BOLETIM DE SEGURANÇA

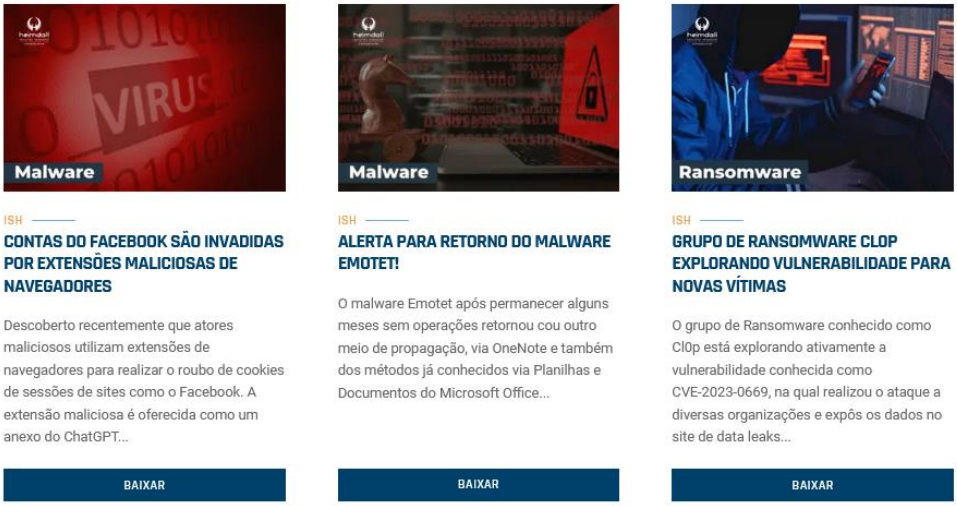
DragonRank realiza manipulação de SEO para ataques em diversas indústrias e regiões

heimdall
security research
A DIVISION OF ISH

TLP: CLEAR

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 Talos identificou recentemente uma série de atividades denominadas “DragonRank”, que se estendem por várias regiões, incluindo Tailândia, Índia, Coreia, Bélgica, Holanda e China. O DragonRank atinge uma ampla gama de setores, como joias, mídia, saúde, produção de vídeo, manufatura, transporte, organizações religiosas, serviços de TI, relações internacionais, agricultura, esportes e nichos como feng shui.

2 INFORMAÇÕES SOBRE A AMEAÇA

As atividades do DragonRank utilizam ferramentas e técnicas frequentemente associadas a grupos de hackers de língua chinesa simplificada. O principal objetivo é comprometer servidores Windows Internet Information Services (IIS) que hospedam sites corporativos, implantando o malware BadIIS. Este malware manipula rastreadores de mecanismos de busca, prejudicando o SEO dos sites afetados. Com os servidores IIS comprometidos, o DragonRank pode redirecionar usuários para sites fraudulentos.

