BOLETIM DE SEGURANÇA

Novo grupo de Ransomware atacando a América do Sul identificado, Arcus Media

heimdall
security research
A DIVISION OF ISH

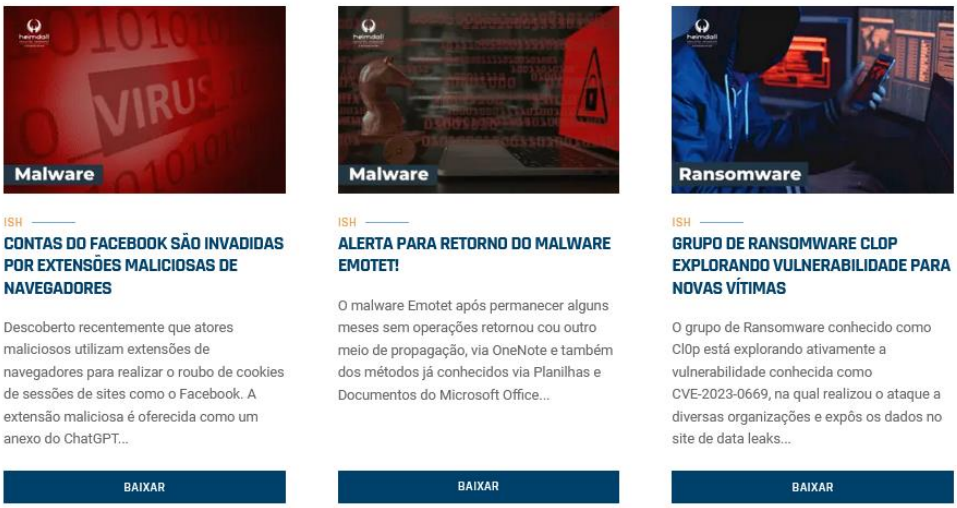
TLP: CLEAR

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 FIGURAS

1 SUMÁRIO EXECUTIVO

Recentemente o time de inteligência Heimdall da ISH, identificou um novo grupo de ransomware chamado **Arcus Media**, atacando organizações da América do Sul, até o momento, em sua maioria os ataques têm tido como alvo principal organizações do Brasil.

Figura 1 – Imagem principal do grupo em sua página .onion.

2 VITIMOLOGIA OU SETORES ALVOS

Até o momento, na página .onion deste novo grupo, foi observado setores como Governo, Saúde, Alimentício, Construção, Contábil entre outros em alguns países, e em sua maioria países da América do Sul, tendo como principal alvo o **Brasil**, conforme imagem abaixo da página .onion do grupo malicioso.

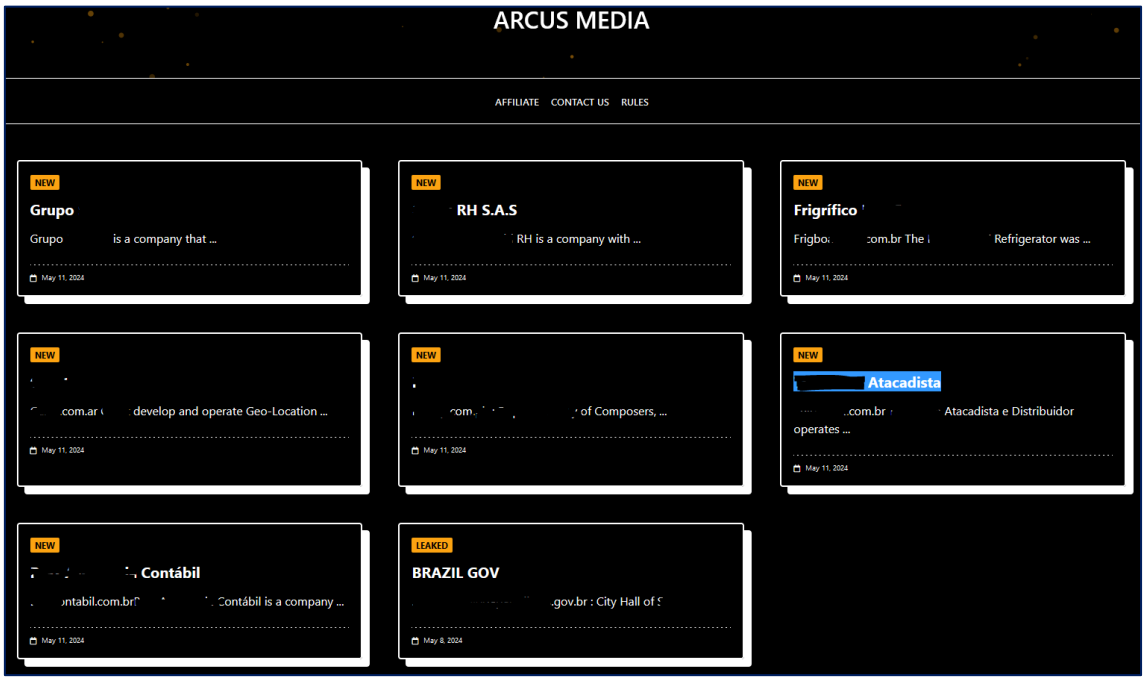


Figura 2 – Publicações das vítimas na página .onion do grupo de ransomware.

Observação, a identidade das organizações publicadas foi ocultada.

3 CONCLUSÃO

Devido ao grupo ser bastante novo e a variedade de setores atacados, ainda não se tem informações concretas sobre o grupo como métodos, cadeia de ataques ou setores alvos específicos, porém destacamos que organizações no Brasil devem estar sempre atentas e preparadas com as melhores técnicas de defesas contra este tipo de ameaça. No tópico posterior, destacamos medidas de segurança importantes que organizações e governos podem tomar como proteção.

4 RECOMENDAÇÕES

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

Investa em tecnologias de segurança

- Soluções avançadas de segurança: Adotar tecnologias como proteção de carga de trabalho em nuvem, Firewalls de Próxima Geração (NGFWs), Endpoint Detection and Response (EDR), e acesso de rede Zero Trust (ZTNA) são fundamentais para fortalecer as defesas contra ransomware.
- Inteligência artificial e machine learning: Utilizar ferramentas que empregam IA e Machine Learning pode ajudar a detectar e responder a ameaças de forma mais eficaz.

Monitoramento e detecção contínua

- Monitoramento 24/7: Implementar sistemas de monitoramento contínuo para identificar atividades suspeitas em tempo real e responder rapidamente a incidentes. Ferramentas de Gerenciamento de Informações e Eventos de Segurança (SIEM) e Orquestração e Resposta de Segurança Automatizada (SOAR) são cruciais para isso.
- Análise de Inteligência de Ameaças: Utilizar serviços gerenciados de segurança que ofereçam análise avançada e inteligência de ameaças pode ajudar a antecipar e responder a ataques emergentes.

Backup regular e seguro

- Realizar backups frequentes: Manter backups atualizados e armazenados de forma segura, preferencialmente fora do local ou na nuvem, é vital para recuperar dados sem precisar pagar resgate.
- Testar a integridade dos backups: Garantir que os backups sejam testados regularmente para verificar a integridade e a confiabilidade dos dados.

Educação e treinamento de colaboradores

- Treinamentos contínuos: Educar os colaboradores sobre boas práticas de cibersegurança e como reconhecer tentativas de phishing e outros métodos de infecção por ransomware.
- Simulações de ataques: Realizar simulações de ataques para preparar a equipe e garantir que todos saibam como reagir em caso de um incidente real.

Boas práticas de cibersegurança

- Atualizações regulares: Manter sistemas operacionais, softwares e aplicativos sempre atualizados para corrigir vulnerabilidades conhecidas.

- Autenticação multifator (MFA): Implementar autenticação multifator para adicionar uma camada extra de segurança aos acessos sensíveis.
- Configuração adequada de antivírus e anti-malware: Garantir que soluções de antivírus e anti-malware estejam devidamente configuradas e

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**

6 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH