BOLETIM DE SEGURANÇA

Grupo russo APT29 realiza adaptações para acesso à nuvem

heimdall
security research
A DIVISION OF ISH

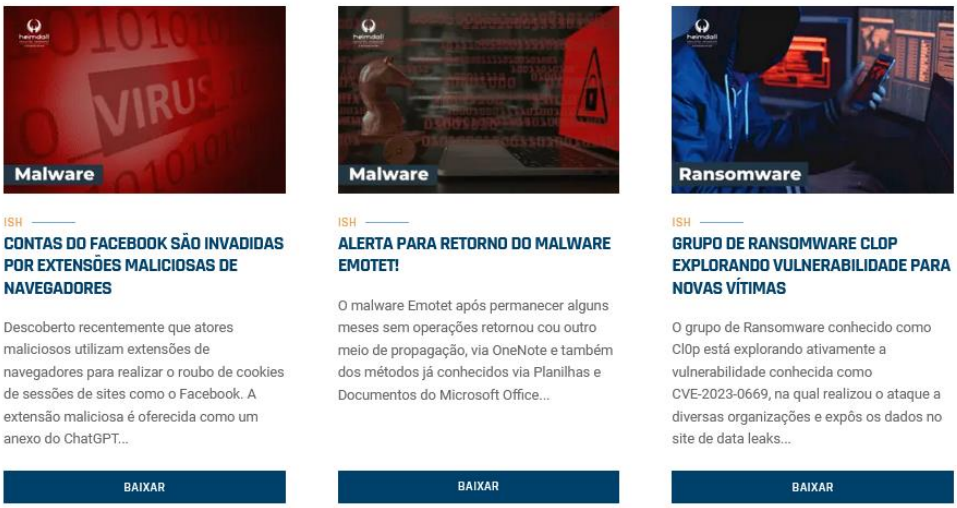
TLP: CLEAR

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

LISTA DE TABELAS

1 SUMÁRIO EXECUTIVO

O Centro Nacional de Segurança Cibernética do Reino Unido (**NCSC**) juntamente com parceiros internacionais de segurança cibernética, realizaram uma avaliação do APT29, que é um grupo de espionagem cibernética, quase certamente parte do SVR, um elemento dos serviços de inteligência russos. Especializado em operações de espionagem digital, o grupo se destaca por suas técnicas sofisticadas e métodos de ataque discretos, visando principalmente entidades governamentais e organizações relacionadas à segurança nacional. Suas atividades são notórias por comprometerem redes de alta segurança, empregando malware e técnicas de engenharia social para obter acesso a informações confidenciais. APT29 tem sido ativo por vários anos, demonstrando capacidades avançadas de persistência e evasão.

2 ATIVIDADE REALIZADA PELO ATOR

Foi detalhado anteriormente pela NCSC como os intervenientes do SVR visaram alvos governamentais, de grupos de reflexão, de saúde e de energia para obterem informações. Observou agora que os intervenientes do SVR expandiram a sua segmentação para incluir a aviação, a educação, a aplicação da lei, os conselhos locais e estaduais, os departamentos financeiros governamentais e as organizações militares.

Os atores SVR também são conhecidos pelo comprometimento da cadeia de suprimentos do software SolarWinds e atividade que teve como alvo organizações que desenvolvem a vacina COVID-19. À medida que as organizações continuam modernizando seus sistemas e a migrando para infraestruturas baseadas na nuvem, o SVR adaptou-se a estas mudanças no ambiente operacional, tendo de ir além dos seus meios tradicionais de acesso inicial, como a exploração de vulnerabilidades de softwares numa rede local, e, em vez disso, visar os próprios serviços na nuvem.

Para acessar a maior parte da rede hospedada na nuvem das vítimas, os invasores devem primeiro obter êxito na autenticação direto no provedor de nuvem. Negar o acesso inicial ao ambiente de nuvem pode impedir que o SVR comprometa com sucesso seu alvo. Em contrapartida, em um sistema local, uma parte maior da rede normalmente fica exposta a agentes de ameaças.

3 ACESSO VIA SERVIÇOS E CONTAS INATIVAS

Campanhas anteriores do SVR revelaram que os agentes maliciosos usaram com sucesso a técnica de *brute force* e a *password cracking* para acessar contas de serviço. Esse tipo de conta normalmente é usado para executar, gerenciando aplicativos e serviços. Como não há nenhum usuário humano por trás delas e não podem ser facilmente protegidas com *multi-factor authentication* (**MFA**), tornando essas contas mais suscetíveis a um comprometimento bem-sucedido. Muitas vezes, as contas de serviço também são altamente privilegiadas, dependendo de quais aplicativos e serviços são responsáveis pelo gerenciamento. Obter acesso a essas contas fornece aos invasores acesso inicial privilegiado a uma rede, para lançar novas operações. As campanhas de SVR também visaram contas inativas pertencentes a usuários que não trabalham mais em uma organização vítima, mas cujas contas permanecem no sistema. Após uma redefinição de senha forçada para todos os usuários durante um incidente, os atores do SVR também foram observados fazendo login em contas inativas e seguindo instruções para redefinir a senha, permitiu que o ator recuperasse o acesso após atividades de despejo de resposta a incidentes.

O acesso à conta geralmente é autenticado por credenciais de nome de usuário e senha ou por tokens de acesso emitidos pelo sistema. O NCSC e parceiros observaram atores do SVR usando tokens para acessar as contas de suas vítimas, sem a necessidade de senha. O tempo de validade padrão dos tokens emitidos pelo sistema varia dependendo do sistema, no entanto, as plataformas em nuvem permitem que os administradores ajustem o tempo de validade conforme apropriado para seus usuários.

4 REGISTRO DE NOVOS DISPOSITIVOS

Em várias ocasiões, o grupo contornou com sucesso a autenticação de senha em contas pessoais usando *password cracking* e reutilização de credenciais, também contornaram o MFA por meio de uma técnica conhecida como "*MFA bombing*" ou "*MFA fatigue*", na qual os atores enviam repetidamente solicitações de MFA para o dispositivo da vítima até que a vítima aceite a notificação. Depois que um ator contorna esses sistemas para obter acesso ao ambiente de nuvem, os atores são observados registrando seu próprio dispositivo como um novo dispositivo no locatário da nuvem. Se as regras de validação de dispositivos não forem configuradas, eles poderão registrar com sucesso seus próprios dispositivos e obter acesso à rede. Ao configurar a rede com políticas de registro de dispositivos, houve casos em que essas medidas defenderam contra estes atores e negaram-lhes acesso ao locatário da nuvem.

Na medida que as defesas melhoram a detecção de atividades suspeitas, estes atores buscam outras formas de permanecerem furtivos na Internet. Um TTP associado a este ator é o uso de proxies residenciais, que normalmente fazem com que o tráfego pareça originar-se de endereços IP dentro dos intervalos dos provedores de serviços de Internet (ISP) usados para clientes residenciais de banda larga e ocultam a verdadeira origem. Isso pode dificultar a distinção entre conexões maliciosas e usuários típicos, reduzindo a eficácia das defesas de rede que usam endereços IP como indicadores de comprometimento e, por isso, é importante considerar uma variedade de fontes de informações, como registros baseados em aplicativos e em host, para detectar atividades suspeitas.

5 CONCLUSÃO

A importância das organizações se protegerem contra-ataques do APT29 reside na capacidade deste grupo de comprometer dados sensíveis, causando prejuízos financeiros, danos à reputação e perda de confiança dos clientes. A segurança na nuvem é fundamental, uma vez que muitas empresas dependem dessa tecnologia para armazenamento de dados e operações críticas. Medidas como a implementação de políticas robustas de segurança, treinamento de funcionários em conscientização sobre phishing e outras táticas de engenharia social, além do uso de ferramentas de detecção e resposta a incidentes, são essenciais para mitigar os riscos de ataques.

6 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Credential Access	T1110	Usa password spray e brute force como vetor inicial de infecção. O SVR usa tokens de acesso roubados para fazer login em contas sem a necessidade de senhas. Envia repetidamente solicitações de MFA para o dispositivo da vítima até que ela aceite a notificação, fornecendo acesso do SVR à conta.
Initial Access	T1078.004	Utiliza credenciais comprometidas para obter acesso a contas de serviços em nuvem, incluindo contas de sistema e inativas.
Command and Control	T1090.002	Usa proxies abertos em intervalos de IP residenciais para combinar com os pools de endereços IP esperados nos logs de acesso.
Persistence	T1098.005	Realiza tentativas de registrar seu próprio dispositivo no locatário da nuvem após adquirir acesso às contas.

Tabela 1 – Tabela MITRE ATT&CK.

7 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

Conscientização e treinamento

- Educar os usuários sobre técnicas de engenharia social, especialmente em relação a ataques de phishing e spear phishing. O grupo frequentemente usa lures sofisticados para enganar os usuários a executarem ações maliciosas.

Atualização e patches

- Manter todos os sistemas operacionais e softwares atualizados. A exploração de vulnerabilidades conhecidas é uma via comum para ataques iniciais. A exploração da vulnerabilidade CVE-2023-38831 no WinRAR é um exemplo recente de como o grupo APT29 ganha acesso aos sistemas alvo.

Segurança de e-mail

- Implementar soluções robustas de segurança de e-mail para detectar e bloquear e-mails de phishing e anexos maliciosos. Isso inclui a inspeção de links e documentos para sinais de maliciosidade antes que eles cheguem aos usuários finais.

Autenticação de múltiplos fatores (MFA)

- Aplicar MFA sempre que possível para adicionar uma camada adicional de segurança. APT29 tem demonstrado capacidades para burlar MFA, mas a implementação de MFA ainda pode significativamente aumentar a dificuldade para os atacantes.

Segurança em nuvem e SaaS

- Dado o foco do APT29 em comprometer contas do Microsoft 365 e usar serviços de armazenamento em nuvem para camuflar suas operações, é crucial implementar políticas de segurança rigorosas para ambientes em nuvem, incluindo a revisão de permissões de aplicativos e monitoramento de atividades suspeitas.

Monitoramento e detecção

- Fortalecer a capacidade de detecção de intrusões e resposta a incidentes. Isso inclui o monitoramento de indicadores de comprometimento (IoCs) conhecidos associados ao APT29 e a análise comportamental para identificar atividades suspeitas que podem indicar uma intrusão.

8 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **NCSC**

heimdall
security research
A DIVISION OF ISH