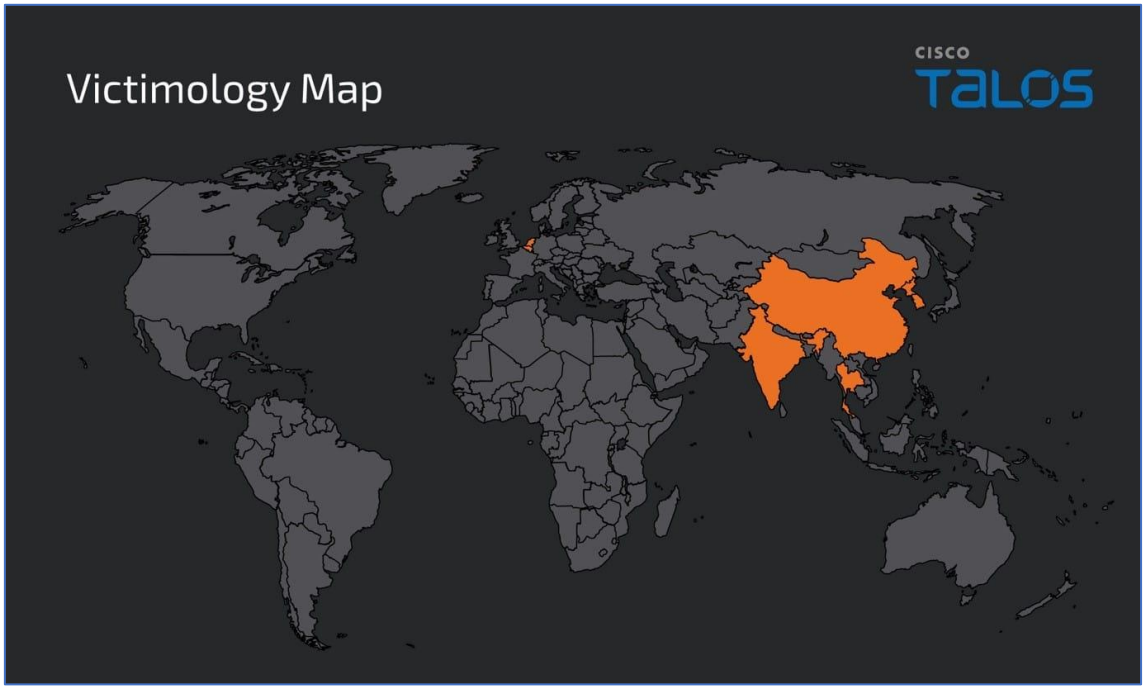


Figura 1 – Mapa de vitimologia.

O grupo manipula SEO alterando algoritmos de busca para melhorar a classificação de sites maliciosos, direcionando tráfego para esses sites, aumentando a visibilidade de conteúdo fraudulento ou prejudicando concorrentes. Esses ataques podem danificar a presença online de empresas, causar perdas financeiras e manchar reputações ao associar marcas a práticas enganosas. Os sites comprometidos são promovidos como plataformas para operações fraudulentas, utilizando palavras-chave relacionadas a pornografia e sexo. Dados de configuração dos servidores de comando e controle (C2) foram traduzidos para vários idiomas. A Talos confirmou que mais de 35 servidores IIS foram comprometidos, servindo como canais para esses ataques. As imagens a seguir mostram dados configurados do servidor C2 e sites fraudulentos nos resultados de busca.

As descobertas indicam que o DragonRank está envolvido em práticas de SEO black hat para promover negócios online de forma antiética. Diferente de outros grupos de crimes cibernéticos de SEO black hat, o DragonRank foca em movimento lateral e escalada de privilégios, infiltrando-se em servidores adicionais e mantendo controle sobre eles. Foi avaliado que são novos na indústria de SEO

black hat, anteriormente atuando em ataques direcionados ou testes de penetração.

Foi investigado o mecanismo de busca utilizando palavras-chave relevantes e servidores C2 do malware PlugX. Pesquisas como “tttseo.com” no Google revelaram anúncios do DragonRank em sites legítimos, focando em métodos de SEO black hat. Alterando o IP para o Japão, confirmou-se a disseminação global das palavras-chave do DragonRank. Além disso, o grupo oferece serviços de postagem em massa em plataformas de mídia social.

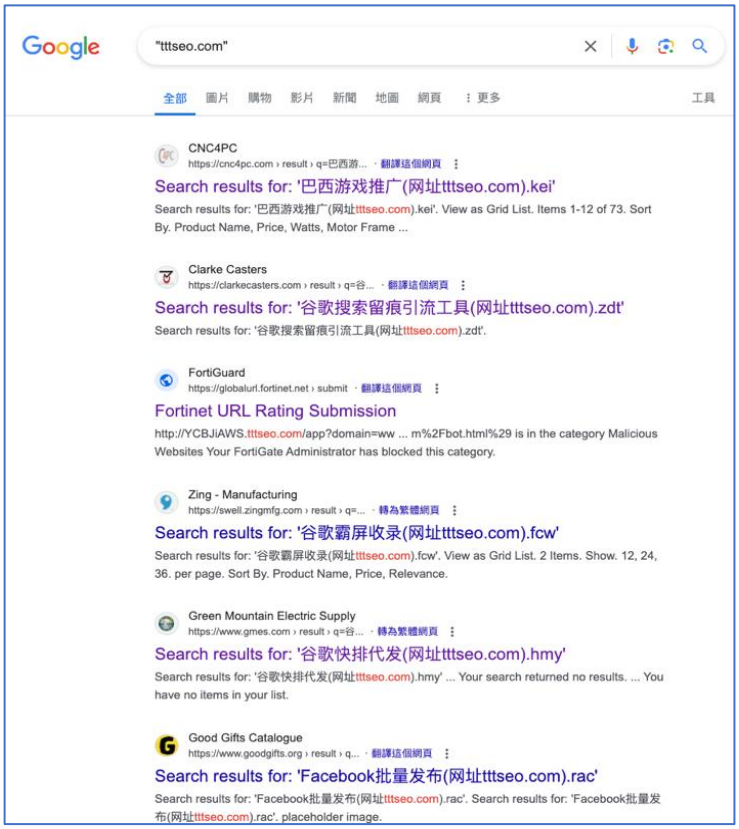


Figura 2 – Serviços oferecidos pelo grupo.

Nesta campanha, o grupo de hackers DragonRank explora vulnerabilidades em serviços de aplicativos web, como phpMyAdmin e WordPress. Ao conseguir executar código remotamente ou carregar arquivos no site alvo, eles implantam um shell da web, ganhando controle sobre o servidor comprometido. Este ponto de entrada inicial é crucial para suas operações. A imagem a seguir mostra o shell da web ASPXspy de código aberto utilizado nesta campanha e seu local de detecção.

- *C:\phpMyAdmin\shell.aspx*
- *C:\AWStats\wwwroot\shell.aspx*

```
<%@ import Namespace="System.Text.RegularExpressions"%>
<%@ Import Namespace="System.Threading"%>
<%@ Import Namespace="System.Data.SqlClient"%>
<%@ import Namespace="Microsoft.VisualBasic"%>
<%@ Assembly Name="System.DirectoryServices,Version=2.0.0.0,Culture=neutral,PublicKeyToken=B03F5F7F11D50A3A"%>
<%@ Assembly Name="System.Management,Version=2.0.0.0,Culture=neutral,PublicKeyToken=B03F5F7F11D50A3A"%>
<%@ Assembly Name="System.ServiceProcess,Version=2.0.0.0,Culture=neutral,PublicKeyToken=B03F5F7F11D50A3A"%>
<%@ Assembly Name="Microsoft.VisualBasic,Version=7.0.3300.0,Culture=neutral,PublicKeyToken=b03f5f7f11d50a3a"%>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<script runat="server">
public string Password="[redacted]";
public string vbhLn="ASPXSpy";
public int TdgGU=1;
protected OleDbConnection Dtdr=new OleDbConnection();
```

Figura 3 – shell da web ASPXspy.

O DragonRank também compromete servidores Windows IIS adicionais na rede alvo, utilizando shells da web ou explorando logins de desktop remoto com credenciais obtidas. Após obter acesso a esses servidores, os invasores utilizam um shell da web ou o Protocolo de Desktop Remoto (RDP) para instalar o PlugX, o BadIIS, ferramentas de extração de credenciais e um utilitário de clonagem de usuário, visando manter um perfil discreto e garantir persistência na rede. Em um dos servidores comprometidos, foi observado que o DragonRank usa um utilitário para clonar permissões de administrador para uma conta de convidado, elevando seus privilégios a administrador e executando a ferramenta de extração de credenciais.

