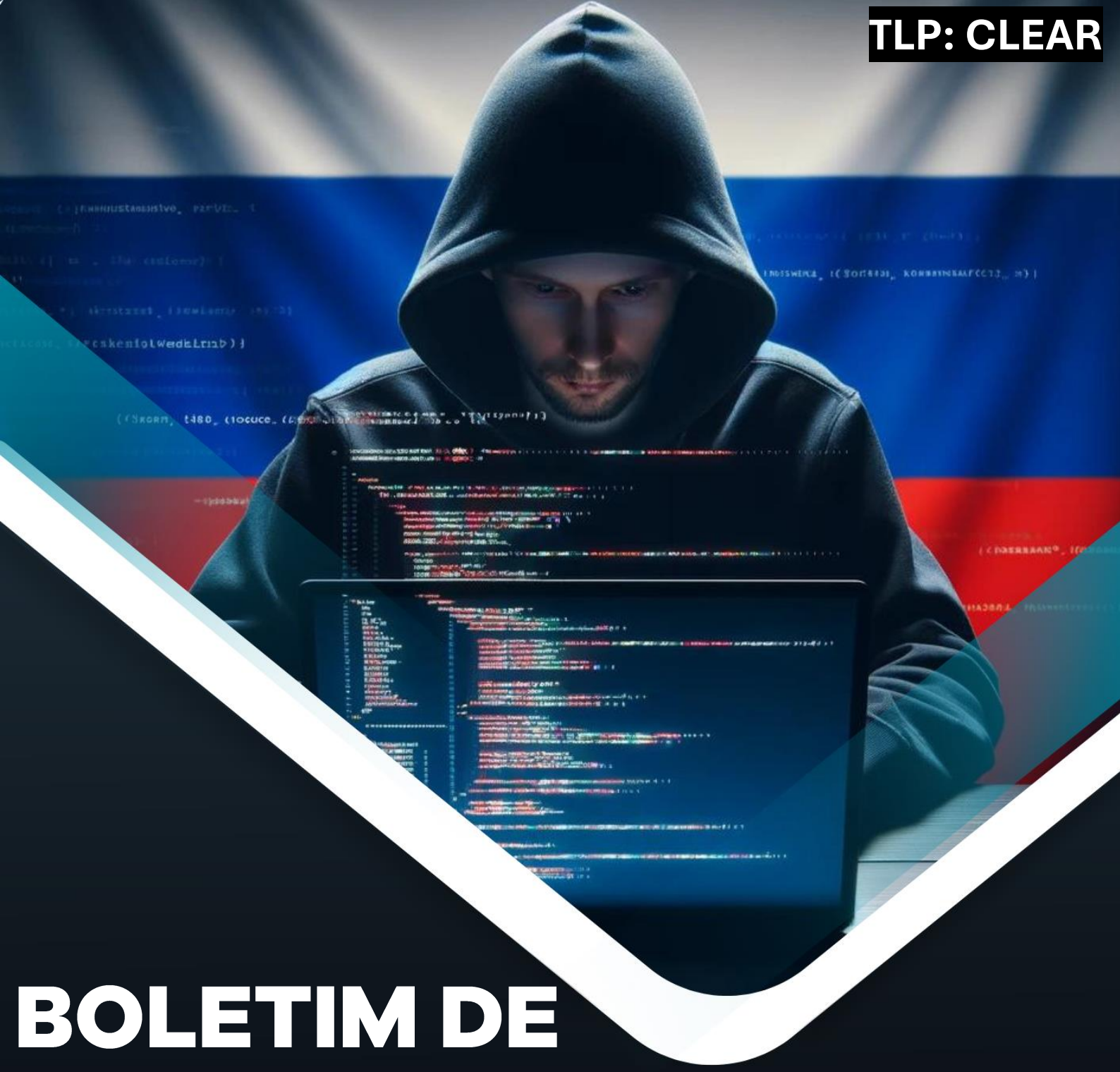
TLP: CLEAR



BOLETIM DE SEGURANÇA

A Microsoft confirmou que espiões russos roubaram código-fonte

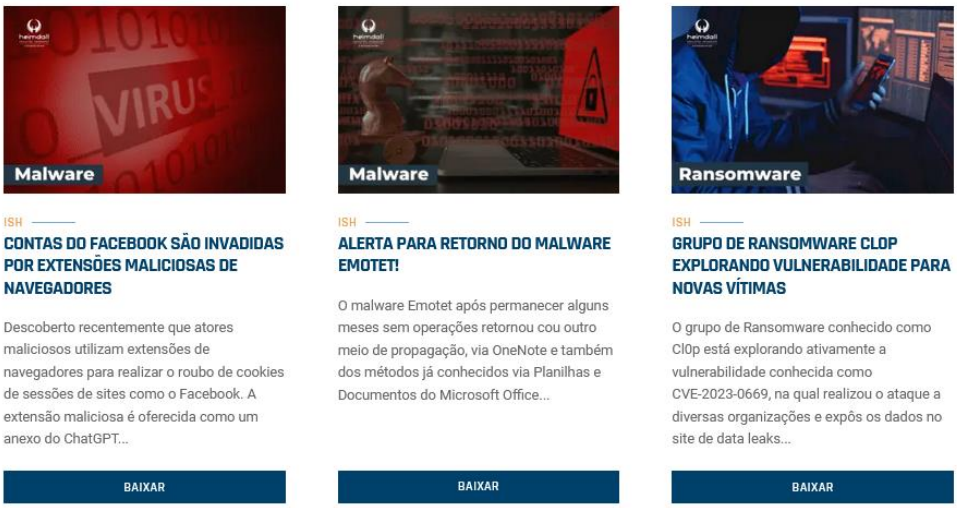
heimdall
security research
A DIVISION OF ISH

