BOLETIM DE SEGURANÇA

Repositórios Docker Hub detectados disseminando malware e páginas de phishing

heimdall
security research
A DIVISION OF ISH

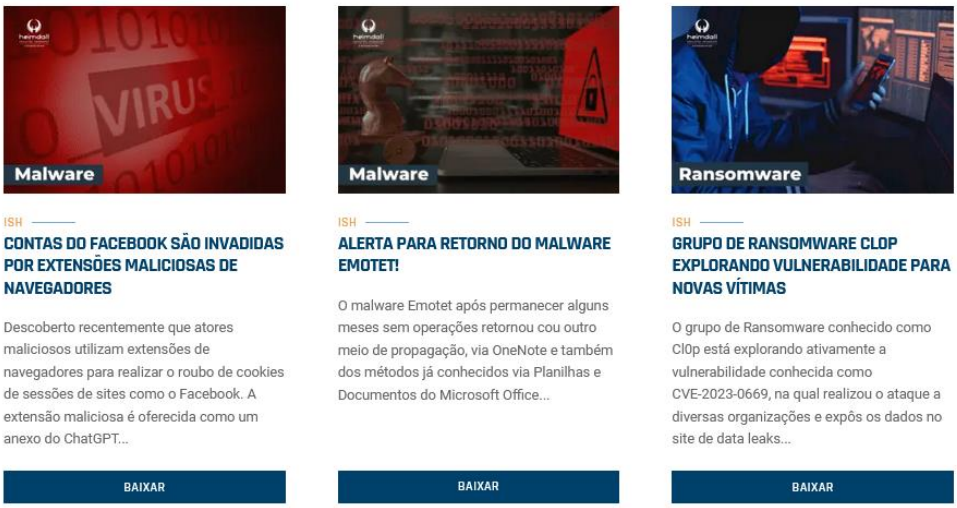
TLP: CLEAR

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 JFrog e Docker realizaram um trabalho em conjunto para mitigar e resolver problemas decorrentes da recente exposição de repositórios no Docker Hub que foram utilizados para disseminar malware e esquemas de phishing. A colaboração visa garantir a segurança e a integridade dos usuários da plataforma, implementando medidas de segurança reforçadas e procedimentos de limpeza eficazes.

2 INFORMAÇÃO SOBRE A CAMPANHA

Foram descobertas de três grandes campanhas de malware no Docker Hub, que inseriram milhões de repositórios "sem imagem" com metadados nocivos. Estes repositórios, desprovidos de imagens de contêiner, não são executáveis, mas contêm metadados prejudiciais. O Docker Hub é uma plataforma essencial para desenvolvedores, oferecendo funcionalidades para desenvolvimento, colaboração e distribuição de imagens Docker, com mais de 15 milhões de repositórios hospedados. Contudo, indica que aproximadamente 20% desses repositórios (cerca de três milhões) continham conteúdo malicioso, variando de spam a malware e sites de phishing, muitos dos quais foram carregados por contas automatizadas.

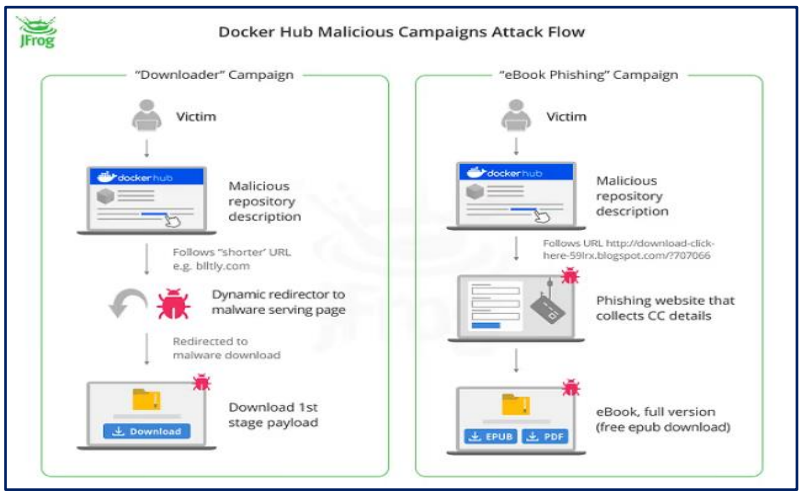


Figura 1 – Fluxo de ataque de campanhas maliciosas do Docker Hub.

Apesar dos esforços dos administradores do Docker Hub em moderar os repositórios submetidos, e da remoção dos repositórios maliciosos identificados, a realidade é que prevenir completamente o carregamento de conteúdo nocivo representa um enorme desafio.

O Docker Hub, é um serviço de registro em nuvem do Docker, que serve como plataforma para armazenar e compartilhar imagens. O elemento chave é o repositório, que armazena descrições e metadados dos contêineres. Além de preservar uma série de imagens Docker, acessíveis por um identificador constante, o Docker Hub se destaca pelos seus recursos comunitários, um dos seus principais diferenciais.

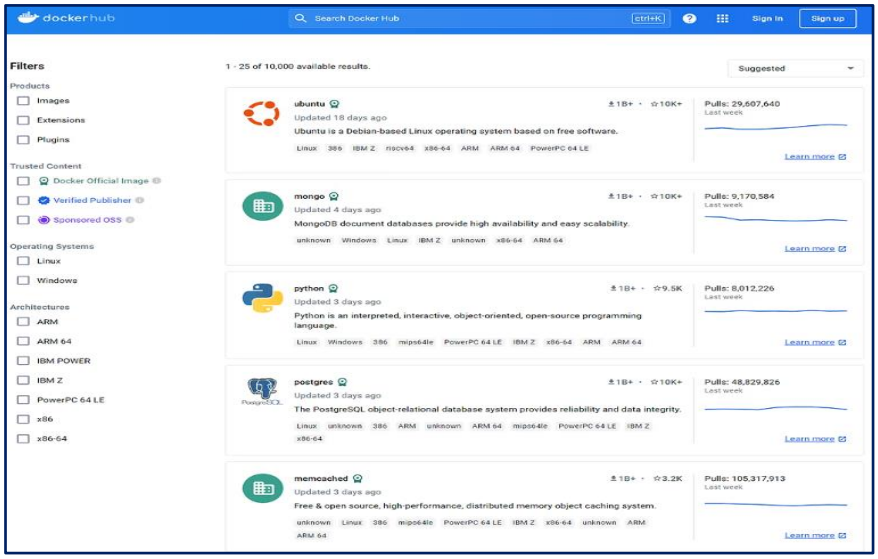


Figura 2 – Biblioteca de repositório do Docker Hub.

A investigação começou com a detecção de irregularidades nos padrões de publicação dos repositórios no Docker Hub. Foi realizada a extração de todos os repositórios "sem imagem" do Docker Hub lançados nos últimos cinco anos. Em seguida, esses repositórios foram organizados conforme a data em que foram criados e a informação foi representada visualmente através de um gráfico.

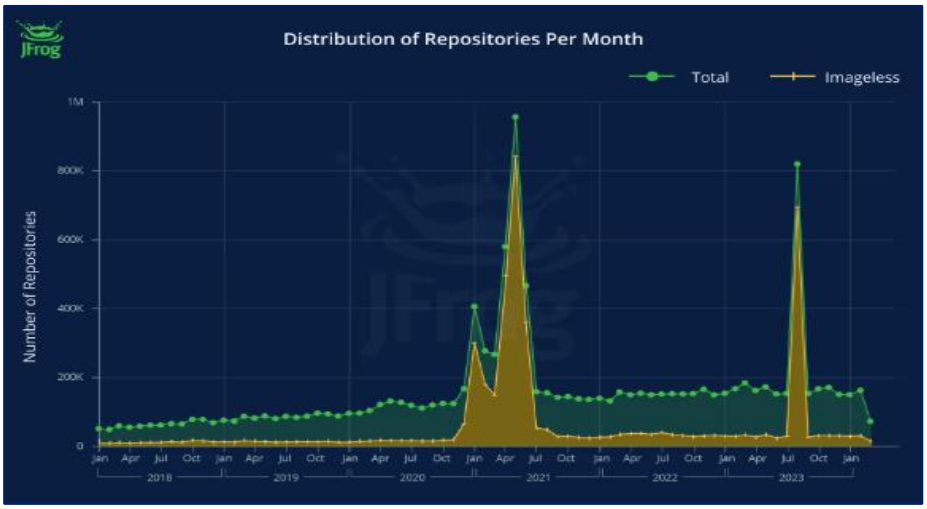


Figura 3 – Gráfico mensal de repositórios criados.

A análise da atividade no Docker Hub revela uma tendência geralmente constante, com exceção de elevações notáveis nos anos de 2021 e 2023. Observando mais de perto, a atividade diária apresenta uma regularidade que reflete o ciclo semanal de trabalho, com um volume maior de criação de repositórios durante os dias da semana e uma diminuição nos finais de semana.

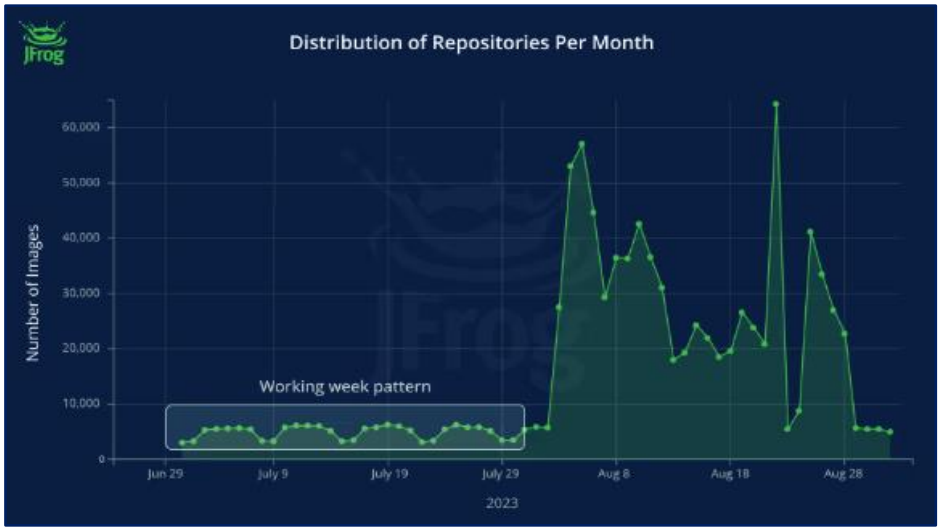


Figura 4 – Anomalia ampliada de 2023.

Os repositórios gerados em dias atípicos revelaram uma quantidade significativa de repositórios que fogem ao padrão esperado. A irregularidade mais evidente é a ausência de imagens de contêineres, apresentando somente documentação, o que inviabiliza a utilização do repositório para extração e execução padrão de uma imagem Docker.

Figura 5 – Exemplo de um repositório malicioso.

Como ilustrado no exemplo acima, o repositório em questão inclui links em sua descrição que encaminham os usuários para um site fraudulento **https[://]www[.******medz*****.]com**. Este site finge oferecer a venda de medicamentos controlados, porém, na realidade, tem o propósito de capturar informações de cartões de crédito dos visitantes.

Apesar da diversidade entre os repositórios anômalos e de serem originados de múltiplos usuários, a maioria apresentava padrões similares. Com isso, foi possível desenvolver uma assinatura digital para classificá-los em grupos familiares ou campanhas. Utilizando essa assinatura nos repositórios que não possuíam imagens, foram identificados e listados os usuários responsáveis pela publicação. Consequentemente, todos os repositórios desses usuários foram marcados como maliciosos. Ao analisar as campanhas em uma linha do tempo, foram observados os intervalos de atividade das maiores operações de malware.

Notadamente, duas delas tiveram picos de atividade no primeiro semestre de 2021, com a publicação de milhares de repositórios todos os dias. A campanha relacionada a downloaders tentou ressurgir em agosto de 2023. Já a campanha de "SEO para Websites" manteve uma estratégia distinta, inserindo um volume menor de repositórios de maneira constante ao longo de três anos.

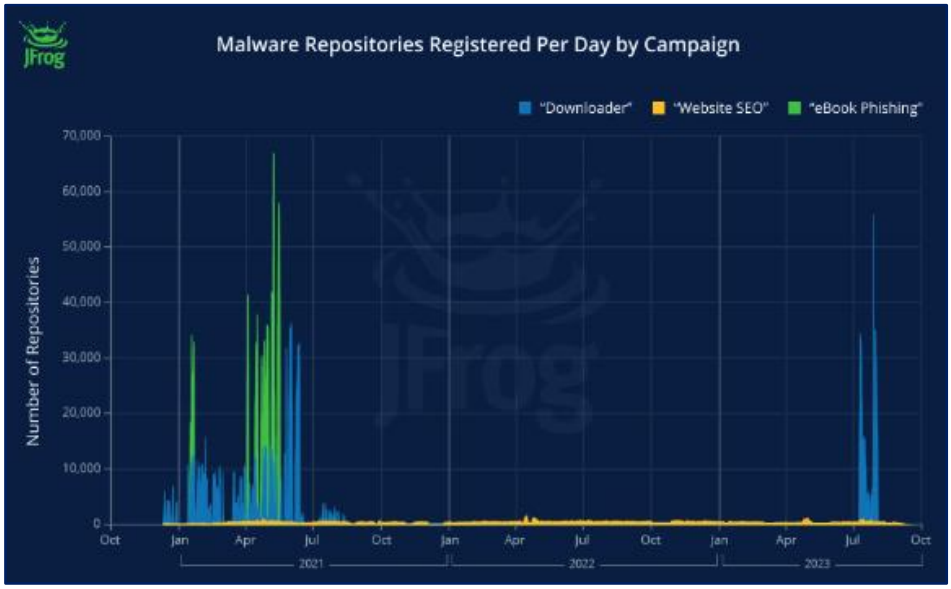


Figura 6 – Repositórios de malware registrados por campanha diariamente.

A tabela a seguir apresenta como os repositórios maliciosos estão distribuídos entre as diferentes campanhas:

Campanha	Nº de repositórios (% de todos os repositórios DH)	Nº de usuários
Website SEO	215451 (1.4%)	194699
Downloader	1453228 (9.7%)	9309
eBook Phishing	1069160 (7.1%)	1042
Other suspicious imageless	76025 (0.5%)	3689
Total	**2.81M (18.7%)**	**208739**

Tabela 1 – Tabela com repositórios maliciosos.

As estratégias de distribuição de repositórios maliciosos variam entre as campanhas observadas. As campanhas "Downloader" e "Phishing de eBooks" tendem a gerar lotes de repositórios falsificados em um intervalo de tempo breve, enquanto a campanha "SEO para Websites" mantém uma produção constante de repositórios, criando poucos a cada dia ao longo de um período estendido, com cada repositório vinculado a um usuário exclusivo.

Com o conhecimento das principais campanhas de malware ativas no Docker Hub, é essencial analisar detalhadamente as táticas e técnicas empregadas por elas:

- Campanha “Downloader”:

- Campanha “Phishing de eBooks”:

- Campanha “SEO para Websites”:

Os repositórios da campanha "**Downloader**" apresentam conteúdos SEO automatizados que promovem o download de materiais pirateados ou truques para jogos eletrônicos. Incluem também um link direcionando para o software prometido. Essa campanha foi executada em dois momentos diferentes, aproximadamente nos anos de 2021 e 2023, e em ambas as ocasiões, a mesma carga maliciosa foi utilizada (conforme análise subsequente).

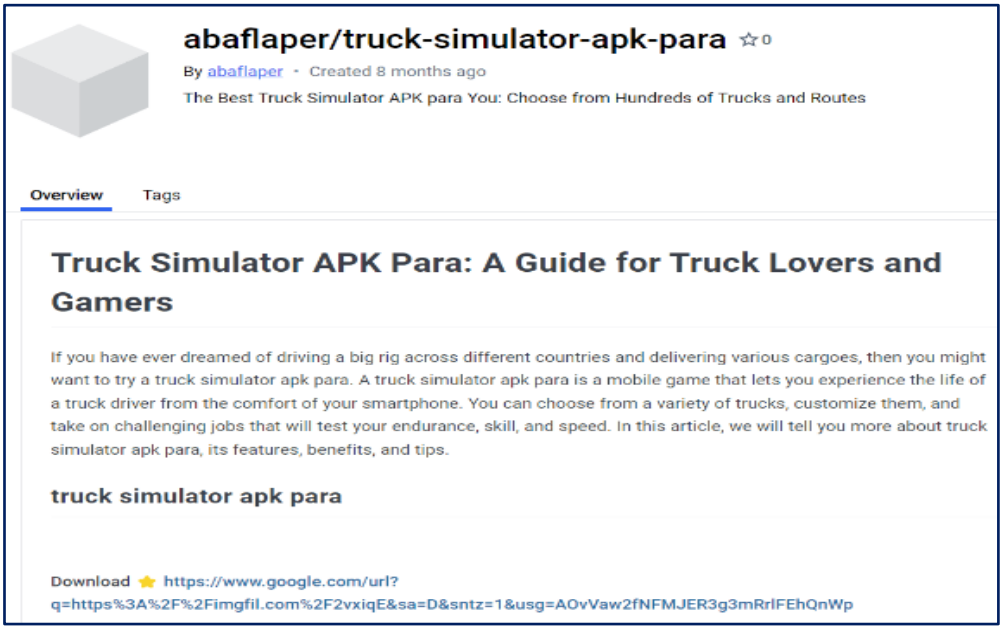


Figura 7 – Exemplo de repositório malicioso com link para download de malware.

Durante a campanha de "**Phishing de e-books**", aproximadamente um milhão de repositórios foram estabelecidos em 2021, convertendo o Docker Hub numa vasta coleção de "e-books piratas". Esses repositórios de spam disponibilizavam e-books para download sem custo, acompanhados de descrições criadas de forma aleatória e links para download.

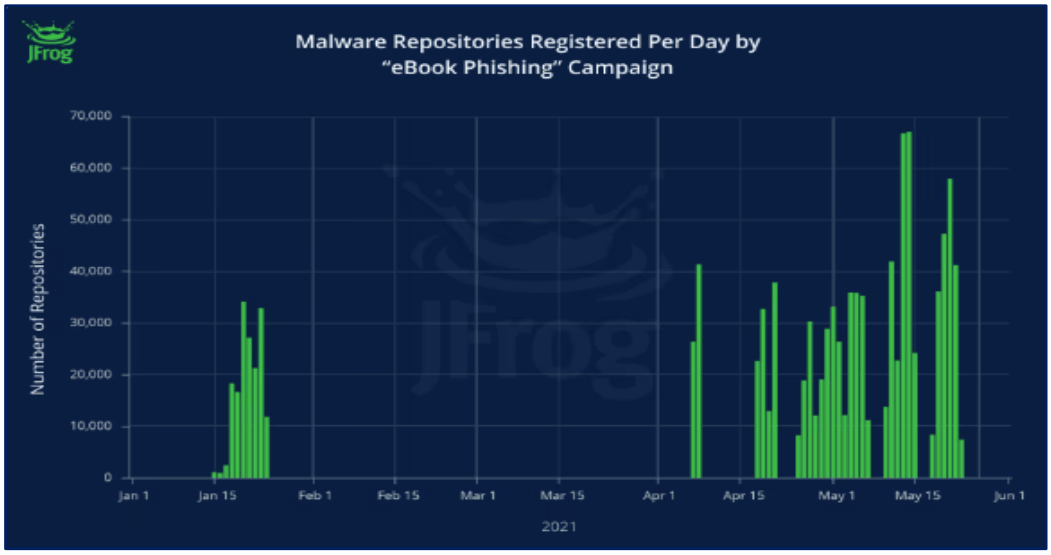


Figura 8 – Repositórios de malware registrados diariamente pela campanha ebook_phishing.

Figura 9 – Exemplo de repositório de phishing de e-books.

Diferentemente das campanhas anteriores, a finalidade da campanha "**SEO de site**" permanece incerto. Os repositórios, apesar de não serem criados com intenções legítimas, contêm conteúdos majoritariamente inofensivo, consistindo em descrições aleatórias e nomes de usuários gerados pelo modelo "axaaaaaxxx", onde 'a' representa uma letra e 'x', um dígito. Todos esses repositórios compartilham um nome comum: website. Pode-se conjecturar que essa campanha serviu como um teste preliminar para futuras ações maliciosas.

Essa campanha se distingue também pelo seu método de registro único. Conforme ilustrado no gráfico, os responsáveis por essa campanha geraram mil repositórios diariamente durante três anos, um contraste com as campanhas prévias que criavam repositórios sem imagens em períodos bem mais curtos. Nesta ocasião, cada usuário criado estava associado a apenas um repositório, em oposição às campanhas passadas, onde um único usuário era responsável pela criação de milhares de repositórios.

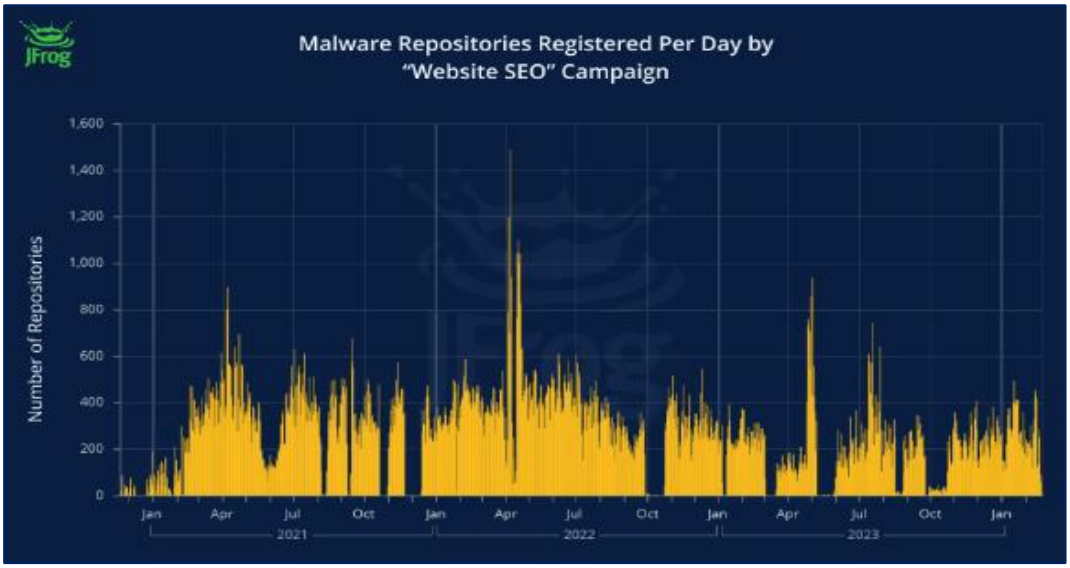


Figura 10 – Repositórios diários de malware registrados pela campanha "Website SEO".

Em vez de mirar diretamente em desenvolvedores e entidades, os atores de ameaças buscaram se valer da confiança depositada na Docker Hub para camuflar suas ações de phishing e disseminação de malware. A existência de aproximadamente três milhões de repositórios mal-intencionados, com alguns operando por mais de três anos, ressalta o abuso persistente da Docker Hub por parte desses invasores e sublinha a importância de uma vigilância ininterrupta nessas plataformas.

3 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:

O Docker Hub implementou um sistema de tags para identificar conteúdos de fontes seguras. As principais tags são:

Docker official image

- Conhecida como a Biblioteca do Docker Hub, reúne repositórios selecionados mantidos por entidades renomadas no desenvolvimento de software, como Python, Ubuntu e Node.

Verified publisher

- Destinada aos repositórios do programa Docker Verified Publisher, engloba conteúdos de editores comerciais autenticados pelo Docker Hub.

Sponsored OSS

- Voltada para projetos de código aberto que recebem apoio do Docker Hub.

Essas tags ajudam os usuários a identificar repositórios confiáveis ao visualizar a descrição de uma imagem, onde um identificador correspondente é exibido ao lado do nome do repositório.

4 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 URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	failhostingpolp[.]ru gts794[.]com blltly[.]com ltlly[.]com byltly[.]com bytlly[.]com cinurl[.]com fancli[.]com geags[.]com gohhs[.]com imgfil[.]com jinyurl[.]com miimms[.]com picfs[.]com shoxet[.]com shurll[.]com ssurll[.]com tinourl[.]com tinurli[.]com tinurll[.]com tiurll[.]com tlniurl[.]com tweeat[.]com urlca[.]com urlcod[.]com urlgoal[.]com urllie[.]com urllio[.]com urloso[.]com urluso[.]com urluss[.]com vittuv[.]com rd[.]lesac[.]ru soneservice[.]shop

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.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **JFrog**
- **Bleepingcomputer**

heimdall
security research
A DIVISION OF ISH