BOLETIM DE SEGURANÇA

Ransomware Qilin é observado roubando credenciais armazenadas no Google Chrome

heimdall
security research
A DIVISION OF ISH

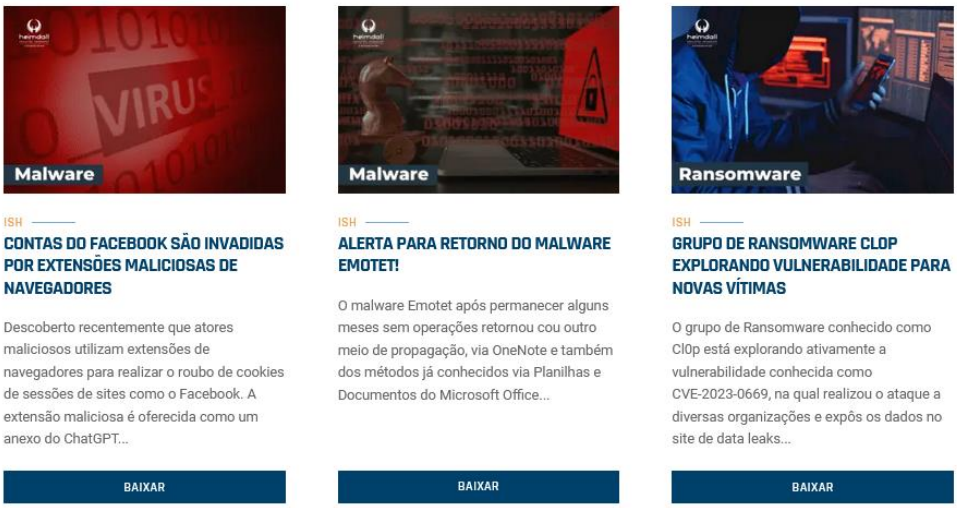
TLP: CLEAR

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

Os agentes de ameaças por trás de um recente ataque de ransomware Qilin roubaram credenciais armazenadas nos navegadores Google Chrome em um pequeno número de endpoints comprometidos. Este incidente destaca a contínua ameaça representada por grupos de ransomware que visam dados sensíveis.

2 INFORMAÇÕES SOBRE A AMEAÇA

O grupo de ransomware Qilin está ativo há pouco mais de dois anos. Em junho de 2024, eles ganharam destaque com um ataque contra uma prestadora de serviços governamentais para vários provedores de saúde e hospitais no Reino Unido. Os ataques do Qilin frequentemente envolviam "dupla extorsão" – roubando dados da vítima, criptografando seus sistemas e, em seguida, ameaçando revelar ou vender os dados roubados se a vítima não pagasse pela chave de criptografia.

Nesse caso, o invasor obteve acesso inicial ao ambiente por meio de credenciais comprometidas. Infelizmente, esse método de acesso inicial não é novo para o Qilin (ou outras gangues de ransomware). A investigação indicou que o portal VPN não tinha proteção de autenticação multifator (MFA). O tempo de permanência do invasor entre o acesso inicial à rede e o movimento posterior foi de dezoito dias, o que pode ou não indicar que um Initial Access Broker (IAB) fez a incursão real. Dezoito dias após o acesso inicial, a atividade do invasor no sistema aumentou, com artefatos mostrando movimento lateral para um controlador de domínio usando credenciais comprometidas. Depois de alcançar o controlador de domínio, o invasor editou a política de domínio padrão para introduzir um Objeto de Política de Grupo (GPO) baseado em logon contendo dois itens. O primeiro, um script do PowerShell chamado IPScanner.ps1, foi gravado em um diretório temporário dentro do compartilhamento SYSVOL (SYStem VOLume) no controlador de domínio específico envolvido. Ele continha um script de 19 linhas que tentava coletar dados de credenciais armazenados no navegador Chrome.

O segundo item, um script em lote chamado logon.bat, continha os comandos para executar o primeiro script. Essa combinação resultou na coleta de credenciais salvas em navegadores Chrome em máquinas conectadas à rede. Como esses dois scripts estavam em um GPO de logon, eles seriam executados em cada máquina cliente conforme ela efetuasse login.

Sempre que um logon ocorria em um endpoint, o logon.bat iniciava o script IPScanner.ps1, que por sua vez criava dois arquivos – um arquivo de banco de dados SQLite chamado LD e um arquivo de texto chamado temp.log.

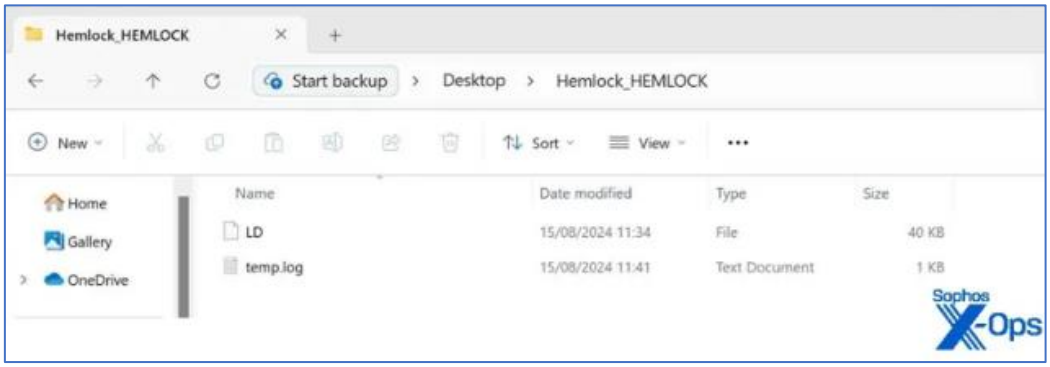


Figura 1 – Demonstração de Hemlock.

Os arquivos foram salvos em um novo diretório criado no compartilhamento SYSVOL do domínio, sendo nomeados conforme o nome do host dos dispositivos onde foram executados (por exemplo, Hemlock).

O arquivo de banco de dados LD inclui a estrutura.

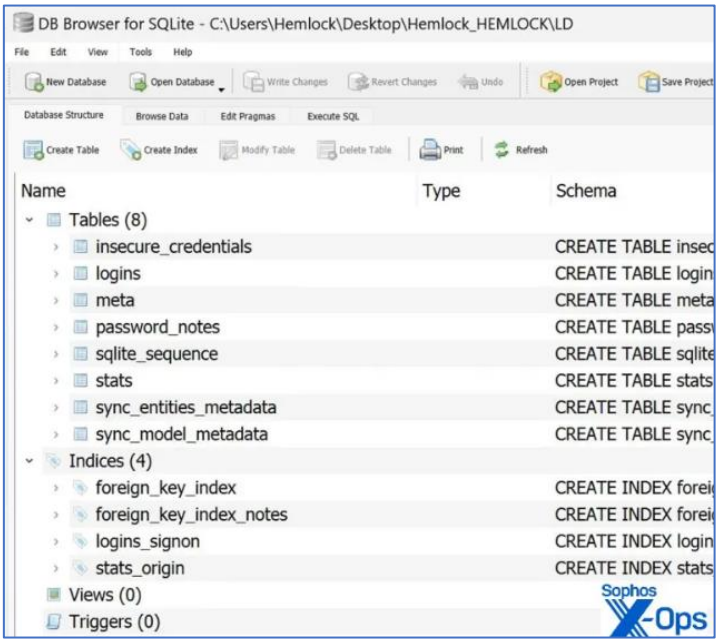


Figura 2 – Arquivo de banco de dados SQLite inserido no SYSVOL.

O invasor, confiante de que não seria descoberto ou perderia o acesso à rede, manteve o GPO ativo por mais de três dias. Isso permitiu que os usuários fizessem logon em seus dispositivos e, sem saber, ativassem o script de coleta de credenciais. Como o GPO de logon foi utilizado, cada usuário teve suas credenciais roubadas a cada login. Para dificultar a avaliação do comprometimento, após roubar e exfiltrar os arquivos com as credenciais, o invasor excluiu todos os arquivos e limpou os logs de eventos do controlador de domínio e das máquinas infectadas. Em seguida, criptografou os arquivos e deixou a nota de resgate, conforme ilustrado na Figura 3. Este ransomware coloca uma cópia da nota em cada diretório do dispositivo onde é executado.

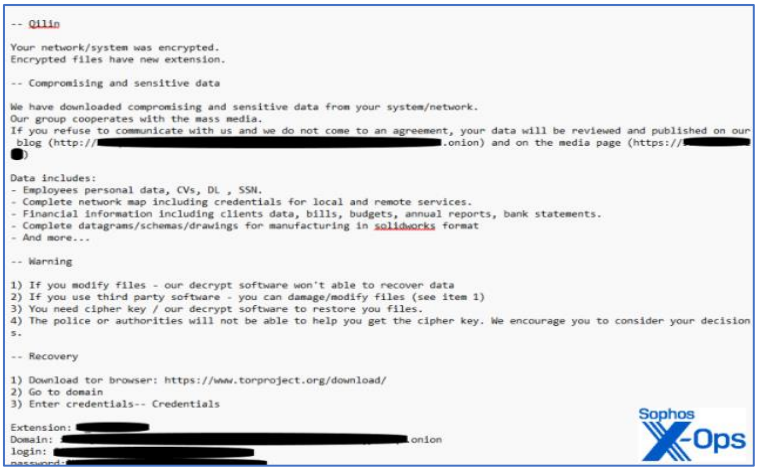


Figura 3 – Arquivo de banco de dados SQLite inserido no SYSVOL.

O grupo Qilin utilizou o GPO mais uma vez como método para comprometer a rede. Eles configuraram o GPO para criar uma tarefa agendada que executava um arquivo em lote denominado run.bat. Este arquivo era responsável por baixar e iniciar o ransomware.

Durante este ataque, o script IPScanner.ps1 focou nos navegadores Chrome, que dominam mais de 65% do mercado, tornando-os alvos ideais para a coleta de senhas. O sucesso do ataque dependia das credenciais armazenadas por cada usuário no navegador. Pesquisas recentes mostram que o usuário médio possui 87 senhas de trabalho e cerca de duas vezes mais senhas pessoais.

Um comprometimento bem-sucedido exigiria que os defensores alterassem todas as senhas do Active Directory e solicitassem que os usuários finais mudassem suas senhas em dezenas ou centenas de sites de terceiros onde salvaram suas credenciais no Chrome. No entanto, os defensores não teriam como garantir que os usuários fizessem isso. Para os usuários finais, a situação seria inversa ao comum: em vez de um site comprometido afetando muitos usuários, um usuário teria dezenas ou centenas de violações separadas. Neste ataque, outros controladores de domínio no mesmo domínio do Active Directory foram criptografados, mas o controlador de domínio onde o GPO específico foi configurado permaneceu sem criptografia.

3 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 multifator (MFA)

- Habilite a MFA para adicionar uma camada extra de segurança, dificultando o acesso não autorizado.

Backup de dados

- Mantenha backups regulares e offline dos dados críticos para garantir a recuperação em caso de ataque.

Atualização de patches de segurança

- Priorize a aplicação de patches de segurança para corrigir vulnerabilidades conhecidas.

Treinamento de funcionários

- Realize treinamentos regulares sobre higiene cibernética e conscientização sobre phishing e outras ameaças.

Monitoramento ativo de vulnerabilidades

- Utilize ferramentas de monitoramento para identificar e mitigar vulnerabilidades em tempo real.

Uso de soluções antimalware avançadas

- Implemente soluções de detecção e resposta a ameaças para identificar e bloquear atividades maliciosas.

Restrição de armazenamento de dados sensíveis em navegadores

- Evite armazenar senhas e outras informações sensíveis em navegadores como o Chrome.

4 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:	64ca549e78ad1bd3a4bd2834b0f81080
sha1:	493ff413528f752c5fce3ceabd89d2ab37397b86
sha256:	93c16c11ffca4ede29338eac53ca9f7c4fbcf68b8ea85ea5ae91a9e00dc77f01v
File name:	enc.exe

Indicadores de compromisso do artefato	
md5:	eb6fff4ee0f03ae5191f11570ff221c5
sha1:	c2dfbf554e068195ecc40bebd0617ce09ad65784
sha256:	54ff98956c3a0a3bc03a5f43d2c801ebcc1255bed644c78bad55d7f7beebd294
File name:	decryptor_399060b2.exe

Indicadores de compromisso do artefato	
md5:	923c5af6fd29158b757fb876979d250b
sha1:	6b3e3ff0495d39c85eca41f336bfd5ff92c97412
sha256:	9e1f8165ca3265ef0ff2d479370518a5f3f4467cd31a7b4b006011621a2dd752
File name:	update.exe

Indicadores de compromisso do artefato	
md5:	31edb01d243e8d989eb7e5aeeeef54dc
sha1:	05f60fc706754b317ffc7839a2b0490f7cd6f71d
sha256:	e4882b8e8e414e983cf003a5c4038043002a004b63c4f0844a15268332597e80
File name:	31edb01d243e8d989eb7e5aeeeef54dc.virus

Indicadores de compromisso do artefato	
md5:	e01776ec67b9f1ae780c3e24ecc4bf06
sha1:	3ef805009f8694e78699932563c09ac3b6bc08a5
sha256:	0629cd5e187174cb69f3489675f8c84cc0236f11f200be384ed6c1a9aa1ce7a1
File name:	552590___7c571a4a-7299-4c71-863b-748b0551804c.elf

Indicadores de compromisso do artefato	
md5:	63b89a42c39b2b56aae433712f96f619
sha1:	50927809fa3f1ec408d7a1715a714831f41160db
sha256:	bf9fc34ef4734520a1f65c1ec0a91b563bf002ac63982cbd2df10791493e9147
File name:	2023-12-15_63b89a42c39b2b56aae433712f96f619

Tabela 1 – Indicadores de Compromissos de artefatos

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Sophos**
- **Thehackernews**

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH