BOLETIM

OBSERVATÓRIO DE CIBERSEGURANÇA

JUNHO 2023 | nº 2/2023

DESTAQUES

Hacktivismo

O hacktivismo pode ser definido como a "junção do ativismo político com o *hacking* informático", a que corresponde um uso "ilegal ou legalmente ambíguo de instrumentos digitais para fins políticos", como sejam *defacements* de *websites*, ataques de negação de serviço distribuída (DDoS), furto de informação, cibersabotagem, entre outros (Samuel, 2004). O termo "hacktivismo" resulta da contração do termo "hacker" e do termo "ativista".

Guerra na Ucrânia

A invasão da Ucrânia por parte da Federação Russa a 24 de fevereiro de 2022 transformou o contexto geopolítico internacional, acentuando polarizações e antagonismos entre países e blocos de influência. Esta situação teve consequências no ciberespaço, nomeadamente com a intensificação de ameaças estatais, paraestatais e hacktivistas que utilizam a esfera digital como teatro de atuação.

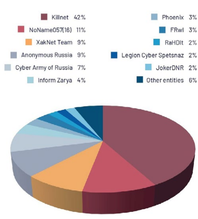
Grupos hacktivistas

Esta circunstância é propensa à criação de novos grupos de hacktivistas, em resultado de predisposições para ações coletivas, com afinidades a um dos polos do conflito. As características destes grupos são ambíguas quanto ao tipo de organização e ao género de apoio que têm. Dada a existência de práticas de falsa bandeira e ambiguidades na imputação a atores no ciberespaço, a identificação destes grupos não é definitiva.

PANORÂMICA

- O CERT-EU (equipa de resposta a incidentes de cibersegurança das instituições da União Europeia - UE) realizou um estudo sobre os efeitos da guerra na Ucrânia no ciberespaço no período entre janeiro de 2022 e fevereiro de 2023.
- Com base numa análise a 806 ciberataques relacionados com a guerra na Ucrânia, o CERT-EU identificou concretamente 18 grupos supostamente hacktivistas apoiantes da Federação Russa.
- O grupo com maior preponderância foi o chamado Killnet, seguido dos Noname057(16), dos XakNet Team, dos Anonymous Russia e dos Cyber Army of Russia. Estes grupos afirmam ter alvos semelhantes entre si e tendem a publicitar-se mutuamente nas redes sociais.
- O tipo de ciberataque mais frequente realizado por estes grupos é o DDoS a *websites*, ataque através do qual múltiplas solicitações enviadas simultaneamente provocam a disrupção de uma plataforma digital.
- Esta análise identifica ainda 32 grupos supostamente hacktivistas pró-Ucrânia. Aqueles que tiveram atividade mais intensa foram os chamados Anonymous, os Team OneFist, os DDoSecrets, os IT Army of Ukraine e os NB65.

Supostos grupos hacktivistas pró-Rússia
(% dos ataques de hacktivistas deste tipo)



Fonte: (CERT-EU)

PERSPETIVA

1 Tipicamente, os hacktivistas tendem a atacar sobretudo empresas, administração pública e infraestruturas críticas e em menor escala os indivíduos em particular; possuem um nível baixo ou médio de capacidades técnicas e de recursos; atuam individualmente, organizados em rede ou como coletivo sem hierarquia; e têm como motivações dominantes os fatores ideológicos (Bruijne *et al.*, 2017).

2 Um dos grupos que marca a história do hacktivismo é o Anonymous. Criado no início deste século e ligado à plataforma 4chan, caracterizava-se por ser fragmentado, descentralizado e por cultivar o anonimato. Ganha notoriedade com os ataques à Cientologia. A sua persistência explica-se pela capacidade de mediatização, identidade reconhecível, informações ambíguas em seu torno, abertura a novos participantes e imprevisibilidade de atuação (Coleman, 2013).

3 Os grupos hacktivistas que emergiram na sequência da guerra na Ucrânia têm características diferentes do hacktivismo do passado: têm um forte pendor patriótico, atuam num contexto de guerra e da sua narrativa, realizam ataques mais sofisticados do que o hacktivismo tradicional e nem sempre é claro se são apoiados por Estados ou não (Burgess, 2022). Neste contexto, o grupo Anonymous ressurgiu assumindo igualmente este tipo de características (Tidy, 2022).

4 Entre os supostos hacktivistas pró-Federação Russa, o grupo Killnet é particularmente ativo. Realiza sobretudo ataques de DDoS aos setores público e privado, com apetência por atacar organizações da saúde, nomeadamente laboratórios farmacêuticos, hospitais e clínicas (Dahan e Pasha, 2023). Entre março de 2022 e fevereiro de 2023, este grupo reclamou para si a autoria de cerca de 90 ataques a organizações em países da Europa e da América do Norte (CERT-EU, 2023)

5 De acordo com o CERT-EU, os países mais atacados pelos supostos hacktivistas pró-Federação Russa e pró-Ucrânia foram a Ucrânia, a Rússia, a Bielorrússia e diversos países da União Europeia, com destaque para a Polónia, a Letónia, a Estónia e a Lituânia. Considerando os dois polos do conflito e todos os grupos envolvidos, os setores mais atacados foram a Administração Pública, a Defesa e as Telecomunicações (CERT-EU, 2023).

6 Tendo em conta a frequência de ciberataques destes grupos que usam DDoS, é importante seguir algumas boas práticas nas organizações para antecipar esta ameaça: identificar na infraestrutura digital os pontos que podem ser vulneráveis a DDoS; ter um plano de resposta a um cenário de ataque; instalar serviços de proteção contra DDoS; testar e avaliar regularmente a capacidade de proteção instalada; e integrar este problema nas análises de risco (ENISA, 2019).

PUBLICAÇÕES E NOTÍCIAS

O **CNCS**, no dia 3 de maio, lançou mais um episódio do *podcast* Comunicar Cibersegurança, desta feita sobre o tema Gestão do Risco e com o convidado Fernando Mendes, sócio fundador da GDPR.pt e da Focus2Comply. Neste terceiro episódio, aborda-se a necessidade de as organizações definirem de forma sistematizada os riscos no ciberespaço. Esta discussão surge no contexto do lançamento de um *Guia para a Gestão dos Riscos* pelo CNCS.

O **Observatório de Cibersegurança do CNCS**, no dia 4 de maio, publicou o *Relatório Tecnologias Emergentes*, no qual são estudadas cinco tecnologias cujos desenvolvimentos próximos podem ter impacto na cibersegurança: a Computação em Nuvem, a Internet das Coisas, a Inteligência Artificial, a Tecnologia 5G e as Tecnologias Quânticas. Este estudo foi realizado por uma equipa do Instituto de Telecomunicações, em articulação com o Observatório de Cibersegurança.

A **ENISA – Agência da União Europeia para a Cibersegurança**, no dia 10 de maio, publicou o *Relatório Campanha do Mês Europeu da Cibersegurança 2022*, em que analisa os resultados desta campanha considerando um inquérito aplicado ao público a quem foi dirigida. O inquérito mostra que a ação obteve bastante alcance, que os conteúdos foram genericamente compreendidos e que houve um incremento nas boas práticas de ciber-higiene no público-alvo.

O **Secretário de Estado da Digitalização e da Modernização Administrativa, Mário Campolargo, e o CNCS, com o apoio do Conselho Superior de Segurança do Ciberespaço**, no dia 16 de maio, lançaram a campanha #LerAntesClicarDepois, através da qual se procura alcançar a generalidade da população com mensagens essenciais sobre boas práticas de ciber-higiene. Esta campanha, para a sua divulgação, conta com a parceira da RTP e de outras entidades públicas e privadas.

O **Instituto Nacional de Estatística (INE)**, no dia 23 de maio, publicou um destaque com os principais resultados relativos à cibersegurança, presentes no Inquérito à Utilização das Tecnologias de Informação e Comunicação nas Empresas. Os dados mostram que "54,4% das empresas declararam ter documentos sobre medidas, práticas ou procedimentos de segurança das TIC em 2022, sendo Portugal o 4.º país da UE com a percentagem mais elevada".

O **CNCS**, nos dias 14, 15 e 16 de junho, na Alfândega do Porto, realiza mais uma conferência C-Days. Este evento contará com inúmeros convidados que irão debater a cibersegurança de um ponto de vista multidisciplinar. O mote deste ano será "Mais confiança". O objetivo é discutir os processos de cibersegurança que podem gerar mais confiança nos cidadãos e nas organizações para as suas relações económicas e sociais, bem como na prevenção de ciberataques.

CNCS Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança