BOLETIM DE SEGURANÇA

Grupo malicioso APT 29 (Midnight Blizzard) direcionados a organizações globais.

heimdall
security research
A DIVISION OF ISH

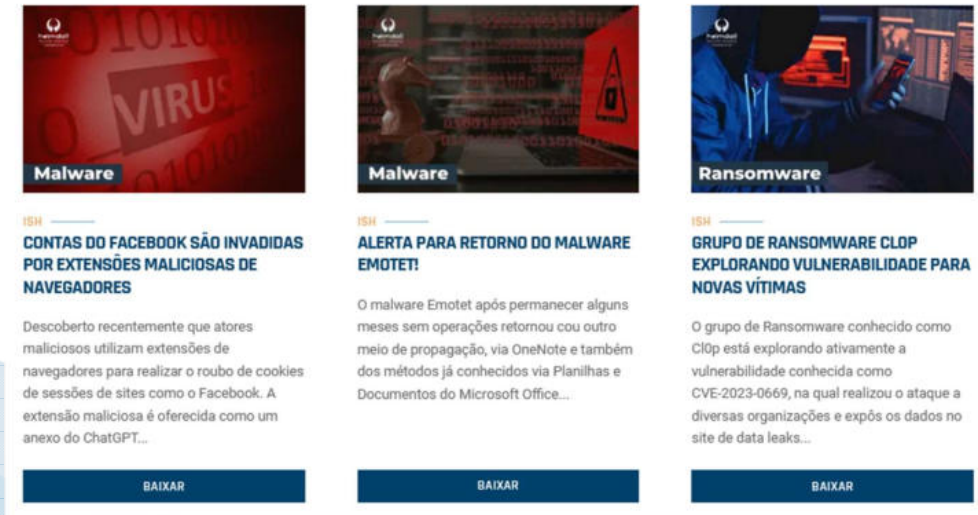
TLP: CLEAR

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

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



heimdall
security research

Sumário

1 SUMÁRIO EXECUTIVO

A Microsoft alertou sobre o ator de ameaça Midnight Blizzard (Conhecidos anteriomente como **Nobelium**), **APT29**, um grupo malicioso apoiado pelo governo Russo. Este grupo é conhecido por ter como alvo principal governos, entidades diplomáticas, organizações não governamentais (ONGs) e prestadores de serviços de TI, principalmente nos EUA e na Europa". O grupo foi responsável por um ataque aos sistemas da Microsoft no final de novembro de 2023 que resultou no roubo de e-mails e anexos de executivos seniores e outros indivíduos dos departamentos jurídico e de segurança cibernética da empresa. A Microsoft informou que este grupo está mirando outras organizações.

2 DETALHES SOBRE O GRUPO

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 recolher informações através de espionagem dedicada e de longa data de interesses estrangeiros que pode ser rastreada até ao 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 Atividades e técnicas observadas do ator de ameaça

Acesso inicial através de password spray

O grupo foi observado realizando ataques de password-spray que comprometeram com sucesso uma conta de locatário de teste herdada e não produtiva que não tinha autenticação multifator (MFA) habilitada. Em um ataque de password-spray o adversário tenta entrar em um grande volume de contas usando um pequeno subconjunto das senhas mais populares ou mais prováveis. Nessa atividade observada da Midnight Blizzard, o ator adaptou seus ataques a um número limitado de contas, usando um baixo número de tentativas para evitar a detecção e evitar bloqueios de contas com base no volume de falhas. Além disso, como explicamos com mais detalhes abaixo, o agente da ameaça reduziu ainda mais a probabilidade de descoberta ao lançar esses ataques a partir de uma infraestrutura de proxy residencial distribuída. Essas técnicas de evasão ajudaram a garantir que o ator ofuscasse sua atividade e pudesse persistir o ataque ao longo do tempo até ter sucesso.

Uso malicioso de aplicativos OAuth

Comprometeram contas de usuários para criar, modificar e conceder altas permissões a aplicativos OAuth que eles podem usar indevidamente para ocultar atividades maliciosas. O uso indevido do OAuth também permite que os agentes de ameaças mantenham o acesso aos aplicativos, mesmo que percam o acesso à conta inicialmente comprometida. A Midnight Blizzard aproveitou seu acesso inicial para identificar e comprometer um aplicativo OAuth de teste legado que tinha acesso elevado ao ambiente corporativo da Microsoft. O ator criou aplicativos OAuth maliciosos adicionais. Eles criaram uma nova conta de usuário para conceder consentimento no ambiente corporativo da Microsoft aos aplicativos OAuth maliciosos controlados pelo ator. O agente da ameaça então usou o aplicativo OAuth de teste herdado para conceder a função *full_access_as_app* do Office 365 Exchange Online , que permite acesso a caixas de correio.

Coleta por meio de serviços Web do Exchange

A Midnight Blizzard aproveitou esses aplicativos OAuth maliciosos para autenticar no Microsoft Exchange Online e direcionar contas de e-mail corporativas da Microsoft.

Uso de infraestrutura de proxy residencial

Como parte de suas múltiplas tentativas de ofuscar a origem do ataque, a Midnight Blizzard usou redes proxy residenciais, roteando seu tráfego através de um grande número de endereços IP que também são usados por usuários legítimos, para interagir com o inquilino comprometido e, posteriormente, com troca on-line. Embora não seja uma técnica nova, o uso de proxies residenciais pela Midnight Blizzard para ofuscar conexões torna inviável a detecção tradicional baseada em indicadores de comprometimento (IOC) devido à alta taxa de mudança de endereços IP.

4 RECOMENDAÇÕES

Devido à elevada utilização de infraestrutura de proxy com uma taxa de transição significativa, não basta confiar na procura por **IOCs** convencionais, como endereços IP de infraestrutura, para identificar atividades associadas à *Midnight Blizzard*. Por isso, aconselha-se seguir certas diretrizes para detectar e minimizar os riscos relacionados a este tipo de ameaça, como:

Defenda-se contra aplicativos OAuth maliciosos

- Auditar o nível de privilégio atual de todas as identidades, tanto de usuários quanto de entidade de serviço.
- Identificar aplicações como OAuth maliciosos realizando buscas para detectar anomalias.
- Implementação do controle de aplicações de acesso condicional para usuários que se conectam a partir de dispositivos não gerenciados.

Proteja-se contra-ataques de password spray

- Elimine senhas inseguras
- Conscientização de segurança por parte dos usuários, revisando assim atividades de logins.
- Quando um ataque ocorrer, redefina todas as senhas de contas que estejam na mira dos atacantes.
- Use detecções de risco para logins de usuários para acionar a autenticação multifator ou alterações de senha.

5 Conclusão

A necessidade de organizações e governos se resguardarem contra o grupo APT29, também conhecido como Midnight Blizzard, é uma questão crítica de segurança cibernética global. Este grupo é conhecido por suas habilidades avançadas em ciberespionagem e ataques sofisticados, representando uma ameaça séria à segurança de informações sensíveis e infraestruturas críticas. A defesa contra tais ameaças exige medidas robustas, incluindo a implementação de sistemas de segurança cibernética de última geração, vigilância contínua das redes, e a conscientização e treinamento rigoroso dos funcionários em práticas de segurança.

Ao proteger-se contra o APT29, organizações e governos não apenas salvaguardam dados importantes, mas também reforçam sua soberania e estabilidade política e econômica diante de ameaças digitais cada vez mais complexas

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Microsoft**
- **Thehackernews**

heimdall
security research
A DIVISION OF ISH