TLP: CLEAR

RELATÓRIO DE PESQUISAS

TGR-STA-1030: Ameaça Persistente com Impacto em Organizações Governamentais Brasileiras

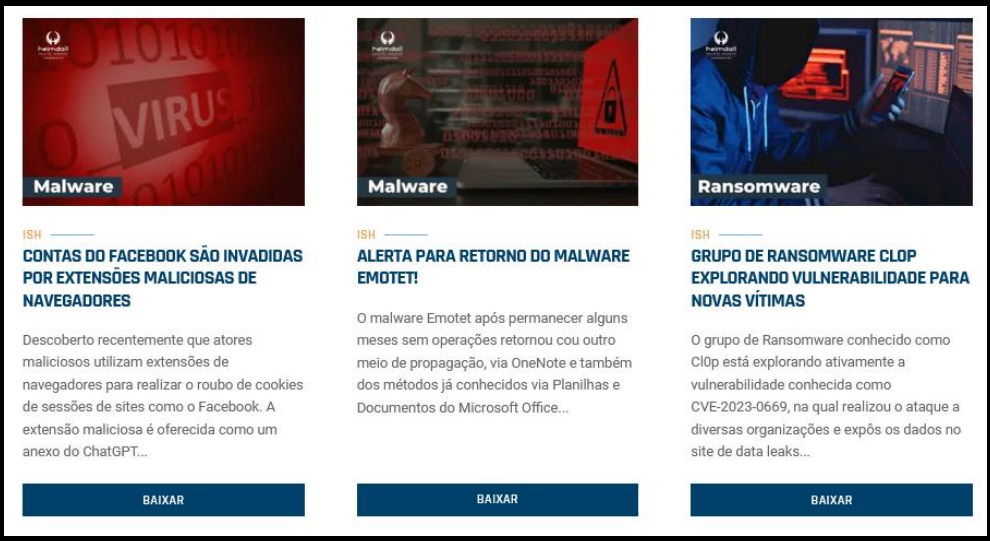
heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

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 Introdução executiva 6
2 Estratégico 6
2.1 Introdução sobre a ameaça 6
2.2 Vitimologia e Segmentos afetados 6
3 Tático 8
3.1 Modelo de negócio da ameaça 8
3.2 Análise da Kill Chain da ameaça 8
3.3 Tabela MITRE ATT&CK 10
4 Recomendações 12
5 Operacional 13
5.1 Indicadores de Comprometimento (IoC) 13
6 Referências 16
7 Autores 16

LISTA DE TABELAS

Tabela 1 – Tabela MITRE ATT&CK. 11
Tabela 2 – Indicadores de Comprometimento. 14
Tabela 3 – Indicadores de Comprometimento. 15

LISTA DE FIGURAS

Figura 1 – Países afetados. 7

1 INTRODUÇÃO EXECUTIVA

Este relatório de segurança, desenvolvido pela equipe de inteligência **Heimdall da ISH Tecnologia**, tem como objetivo proporcionar uma compreensão aprofundada e um dimensionamento preciso das ameaças cibernéticas identificadas. O documento está estruturado em três níveis de abordagem: ***Estratégico***, ***Tático*** e ***Operacional***, garantindo uma visão completa e integrada das ameaças e ações recomendadas.

2 ESTRATÉGICO

2.1 INTRODUÇÃO SOBRE A AMEAÇA

A campanha analisada corresponde a uma operação estruturada de **ciberespionagem de natureza estatal**, atribuída ao grupo **TGR-STA-1030 (UNC6619)**. O objetivo central da atividade é a obtenção de **inteligência estratégica e geopolítica**, com foco em informações relacionadas a políticas públicas, acordos comerciais, cadeias de suprimento e planejamento de infraestrutura crítica.

As ações identificadas demonstram alto grau de planejamento e discrição operacional, indicando um adversário com capacidade técnica avançada e alinhamento a interesses governamentais. O impacto potencial para o Brasil é relevante, especialmente para organizações dos setores de **energia, mineração, telecomunicações e administração pública**, que concentram dados de valor estratégico para a soberania nacional e para a competitividade econômica.

2.2 VITIMOLOGIA E SEGMENTOS AFETADOS

Alcance Geográfico: Foram identificadas organizações comprometidas em **37 países**, com atividades de reconhecimento direcionadas a infraestruturas governamentais de **155 nações**, evidenciando campanha de escala global e caráter persistente.

Setor Governamental: O grupo direciona esforços a ministérios e departamentos de alto escalão, incluindo pastas de **Interior, Relações Exteriores, Finanças, Comércio, Economia, Imigração e Justiça**. No Brasil, há evidências de comprometimento relacionado ao **Ministério de Minas e Energia (MME)**.

Infraestrutura Crítica: Entidades dos setores de **Energia, Mineração, Telecomunicações e Aviação** figuram entre os principais alvos, com interesse particular em organizações ligadas a **terras raras e recursos naturais estratégicos**.

Perfil das Vítimas: Os alvos incluem decisores políticos, diplomatas e técnicos com acesso a documentos sensíveis. A motivação observada é essencialmente de **espionagem estratégica**, sem indícios de finalidade financeira direta.

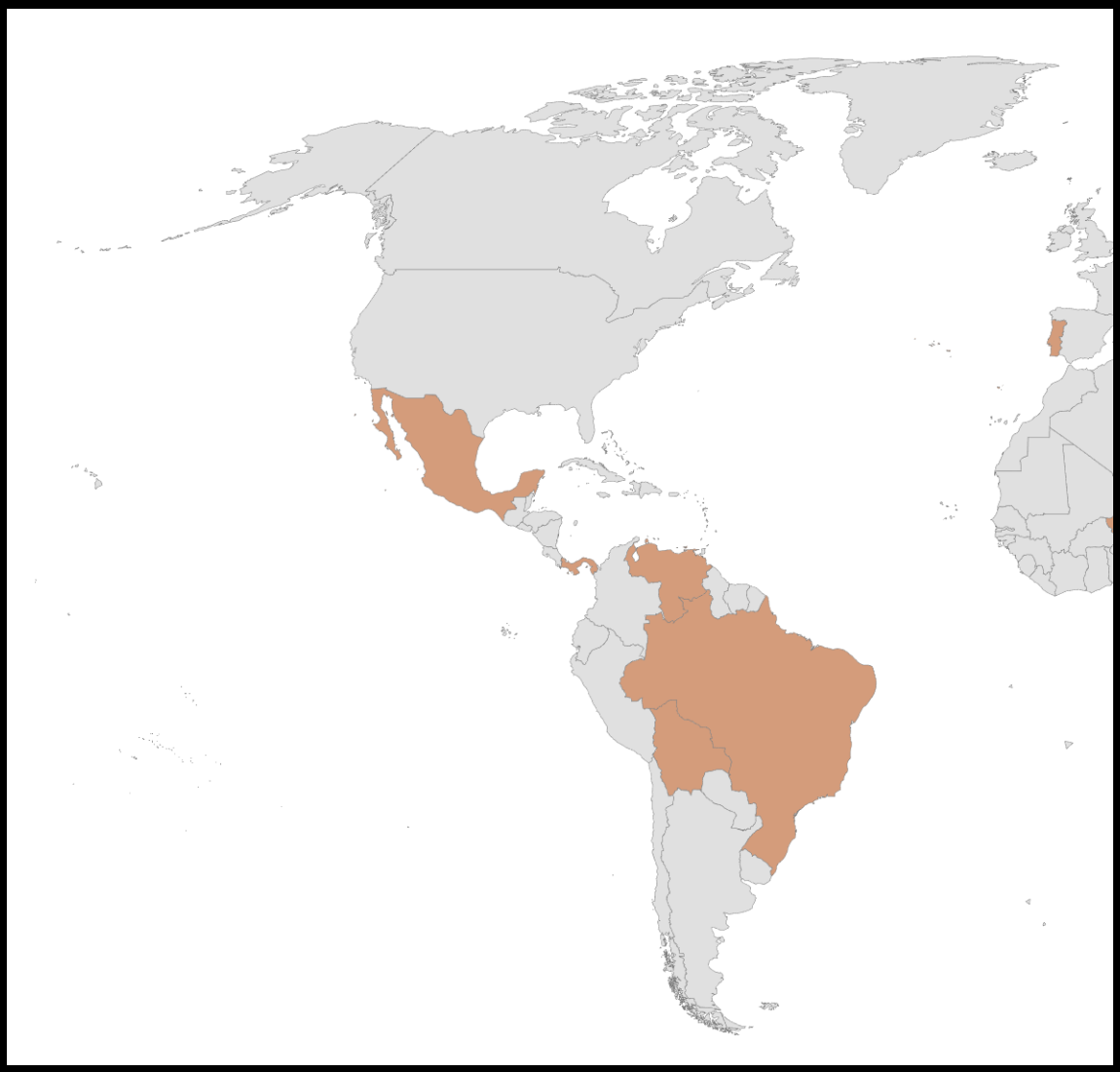


Figura 1 – Países afetados.

3 TÁTICO

3.1 MODELO DE NEGÓCIO DA AMEAÇA

O TGR-STA-1030 opera sob um **modelo de espionagem de longo prazo**, priorizando a coleta silenciosa de dados em vez de ações destrutivas ou extorsivas. A estratégia baseia-se em quatro pilares:

- **Acesso inicial seletivo**, combinando engenharia social e exploração de vulnerabilidades públicas logo após sua divulgação;
- **Infraestrutura de comando e controle multicamada**, frequentemente hospedada em países com forte Estado de Direito para dificultar atribuição e bloqueio;
- **Manutenção prolongada do acesso**, com uso de rootkits e webshells para garantir resiliência operacional;
- **Extração direcionada de informação**, focada em documentos de valor diplomático, econômico e energético.

A operação prioriza técnicas "living-off-the-land" e ferramentas amplamente utilizadas em testes de intrusão, o que reduz a probabilidade de detecção e confere aparência de tráfego legítimo.

3.2 ANÁLISE DA KILL CHAIN DA AMEAÇA

Reconhecimento

- Varredura de serviços expostos e identificação de ativos governamentais;
- Mapeamento de tecnologias vulneráveis e perfis de usuários de interesse.

Preparação

- Criação de arquivos ZIP maliciosos com temática institucional;
- Desenvolvimento de exploits para falhas N-day amplamente divulgadas.

Entrega

- Spear-phishing com documentos isca;
- Abuso de serviços legítimos (ex.: Mega, GitHub) para hospedagem de payloads.

Exploração e Instalação

- Execução do loader **DiaoYu.exe** com verificações anti-sandbox;
- Exploração de vulnerabilidades como **CVE-2019-11580 (Atlassian Crowd)**.

Comando e Controle

- Utilização de frameworks como **Cobalt Strike, Havoc, Sliver e VShell**;
- Comunicação por portas não padrão e domínios com reputação neutra.

Persistência e Movimentação Lateral

- Implantação do rootkit **ShadowGuard (eBPF)** para ocultação de processos;
- Webshells **Behinder, Godzilla e Neo-reGeorg** para acesso redundante.

Ações sobre Objetivos

- Coleta e exfiltração de documentos estratégicos, dados de imigração e planos de energia.

3.3 TABELA MITRE ATT&CK

Este tópico apresenta as Táticas, Técnicas e Procedimentos (TTPs) identificados nesta ameaça, conforme o framework MITRE ATT&CK, oferecendo uma visão tática detalhada sobre o comportamento do adversário. O objetivo é permitir o mapeamento das técnicas utilizadas pelos atacantes, facilitando a implementação de contramedidas eficazes e o aprimoramento das defesas de segurança.

Tática	Técnica	Detalhes
Reconhecimento	T1595 – Active Scanning	Os adversários podem executar varreduras de reconhecimento ativo para coletar informações que podem ser usadas durante ataques.
Acesso Inicial	T1566.001 – Spearphishing Link	Os adversários podem enviar mensagens de phishing para obter acesso aos sistemas das vítimas. Todas as formas de phishing são técnicas de engenharia social realizadas eletronicamente. O phishing pode ser direcionado, conhecido como spearphishing. Nesse tipo de ataque, o adversário visa um indivíduo, empresa ou setor específico. De forma mais geral, os adversários podem realizar phishing não direcionado, como em campanhas massivas de spam com malware.
Execução	T1204 – User Execution	Um adversário pode se basear em ações específicas do usuário para obter sucesso. Os usuários podem ser submetidos a engenharia social para induzi-los a executar código malicioso, por exemplo, abrindo um arquivo ou link malicioso.
Persistência	T1505.003 – Web Shell	Os adversários podem abusar de recursos legítimos de desenvolvimento extensível de servidores para estabelecer acesso persistente aos sistemas
Comando e Controle	T1071 – Application Layer Protocol	Os adversários podem se comunicar usando protocolos da camada de aplicação do modelo OSI para evitar a detecção/filtragem de rede, misturando-se ao tráfego existente. Os comandos para o sistema remoto, e frequentemente os resultados desses comandos, estarão incorporados ao tráfego do protocolo entre o cliente e o servidor.
Exfiltração	T1041 - Exfiltration Over C2 Channel	Os adversários podem roubar dados por meio da exfiltração dos mesmos através de um canal de comando e controle existente. Os dados roubados

		são codificados no canal de comunicação normal utilizando o mesmo protocolo das comunicações de comando e controle.

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:

- **Fortalecer a proteção de e-mail contra phishing**, bloqueando anexos ZIP/RAR com executáveis, aplicando sandbox para análise dinâmica e reforçando políticas DMARC/DKIM/SPF com treinamento contínuo dos usuários.
- **Priorizar a gestão de vulnerabilidades N-day**, com aplicação imediata de patches em plataformas como Exchange, SAP, Atlassian e WinRAR, além do uso de virtual patching via WAF/IPS.
- **Implementar detecção comportamental para frameworks de pós-exploração**, como Cobalt Strike, Sliver, Havoc e VShell, com monitoramento de beaconing e comunicação por portas não padrão.
- **Monitorar criação e uso de webshells** (Behinder, Godzilla, Neo-reGeorg) em servidores web, com verificação de arquivos suspeitos e alterações em diretórios de aplicações.
- **Reforçar a visibilidade sobre atividades eBPF e kernel**, visando identificar rootkits como ShadowGuard e anomalias de ocultação de processos.
- **Bloquear e auditar uso de proxies residenciais e Tor**, correlacionando acessos administrativos provenientes dessas redes.
- **Segmentar ambientes críticos**, restringindo acesso administrativo a sistemas de energia, mineração e governo por meio de PAM e MFA.
- **Habilitar logging avançado de rede e DNS**, com retenção suficiente para correlação de domínios semelhantes aos IoCs observados.
- **Implantar EDR/XDR com regras específicas para loaders** como DiaoYu.exe e atividades de execução suspeita após abertura de ZIPs.
- **Estabelecer monitoramento contínuo de integridade de servidores**, com verificação de arquivos sensíveis, criação de serviços anômalos e conexões de saída incomuns para infraestrutura C2.

5 OPERACIONAL

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 Comprometimento (IoCs) relacionadas a análise do(s) artefato(s) deste relatório.

5.1 INDICADORES DE COMPROMETIMENTO (IOC)

Indicadores do artefato	
md5:	97b3f5d523bdb226514675ea1c4a4962
sha1:	c926186e9c39ef9e522fed57f19aff80ef3eb904
sha256:	9ed487498235f289a960a5cc794fa0ad0f9ef5c074860fea650e88c525da0ab4
File name:	9ed487498235f289a960a5cc794fa0ad0f9ef5c074860fea650e88c525da0ab4.zip

Indicadores do artefato	
md5:	dcd660f26aceb67e48e1096a8a209f70
sha1:	1363a0f9381ae791ca3e5483949759367e5015da
sha256:	5175b1720fe3bc568f7857b72b960260ad3982f41366ce3372c04424396df6fe
File name:	5175b1720fe3bc568f7857b72b960260ad3982f41366ce3372c04424396df6fe.dll

Indicadores do artefato	
md5:	c0950bc8dc3b66a9c1d4db1bda010bc4
sha1:	8ca2947d5906580aebbf5e962d255bfd6f10be89
sha256:	358ca77ccc4a979ed3337aad3a8ff7228da8246eebc69e64189f930b325daf6a
File name:	msedgeupdate.dll

Indicadores do artefato	
md5:	f67508174a0aca32dd1f2e9fe14bd753
sha1:	ab1cf3602664f81c851ed8cedcbc5c04037a3f52
sha256:	293821e049387d48397454d39233a5a67d0ae06d59b7e5474e8ae557b0fc5b06
File name:	DllSafeCheck64.dll

Indicadores do artefato	
md5:	48269c797226e181717f41b8b8e6f650
sha1:	e267c833c81728392fea9e91d75587e90684357a
sha256:	c876e6c074333d700adf6b4397d9303860de17b01baa27c0fa5135e2692d3d6f
File name:	12rip.exe

Indicadores do artefato	
md5:	49da92e2e969a4428bdd63d1aa644285
sha1:	40207818fa8237745e876a791ee1928b76e71cba
sha256:	b2a6c8382ec37ef15637578c6695cb35138ceab42ce4629b025fa4f04015eaf2
File name:	igtsb.exe

Indicadores do artefato	
md5:	96051c7d592bcb71d5defdf51f237507
sha1:	810753df130ec0f54abe100e3e35978a8bc533b8
sha256:	5ddeff4028ec407ffdaa6c503dd4f82fa294799d284b986e1f4181f49d18c9f3
File name:	DllSafeCheck64.dll

Indicadores do artefato	
md5:	b9c350a7f6ef64e2d0fb3e1361683ca4
sha1:	8784e151e3410d36d128021a6ce3b49fa91d047a
sha256:	182a427cc9ec22ed22438126a48f1a6cd84bf90fddb6517973bcb0bac58c4231
File name:	zea65554.exe

Indicadores do artefato	
md5:	a20e887f5f353a44b2054415fa9d5985
sha1:	8fff81911ae6900a6170014f3fb337a9f6763f62
sha256:	23ee251df3f9c46661b33061035e9f6291894ebe070497ff9365d6ef2966f7fe
File name:	DiaoYu.exe

Indicadores do artefato	
md5:	7333a243a53f0b29bc7325bb2450b881
sha1:	683a4c997079c6f0d0c363096075cee2c7e4e843
sha256:	66ec547b97072828534d43022d766e06c17fc1cafe47fbd9d1ffc22e2d52a9c0
File name:	66ec547b97072828534d43022d766e06c17fc1cafe47fbd9d1ffc22e2d52a9c0.zip

Tabela 2 – Indicadores de Comprometimento.

Indicadores de IPs e Domínios

Indicadores de IPs e Domínios	
Domínio	abwxjp5[.]me brackusi0n[.]live dog3rj[.]tech emezonhe[.]me gouvn[.]me msonline[.]help pickupweb[.]me pr0fu5a[.]me q74vn[.]live servgate[.]me zamstats[.]me zrheblirsy[.]me
IP	138.197.44[.]208 142.91.105[.]172 146.190.152[.]219 157.230.34[.]45 157.245.194[.]54 159.65.156[.]200 159.203.164[.]101 178.128.60[.]22 178.128.109[.]37 188.127.251[.]171

	188.166.210[.]146 208.85.21[.]30

Tabela 3 – Indicadores de Comprometimento.

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**
- **CTI Purple Team *by* ISH Tecnologia**

7 AUTORES

- **Thiago Cesar Maciel da Paixão**

heimdall
security research
A DIVISION OF ISH