BOLETIM DE SEGURANÇA

Ataques de ransomware à infraestrutura global por hackers vinculados à China e Coreia do Norte

heimdall
security research
A DIVISION OF ISH

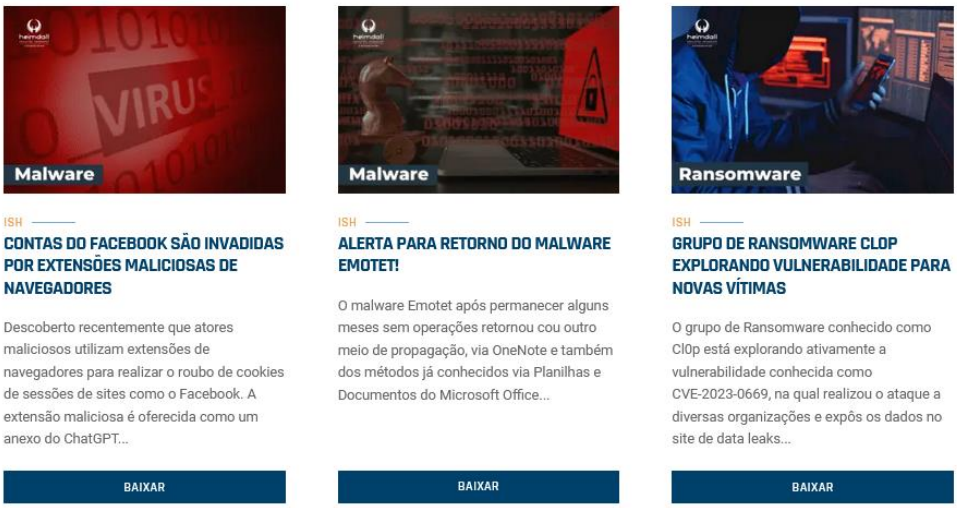
TLP: CLEAR

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

1 SUMÁRIO EXECUTIVO

Agentes de ameaças, supostamente ligados à China e à Coreia do Norte, foram identificados em ataques de ransomware e criptografia de dados que visavam setores governamentais e de infraestrutura crítica globalmente de 2021 a 2023.

2 INFORMAÇÕES SOBRE A AMEAÇA

As empresas de segurança cibernética SentinelOne e Recorded Future, em um relatório conjunto, associaram um grupo de atividades ao ChamelGang (ou CamoFei) e outro a atividades anteriormente ligadas a grupos apoiados pelos governos chinês e norte-coreano. Os ataques do ChamelGang incluíram o uso do ransomware CatB contra o All India Institute of Medical Sciences (AIIMS), a Presidência do Brasil em 2022, uma entidade governamental no Leste Asiático e uma organização de aviação na Índia. Os pesquisadores de segurança Aleksandar Milenkoski e Julian-Ferdinand Vögele observaram que os atores de ameaças estão cada vez mais usando ransomware em suas operações para diversos fins, incluindo ganho financeiro, interrupção, distração, atribuição incorreta ou remoção de evidências. Os ataques de ransomware neste contexto não servem apenas como uma saída para sabotagem, mas também permitem que os agentes da ameaça encobrem os seus rastos, destruindo artefactos que, de outra forma, poderiam alertar os defensores da sua presença.

O ChamelGang, documentado pela primeira vez em 2021 pela Positive Technologies, é avaliado como um grupo do nexo da China que opera com motivações tão variadas como coleta de inteligência, roubo de dados, ganho financeiro, ataques de negação de serviço (DoS) e operações de informação, de acordo com a empresa taiwanesa de segurança cibernética TeamT5. O ChamelGang é conhecido por ter uma variedade de ferramentas em seu arsenal, incluindo BeaconLoader, Cobalt Strike, backdoors como AukDoor e DoorMe, e uma cepa de ransomware conhecida como CatB, que foi identificada como usada em ataques direcionados ao Brasil e à Índia com base em semelhanças na nota de resgate, no formato do endereço de e-mail de contato, no endereço da carteira de criptomoedas e na extensão do nome do arquivo criptografado.

Os ataques em 2023 também utilizaram uma versão atualizada do BeaconLoader para fornecer o Cobalt Strike para atividades de reconhecimento e pós-exploração, como descarte de ferramentas adicionais e exfiltração do arquivo de banco de dados NTDS.dit. Vale destacar que malwares personalizados utilizados pelo ChamelGang, como DoorMe e MGDrive (cuja variante do macOS é chamada Gimmick), também foram vinculados a outros grupos de ameaças chineses, como REF2924 e Storm Cloud, aludindo mais uma vez à possibilidade de um " Intendente digital fornecendo malware a grupos operacionais distintos."

Outro conjunto de intrusões envolveu o uso do Jetico BestCrypt e do Microsoft BitLocker em ataques cibernéticos que afetam vários setores verticais da indústria na América do Norte, América do Sul e Europa. Estima-se que cerca de 37 organizações, predominantemente do setor industrial dos EUA, tenham sido visadas. As táticas observadas no cluster, pelas duas empresas de segurança cibernética, são consistentes com aquelas atribuídas a uma equipe de hackers chinesa chamada APT41 e a um ator norte-coreano conhecido como Andariel , devido à presença de ferramentas como o web shell China Chopper e um backdoor conhecido como DTrack. .

3 CONCLUSÃO

Os pesquisadores afirmam que as operações de espionagem cibernética disfarçadas de atividades de ransomware oferecem uma oportunidade para os países adversários alegarem negação plausível, atribuindo as ações a atores cibercriminosos independentes, em vez de entidades patrocinadas pelo Estado. Foi observado também que o uso de ransomware por grupos de ameaças de ciberespionagem confunde os limites entre o crime cibernético e a espionagem cibernética, proporcionando aos adversários vantagens tanto do ponto de vista estratégico quanto operacional.

4 RECOMENDAÇÕES

Atualize regularmente

- Mantenha todos os sistemas, softwares e aplicativos atualizados.

Backup de dados

- Faça backup regular de seus dados importantes e garanta que esses backups sejam protegidos contra ataques.

Antivírus e anti-malware

- Use soluções de antivírus e anti-malware e mantenha-as atualizadas.

Educação em segurança cibernética

- Eduque-se e a sua equipe sobre as melhores práticas de segurança cibernética, incluindo a identificação de e-mails e sites suspeitos.

Restrição de privilégios

- Restrinja os privilégios de usuário e sistema sempre que possível, para minimizar o impacto potencial de um ataque de ransomware.

Ferramentas de detecção de intrusão

- Utilize ferramentas de detecção de intrusão para identificar qualquer atividade suspeita o mais rápido possível.

Plano de resposta a incidentes

- Tenha um plano de resposta a incidentes em vigor para garantir uma ação rápida e eficaz em caso de um ataque.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- [Thehackernews]

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH