BOLETIM DE SEGURANÇA

Rede corporativa do TeamViewer violada supostamente por grupo APT

heimdall
security research
A DIVISION OF ISH

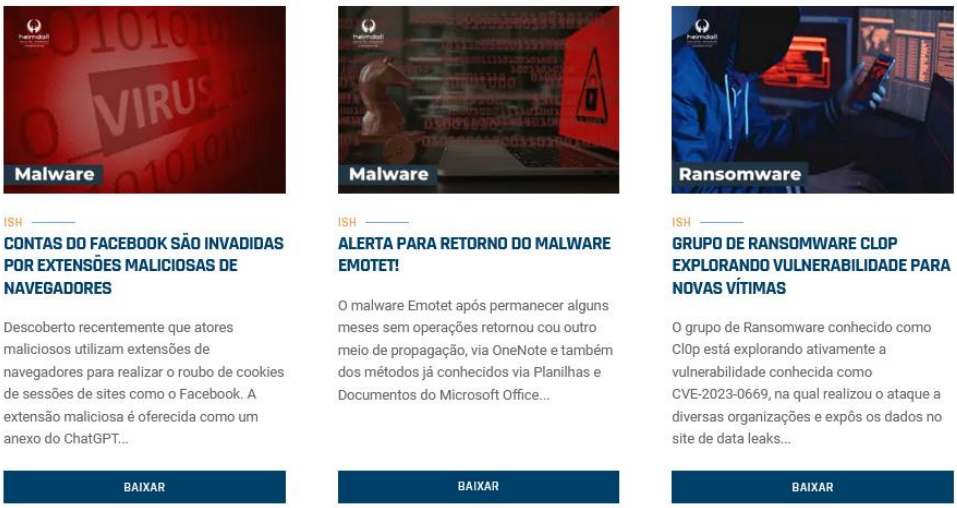
TLP: CLEAR

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

A TeamViewer anunciou que sua rede corporativa foi comprometida por um grupo APT, possivelmente o APT29 (Midnight Blizzard). A violação foi detectada em 26 de junho de 2024, mas não há evidências de que os dados dos clientes ou o ambiente do produto tenham sido afetados. O uso massivo do software em ambientes corporativos e de consumo torna qualquer violação uma preocupação significativa, pois pode fornecer acesso completo a redes internas.

2 ATUALIZAÇÃO DO TEAMVIEWER SOBRE O INCIDENTE

Em sua página de transparência a organização emitiu o seguinte comunicado sobre o incidente" As descobertas atuais da investigação apontam para um ataque na quarta-feira, 26 de junho, *vinculado às credenciais de uma conta de funcionário* padrão em nosso ambiente de TI corporativo. Com base no monitoramento contínuo de segurança, nossas equipes identificaram comportamento suspeito dessa conta e imediatamente colocaram medidas de resposta a incidentes em ação. Junto com nosso suporte externo de resposta a incidentes, atualmente atribuímos essa atividade ao agente de ameaça conhecido como APT29 / Midnight Blizzard. Com base nas descobertas atuais da investigação, o ataque foi contido no ambiente de TI corporativo e não há evidências de que o agente de ameaça obteve acesso ao nosso ambiente de produto ou aos dados do cliente.

3 GRUPO APT29 MIDNIGHT BLIZZARD

O Grupo APT29, também conhecido como Midnight Blizzard, é uma unidade cibernética de elite vinculada ao governo russo, notoriamente associada ao Serviço de Inteligência Estrangeira da Rússia (SVR). Este grupo é reconhecido por suas operações sofisticadas de espionagem cibernética, com foco em roubo de informações sensíveis de governos, organizações internacionais e empresas de alta tecnologia. Utilizando técnicas avançadas de spear-phishing e exploits zero-day, o APT29 conseguiu comprometer redes e sistemas em todo o mundo. Notavelmente, esteve envolvido no ataque SolarWinds em 2020, que afetou várias agências governamentais dos EUA. Suas campanhas de ataque são caracterizadas por um planejamento meticuloso e uso de ferramentas customizadas. Além disso, o APT29 é conhecido por adotar novas técnicas rapidamente, evidenciando sua capacidade de adaptação e evolução contínua. Suas atividades continuam a representar uma ameaça significativa à segurança cibernética global.

4 TÁTICAS UTILIZADAS PELO GRUPO

O Grupo APT29, emprega uma variedade de táticas avançadas para comprometer e manter o acesso a redes e sistemas. Abaixo destacamos algumas das táticas principais utilizadas por este grupo:

Spear phishing

- APT29 frequentemente utiliza e-mails de spear phishing altamente direcionados para enganar alvos específicos e obter credenciais de login ou distribuir malware.

Exploits Zero-Day

- Eles aproveitam vulnerabilidades zero-day, que são falhas de segurança desconhecidas pelos fornecedores de software, para comprometer sistemas sem detecção imediata.

Backdoors e trojans

- O grupo desenvolve e utiliza backdoors e trojans personalizados, como o WellMess e o WellMail, para manter acesso persistente aos sistemas comprometidos.

Alguns dos malwares já utilizados pelo grupo:

1. **WellMess** e **WellMail**: Utilizados para ataques direcionados a pesquisas de vacinas contra COVID-19, esses malwares permitem controle remoto e exfiltração de dados.
2. **SUNBURST**: Famoso pelo ataque à cadeia de suprimentos da SolarWinds, o SUNBURST foi usado para comprometer múltiplas organizações globais.

3. **GoldMax**: Um backdoor que existe em versões para Windows e Linux, projetado para persistência e evasão de detecção.
4. **TrailBlazer**: Um malware modular descoberto durante investigações que se esconde como arquivos legítimos e mantém comunicação disfarçada com servidores de comando e controle.
5. **GoldFinder** e **Sibot**: Utilizados para criar persistência e coletar dados de vítimas comprometidas, frequentemente vistos em campanhas prolongadas de espionagem.

Movimento lateral

- Após comprometer um sistema inicial, o APT29 utiliza técnicas como credenciais roubadas e ferramentas internas, como PsExec e WMI, para se mover lateralmente dentro da rede da vítima.

Exfiltração de dados

- Para roubar informações, o grupo utiliza métodos furtivos de exfiltração, incluindo criptografia de dados e uso de canais de comunicação seguros para transferir os dados roubados.

Living off the Land (LotL)

- APT29 faz uso de ferramentas e comandos legítimos presentes nos sistemas operacionais das vítimas para evitar detecção por sistemas de segurança.

Obfuscação e evasão

- Eles empregam técnicas avançadas de ofuscação para esconder o código malicioso e usam técnicas de evasão para evitar a detecção por softwares de segurança.

Controle C2 (Command and Control)

- Utilizam infraestruturas complexas de comando e controle para gerenciar os dispositivos comprometidos e coordenar suas operações de ataque.

Persistência

- Para garantir o acesso contínuo aos sistemas, APT29 utiliza diversos métodos de persistência, incluindo a modificação de registros, criação de serviços maliciosos e utilização de Scheduled Tasks.

Inteligência operacional

- Antes de iniciar um ataque, o grupo realiza um reconhecimento detalhado para entender a infraestrutura de TI da vítima e identificar pontos fracos.

5 RISCOS DA VIOLAÇÃO PARA ORGANIZAÇÕES

A violação do TeamViewer representa riscos significativos para as organizações globalmente. Hackers podem obter acesso não autorizado a sistemas internos, facilitando a espionagem industrial e o roubo de propriedade intelectual. Há também o risco de interrupções de serviços essenciais devido a ataques de ransomware ou sabotagem. A perda de dados sensíveis de clientes e funcionários pode ocorrer, resultando em danos à reputação e perda de confiança. Além disso, as empresas podem enfrentar custos adicionais para segurança, resposta a incidentes e recuperação.

6 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Initial Access	Spearphishing Attachment (T1566.001) Exploitation for Client Execution (T1203)	O APT29 usa e-mails com anexos maliciosos para enganar usuários e obter acesso inicial. Exploração de vulnerabilidades em software do cliente para executar código malicioso.
Execution	Command and Scripting Interpreter: PowerShell (T1059.001) User Execution: Malicious File (T1204.002)	Utilização do PowerShell para executar comandos e scripts maliciosos. Requer que o usuário execute um arquivo malicioso.
Persistence	Create Account: Local Account (T1136.001) Registry Run Keys / Startup Folder (T1547.001)	Criação de contas de usuário locais para manter acesso persistente. Modificação de chaves de registro para executar malware durante a inicialização do sistema.
Privilege Escalation	Abuse Elevation Control Mechanism: Bypass User Access Control (T1548.002) Exploitation for Privilege Escalation (T1068)	Bypass de mecanismos de controle de elevação de privilégios para obter privilégios administrativos. Exploração de vulnerabilidades para elevar privilégios.
Defense Evasion	Obfuscated Files or Information (T1027) Masquerading (T1036)	Utilização de técnicas de ofuscação para evitar a detecção. Disfarce de arquivos ou processos maliciosos como legítimos.
Credential Access	Credentials from Password Stores (T1555) Input Capture: Keylogging (T1056.001)	Extração de credenciais de armazenamentos de senha, como o Windows Credential Manager. Captura de entradas de teclado para roubar credenciais.
Discovery	Network Service Scanning (T1046) System Network Configuration Discovery (T1016)	Varredura de serviços de rede para mapear a infraestrutura da vítima. Coleta de informações sobre a configuração de rede do sistema.
Lateral Movement	Remote Services: Remote Desktop Protocol (T1021.001) Pass the Ticket (T1550.003)	Utilização do protocolo RDP para mover-se lateralmente na rede. Uso de tickets Kerberos para autenticação e movimento lateral
Collection	Data from Local System (T1005) Input Capture: Credential Dumping (T1003)	Coleta de dados armazenados localmente nos sistemas comprometidos. Captura de credenciais através de técnicas de despejo de memória.
Exfiltration	Exfiltration Over C2 Channel (T1041) Automated Exfiltration (T1020)	Exfiltração de dados através de canais de comando e controle. Uso de scripts ou ferramentas automatizadas para exfiltrar dados.

Command and Control	Application Layer Protocol: Web Protocols (T1071.001) Non-Standard Port (T1571)	Utilização de protocolos web para comunicação de comando e controle. Utilização de portas não padrão para comunicação de comando e controle para evitar detecção.

Tabela 1 – Tabela MITRE ATT&CK.

7 RECOMENDAÇÕES

São elencados abaixo pela ISH, medidas que poderão ser adotadas visando a mitigação da referida *ameaça*, como por exemplo:

Monitoramento de logs

- Revisar logs de acesso do TeamViewer para atividades incomuns.
- Verificar tentativas de login falhas ou sessões iniciadas fora do horário normal.

Análise de tráfego de rede

- Inspecionar tráfego de rede para detectar conexões suspeitas ou anômalas.
- Utilizar ferramentas de análise de comportamento para identificar padrões incomuns.

Verificação de integridade

- Realizar verificações de integridade em arquivos críticos do sistema.
- Comparar versões atuais de software com versões conhecidas e seguras.

Ferramentas de detecção de intrusões (IDS/IPS)

- Configurar IDS/IPS para alertar sobre atividades suspeitas relacionadas ao TeamViewer.
- Atualizar assinaturas e regras de detecção regularmente.

Segurança de endpoints

- Utilizar soluções de endpoint detection and response (EDR) para monitorar e analisar comportamentos suspeitos nos dispositivos.
- Implementar autenticação multifator (MFA) para acesso ao TeamViewer.

Treinamento e conscientização

- Treinar funcionários sobre práticas seguras de uso do TeamViewer.
- Encorajar a notificação imediata de qualquer atividade suspeita.

Auditoria de acesso

- Conduzir auditorias regulares de acessos concedidos via TeamViewer.
- Revogar acessos desnecessários ou obsoletos.

8 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Nota TeamViewer**
- **Microsoft**
- **MITRE ATT&CK**

9 AUTOR

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH