BOLETIM DE SEGURANÇA

Novo ransomware Eldorado ameaçando VMs Windows e VMware ESXi

heimdall
security research
A DIVISION OF ISH

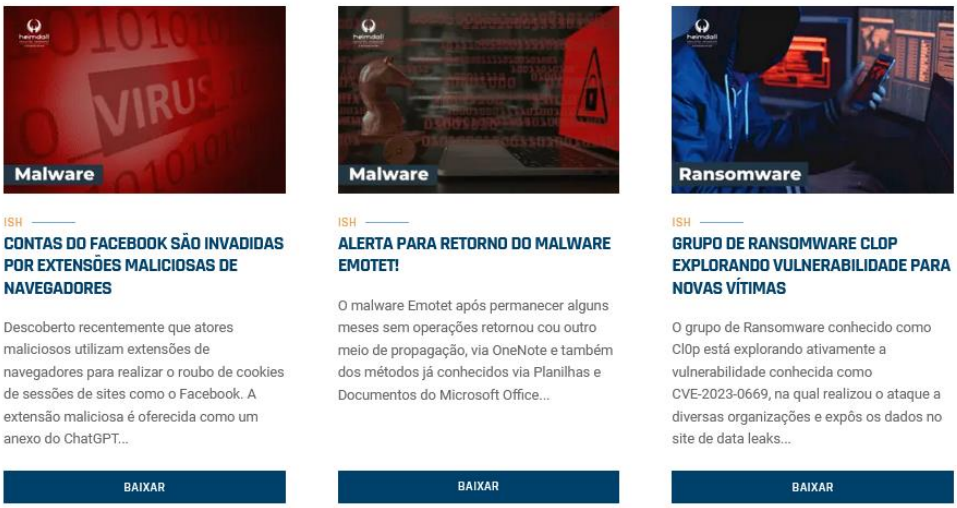
TLP: CLEAR

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

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Pesquisadores de segurança da Group-IB identificaram uma nova ameaça emergente no cenário de cibersegurança, o ransomware como serviço (RaaS) denominado "Eldorado", atingindo sistemas Windows e VMware ESXi.

2 INFORMAÇÕES SOBRE A AMEAÇA

O ransomware “Eldorado” está causando preocupação ao atingir sistemas Windows e VMware ESXi. Essa nova ameaça, escrita em Golang, já infectou pelo menos 16 organizações, principalmente nos Estados Unidos, desde março. O Eldorado oferece variantes para ambas as plataformas, com recursos de criptografia e distribuição incomuns. Seus criadores optaram por usar a linguagem Go para garantir capacidades de plataforma cruzada, e o malware utiliza o algoritmo Chacha20 para criptografar arquivos e o RSA-OAEP para criptografia de chaves. Além disso, o Eldorado usa o protocolo Server Message Block (SMB) para criptografar arquivos em redes compartilhadas. A operação de ransomware também permite que afiliados personalizem amostras de ransomware para suas vítimas, tornando-a ainda mais perigosa.

O grupo Eldorado também opera um site dedicado à divulgação de dados vazados, no qual as vítimas são listadas. Contudo, este site encontrava-se fora do ar quando este artigo foi escrito.

Figura 1 – Vítimas do Eldorado.

Eldorado é um ransomware desenvolvido em Go que possui a capacidade de criptografar tanto plataformas Windows quanto Linux. Para isso, ele utiliza duas variantes distintas que compartilham diversas similaridades operacionais. Pesquisadores tiveram acesso a um criptografador fornecido pelo desenvolvedor, juntamente com um manual do usuário. Este manual indicava que existem variantes de 32 e 64 bits disponíveis, direcionadas especificamente para hipervisores VMware ESXi e sistemas Windows.

De acordo com a Group-IB, o Eldorado representa um empreendimento exclusivo, não se baseando em recursos de construtoras previamente publicadas. Este malware emprega o algoritmo de criptografia ChaCha20, gerando uma chave única de 32 bytes e um nonce de 12 bytes para cada arquivo que é bloqueado.

Essas chaves e nonces são então criptografados utilizando o algoritmo RSA, com o esquema Optimal Asymmetric Encryption Padding (OAEP), garantindo uma camada adicional de segurança na criptografia dos dados. Após o processo de criptografia, os arquivos são modificados para incluir a extensão ".00000001", tornando-os inacessíveis aos usuários comuns. Junto a essa alteração, são adicionadas notas de resgate intituladas "HOW_RETURN_YOUR_DATA.TXT" em diretórios críticos, como as pastas Documentos e Área de Trabalho, destacando a presença de um ataque de ransomware. Além da extensão alterada, essas notas de resgate servem como um aviso claro do sequestro de dados, fornecendo instruções sobre como proceder para recuperar as informações criptografadas. Os usuários, ao tentarem acessar seus arquivos, se deparam com esses avisos, o que os direciona a um possível contato com os responsáveis pelo ataque.

Dessa forma, a estratégia de disseminação das notas de resgate e a alteração das extensões dos arquivos são partes essenciais do ataque, garantindo que a vítima perceba rapidamente a gravidade da situação. A presença desses elementos nas pastas mais usadas aumenta a probabilidade de que os usuários vejam o aviso logo após o ataque.

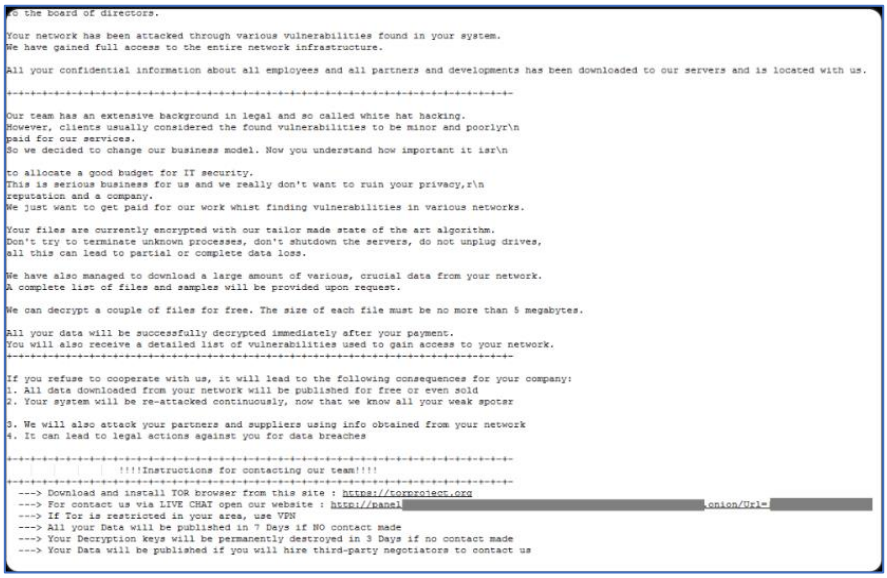


Figura 2 – Nota de resgate.

O Malware utiliza criptografia para compartilhamentos de rede via protocolo SMB, amplificando seu impacto e removendo cópias de volume de sombra em máquinas Windows comprometidas para bloquear a recuperação de dados. Ele exclui arquivos DLLs, LNK, SYS e EXE, além de arquivos e diretórios essenciais para o sistema, evitando que o sistema fique inutilizável ou que não consiga inicializar. Para prevenir a detecção e análise, ele é programado para se autoexcluir por padrão, dificultando o trabalho das equipes de resposta. No Windows, é possível especificar diretórios para criptografar, ignorar arquivos locais, focar em compartilhamentos de rede específicos e impedir a autoexclusão do malware. Em contrapartida, no Linux, a personalização se limita à definição dos diretórios a serem criptografados, sem a possibilidade de ajustes mais complexos.

3 INDICADORES DE COMPROMISSOS

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de compromisso do artefato	
md5:	315a9d36ed86894269e0126b649fb3d6
sha1:	caaa1f85dd333c9d19767b5de527152d5acbc2a4
sha256:	cb0b9e509a0f16eb864277cd76c4dcaa5016a356dd62c04dff8f8d96736174a7
File name:	trump.exe

Tabela 1 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
IP	173.44.141[.]152

Tabela 2 – Indicadores de Compromissos de Rede.

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

4 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:

Autenticação MFA

- Implemente autenticação multifator (MFA) e soluções de acesso baseadas em credenciais.

Utilização de Endpoints

- Use o Endpoint Detection and Response (EDR) para identificar e responder rapidamente a indicadores de ransomware.

Realização de backups

- Faça backups de dados regularmente para minimizar danos e perdas de dados.

Análise por IA

- Utilize análises baseadas em IA e detonação avançada de malware para detecção e resposta a intrusões em tempo real.

Patches de segurança

- Priorize e aplique periodicamente patches de segurança para corrigir vulnerabilidades.

Conscientização de segurança

- Eduque e treine funcionários para reconhecer e relatar ameaças à segurança cibernética.

Auditorias de segurança

- Realize auditorias técnicas anuais ou avaliações de segurança e mantenha a higiene digital.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Group-ib**
- **Thehackernews**

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH