BOLETIM DE SEGURANÇA

Nova campanha de malware tem como alvo usuários de Windows

heimdall
security research
A DIVISION OF ISH

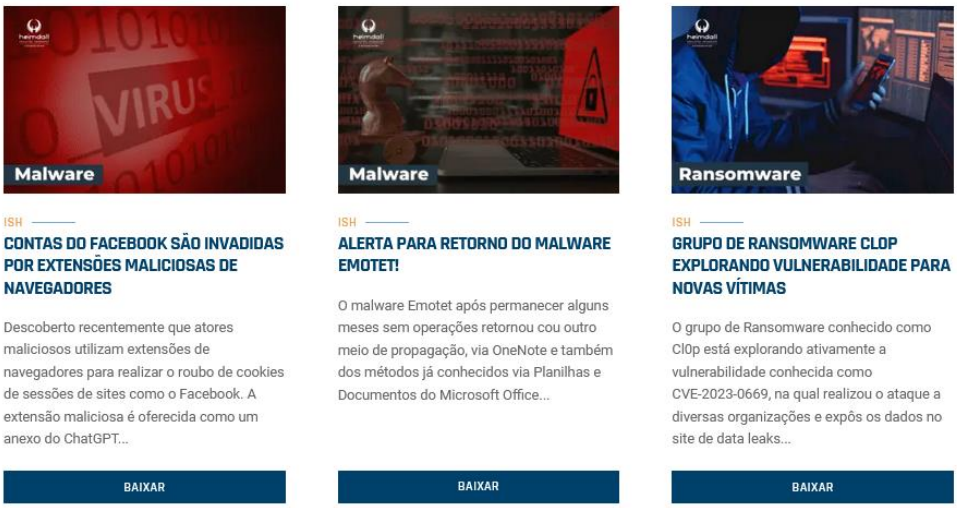
TLP: CLEAR

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

A equipe de *Threat Research da Securonix* (**STR**) identificou uma campanha de ataque complexidade, provavelmente ligada ao grupo *Kimsuky* da Coreia do Norte. A campanha, denominada **DEEP#GOSU**, utiliza novos e antigos códigos/stagers. Embora o Kimsuky já tenha atacado vítimas sul-coreanas, a nova estratégia é notável por seu uso de scripts *PowerShell* e *VBScript* para infecções discretas. Esses scripts permitem aos invasores monitorar atividades como a área de transferência e as teclas digitadas. A campanha **DEEP#GOSU** emprega um trojan para controlar hosts infectados, com scripts de fundo para persistência e monitoramento. A comunicação é feita através de serviços legítimos como **Dropbox** e **Google Docs**, permitindo que o malware se misture ao tráfego de rede, permitindo atualizações dinâmicas do malware. A entrada provável do malware é através de um anexo de e-mail malicioso disfarçado como um arquivo .lnk.

2 DETALHES DA CAMPANHA DE ATAQUE

A utilização de arquivos .lnk como ferramenta por agentes maliciosos não é algo inédito. Contudo, a abordagem do DEEP#GOSU para a execução do código diverge significativamente do que usualmente é observado. Inicialmente, a extensão do comando é notavelmente vasta, indicando que o PowerShell em questão foi desenvolvido para realizar múltiplas funções de alta complexidade. Aém disso, o arquivo de atalho, com aproximadamente 2,2 MB, sugere que há mais conteúdo nele do que aparenta inicialmente.

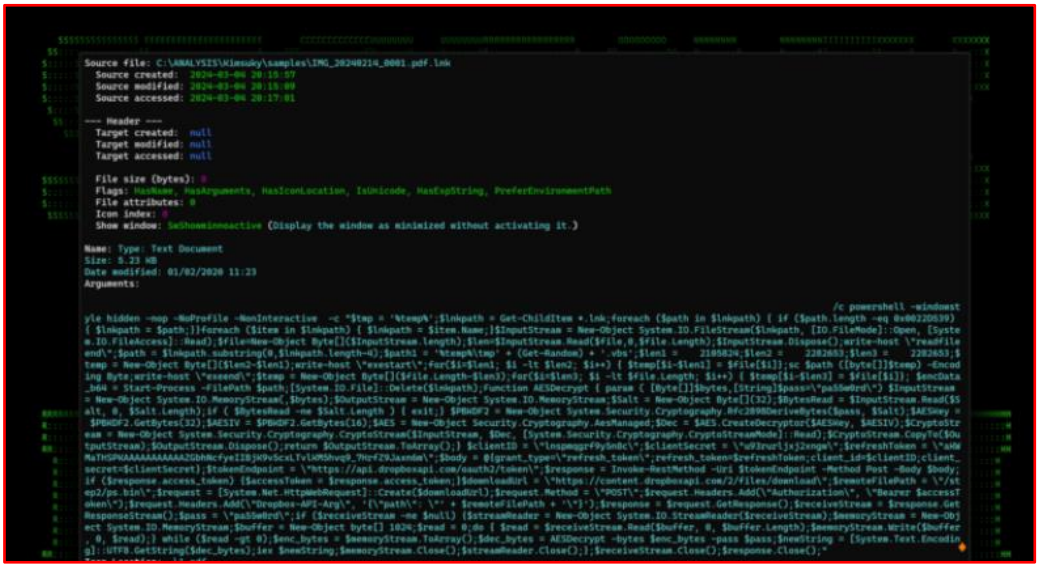


Figura 1 – Execução de linha de comando.

O arquivo de atalho contém um script PowerShell que é capaz de extrair e executar códigos maliciosos baixados da internet, além de limpar seus próprios rastros. Ele usa criptografia e serviços em nuvem para recuperar a carga útil, o que sugere um alto grau de sofisticação. Esse arquivo contém mais de 2 MB devido à presença de um PDF incorporado, que é adicionado após uma longa sequência de caracteres “A”. Isso pode ser uma estratégia para aumentar o tamanho do arquivo e evitar detecções de antivírus. Ao visualizá-lo com um editor hexadecimal, é possível ver o final do código de atalho, o início da sequência de caracteres “A” e, após o término dos “A”, o início de um cabeçalho PDF.

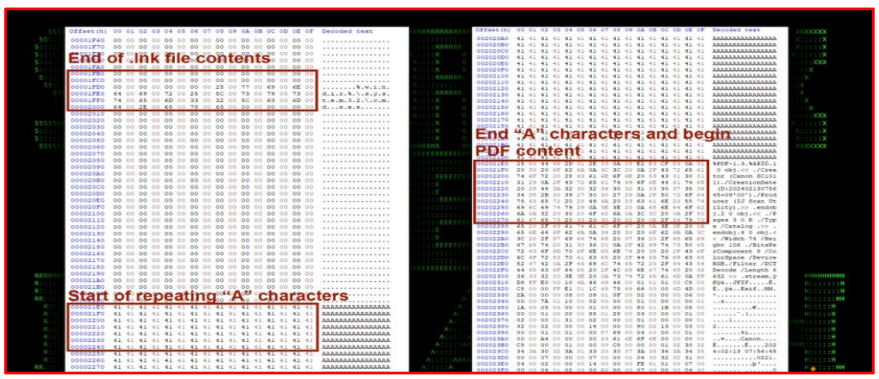
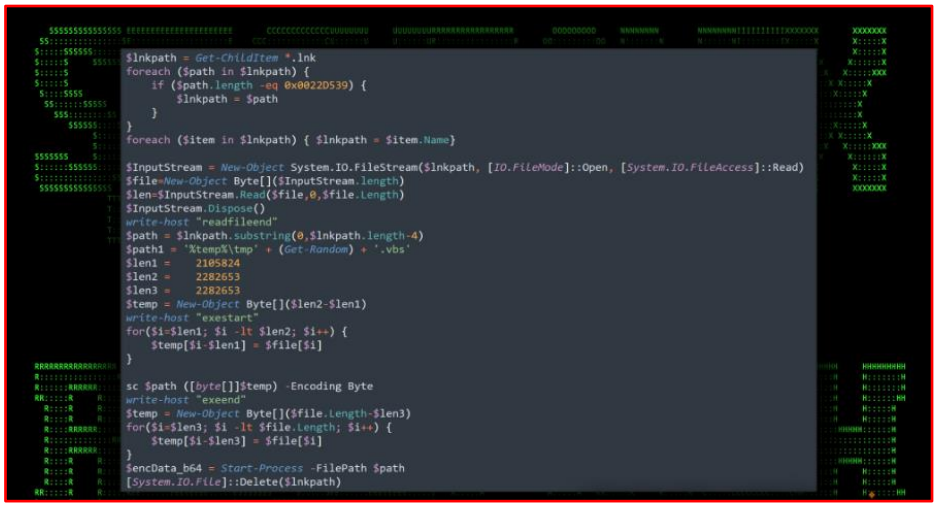


Figura 2 – Arquivo PDF incorporado destacado.

O arquivo de atalho em questão tem um PDF anexado a ele. Este arquivo de atalho contém um código PowerShell que realiza várias operações. O código PowerShell mencionado foi extraído do arquivo de atalho e foi simplificado para melhor compreensão.

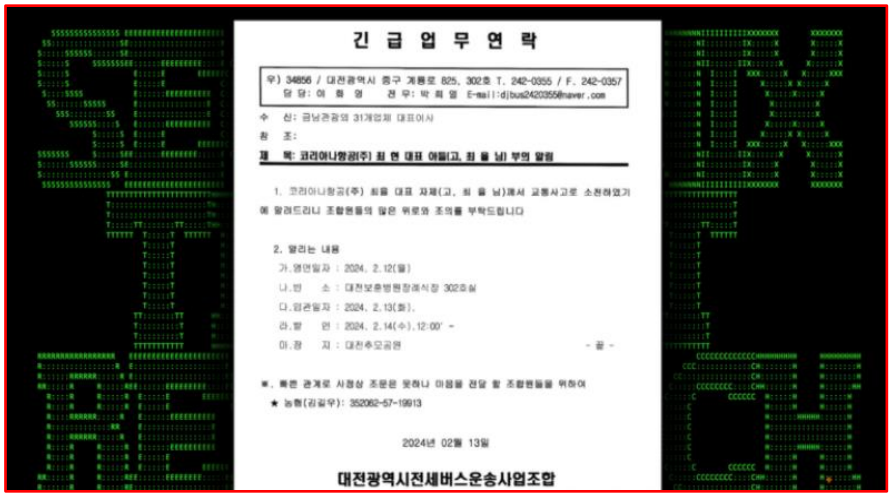


```powershell
$lnkpath = Get-ChildItem *.lnk
foreach ($path in $lnkpath) {
    if ($path.length -eq 0x0022D539) {
        $lnkpath = $path
    }
}
foreach ($item in $lnkpath) { $lnkpath = $item.Name}

$InputStream = New-Object System.IO.FileStream($lnkpath, [IO.FileMode]::Open, [System.IO.FileAccess]::Read)
$file=New-Object Byte[]($InputStream.length)
$len=$InputStream.Read($file,0,$file.Length)
$InputStream.Dispose()
write-host "readfileend"
$path = $lnkpath.substring(0,$lnkpath.length-4)
$path1 = '%temp%\tmp' + (Get-Random) + '.vbs'
$len1 =    2105824
$len2 =    2282653
$len3 =    2282653
$temp = New-Object Byte[]($len2-$len1)
write-host "exestart"
for($i=$len1; $i -lt $len2; $i++) {
    $temp[$i-$len1] = $file[$i]
}

sc $path ([byte[]]$temp) -Encoding Byte
write-host "exeend"
$temp = New-Object Byte[]($file.Length-$len3)
for($i=$len3; $i -lt $file.Length; $i++) {
    $temp[$i-$len3] = $file[$i]
}
$encData_b64 = Start-Process -FilePath $path
[System.IO.File]::Delete($lnkpath)
```

Figura 3 – Extração do arquivo pdf.

O script realiza a extração do conteúdo PDF de um arquivo *.lnk*. Ele faz isso com base em posições de bytes específicas, que estão entre os valores de byte 2105824 e 2282653 (**$len1** a **$len2**). Durante a execução, o script registra o progresso de cada operação, como "**readfileend**", "**exestart**" e "**exeend**". O alias "sc" é empregado para criar um novo objeto que armazena o arquivo PDF. Posteriormente, o conteúdo extraído é salvo em uma nova variável **$path** e é executado usando o comando PowerShell Start-Process. O conteúdo do PDF é então aberto no visualizador de PDF padrão do sistema, sob o nome "IMG_20240214_0001.pdf". Por fim, todos os arquivos são excluídos.

A astúcia dessa estratégia reside no fato de que, tecnicamente, não existe nenhum arquivo PDF no arquivo zip inicial que é enviado para a vítima. Quando a vítima clica no arquivo de atalho disfarçado de PDF, um arquivo PDF é imediatamente exibido, dissipando assim quaisquer suspeitas de que algo inusitado possa ter ocorrido. O documento PDF está em coreano e aparenta ser um anúncio sobre o filho do CEO da Korean Airlines, Choi Hyun (o falecido Choi Yul), informando que o filho morreu em um acidente de carro. O documento também contém detalhes e datas do funeral.



긴 급 업 무 연 락

우) 34856 / 대전광역시 중구 계룡로 825, 302호 T. 242-0355 / F. 242-0357
담 당: 이 희 영 전 무: 박 희 영 E-mail:djbus2420356@naver.com

수 신: 금남관광의 31개업체 대표이사

참 조:

제 목: 코리아니항공(주) 최 연 대표 아들(고. 최 율 님) 부의 알림

1. 코리아니항공(주) 최율 대표 자제(고. 최 율 님)께서 교통사고로 소천하였기에 알려드리니 조합원들의 많은 위로와 조의를 부탁드립니다.

2. 알리는 내용

가.영연일자 : 2024. 2.12(월)

나.빈 소 : 대전보훈병원장례식장 302호실

다.입관일자 : 2024. 2.13(화).

라.발 인 : 2024. 2.14(수).12:00' ~

마.장 지 : 대전추모공원 - 끝 -

※. 빠른 관계로 시경상 조문은 못하니 이점을 양달 할 조합원들을 위하여

★ 농협(김길우): 352062-57-19913

2024년 02월 13일

대전광역시전세버스운송사업조합

Figura 4 – Documento isca.

Além de abrir e rodar o documento PDF, o arquivo de atalho também dispara a próxima fase da carga maliciosa do malware a partir de um URL do Dropbox (*hxxps://content.dropboxapi[.]com/2/files/download/step2/ps.bin*). Contrariando o que o nome sugere, o arquivo **ps.bin** é, na realidade, um outro script do PowerShell que será discutido posteriormente. Como o Dropbox exige autenticação, todos os parâmetros necessários são integrados ao script PowerShell original do atalho. Com o código do PowerShell já limpo, a seção do script que é responsável por baixar e rodar a próxima fase da carga maliciosa (**$newString**) é ressaltada.

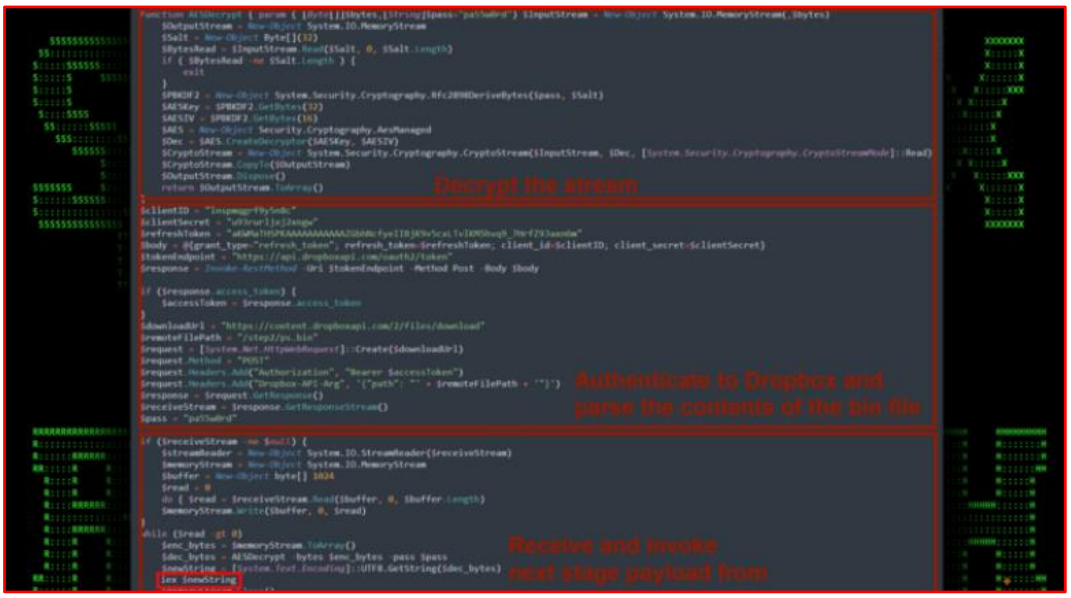


Figura 5 – Carga útil para o estágio do Dropbox.

O arquivo de atalho inicial foi adquirido e acionou um carregamento remoto do Dropbox denominado **ps3.bin**. O script do PowerShell contido no arquivo .bin estabelece uma função (**Load**) que realiza diversas ações, incluindo baixar, descompactar, carregar e executar dinamicamente o código assembly .NET de um URL do Dropbox distinto.

Estabelece uma função de descompressão auxiliar (GzExtract):

- Essa função interna aceita uma matriz de bytes na forma de dados GZIP compactados como entrada.
- Descompacta esses dados e devolve a matriz de bytes resultante.

Carregando assemblies .NET dinamicamente:

- O script carrega dinamicamente assemblies associados a System.Drawing , System.Windows.Forms e PresentationCore.
- Isso possibilita que o script utilize recursos avançados de interface gráfica que foram utilizados anteriormente para recursos como capturas de tela ou gravação de tela pelo malware Dark Pink, entre outros.

Autenticação com o Dropbox e download da carga remota do próximo estágio:

- De maneira similar ao script do PowerShell do arquivo de atalho, ele autentica no Dropbox novamente utilizando um token de atualização, ID do cliente e segredo do cliente para obter um token de acesso.
- Um arquivo denominado r_enc.bin é baixado do Dropbox (estágio 3).
- Após o download do arquivo, ele tenta descompactar a carga utilizando a função GzExtract definida anteriormente.
- O script sugere que essa carga útil é um assembly .NET em formato binário, embora esteja compactado para evitar detecção.

Carregando e executando dinamicamente o assembly .NET:

- Ele carrega o assembly .NET descompactado na memória sem gravá-lo no disco, o que pode auxiliar na redução de detecções de AV.
- Ele percorre os tipos e métodos dentro do assembly carregado para localizar e invocar um método específico (makeProbe1). A invocação é comentada, mas sugere que o método seria executado com um parâmetro codificado, que é parcialmente exibido e depois truncado.
- Esse carregamento e execução dinâmicos permitem que o malware execute praticamente qualquer ação suportada pela estrutura .NET, com base no código do assembly baixado.

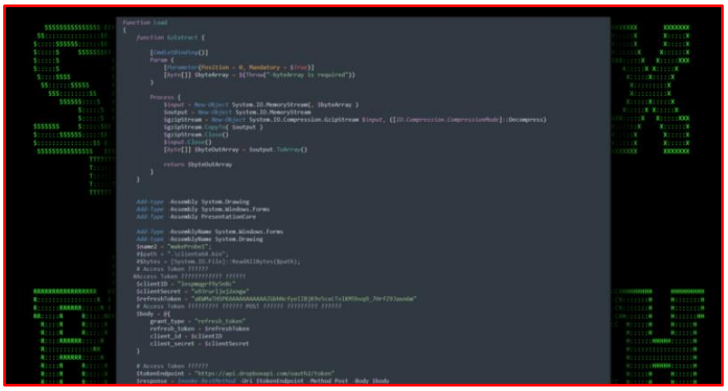


Figura 6 – Script powershell ps.bin.

O script também chama um método em uma instância de objeto utilizando reflexão no PowerShell. O parâmetro para essa chamada parece ser uma string codificada em **Base64**. A string pode ser observada na figura subsequente.

Figura 7 – Script powershell ps.bin chamando carga útil.

O malware empregado no DEEP#GOSU constitui uma ameaça multietapas e sofisticada, projetada para operar de maneira discreta em sistemas Windows, com ênfase especial no monitoramento de rede. A execução do malware dependia do PowerShell e do VBScript, com um nível surpreendentemente baixo de ofuscação. Cada etapa era criptografada com AES, uma senha comum e IV, o que provavelmente reduziria as detecções por varreduras simples de rede ou arquivo. As funcionalidades do malware incluíam registro de teclas, monitoramento da área de transferência, execução dinâmica de carga útil, exfiltração de dados e persistência. Para garantir acesso remoto completo, ele utilizava software RAT, tarefas programadas e scripts PowerShell autoexecutáveis através de jobs.

