heimdall

security research

A DIVISION OF ISH

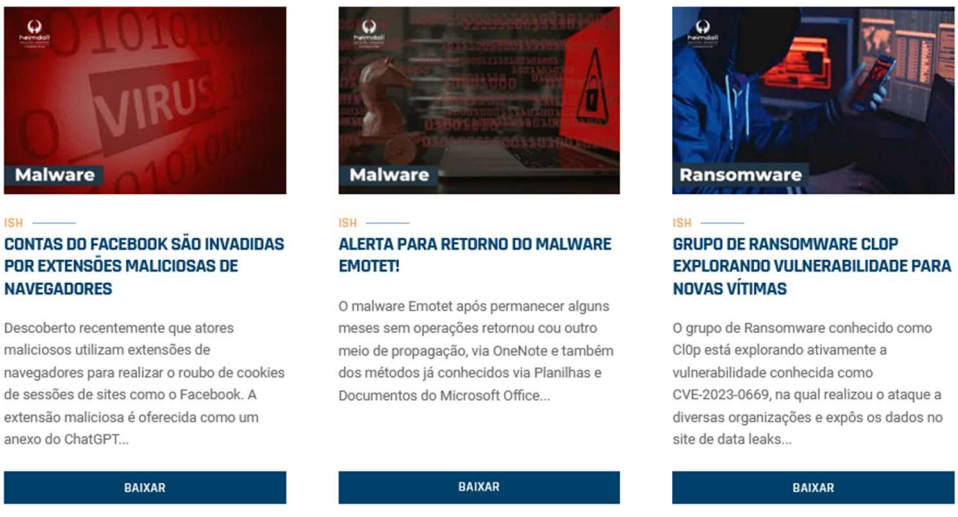
Nova operação de Ransomware identificada, 8base Ransomware

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



Sumário

1 Nova operação 6
2 Recomendações 8
3 Referências 9

Lista de Figuras

Figura 1 – Página principal do Ransomware. 6
Figura 2 – Regras para as vítimas realizarem o contato e pagamento. 6
Figura 3 – Conteúdo da nota de resgate. 7

1 NOVA OPERAÇÃO

Recentemente, fora identificado uma nova operação de ransomware que atingiu até o momento diversas organizações, bem como verificado que atua da mesma forma que demais operações de ransomwares até o momento.

Esta operação foi identificada como **8base Ransomware**, havendo apenas até o momento detalhes sobre o seu site de data leak e nota de resgate.

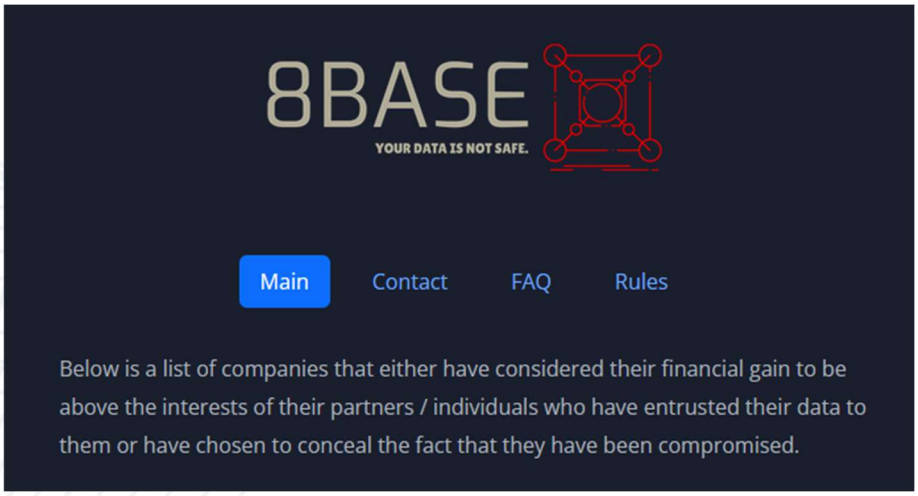


Figura 1 – Página principal do Ransomware.

Bem como apresenta algumas regras para a vítima.

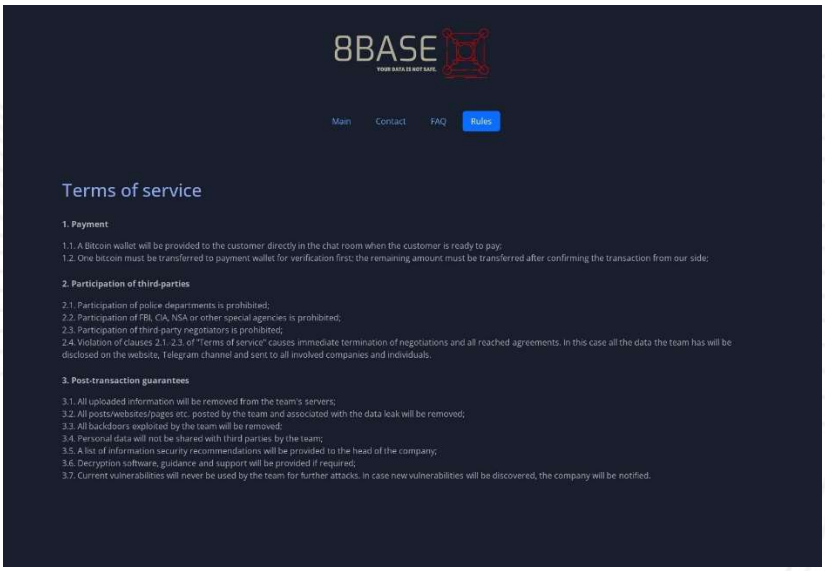


Figura 2 – Regras para as vítimas realizarem o contato e pagamento.

Nas publicações realizadas das empresas, foi identificado a utilização de serviço de nuvem para publicação e download de dados de empresas que foram vítimas e tiveram seus dados exfiltrados.

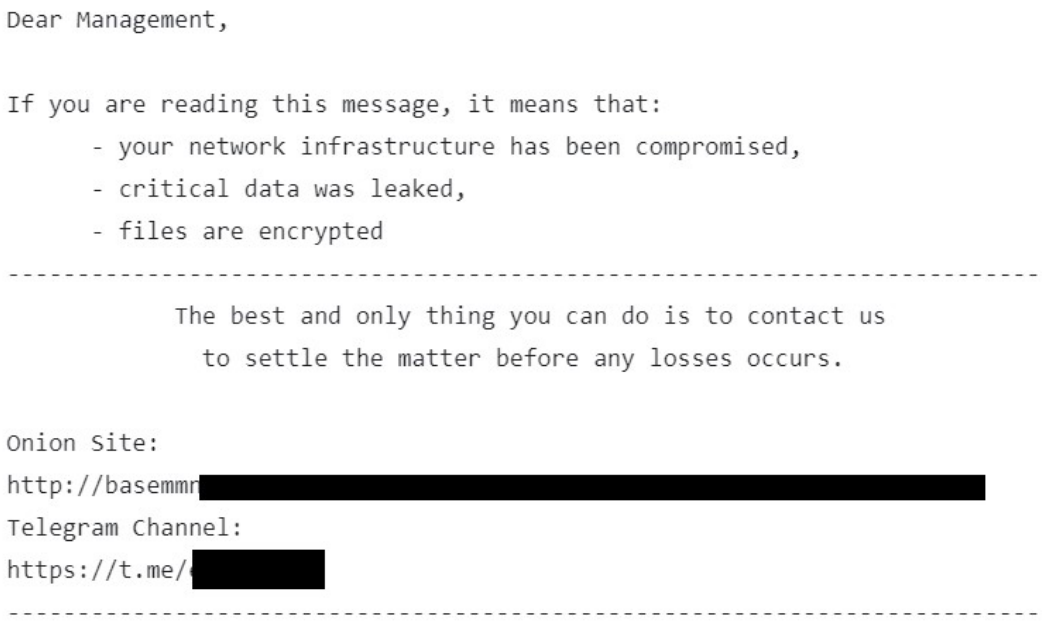


Figura 3 – Conteúdo da nota de resgate.

Até o momento, não fora observado amostras disponíveis ou demais detalhes de sua operação, havendo a existência destes dados posteriormente, estes serão compartilhados.

2 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:

- **Realização de *backups* regulares:** Armazene cópias de segurança de todos os dados importantes em um local seguro e desconectado.
- **Realização de atualizações de *softwares*:** Mantenha todos os *softwares* de ativos atualizados, incluindo sistemas operacionais e aplicativos.
- **Utilização de proteção de rede**, como *firewalls*, antivírus e outras medidas de segurança para proteger sua rede.
- **Realização do trabalho de conscientização** com os colaboradores, ensinando aos mesmos a reconhecer e evitar ameaças, como *phishing* e/ou clicar em *links* maliciosos.
- **Monitoração regular da sua rede e sistemas** para identificar e responder rapidamente a qualquer atividade suspeita.
- **Criação e aplicação de um plano de resposta de incidentes**, sendo que em caso de ataques de *ransomware* poderão ser utilizados e conterão informações como questões relacionadas a *backups* e recuperação de sistema.

3 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**

heimdall
security research

A DIVISION OF ISH