra 1.500 sistemas do governo ucraniano.

No dia 27/2/2022, na **BBC News Brasil**, na reportagem: "*A guerra cibernética paralela entre Rússia e Ucrânia*", Anatoliy Tchach, encarregado de negócios da Ucrânia no Brasil, disse que o site oficial da embaixada e os e-mails dos funcionários estavam inoperantes em razão de ataques cibernéticos maciços.

Em 28/2/2022, segundo o **site SecurityWeek**, com a reportagem: "*Russia vs Ukraine – The war in cyberspace*", no dia 24/2 sites do governo ucranianos foram atacados por ataque de DDoS e empresas de segurança cibernética detectaram fragmentos de malware destrutivo. O Secretário da OTAN, Jens Stoltenberg, alertou que os ataques podem infringir o artigo 5° da OTAN, que considera um ataque a qualquer aliado a OTAN é um ataque a todos os membros. Hackers do grupo Anonymous reivindicaram a desconfiguração de sites russos. E a ESET alertou sobre golpes que exploram guerra na Ucrânia, pois alguns hackers participam de campanhas falsas de ajuda as vítimas de guerra como iscas para roubarem dinheiro ou dados. Assim, verifica-se que há um confronto entre grupos hackers que tanto defendem quanto atacam, conforme as suas convicções e causas.

Conforme a **CNN – Portugal**, em 06/3/2022, na reportagem: "*Ucrânia quer retirar a Rússia da internet. O que poderia acontecer*?", as grandes corporações colaboram com as sanções contra a Rússia, a Apple deixou de vender seus produtos e limitou alguns de seus serviços na Rússia. Facebook, Google e Twitter também suspenderam seus serviços na Rússia (veja texto "Guerra Cibernética" no site inovação143). O governo ucraniano enviou uma carta para a ICANN, organização sem fins lucrativos que supervisiona nomes de domínios e endereço de IP na internet, pedido que a Rússia fosse desligada da internet, mas dificilmente esse pedido será atendido, segundo os especialistas em internet.

Guerra cibernética é uma guerra silenciosa, sem alardes, sem rostos, mas que pode atingir a todos e a qualquer momento nesse mundo cada vez mais informatizado.

Reflexões: em pleno séc. XXI o homem não aprendeu que nas guerras não há vencedores... mas sim vítimas! Pessoas que muitas vezes não estão relacionadas com a motivação da guerra, não

apoiam a guerra, não querem guerra, porque a guerra só destrói, desumaniza, é o flagelo da humanidade. Conhecimentos deveriam ser empregados em diminuir a desigualdade social, no equilíbrio do clima na terra, na proteção da “casa de todos”: o planeta terra!

Autor: Afonso F. Fernandes, é colaborador do site inovação143, professor universitário, analista em segurança da informação, administrador, economista, biólogo, doutor em economia e doutorando em administração.

Contato: (92) 984531621 ou afonsofernandes65@hotmail.com

Referências

1. https://www.diariodoaco.com.br/noticia/0095554-a-guerra-cibernetica-ja-e-uma-realidade-e-as-empresas-precisam-se-preparar

2. https://www.securityweek.com/blackenergy-group-uses-destructive-plugin-ukraine-attacks

3. https://www.securityweek.com/microsoft-symantec-share-notes-russian-hacks-hitting-ukraine

4. https://www.securityweek.com/cyberattacks-ukraine-new-worm-spreading-data-wiper-ransomware-smokescreen

5. https://www.bbc.com/portuguese/internacional-60551648

6. https://g1.globo.com/tecnologia/noticia/2022/03/02/ucranianos-mobilizam-vale-do-silicio-na-guerra-contra-russia.ghtml

7. https://cnnportugal.iol.pt/guerra/ucrania-quer-retirar-a-russia-da-internet-o-que-poderia-acontecer/20220306/6221ce540cf2c7ea0f1d083f

8. https://istoe.com.br/gigantes-da-tecnologia-boicotam-seus-servicos-na-russia/

9. https://www.bbc.com/portuguese/internacional-60551648