Medusa, o grupo de “snipers” do cibercrime que escolhe a dedo as empresas a atacar, já fez uma vítima em Portugal

observador.pt/especiais/medusa-o-grupo-de-snipers-do-cibercrime-que-escolhe-a-dedo-as-empresas-a-atacar-ja-fez-uma-vitima-em-portugal

Cátia Rocha

É um grupo com uma operação profissional e orientado para o lucro financeiro gerado por resgates. Em 2023, o grupo foi responsável por um ataque em Portugal e umas quantas dezenas na Europa.

18 abr. 2025, 19:42 1

“!!!READ_ME_Medusa” é o nome do ficheiro que ninguém quer encontrar no computador. É o sinal de que o sistema está nas mãos do grupo cibercriminoso Medusa, conhecido pelos ataques de *ransomware* — ou seja, infiltra-se, encripta a informação e exige um resgate às empresas (ou outras entidades) para que possam reaver o acesso aos sistemas e aos dados. Enquanto na mitologia grega quem olhava para a Medusa se transformava em pedra, quem é atacado pelo grupo fica com os sistemas “petrificados”, a menos que esteja **disposto a pagar uns milhares ou milhões de dólares em bitcoin (o que não é aconselhado pelos peritos).**

O grupo é relativamente recente no mundo do cibercrime — as primeiras atividades foram identificadas em junho de 2021. Mas os poucos anos de atividade não são sinónimo de amadorismo. **“É um grupo jovem, mas altamente profissional, muito especializado”**, assegura Bruno Castro, CEO da empresa portuguesa de cibersegurança VisionWare. “Têm quatro anos de atividade, mas já têm bastante reconhecimento em termos de cibercrime.” Hugo Nunes, da área de informação sobre ciberameaças da Thales S21Sec, reforça que “estão consistentemente no top 10 dos grupos com mais vítimas” e, por isso, no radar de quem trabalha em cibersegurança.

A relevância deste grupo até motivou um alerta conjunto do FBI e da CISA, a Agência de Cibersegurança e Segurança de Infraestruturas dos EUA. Na nota divulgada em março, encorajam-se as empresas norte-americanas (e não só) a “mitigar vulnerabilidades conhecidas” nos sistemas e *software* para tentarem proteger-se das atividades do grupo.

De acordo com os dados revelados pelo FBI, **o grupo e os seus afiliados fizeram mais de 300 vítimas até fevereiro deste ano**. Já foram alvo do grupo Medusa empresas de infraestruturas críticas e dos setores “médico, da educação, legal, seguros, tecnologia e indústria”. Em 2023, por exemplo, foi público que o grupo conseguiu infiltrar-se no distrito escolar de Minneapolis, nos EUA, acedendo a mais de 100 GB de informação de milhares de estudantes. A ação do grupo afetou os sistemas da rede de escolas, obrigando na altura ao cancelamento de todas as atividades extracurriculares, escreveu a CBS News.

A atividade do grupo está longe de se limitar aos EUA. O Centro Nacional de Cibersegurança (CNCS) indica ao Observador que, "em 2023, o grupo foi responsável por **um ataque no ciberespaço nacional"**, sem adiantar mais informação. Mas, ao Observador, Hugo Nunes, da Thales S21Sec, menciona que se tratou de uma empresa na **"área da hotelaria"**. Também a VisionWare confirma esse ataque "com sucesso" em Portugal há dois anos, com Bruno Castro a detalhar que a empresa esteve "envolvida no processo de resposta, no processo de repressão e na investigação forense", garantindo que **não houve pagamento de resgate.** "Na VisionWare somos completamente contra o pagamento de resgate, em que formato seja, isso é alimentar uma rede criminosa."

O CNCS declara que, em 2024, não foram registadas mais atividades do grupo em Portugal. Mas, através do "contacto com congéneres europeus", a entidade responsável pela cibersegurança em Portugal dá conta da deteção de ataques feitos pelo grupo em território europeu. "Em 2024, este Medusa foi responsável por mais de 30 ataques no Reino Unido, mantendo uma cobertura, quase integral, do território europeu, nomeadamente nove ataques em Itália, seis em França e cinco na Alemanha".

Em resposta às questões do Observador, a ENISA (Agência da União Europeia para a Cibersegurança) confirma a **"monitorização contínua de atividade de *ransomware*, incluindo do Medusa RaaS** [*ransomware as a service*]". Porém, é parca em pormenores sobre esta atividade, assumindo unicamente que "a principal atividade do grupo se centra nos EUA" e que "foram apenas feitas algumas alegações relativamente a organizações em Estados-membros da UE entre 2023 e 2024, em vários setores".

Grupo usa táticas de dupla extorsão. Resgates podem ir dos 100 mil aos 15 milhões de dólares

O grupo Medusa é um dos vários que opera na área do *ransomware as a service*. Mas tem várias particularidades. Segundo o CNCS, os primeiros passos de trabalho assentam "quase sempre" na "exploração de credenciais compradas nos mercados da *deep web*, com o objetivo de garantir o acesso inicial" às vítimas. Mas há mais técnicas, como "a exploração de vulnerabilidades conhecidas ou o *phishing*". Os casos mais conhecidos de *phishing* envolvem o fazer-se passar por alguma empresa (um banco, serviço de *streaming* ou uma empresa de eletricidade) para "fisgar" dados.

A nota do FBI divulgou que o grupo recruta afiliados através de fóruns de cibercrime. A possibilidade de trabalhar em exclusivo para o grupo, que se organiza como se fosse uma empresa, pode envolver pagamentos que variam entre os 100 dólares (cerca de 88 euros) e um milhão de dólares (880 mil euros), consoante a complexidade das tarefas.

A partir do momento em que há acesso à vítima, o grupo tenta "evadir-se das defesas e movimenta-se lateralmente para ver como é que são os sistemas, tenta de alguma forma ganhar privilégios para depois exfiltrar os dados", ou seja, retirá-los do sistema, explica Hugo Nunes, da Thales S21Sec. Só depois é que vem a parte de encriptação dos sistemas, que os torna **"inutilizáveis"**, explica.

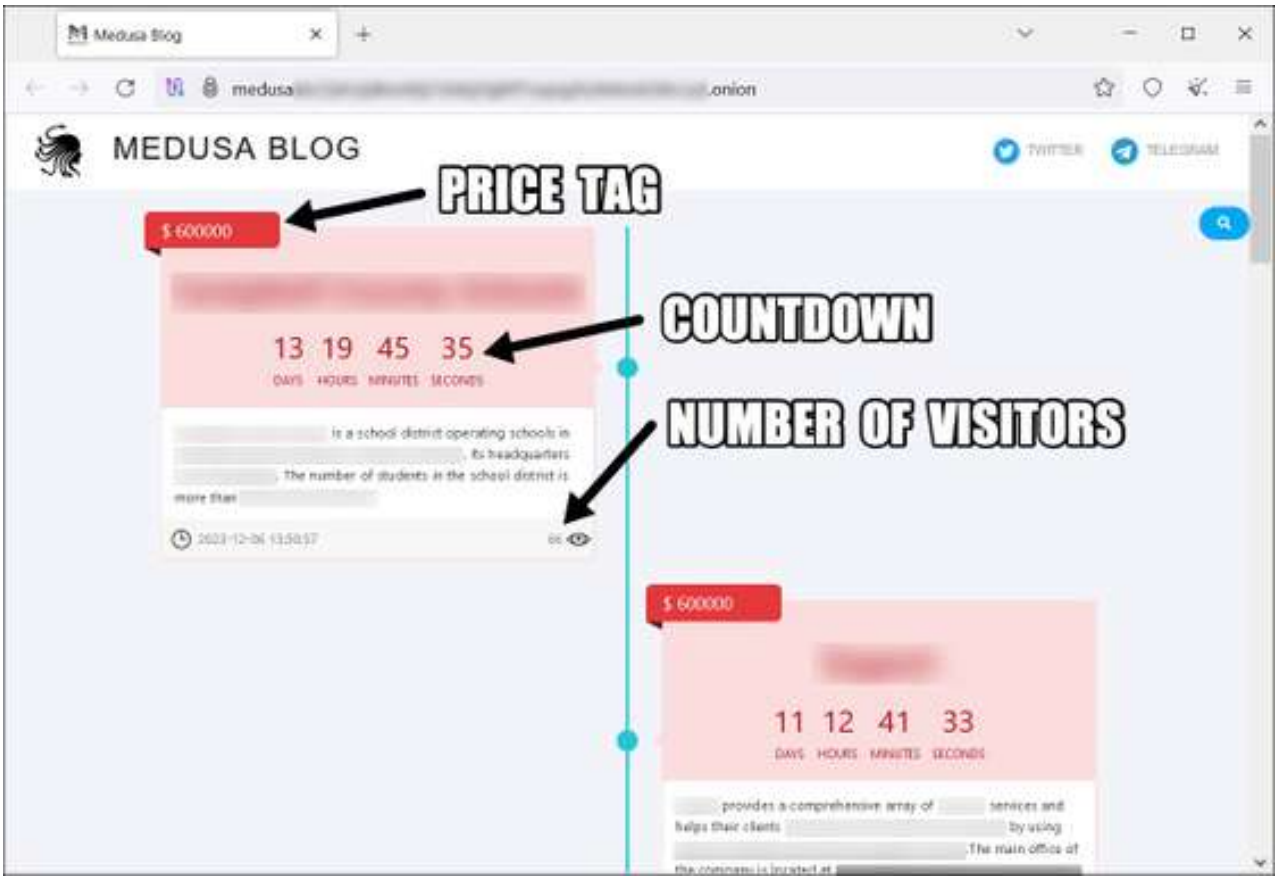
Os contactos com as vítimas podem acontecer de várias formas. “Temos indicações de que este grupo, por vezes, faz contacto direto, por email, por telefone, com a organização afetada”, acrescenta o especialista da Thales S21Sec. O contacto tem o intuito de “forçar a vítima a pagar o resgate, a pagar em bitcoins, que é a transação que querem, para depois lhes fornecer a chave de desencriptação dos dados”.

O grupo é referido ainda como sendo muito **preciso** relativamente às empresas que quer atingir. “Na nossa área, isto são os *snipers*“, explica Bruno Castro, da VisionWare. “Há tempo, há paciência, há investimento para atacar aquela organização. Não é outra, é aquela”, explicando que este não é um grupo que opte por lançar ataques massivos e ficar à espera de quem caia. “Desde a escolha das pessoas que vão fazer o ataque e depois saltarem para a organização, na tentativa de procurar portas abertas no perímetro dessa empresa na ligação com o ciberespaço… tudo isso é estudado com tempo.” O investimento e a organização do grupo fazem com que, **“quando há um ataque, a probabilidade de sucesso seja alta**“, garante o especialista.

"Na nossa área, isto são os snipers", explica Bruno Castro, da VisionWare. "Há tempo, há paciência, há investimento para atacar aquela organização."

Também há outra particularidade: o grupo tem um *blog* onde divulga alegados *“leaks”* de dados das organizações atingidas. No ficheiro que é ‘plantado’ nos computadores, o grupo afirma que a organização afetada “pode sofrer problemas significativos”, desde a “perda de propriedade intelectual valiosa e outra informação sensível” até ao “mau uso de informação/abuso, perda de confiança dos clientes, danos à marca e danos reputacionais e questões regulatórias”, conforme mostram as imagens recolhidas por empresas como a Palo Alto Networks.

O blog do grupo é usado para pressionar as vítimas, realçam os especialistas na área da cibersegurança. “Publicam no *site* na *dark web* e colocam um contador para gerar ainda mais pressão às vítimas: ‘têm x dias, x horas para pagar, se não vamos divulgar os dados'”, exemplifica Hugo Nunes, da Thales S21Sec. **“É um jogo psicológico com a contagem decrescente, para dar a entender que há urgência em pagar o resgate.”**



Uma das imagens do blog onde o grupo divulga quanto tempo as suas vítimas têm para pagar o resgate

Nos exemplos vistos pelas empresas de cibersegurança, o *blog* do grupo dá informação não só sobre a atividade da organização afetada como indica quantas vezes é que o *leak* de dados já foi visto. Também é possível perceber que há diferentes modalidades de preço: por exemplo, acrescentar mais um dia ao prazo custa 10 mil dólares, enquanto apagar todos os dados ou descarregá-los custa 600 mil dólares. Uma compilação de dados recente, feita pela empresa de cibersegurança Symantec a partir da informação do *blog* do grupo, refere que os resgates exigidos às empresas variam entre 100 mil e 15 milhões de dólares (cerca de 88 mil e 13,24 milhões de euros, respetivamente).

Bruno Castro, CEO da VisionWare, acrescenta que o grupo é orientado “pela procura de dividendos”. “Não quer criar caos, alarmismo, nem mediatismo (…), é claramente uma ótica de angariar dinheiro da forma mais tranquila possível e menos mediática para que a vítima pague e lhes permita obter retorno financeiro, ponto final. É uma equação claramente financeira/empresarial.”

"É um jogo psicológico com a contagem decrescente, para dar a entender que há urgência em pagar o resgate."

Hugo Nunes, da equipa que vigia ciber-ameaças da Thales S21Sec

Este especialista considera que o grupo tem dois grandes perfis de vítimas preferenciais.

Um deles é “o perfil de [quem tem] dados volumosos — universidades, Estado, *big data* — *p*orque os dados são rentáveis por si só”, explica. Estas organizações são alvos do grupo pelo facto de terem muitos dados e serem serviços acedidos por muita gente. Quando é feito o ataque e os sistemas ficam encriptados gera-se “uma disrupção de serviço”, um ponto adicional de pressão para as vítimas. “A entidade vai querer pagar rapidamente porque o impacto é muito grande”, exemplifica Bruno Castro. “Quantos mais dados houver e maior for a disrupção de serviço, o impacto social ou em clientes, maior é a apetência da vítima para pagar rapidamente.”

O segundo perfil de alvos passa por empresas “em que há acesso direto ao dinheiro ou em que se coloque em causa serviços essenciais ou críticos da sociedade”. Bruno Castro realça que, mesmo que não sejam pagos resgates, os dados retirados de empresas “por si só já são um ativo financeiro”, que pode “ser revendido na *dark web*“.

Empresas devem ter em prática medidas de ciberhigiene

Não há receitas infalíveis para tentar prevenir ataques informáticos, mas os especialistas consideram que **ter um higiene cibernética é meio caminho andado**. Por exemplo, tendo em conta que um dos objetivos do grupo passa por comprometer contas de serviços como o Gmail ou o Outlook (amplamente usados por empresas e indivíduos) “é imperativo que os utilizadores ativem os mecanismos de duplo fator de autenticação como forma de proteção mínima”, aconselha o CNCS. É ainda necessário manter as “palavras-passe secretas e seguras”, de preferência **“usando uma frase com 12 caracteres ou mais, sem termos óbvios”.**

Ainda em relação às palavras-passe, Hugo Nunes aconselha a “não reutilização de *passwords*” — por exemplo, quando se usa a mesma palavra para aceder ao email e às redes sociais. Além disso, aconselha a manutenção “dos sistemas onde se acede ao email, nomeadamente o telemóvel ou o computador, sempre com a atualização mais recente.” Também recomenda atenção “a emails não solicitados, à proveniência e se aquilo que é proposto no email é realmente fidedigno e não implica riscos para nós ou para o sistema”.

Mas Bruno Castro considera que o chamado *bê-á-bá* da cibersegurança pode não ser suficiente para quem opera num setor apetecível para um grupo deste género. “O esforço envolvido do lado de lá é muito elevado, há atores especializados, portanto tem de existir um nível de maturidade” mais alto.

“Têm de ser aplicadas todas as medidas preventivas, sem dúvida, mas tem que haver mais: são precisas ações de *compliance*, tem de haver a capacidade de autoavaliar as infraestruturas de segurança continuamente, fazer auditorias de segurança internas, para avaliar o nível de maturidade e de risco e poder corrigir as falhas onde elas existam”, exemplifica.

Também destaca que estas práticas podem ser complementadas por “uma plataforma de monitorização e alarmística, que detete movimentos estranhos na rede”. Ou seja, entre o tempo de intrusão e o momento em que são roubados e encriptados os dados dá-se o chamado “tempo oculto”, explica. “É nessa altura que temos de ter uma guarda armada, 24 horas, sete dias por semana, que monitorize todos os movimentos suspeitos e que possa gerar um alerta.”