3 CONCLUSÃO

A proteção contra ameaças cibernéticas, como o DEEP#GOSU, é crucial para as organizações. Ela preserva a confiança do cliente, a imagem da empresa e atende aos requisitos regulatórios. As organizações devem priorizar a segurança cibernética e adotar estratégias eficazes para mitigar riscos. A implementação de controles de segurança, como os CIS Controls, pode melhorar a postura de segurança e reduzir as ameaças cibernéticas.

4 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Defense Evasion	T1027 T1027.010 T1070.004 T1140	Arquivos ou informações ofuscados Arquivos ou informações ofuscados: Ofuscação de comando Remoção de indicador: Exclusão de arquivo Desofuscar/decodificar arquivos ou informações
Discovery	T1057 T1082 T1083	Descoberta de processos Descoberta de informações do sistema Descoberta de arquivos e diretórios
Execution	T1059 T1059.001 T1059.005 T1204.001	Intérprete de comandos e scripts Intérprete de comandos e scripts: PowerShell Intérprete de comandos e scripts: Visual Basic Execução do usuário: link malicioso
Exfiltration	T1567.002	Exfiltração por serviço Web: exfiltração para armazenamento em nuvem
Persistence	T1053	Tarefa/Trabalho Agendado
Command and Control	T1102 T1132.001 T1219 T1573	Web Service Codificação de dados: Codificação padrão Software de acesso remoto Canal criptografado
Collection	T1115 T1056.001	Dados da área de transferência Captura de entrada: Keylogging

Tabela 1 – Tabela MITRE ATT&CK.

5 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:

Antivírus

- Mantenha atualizado o sistema de antivírus ou firewall. As atualizações de software e de aplicativos contêm funcionalidades de segurança vitais para ajudar a proteger os dispositivos da ação de cibercriminosos.

Senhas seguras

- Evite repetir senhas em mais de uma conta e não crie senhas com base em informações pessoais. Troque as suas senhas periodicamente.

Ativar a verificação em duas etapas (MFA)

- Proteja as contas mais importantes (como e-mail, banco, redes sociais e compras online) garantindo que a verificação em duas etapas esteja ativa em cada uma delas.

Acessar sites seguros

- Verifique se o site que você está acessando possui o certificado de segurança no início da URL.

Cuidado com dados pessoais

- Esteja atento a ligações por telefone pedindo dados pessoais, principalmente de serviços que você não solicitou.

6 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:	1e66ac680d0edfe18d97b89e46c7e82e
sha1:	10c3dc54cb7417a386cc6fb52ec60c85af1fb0bc
sha256:	f262588c48d2902992ffd275d2be6362fe7f02e2f00a44ab8c75ac1a2827c6e9
File name:	IMG_20240214_0001.pdf.lnk

Indicadores de compromisso do artefato	
md5:	e269a6500fbdc750afeb18d2d05f8eea
sha1:	ea4066919291edbf3bc33a880f86d6e9dc633ddd
sha256:	46a5d54c264152ce915792af31c75824a558af7d7340d78b34e146d8c6249e79
File name:	트레이딩 스파르타코스 강의안-100불남(2차).zip

Indicadores de compromisso do artefato	
md5:	eb08ab3854168c834ab154facfe695a3
sha1:	38bf08bcb887be7d71adbf27743ac5817da46fbe
sha256:	1b75f70c226c9ada8e79c3fdd987277b0199928800c51e5a1e55ff01246701db
File name:	트레이딩_스파르타코스_강의안_100불남_2차.pdf.lnk

Indicadores de compromisso do artefato	
md5:	6786bdddb0318e17d56cf08dfc5e91b9
sha1:	3ff167cb9658c9a8a31ec437657a6ff6105eb91a
sha256:	60666cacdd6806ed05771f32eaa719e3efd2f4db55f28a447d383c3eac1dc72e
File name:	dl.ps

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	https://content.dropboxapi.com/2/files/download/step2/ps.bin https://content.dropboxapi.com/2/files/download/step2/r_enc.bin https://content.dropboxapi.com/2/files/download/step2/info_sc.txt https://content.dropboxapi.com/2/files/download/step2/info_ps.bin https://content.dropboxapi.com/2/files/download/step2/ad_ps.bin https://content.dropboxapi.com/2/files/download/step2/info_sc.txt

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.

7 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Securonix**
- **Thehackernews**

heimdall
security research
A DIVISION OF ISH