



**heimdall**  
security research

---

A DIVISION OF ISH



# **Novo Ransomware do Monti para máquinas Linux**



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



ISH  
**CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES**

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR



ISH  
**ALERTA PARA RETORNO DO MALWARE EMOTET!**

O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR



ISH  
**GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VITIMAS**

O grupo de Ransomware conhecido como Clop está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

## Sumário

1	Introdução.....	7
2	Análise do Ransomware.....	8
3	Conclusão.....	12
4	TTPs – MITRE ATT&CK.....	13
5	IoCs .....	14
6	Referências.....	15

## **Lista de Tabelas**

Tabela 1 – Argumentos de linha de comando aceitos pela variante.	8
Tabela 2 – Tabela MITREE ATT&CK	13
Tabela 3 – Indicadores de Compromissos artefatos de host.	14

## **Lista de Figuras**

Figura 1 – Comparação das antigas e nova variante identificada do Monti com o BinDiff. ....	7
Figura 2 – Trecho do código utilizado para finalizar máquinas virtuais. ....	8
Figura 3 – Função utilizada para adulterar arquivos.....	9
Figura 4 – Novo conteúdo de /etc/motd. ....	9
Figura 5 – Trecho de código para verificar a presença da string “MONTI” através dos últimos 261 bytes do arquivo a ser criptografado. ....	10
Figura 6 – Extensões anexadas aos arquivos criptografados. ....	11
Figura 7 – Nota de resgate apresentada após a criptografia.....	11

# 1 INTRODUÇÃO

O Ransomware Monti, o qual possui variantes baseadas em sistemas operacionais Windows e Linux veio a chamar atenção de pesquisadores de segurança cibernética quando foi descoberto pela primeira vez em junho de 2022, justamente por conta de sua notável semelhança com o Ransomware Conti (não apenas no nome, mas também nas táticas que os atores de ransomwares utilizam).

O grupo de ransomware que utilizou o nome de “**Monti**” também veio a emular as táticas, técnicas e procedimentos amplamente reconhecidos (TTPs) da equipe Conti, incorporando um número substancial de suas ferramentas e até mesmo utilizando o código-fonte vazado do Conti.

Diante disto, a empresa Trend Micro publicou um relatório se baseando na operação e no novo ransomware para Linux dos atores de ameaças do Monti. O grupo teria realizado uma pausa de dois meses na exposição de vítimas em seu site de vazamento, retornando posteriormente com suas atividades criminosas visando organizações nos setores jurídicos e governamentais. O ransomware utilizado era para a versão em Linux, sendo identificado que não se baseava no código-fonte vazado da Conti, sendo empregado uma nova versão do criptografador com base em comportamentos.

A empresa realizou a comparação da nova variante com outras variantes antigas e do Conti, havendo uma taxa de 29% de similaridade, em comparação com a antiga variante do Monti que obteve o resultado de 99%.

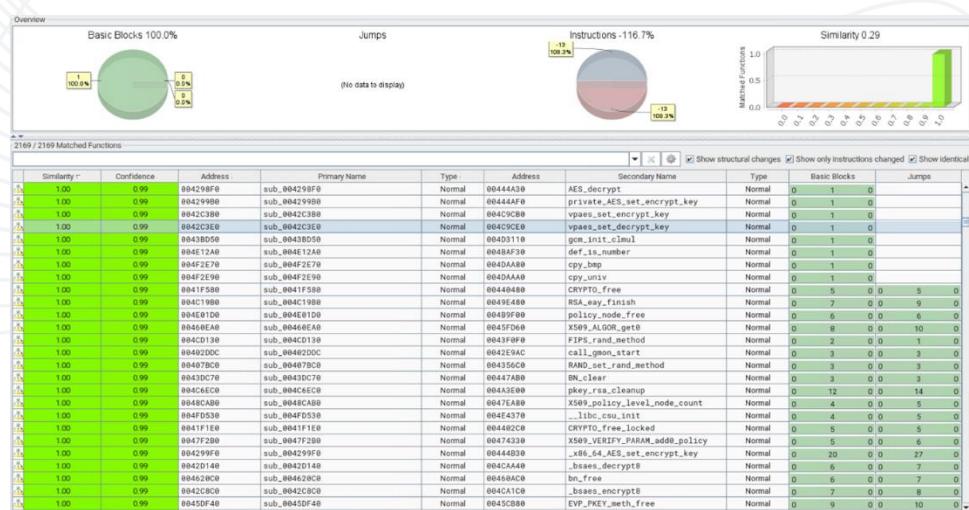


Figura 1 – Comparação das antigas e nova variante identificada do Monti com o BinDiff.

## 2 ANÁLISE DO RANSOMWARE

A nova variante para Linux possui a aceitação de alguns argumentos de linhas de comandos, omitindo alguns argumentos de sua variante mais antiga e adicionando o parâmetro “--whitelist”. A tabela abaixo exemplifica os parâmetros utilizados pela variante.

Argumento	Descrição
--help	Exibe a opção de ajuda dos argumentos.
--path <string>	Caminho que pode ser utilizado para criptografar.
--whitelist <string>	Lista de VMs a serem ignoradas
--vmkill	Opção para “matar” a máquina virtual.
--detach	Separe o terminal

Tabela 1 – Argumentos de linha de comando aceitos pela variante.

Em comparação com a versão anterior, a versão atual também emprega o parâmetro “--type=soft” para encerrar máquinas virtuais no sistema (em oposição ao parâmetro --type=hard). A mudança para --type=soft pode sugerir que os atores de ameaças por trás do Monti podem ter escolhido esta abordagem para minimizar o risco de detecção imediata durante a realização de suas atividades.

```

if ( v33[0] != v33[1] )
{
    do
    {
        v11 = *v10;
        v12 = fork();
        if ( v12 == -1 )
        {
            perror("fork");
        }
        else
        {
            if ( !v12 )
            {
                execlp("esxcli", "esxcli", "vm", "process", 5234374LL, "--type=soft", "--world-id", v11, 0LL);
            }
        }
    }
}

```

Figura 2 – Trecho do código utilizado para finalizar máquinas virtuais.

Os desenvolvedores do Monti também adulteraram os arquivos “/etc/motd” e “index.html”, substituindo seu conteúdo por uma nota de resgate anunciando que o servidor foi infiltrado com sucesso. Vale salientar que MOTDS (ou Mensagem do Dia) é uma mensagem de texto exibida quando um usuário afeta login em um sistema operacional Linux.

```
sub_4042B0("/etc/motd", off_7633E8);           // RANSOM NOTE
sub_4042B0("/usr/lib/vmware/hostd/docroot/index.html", buf);
```

Figura 3 – Função utilizada para adulterar arquivos.

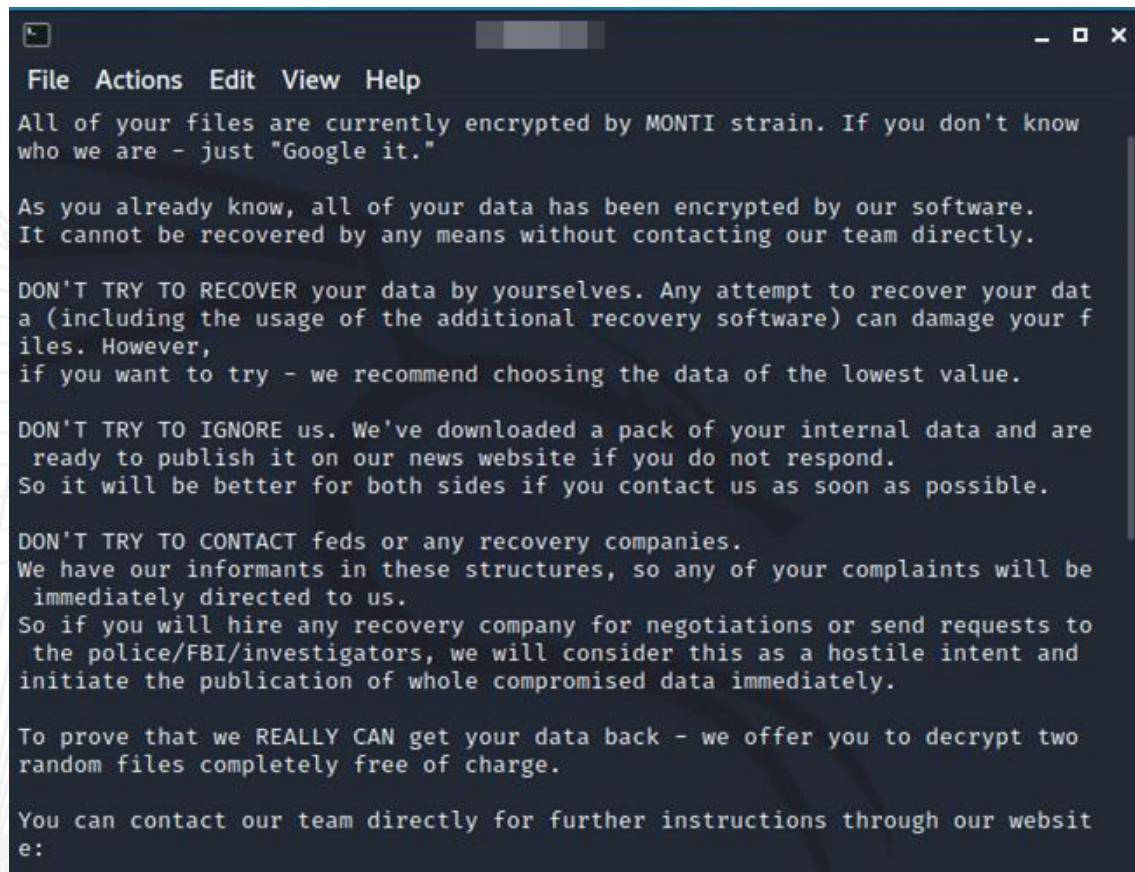


Figura 4 – Novo conteúdo de /etc/motd.

Quanto a infecção, uma das adições da nova variante é que ela anexa os bytes “MONTI” seguidos por 256 bytes adicionais que estão vinculados à chave de criptografia.

Antes de prosseguir com a sua rotina de criptografia, o ransomware verificará condições específicas. Primeiro ele verifica se o tamanho do arquivo é de 261 bytes ou menos, o que corresponde ao tamanho do marcador de infecção que ele anexa após a sua criptografia. Caso esta condição for atendida, o ransomware continua com o processo de infecção.

Se a condição inicial não for atendida, o Monti verificará os últimos 261 bytes do arquivo para verificar a presença da string "MONTI". Se caso a string for detectada, o arquivo será ignorado, significando que já foi criptografado. No entanto, se caso a sequência não for encontrada, o malware prosseguirá com o processo de criptografia do arquivo.

```
lseek(v4, -261LL, 2);
v5 = old;
v6 = "[%s] Error reading file meta before crypt.\n";
if ( read(v4, &buf, 5uLL) == -1 )
{
    ERROR_LABEL:
    LOGGING_4058D0(v6, v5);
    LOWORD(v32) = 2;
    fcntl(v4, 7, &v32);
    close(v4);
    return 0;
}
lseek(v4, 0LL, 0);
if ( buf == 0x544E4F4D && BYTE4(buf) == 0x49 )// 0x544E4F4D => "TNOM" 0x49 => "I"
{
    v5 = old;
    v6 = "[%s] File already encrypted.\n";
    goto ERROR_LABEL;
}
```

Figura 5 – Trecho de código para verificar a presença da string "MONTI" através dos últimos 261 bytes do arquivo a ser criptografado.

Com base na análise realizada pela Trend Micro, a nova variante do ransomware utiliza o algoritmo de criptografia **AES-256-CTR** utilizando o "evp\_enc" da biblioteca OpenSSL em vez de Salsa20 (a qual é utilizada pela antiga variante).

Além disso, a amostra emprega vários métodos de criptografia para arquivos, onde ela depende exclusivamente do tamanho do arquivo para seu processo de criptografia.

Quanto as versões anteriores, a nova versão anexa a extensão de arquivo ".monti" aos arquivos criptografados e coloca sua nota de resgate "readme.txt" em todos os diretórios.

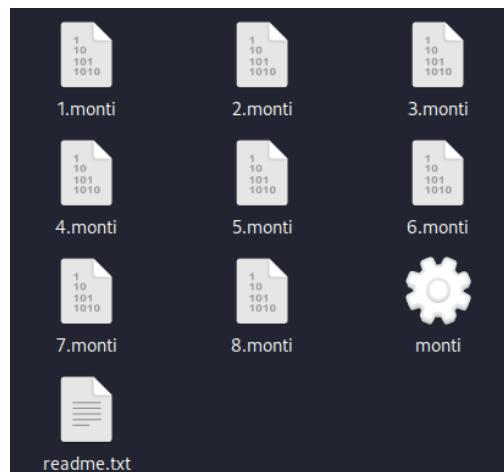


Figura 6 – Extensões anexadas aos arquivos criptografados.

```
*~/Desktop/a/readme.txt - Mousepad
File Edit Search View Document Help
File New Open Save Close Find Replace Cut Copy Paste Undo Redo
1 All of your files are currently encrypted by MONTI strain. If you don't know who we are - just "Google it."
2
3 As you already know, all of your data has been encrypted by our software.
4 It cannot be recovered by any means without contacting our team directly.
5
6 DON'T TRY TO RECOVER your data by yourselves. Any attempt to recover your data (including the usage of the additional
   recovery software) can damage your files. However,
7 if you want to try - we recommend choosing the data of the lowest value.
8
9 DON'T TRY TO IGNORE us. We've downloaded a pack of your internal data and are ready to publish it on our news website if
   you do not respond.
10 So it will be better for both sides if you contact us as soon as possible.
11
12 DON'T TRY TO CONTACT feds or any recovery companies.
13 We have our informants in these structures, so any of your complaints will be immediately directed to us.
14 So if you will hire any recovery company for negotiations or send requests to the police/FBI/investigators, we will
   consider this as a hostile intent and initiate the publication of whole compromised data immediately.
15
16 To prove that we REALLY CAN get your data back - we offer you to decrypt two random files completely free of charge.
17
18 You can contact our team directly for further instructions through our website :
19
20 TOR VERSION :
21 (you should download and install TOR browser first https://torproject.org)
22
23
24
25 Our blog :
26 (also through TOR)
27
28
29
30 YOU SHOULD BE AWAKE!
31 We will speak only with an authorized person. It can be the CEO, top management, etc.
32 In case you are not such a person - DON'T CONTACT US! Your decisions and action can result in serious harm to your company!
33 Inform your supervisors and stay calm!
34
```

Figura 7 – Nota de resgate apresentada após a criptografia.

De acordo com a Trend Micro, as amostras analisadas sugeriram que o ator de ameaça estaria testando a funcionalidade do código de descriptografia, parecendo que esqueceram de remover o código ao implantar a amostra. Vale salientar que o código é atualmente ineficaz, pois requer uma chave privada conhecida apenas pelo autor do malware e não possui conexão com a rotina do malware.

### 3 CONCLUSÃO

---

De acordo com o relatório, os agentes de ameaças por trás do Monti ainda estariam utilizando partes do código-fonte do Conti para desenvolver a nota variante, mas utilizaram justamente mudanças significativas do código, especialmente na criptografia.

Logo, é necessário realizar o acompanhamento deste agente de ameaça visando entender a sua evolução e quais serão os seus objetivos.

## 4 TTPs – MITRE ATT&CK

---

Tática	Técnica	Detalhes
Execução TA0002	Módulos Compartilhados T1129	Função de link em tempo de execução no Linux
Evasão de Defesa TA0005	Arquivos ou informações ofuscadas T1027	Codificações utilizadas e algoritmos de criptografias.
	Desofuscar/Decodificar arquivos ou informações T1140	Descriptografar dados usando AES via extensões x86
	Verificações do sistema T1497.001	Strings anti-VM de referência direcionadas a VMware
Descoberta TA0007	Descoberta de informações do sistema T1082	Obter informações do sistema no Linux
	Descoberta de arquivos e diretórios T1083	Enumerar arquivos no Linux
	Verificações do sistema T1497.001	Strings anti-VM de referência direcionadas a VMwa

Tabela 2 – Tabela MITREE ATT&CK

## 5 IOCs

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 de artefato malicioso/ analisado	
<b>md5:</b>	0ce82210b5678f3f7e28ad0244e56af9
<b>sha1:</b>	a0c9dd3f3e3d0e2cd5d1da06b3aac019cdbe74ef
<b>sha256:</b>	cd8ad31e1d760b4f79eb1c3d5ff15770eb88fa1c576c02775ec659ff872c1bf7
<b>File name:</b>	Montibgjccgddhc2_browsingElf.elf

Indicadores de compromisso de artefato malicioso/ analisado	
<b>md5:</b>	ecdbfee4904dcbae2e20f050b5b69b3
<b>sha1:</b>	f1c0054bc76e8753d4331a881cdf9156dd8b812a
<b>sha256:</b>	44c0774f53ab5071ee2969c5e44df56b13f5047e3fca6108375e6055998b86f2
<b>File name:</b>	ecdbfee4904dcbae2e20f050b5b69b3.exe

Tabela 3 – Indicadores de Compromissos artefatos de host.

## 6 REFERÊNCIAS

---

- Heimdall by ISH Tecnologia
- [Relatório](#) Publicado pela Trend Micro – Ransom MONTI Linux