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



SUMÁRIO

1 DECLARAÇÃO DA MICROSOFT

A **Microsoft confirmou que ciberespiões russos, responsáveis pela invasão de contas de e-mail de seus executivos, roubaram código-fonte e obtiveram acesso a sistemas internos**. A primeira divulgação ocorreu em janeiro, quando a Microsoft declarou que os atores de ameaça **Midnight Blizzard** (uma equipe apoiada pelo Kremlin, também conhecida como **Cozy Bear e APT29**), teriam "bisbilhotado" uma porcentagem muito pequena de contas de e-mails corporativos da Microsoft, roubando mensagens e arquivos internos pertencentes à equipe de liderança, assim como a funcionários jurídicos e de segurança cibernética. De acordo com a Microsoft em janeiro: "Não há evidências de que o autor da ameaça tenha acessado os ambientes dos clientes, sistemas de produção, código-fonte ou sistemas de IA".

No novo comunicado, a Microsoft afirmou que "Nas últimas semanas, observou-se evidências de que a Midnight Blizzard está utilizando informações inicialmente exfiltradas dos sistemas de e-mails corporativos para obter, ou tentar obter, acessos não autorizados". "Isso inclui acesso a alguns repositórios de código-fonte e a sistemas internos da empresa".

A Microsoft declarou que "não há evidências" até o momento de que os criminosos russos tenham comprometido qualquer sistema voltado para o cliente. Entretanto, isso não se deve à falta de tentativas. "**É evidente que a Midnight Blizzard está tentando usar segredos de diferentes tipos que encontrou**".

"Alguns desses segredos foram compartilhados entre clientes e a Microsoft por e-mail e, à medida que descobriram e-mails exfiltrados, entraram em contato com os clientes para ajudá-los e tomar medidas de mitigação. A Microsoft também afirmou que a Midnight Blizzard **aumentou o volume de alguns aspectos do ataque, como sprays de senhas, em até dez vezes em fevereiro, em comparação com o já alto volume observado em janeiro de 2024**.

Vale salientar que o ataque contínuo por parte dos atores da Midnight Blizzard é caracterizado por um comprometimento significativo e sustentado dos recursos, coordenação e foco por parte do ator de ameaça. Ao utilizar as informações exfiltradas, os atores podem usá-las para aprimorar suas campanhas e aumentar sua capacidade, ampliando também o cenário de ameaça global.

2 QUEM É MIDNIGHT BLIZZARD?

Midnight Blizzard (também conhecido como NOBELIUM) é um ator de ameaça baseado na Rússia, atribuído pelos governos dos EUA e do Reino Unido como o Serviço de Inteligência Estrangeira da Federação Russa, também conhecido como SVR. O seu foco é **coletar informações através de espionagem dedicada e de longa data de interesses estrangeiros**, que pode ser rastreada até o início de 2018. As suas operações envolvem frequentemente o comprometimento de contas válidas e, em alguns casos altamente direcionados, técnicas avançadas para comprometer mecanismos de autenticação dentro de uma organização para expandir o acesso e escapar da detecção.

Midnight Blizzard é consistente e persistente em sua segmentação operacional, e seus objetivos raramente mudam. As atividades de espionagem e coleta de informações da Midnight Blizzard alavancam uma variedade de acesso inicial, movimento lateral e técnicas de persistência para coletar informações em apoio aos interesses da política externa russa. Eles utilizam diversos métodos de acesso inicial, desde credenciais roubadas até ataques à cadeia de suprimentos, exploração de ambientes locais para migração lateral para a nuvem, e exploração da cadeia de confiança dos provedores de serviços para obter acesso a clientes downstream.

A Midnight Blizzard também é especialista em identificar e abusar de aplicativos OAuth para movimentação lateral entre ambientes de nuvem e para atividades pós-comprometimento, como coleta de e-mail. OAuth é um padrão aberto para autenticação e autorização baseada em token, que permite que aplicativos obtenham acesso a dados e recursos com base em permissões definidas por um usuário.

Midnight Blizzard é rastreado por fornecedores de segurança parceiros como APT29, UNC2452 e Cozy Bear.

3 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Comunicado Microsoft – APT29**

heimdall
security research
A DIVISION OF ISH