BOLETIM DE SEGURANÇA

Novo trojan bancário tem como alvo usuários brasileiros

heimdall
security research
A DIVISION OF ISH

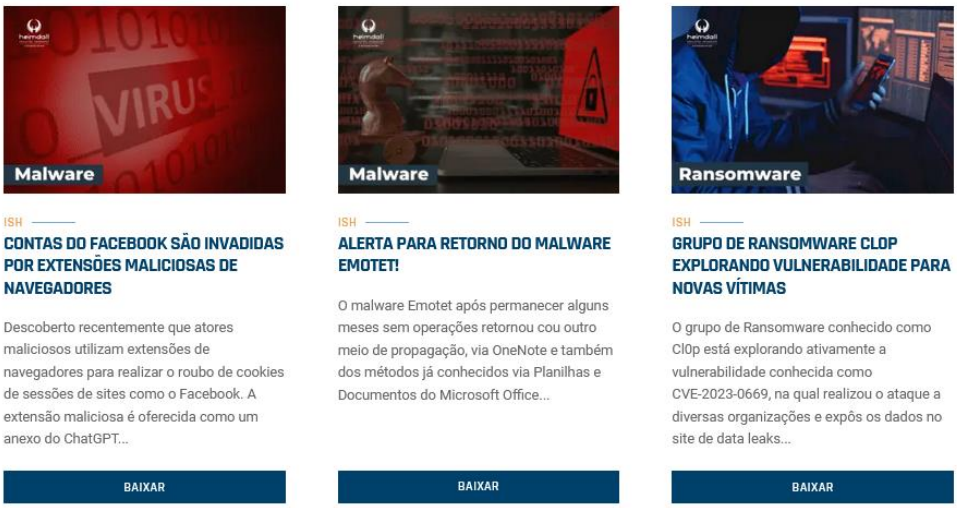
TLP: CLEAR

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

1 Sumário Executivo 6
2 Informações sobre a ameaça 7
3 Conclusão 12
4 Recomendações 13
5 Indicadores de Compromissos 14
6 Referências 16

LISTA DE TABELAS

Tabela 1 – Indicadores de Compromissos de artefatos. 14
Tabela 2 – Indicadores de Compromissos de Rede. 15

LISTA DE FIGURAS

Figura 1 – Fluxo de ataque. 6
Figura 2 – Telemetria do servidor C2. 7
Figura 3 – Arquivo PDF malicioso. 8
Figura 4 – URL incorporada. 8
Figura 5 – Arquivo MSI descompactado. 9
Figura 6 – O "ActionText" no arquivo MSI e a pasta extraída 10
Figura 7 – Carregamento da DLL maliciosa. 10
Figura 8 – Lista de vítimas 11

1 SUMÁRIO EXECUTIVO

Recentemente o FortiGuard Labs descobriu um agente de ameaça que emprega um arquivo PDF malicioso para propagar o Trojan bancário chamado **CHAVECLOAK**. Esse ataque intrincado envolve o download de um arquivo ZIP em PDF e, posteriormente, a utiliza-se de técnicas de carregamento lateral de DLL para executar o malware final. Notavelmente, o CHAVECLOAK foi projetado especificamente para atingir usuários no Brasil, com o objetivo de roubar informações confidenciais ligadas a atividades financeiras.

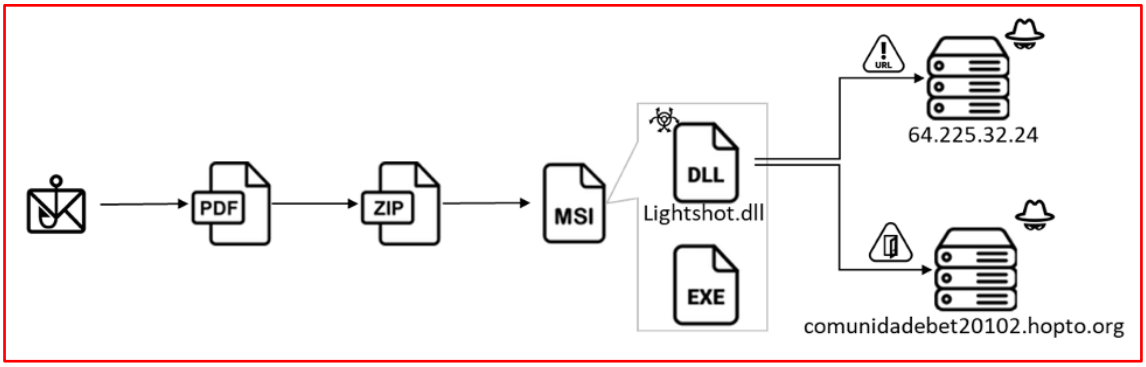


Figura 1 – Fluxo de ataque.

2 INFORMAÇÕES SOBRE A AMEAÇA

No cenário dos atores de ameaças cibernéticas da América do Sul, os trojans bancários empregam uma série de táticas, como phishing, anexos maliciosos e manipulação de navegadores. Alguns exemplos incluem o **Casbaneiro** (Metamorfo/Ponteiro), **Guildma**, **Mekotio** e **Grandoreiro**, que são especializados na obtenção ilícita de credenciais bancárias on-line e dados pessoais, representando uma ameaça significativa para usuários em países como Brasil e México. A telemetria do servidor de *Command and Control* (**C2**) do CHAVECLOAK é mostrada na figura abaixo.

Figura 2 – Telemetria do servidor C2.

O arquivo pdf, contém documentos relativos a um contrato, com instruções escritas em português, atraindo suas vítimas, induzindo-as a clicar em um botão para que possam ler e assinar os documentos em anexo. Entretanto, um link de download malicioso é discretamente incorporado ao objeto de fluxo, que revela a URL decodificada. Esta URL é processada por meio do serviço gratuito de encurtamento de link "Goo.su", levando o redirecionamento ao ***hxxps://webattach.mail.yandex.net/message_part_real/NotaFiscalEsdeletronicasufactrub66667kujhdfdjrWEWGFG09t5H6854JHGJUUR[.]zip*** para baixar o arquivo ZIP. Após a descompactação, o arquivo gera o arquivo MSI "*NotafiscalGFGJKHKHGUURTURTF345.msi*".

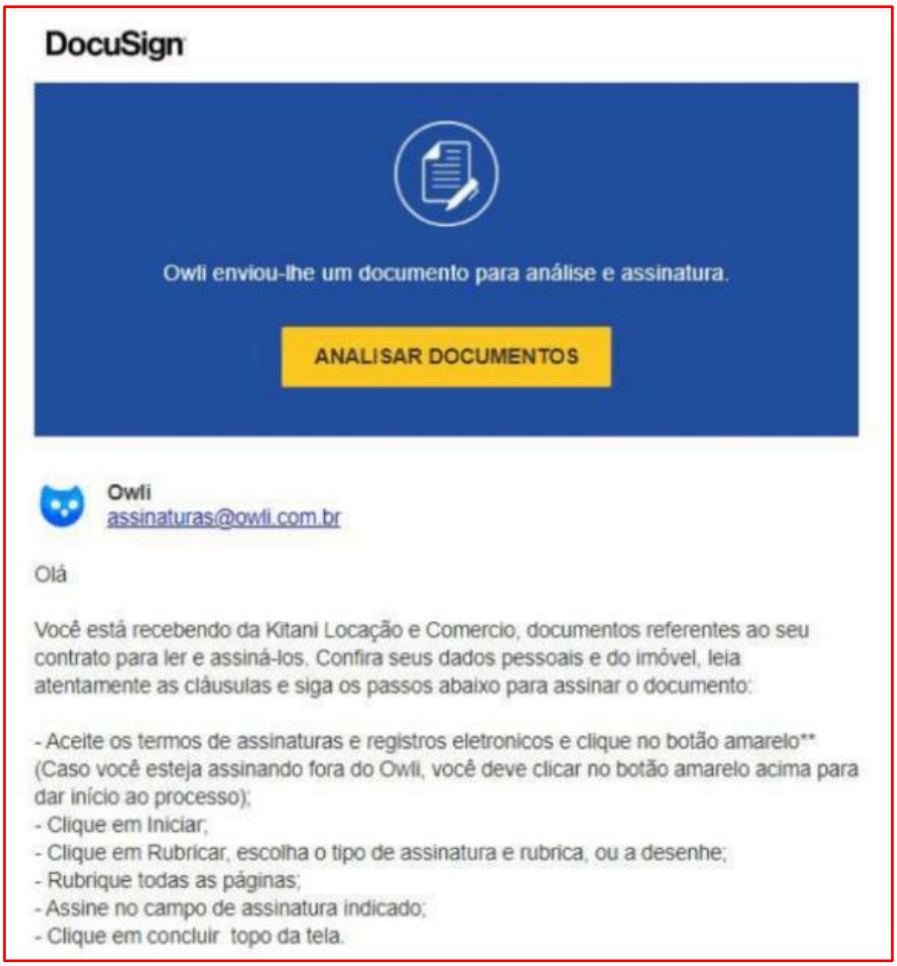


Figura 3 – Arquivo PDF malicioso.

Figura 4 – URL incorporada.

Após a descompactação do instalador MSI, podemos observar vários arquivos TXT relacionados a configurações de diferentes idiomas, um arquivo de

execução legítimo e uma DLL maliciosa chamada “Lightshot.dll”. Nota-se que, a data de modificação deste arquivo DLL é mais recente do que a de todos os outros arquivos do instalador, enfatizando ainda mais sua natureza incomum.

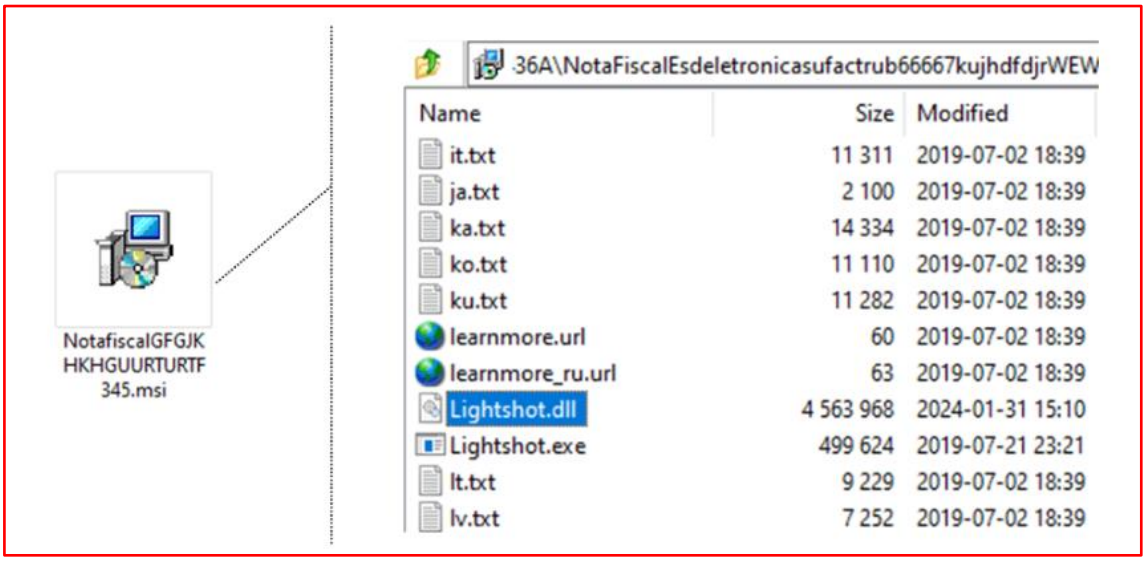


Figura 5 – Arquivo MSI descompactado.

Na análise realizada no instalador MSI foi revelada toda a sua configuração, que está escrita em português. Ele executa o arquivo “**Lightshot.exe**”, extraindo e depositando os arquivos em “**%AppData%\Skillbrains\lightshot\5.5.0.7**”. O arquivo “Lightshot.exe” então implanta técnicas de sideload de DLL para ativar a execução da DLL maliciosa, “Lightshot.dll”. Essa técnica permite que o executável legítimo carregue e execute o código malicioso discretamente, facilitando atividades não autorizadas, como roubo de dados. As ações conduzidas por “Lightshot.dll” envolvem operações secretas e prejudiciais, incluindo a aquisição não autorizada de informações confidenciais. O carregamento lateral de DLL representa uma ameaça significativa à segurança, permitindo que o malware explore processos legítimos para fins nefastos sem detecção.

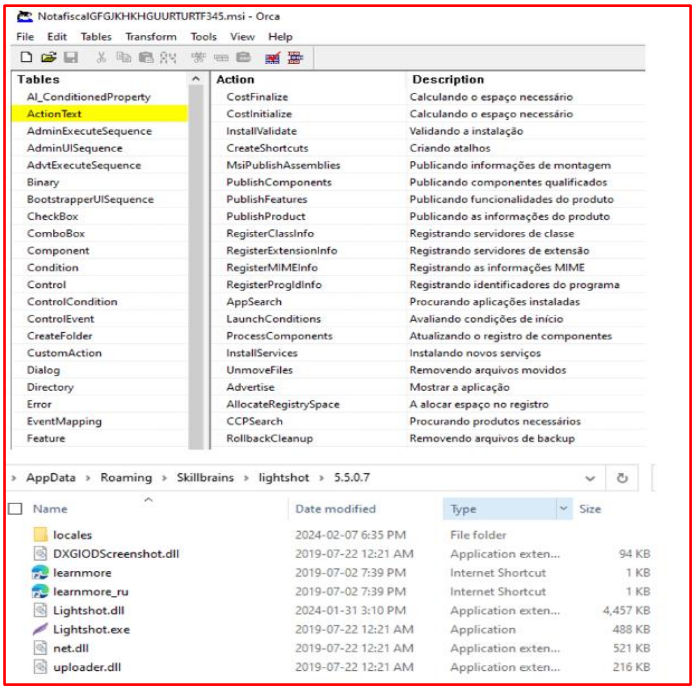


Figura 6 – O "ActionText" no arquivo MSI e a pasta extraída

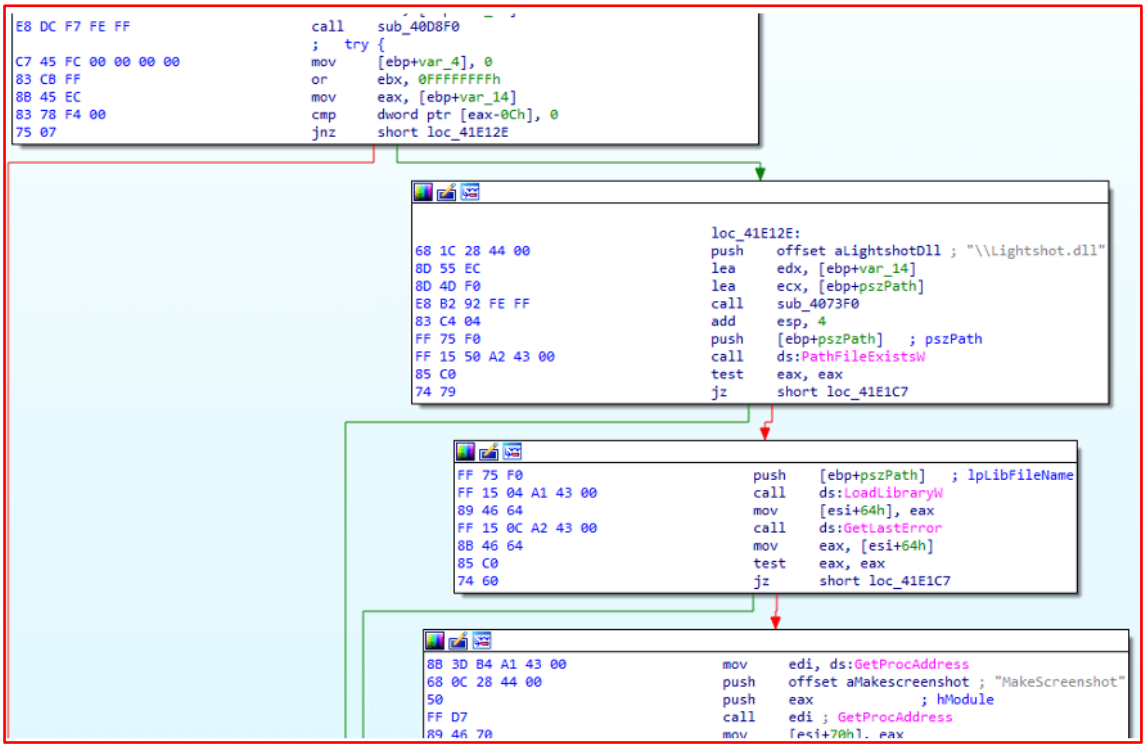


Figura 7 – Carregamento da DLL maliciosa.

No início, o processo invoca "**GetVolumeInformationW**" para coletar detalhes sobre o sistema de arquivos e o volume associado relacionado ao diretório raiz especificado, utilizando o valor HEX obtido para gerar um arquivo de log em "**%AppData%[HEX ID]lIG.log**". Em seguida, ele adiciona um valor de registro chamado "**Lightshot**" a

“**HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**”, garantindo a execução automática do programa “Lightshot.exe” no login do usuário. Assim que o registro e a persistência forem concluídos, ele envia uma solicitação HTTP para *hxxp://64[.]225[.]32[.]24/shn/inspecionando.php*. Se a geoverificação confirmar que a vítima está no Brasil, ela registra os dados no servidor, acessível através do caminho “**clients.php**”.

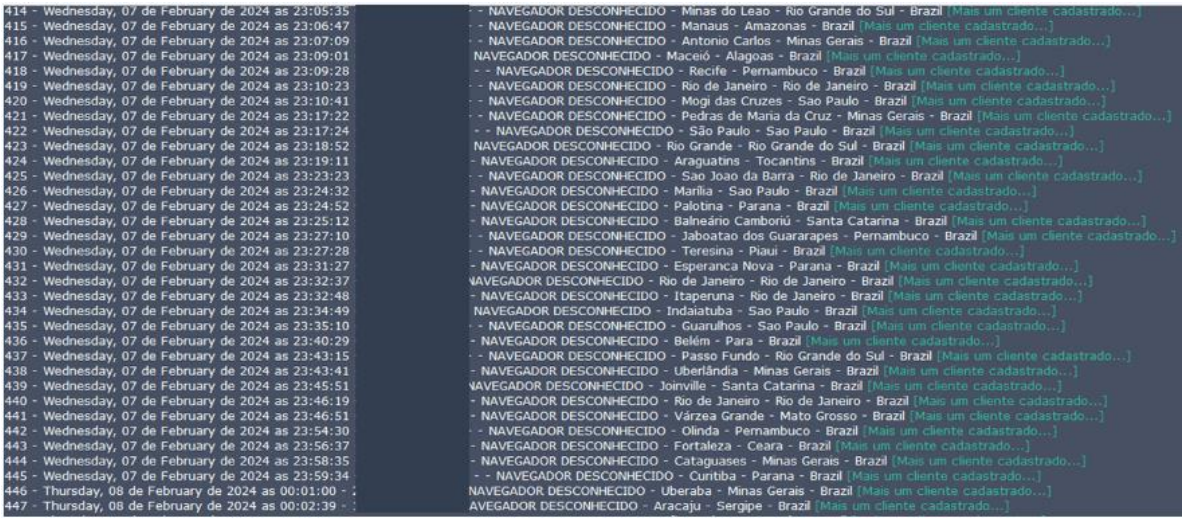


Figura 8 – Lista de vítimas

3 CONCLUSÃO

O surgimento do **CHAVECLOAK** destaca o cenário em constante evolução das ameaças cibernéticas voltadas para o setor financeiro, que tem como foco específico usuários brasileiros. Esse Trojan emprega técnicas avançadas, como PDFs maliciosos, downloads de arquivos ZIP, sideload de DLL e pop-ups enganosos. Ele se une a um grupo de trojans bancários proeminentes, cujo alvo principal é a América do Sul. O malware é configurado para língua portuguesa, indicando uma abordagem estratégica para a região, e monitora ativamente as interações das vítimas com portais financeiros. Sua sofisticação exemplifica os desafios enfrentados pelos trojans bancários contemporâneos, exigindo vigilância constante e medidas proativas de segurança cibernética para proteger contra as ameaças em constante evolução no cenário financeiro sul-americano

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 Regular de Software

- Mantenha todos os sistemas, aplicativos e dispositivos atualizados com as últimas correções de segurança. Isso ajuda a fechar vulnerabilidades conhecidas.

Firewalls e Filtros de Tráfego

- Configure firewalls e filtros de tráfego para bloquear conexões não autorizadas e monitorar o tráfego de rede em busca de atividades suspeitas.

Controle de Acesso

- Implemente políticas rigorosas de controle de acesso. Restrinja o acesso apenas a usuários autorizados e limite privilégios administrativos.

Treinamento de Conscientização em Segurança

- Eduque os funcionários sobre práticas seguras de navegação na web, identificação de phishing e uso seguro de dispositivos.

Segurança de Email

- Implemente filtros antispam e antiphishing para evitar que emails maliciosos cheguem às caixas de entrada dos usuários.

Backup Regular de Dados

- Faça backups frequentes dos dados críticos e verifique sua integridade. Isso ajuda a recuperar informações em caso de infecção.

Segurança de Endpoints

- Proteja computadores e dispositivos finais com soluções antivírus/antimalware e ferramentas de detecção de intrusões.

Restrição de Execução de Arquivos Suspeitos

- Bloqueie a execução de arquivos desconhecidos ou suspeitos por meio de políticas de segurança.

Avaliações de Segurança

- Realize testes regulares de penetração e avaliações de segurança para identificar e corrigir possíveis vulnerabilidades antes que sejam exploradas.

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:	13085c8d534b6b32564fe6c366ee1bea
sha1:	8f7db4b0bfe53475c63f4e8f31b89e4c67231616
sha256:	51512659f639e2b6e492bba8f956689ac08f792057753705bf4b9273472c72c4
File name:	51512659f639e2b6e492bba8f956689ac08f792057753705bf4b9273472c72c4

Indicadores de compromisso do artefato	
md5:	ffd9942fb2b9e4d5d70ad6c0aa5033b4
sha1:	763205980a62c43e602983c3ba5a493604280958
sha256:	48c9423591ec345fc70f31ba46755b5d225d78049cfb6433a3cb86b4ebb5a028
File name:	NotaFiscalEsdeletronicasufactrub66667kujhdfdjrWEWGFG09t5H6854JHGJUUR.zip

Indicadores de compromisso do artefato	
md5:	c371047910a709f65fd85d10cde0ca4f
sha1:	8992089394435b280c4e36aee7de673a5adf5af9
sha256:	4ab3024e7660892ce6e8ba2c6366193752f9c0b26beedca05c57dcb684703006
File name:	NotafiscalGFGJKHKHGUURTURTF345.msi

Indicadores de compromisso do artefato	
md5:	fea6fc878029babdca3a1579be0ae771
sha1:	6f3e607d54e98d884c3d280e73abf5be85fd6168
sha256:	131d2aa44782c8100c563cd5febf49fcb4d26952d7e6e2ef22f805664686ffff
File name:	Lightshot.dll

Indicadores de compromisso do artefato	
md5:	c5d3742910f8d35b510a0ad133654add
sha1:	556b298fc3728ca599b4231d1311f2e49f3e00d1
sha256:	8b39baec4b955e8dfa585d54263fd84fea41a46554621ee46b769a706f6f965c
File name:	Fact079858vbfgr.rar

Indicadores de compromisso do artefato	
md5:	ef5f927bb98df4df685ef472b162ae3f
sha1:	827e969a7cdd2b77dc91287cbd4def46cf1ae2f0
sha256:	634542fdd6581dd68b88b994bc2291bf41c60375b21620225a927de35b5620f9
File name:	Fact079858vbfgr.exe

Tabela 1 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	hxxps://webattach.mail.yandex.net/message_part_real/NotaFiscalEsdeletronicasufactrub66667kujhdfdjrWEWGFG09t5H6854JHGJUUR[.]zip, hxxps://goo[.]su/FTD9owO
Domínio	mariashow[.]ddns[.]net, comunidadebet20102[.]hopto[.]org
IP	64[.]225[.]32[.]24

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.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Fortinet**
- **Thehackernews**

heimdall
security research
A DIVISION OF ISH