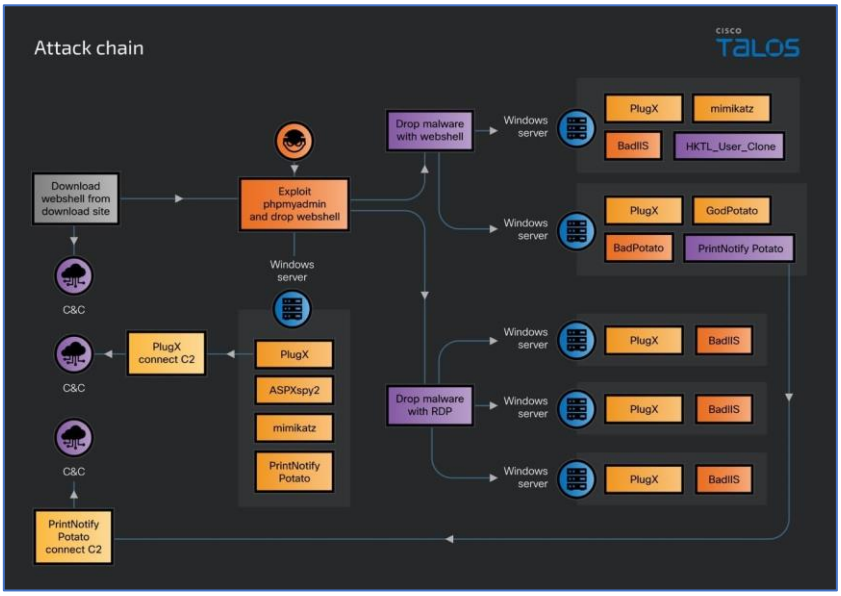


Figura 4 – Cadeia de ataque.

Durante a análise do mais recente loader, foi utilizado o VirusTotal e outros repositórios de malware na nuvem. Identificou-se um carregador PlugX similar com o mesmo caminho de registro, valores e algoritmo XOR com a chave “0xD1” no VirusTotal. Essa instância serviu para recuperar arquivos originais e seus sites de download. Apesar das diferenças nas fontes de upload e nos países envolvidos, o carregador PlugX e sua carga útil eram idênticos, com hashes correspondentes.

PlugX é uma ferramenta de acesso remoto (RAT) conhecida, com plugins modulares e configurações proprietárias, usada por agentes de ameaças cibernéticas chineses há mais de dez anos. A configuração do PlugX nesta campanha inclui todos os valores necessários para executar o executável.

Também foi encontrado o mesmo loader e payload do PlugX em um arquivo chamado “ddos.zip”, disfarçado como uma ferramenta de gerenciamento de ataques DDoS. Todos os arquivos dentro deste zip são variantes do carregador PlugX. Isso sugere que o grupo de hackers pode ser novo no crime cibernético, mostrando pouca preocupação em manter uma fachada respeitável. O arquivo inclui um manual de aplicativo para atrair usuários a executar o malware, sob o pretexto de operar uma ferramenta DDoS. O arquivo tem duas subpastas: uma como interface de controle do servidor e outra como utilitário de instalação do cliente, ambas contendo versões do malware PlugX. A primeira variante é idêntica à analisada, enquanto a segunda usa um driver assinado digitalmente para executar o payload do PlugX. O manual e o nome da pasta estão em chinês simplificado, indicando que o arquivo é direcionado a regiões onde esse idioma é falado.

3 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Discovery	T1016 T1057 T1033 T1069.001 T1082	Consiste em técnicas que um adversário pode usar para obter conhecimento sobre o sistema e a rede interna.
Credential Access	T1555	Consiste em técnicas para roubar credenciais como nomes de contas e senhas. Técnicas usadas para obter credenciais incluem keylogging ou credential dumping.
Command and Control	T1105	Consiste em técnicas que adversários podem usar para se comunicar com sistemas sob seu controle dentro de uma rede de vítima.
Defense Evasion	T1070	Consiste em técnicas que os adversários usam para evitar a detecção durante seu comprometimento.
Persistence	T1098 T1136	Consiste em técnicas que os adversários usam para manter o acesso aos sistemas em reinicializações, credenciais alteradas e outras interrupções que podem cortar seu acesso.
Lateral Movement	T1021.001	Consiste em técnicas que os adversários usam para entrar e controlar sistemas remotos em uma rede.

