Ciberataques coordenados atingem aliados e colocam NATO na linha de fogo

itsecurity.pt/news/analysis/ciberataques-coordenados-atingem-aliados-e-colocam-nato-na-linha-de-fogo

Os recentes **ciberataques** dirigidos a **países da NATO**, incluindo **Portugal**, levantam questões sobre a **origem, a motivação e o impacto desta campanha**. Num cenário global onde a cibersegurança se tornou uma extensão das **dinâmicas geopolíticas**, os ataques a infraestruturas críticas, empresas e entidades governamentais evidenciam uma crescente sofisticação e coordenação.

A digitalização da economia e dos serviços públicos expande a superfície de ataque, tornando os países mais vulneráveis a ameaças que vão além do crime organizado, envolvendo também grupos patrocinados por Estados. Estes atores recorrem ao ciberespaço para fins estratégicos, seja através de espionagem, desinformação ou ações de disrupção, num contexto onde a distinção entre ciberguerra e ataques oportunistas se esbate cada vez mais.

"A nossa missão de atacar os membros da NATO continua! De momento, […] vamos atacar Portugal", declarou um alegado grupo do Telegram que reúne alegados cibercriminosos indonésios, segundo a CNN Portugal. A mensagem surgiu em referência ao ciberataque à Agência para a Integração, Migrações e Asilo (AIMA), em dezembro de 2024, que levou à desativação temporária do seu site. O incidente evidencia a vulnerabilidade das infraestruturas digitais nacionais face a ciberameaças internacionais e reforça as preocupações sobre a crescente sofisticação das campanhas cibercrimininais, sublinhando a urgência de medidas preventivas mais robustas.

A NATO foi contactada, mas, até à publicação deste artigo, não prestou declarações.

De criminosos a atores estatais: quem está por trás dos ataques?

A ligação entre os ciberataques e a atual conjuntura geopolítica é inegável, com evidências crescentes de colaboração entre grupos criminosos e Estados hostis. O Relatório Riscos & Conflitos 2024 do Observatório de Cibersegurança do Centro Nacional de Cibersegurança (CNCS), publicado em 2024 a respeito do ano anterior, destaca que *"os cibercriminosos, os atores estatais e os hacktivistas foram os agentes de ameaça mais relevantes a atuar no ciberespaço de interesse nacional em 2023"*. O relatório menciona que *"o contexto de guerras na Ucrânia e no Médio Oriente promoveu a polarização internacional e movimentações de diversos atores para se afirmarem de forma estratégica e ideológica no ciberespaço, algo que começa a intensificar-se a partir de 2022"*. Além disso, os ataques têm como objetivo desestabilizar as infraestruturas críticas e obter informações sensíveis.

O Director Global Field CTO da Sophos, Chester Wisniewski, partilhou a sua experiência como especialista na matéria e revelou que *"a Rússia contenta-se em causar dor e incómodo aos aliados da Ucrânia e faz vista grossa quando os seus grupos criminosos atacam essas entidades"*. Já no caso da China, Chester Wisniewski destaca que, tal como documentado no relatório Pacific Rim da Sophos sobre os ataques da China às firewalls da empresa, estes casos *"parecem tratar-se*

mais de entidades não governamentais que desenvolvem trabalho de exploit em nome de atacantes e espiões de Estados-nação". No entanto, *"em ambos os casos, há provas de cooperação, mesmo que os objetivos finais sejam diferentes"*, diz.

De acordo com Bruno Castro, Fundador e CEO da VisionWare, entre os principais atores envolvidos nestas operações está o grupo pró-Rússia NoName057 (16), responsável por ataques de DDoS a países da NATO desde 2022, e a unidade militar russa GRU 29155, também conhecida como Cadet Blizzard ou Ember Bear, que já utilizou malware – como o WhisperGate na Ucrânia – para comprometer redes na Europa e América do Norte, aponta o especialista.

As principais táticas dos ciberataques

"Os ciberataques recentes contra países da NATO têm-se caracterizado por uma crescente sofisticação e diversificação nas técnicas utilizadas", defende Bruno Castro, referindo-se a ataques de DDoS, campanhas de phishing avançadas e infiltrações em infraestruturas críticas. O especialista deu o exemplo de uma missão – a "Baltic Sentry" – que a NATO lançou com o objetivo de proteger infraestruturas submarinas, após sabotagens em cabos de telecomunicações no Mar Báltico, indício claro da escalada desta guerra.

"Como vimos nos recentes avisos do NCSC (Reino Unido), CISA (EUA) e ACSC (Austrália), os dispositivos edge estão a ser cada vez mais visados para obter acesso às redes das vítimas", revela Chester Wisniewski. *"Publicámos uma extensa série de posts que documentam como a China teve como alvo os dispositivos de rede numa campanha que durou cinco anos, e esta atividade […] tem continuado sem parar"*, explica também. Além disso, os criminosos recorrem a abordagens diretas, como o envio massivo de spam seguido de tentativas de contacto via Microsoft Teams e Slack, passando-se por equipas de apoio técnico para obter controlo remoto de dispositivos.

A Inteligência Artificial (IA) tem sido uma aliada do cibercrime, sobretudo na criação de conteúdos de phishing mais credíveis e na automatização de esquemas fraudulentos via mensagens. *"Em Portugal, por exemplo, isto também pode facilitar a escrita de mensagens de spam credíveis em português, uma vez que os modelos de IA sabem a diferença entre o português do Brasil e o português nativo"*, alerta Chester Wisniewski. Neste sentido, Bruno Castro também aponta a IA como *"uma tendência […] em burlas, principalmente através de deepfakes de imagem e voz. Ainda que não seja algo muito comum nos noticiários, já acontece e a tendência será aumentar com o tempo"*.

No entanto, apesar das inovações tecnológicas, o ransomware continua a ser uma ameaça persistente, com ataques baseados em táticas simples, mas eficazes. *"O que estão a fazer está a funcionar, pois maioritariamente roubam palavras-passe e exploram dispositivos de rede não corrigidos. Não há necessidade de fazer nada de novo ou sofisticado, porque as vítimas ainda não estão a 'tapar os buracos' mais básicos"*, realça Chester Wisniewski.

Ataques a serviços públicos e privados: as principais diferenças

Embora os ciberataques afetem tanto entidades públicas quanto privadas, as motivações subjacentes podem diferir. *"Ciberataques direcionados a empresas maioritariamente envolvem objetivos financeiros, enquanto ciberataques direcionados a entidades públicas, além de também envolverem esse interesse monetário, englobam ainda motivações de disrupção social e objetivos políticos"*, explica Bruno Castro. A Administração Pública detém um ativo de elevado valor para o cibercrime: *"os dados massivos sobre os seus cidadãos que, pelo potencial de utilização em*

ações de fraude, são de enorme valor para a comunidade cibercriminosa". Esta realidade torna essencial que as entidades públicas adotem estratégias de segurança robustas e ajustadas ao risco, algo que, segundo Bruno Castro, ainda representa um desafio: *"é fundamental que trabalhem continuamente de forma a avaliar a sua capacidade de proteção, resiliência e resposta a ciberataques. Nesse campo, o setor privado estará mais bem preparado em termos de know-how"*.

Chester Wisniewski explica que, embora a distinção entre ataques ao setor público e privado esteja a diminuir, existe uma tendência crescente na exploração das cadeias de abastecimento. *"No setor privado, isto permite que criminosos que têm motivações financeiras tentem atacar muitas organizações ao mesmo tempo; e no setor público pode traduzir-se em que tentem muitas vezes explorar fraquezas nas relações de confiança com terceiros"*.

Impacto em Portugal

Portugal não escapa a esta realidade. De acordo com a CNCS *"os indivíduos e as PME foram as vítimas mais frequentes de ciberataques durante 2023. Contudo, a administração pública local foi o tipo de alvo que mais impactos sofreu"*. Ao transformar o ano de 2024 em números, os incidentes de cibersegurança registados no ciberespaço de interesse nacional atingiu um total de 11.163 casos, segundo dados do CNCS. Este aumento está parcialmente ligado a uma maior capacidade de deteção por parte de fontes automatizadas, especialmente na identificação de malware, o que proporcionou ao CERT.PT uma visibilidade mais ampla sobre o panorama nacional. No entanto, mesmo excluindo estas fontes, o número de incidentes registados foi de 2.761, representando um crescimento de 36% face a 2023, ano em que foram reportados 2.025 incidentes.

O relatório do CNCS revela que, além das infeções por malware – responsáveis por 7.965 incidentes –, os ataques que exploram o fator humano continuam a ser uma preocupação significativa. O phishing, com 790 registos, e a engenharia social, com 772, figuram entre os métodos mais utilizados pelos cibercriminosos, muitas vezes associados a esquemas de burla online.

Os ataques de cibersegurança mais frequentes em Portugal em 2024 envolveram sobretudo campanhas de phishing e esquemas de engenharia social, confirma o CNCS. No caso do phishing, verificou-se a personificação de entidades dos setores da saúde, energia, bancário, transportes e administração pública, com o objetivo de capturar dados sensíveis ou instalar malware. Já no domínio da engenharia social, destacaram-se fraudes como o CEO Fraud – em que atacantes se fazem passar por executivos ou fornecedores para solicitar pagamentos indevidos –, chamadas fraudulentas através de vishing e spoofing, burlas online ligadas a aplicações de pagamentos e investimentos em criptomoedas, o esquema "Olá Mãe/Olá Pai" e tentativas de sextortion. O CERT.PT identificou ainda vulnerabilidades críticas como a CVE-2024-24919, associada a VPN e à exfiltração de dados, e a CVE-2019-18935, que permite a execução remota de código em aplicações web.

As vulnerabilidades mais exploradas incluem sistemas desatualizados, falta de autenticação multifator e erros de configuração, mas o fator humano continua a ser, de facto, o elo mais fraco. "O fácil acesso, e a baixo custo, das novas ferramentas de ciberataque capacitam rapidamente a comunidade menos evoluída do cibercrime, tornando-os mais eficazes e ameaçadores", explica o CEO da VisionWare.

Apesar da crescente ameaça, Portugal tem demonstrado um progresso significativo em cibersegurança. *"O Global Cybersecurity Index 2024, desenvolvido pela União Internacional das Telecomunicações da ONU, coloca Portugal no grupo de elite 'Tier 1 – Role-modelling', que inclui os 20 países com o nível mais elevado de maturidade*

em cibersegurança”, sublinha. No entanto, reforça que este é um esforço contínuo, e as empresas devem estar atentas à necessidade de evoluir as suas estratégias de proteção.

Recomendações e boas práticas

Bruno Castro salienta que *“é obrigatório que as organizações evoluam a sua capacidade de deteção e resposta em concordância com a inovação aplicada no cibercrime, caso contrário, ficarão obsoletas face às ameaças emergentes”*. Como recomendação, o especialista destaca a importância de um Security Operations Center (SOC), que *“pode ajudar bastante na medida em que irá combinar as tecnologias essenciais para a monitorização, deteção e resposta a ameaças oriundas do ciberespaço”*. Bruno Castro acrescenta ainda a realização de ações de stress e auditorias aos modelos de segurança instituídos nas organizações no intuito de detetar falhas, sejam elas tecnológicas, aplicacionais ou em procedimentos.

Para mitigar os riscos, no seu relatório de Riscos & Conflitos, o CNCS recomenda que as empresas portuguesas adotem medidas de cibersegurança robustas. Entre as principais recomendações estão a formação e sensibilização através de *“ações de sensibilização contra a engenharia social junto dos colaboradores”*. Em paralelo, o Centro Nacional de Cibersegurança recomenda *“manter os sistemas, as aplicações e o antivírus atualizados”* e *“salvaguardar cópias de segurança em localização secundária e desconectada da rede”*.

Apesar da crescente sofisticação dos ataques, a chave para a defesa eficaz continua a ser o fator humano. *“As pessoas. É tão simples quanto isso. […] No final do dia, são as pessoas bem treinadas que tomam as decisões e conseguem deter os ataques”*, conclui Chester Wisniewski, reforçando a necessidade de um investimento contínuo na formação e preparação das equipas de segurança.