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:

Use softwares de proteção

- Instale e mantenha atualizados antivírus, anti-malware e anti-ransomware. Esses programas ajudam a detectar e bloquear ameaças antes que causem danos.

Mantenha sistemas e aplicativos atualizados

- Atualize regularmente seus sistemas operacionais, softwares e aplicativos para corrigir falhas de segurança que podem ser exploradas por hackers.

Proteja sua rede

- Utilize firewalls para monitorar e controlar o tráfego de dados entre seus dispositivos e a internet. Isso ajuda a bloquear acessos não autorizados1.

Educação e treinamento

- Treine seus colaboradores para reconhecer e evitar ameaças cibernéticas, como phishing e links suspeitos. Senhas fortes e práticas seguras de navegação são essenciais.

Criptografia de dados

- Criptografe dados sensíveis para garantir que apenas pessoas autorizadas possam acessá-los. Isso adiciona uma camada extra de proteção contra invasões.

Backups regulares

- Faça backups frequentes de seus dados importantes e armazene-os em locais seguros, como na nuvem e em discos rígidos externos. Isso garante que você possa recuperar informações em caso de ataque.

Gerenciamento de credenciais

- Use senhas fortes e únicas para cada conta e altere-as regularmente. Considere o uso de gerenciadores de senhas para facilitar o controle.

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:	e9194bd20e9bd6f6f5e572796514b285
sha1:	43e00adbbc09e4b65f09e81e5bd2b716579a6a61
sha256:	72fc4ba4d8e9a7b11fa0b76611e85b7aaf3558ac08dc8e9628fad48d72fb8190
File name:	FVTProect32.sys

Indicadores de compromisso do artefato	
md5:	7d8c5f7d684971923fc11d0033bef90d
sha1:	ab7ebc82930e69621d9bccb6698928f4a3719d29
sha256:	9277f848a5348e447e02cf94beae392815a235264443fdd69a3ff6eb48f040a8
File name:	NULL

Indicadores de compromisso do artefato	
md5:	ad7e5df7a54b38176476cdc545129d41
sha1:	75e3e83511ce6d400902e5a8320db9a3f3d26e44
sha256:	ffa94d76d4423e43a42c7944c512e1a71827a89ad513d565f82eb8fe374ef74d
File name:	Acrobat.dll

Indicadores de compromisso do artefato	
md5:	f2047fae637746ef4d7a4d2f81c2894f
sha1:	75245e8bdd4884016915ba0ff0c94940342379bc
sha256:	3503d6ccb9f49e1b1cb83844d1b05ae3cf7621dfec8dc115a40abb9ec61b00bb
File name:	Acrobat.dll

Indicadores de compromisso do artefato	
md5:	7968fb0f54637e2fa745ed5410fc6886
sha1:	8b921434de690d153c4c4cdf21d390fc85f0d4f0
sha256:	614920f1a8550070a983f2ad22d6358c6742a9e02802b025eeea8db8c3d41fb7
File name:	AppInstall.exe

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	http://a.googie[.]pw/xx1.php http://a.googie[.]pw/zz1.php http://b.googie[.]pw/xx1.php http://b.googie[.]pw/zz1.php http://web.googie[.]pw/xx1.php http://web.googie[.]pw/zz1.php http://www.ig26[.]com/xx1.php http://www.ig26[.]com/zz1.php http://www.googie[.]pw/xx1.php http://www.googie[.]pw/zz1.php http://www.yx52[.]pw/xx1.php http://www.yx52[.]pw/zz1.php http://35.247.175[.]184:443/1.aspx https://admin1.tttseo[.]com/ht.zip http://ddos.tttseo[.]com/ddos/ddos.zip
IP	154.23.179[.]133:888 154.23.179[.]133:443 202.162.108[.]48:443

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**
- Talos
- Thehackernews

7 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH