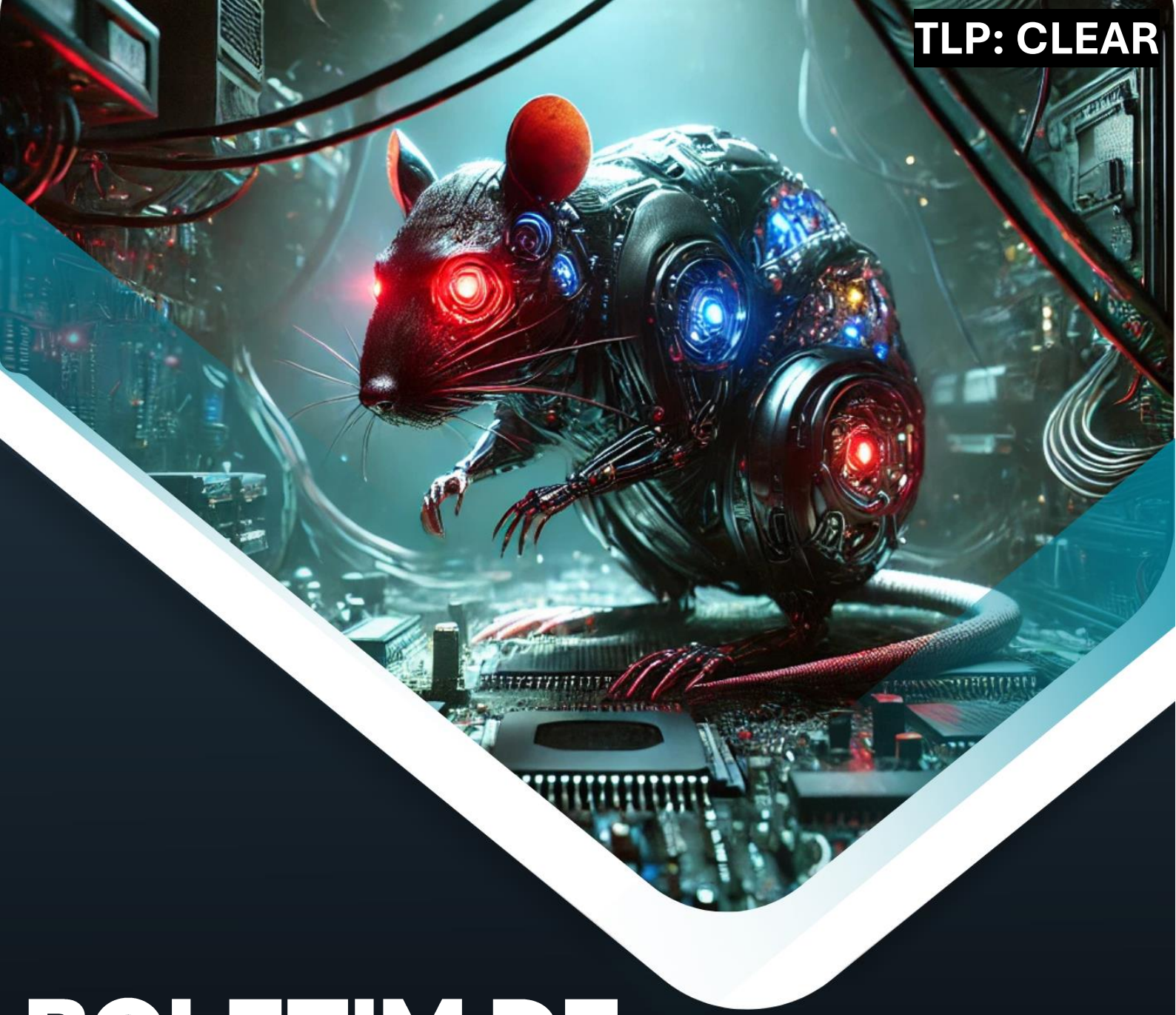
TLP: CLEAR



BOLETIM DE SEGURANÇA

Campanha do AsyncRAT Reloaded utilizando Python e TryCloudflare para distribuição de malware

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

heimdall
security research
A DIVISION OF ISH

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 INTRODUÇÃO EXECUTIVA

Este relatório de segurança, desenvolvido pela equipe de **Inteligência de Ameaças da ISH, Heimdall**, 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 SEGMENTO DE MERCADO

Os alvos potencialmente afetados por essa ameaça que será descrita neste relatório, incluem:

- *Setor financeiro*
- *Empresas de tecnologia e desenvolvimento de software*
- *Setor de saúde*
- *Governo e órgãos públicos*
- *Empresas de telecomunicações e provedores de internet*
- *Setor industrial e manufatura*
- *Setor educacional e instituições de pesquisa*

2.2 IMPACTO FINANCEIRO POTENCIAL

- *Roubo de dados sensíveis e penalidades regulatórias*
- *Fraudes financeiras e transações clandestinas*
- *Interrupção operacional e custos de recuperação*
- *Extorsão e ransomware secundário*
- *Impacto na reputação e perda de clientes*
- *Custos legais*
- *Despesas com segurança e reestruturação de TI*

2.3 OBJETIVO DA AMEAÇA

O principal objetivo desta campanha é obter controle remoto não autorizado de sistemas alvo, permitindo que os atacantes exfiltrem informações confidenciais, monitorem atividades dos usuários e executem comandos maliciosos, tudo isso enquanto permanecem indetectáveis.

3 TÁTICO

3.1 INFORMAÇÕES SOBRE A AMEAÇA

Uma recente campanha de malware utilizando o **AsyncRAT**, um trojan de acesso remoto, distribuído através de técnicas sofisticadas que envolvem o uso de scripts em Python e a infraestrutura legítima do TryCloudflare. Essa abordagem permite que os atacantes controlem sistemas infectados de forma furtiva, exfiltrando dados e executando comandos sem serem detectados. A campanha se inicia com e-mails de phishing contendo links para arquivos maliciosos hospedados em serviços legítimos, dificultando a detecção por soluções de segurança tradicionais.

A campanha começa com um e-mail de phishing que contém um link para um arquivo ZIP hospedado no Dropbox. Este arquivo ZIP inclui um atalho de internet (.URL) que, quando aberto, direciona o usuário a um arquivo .LNK hospedado em um subdomínio do TryCloudflare. A sequência de infecção continua com a execução de scripts que eventualmente baixam e executam o AsyncRAT no sistema da vítima.

3.2 OPERAÇÃO E CAPACIDADE DA AMEAÇA

O AsyncRAT é projetado para comunicação assíncrona eficiente, permitindo que os atacantes controlem sistemas infectados de maneira furtiva. Suas capacidades incluem captura de tela, registro de teclas digitadas, exfiltração de arquivos e execução de comandos arbitrários. A utilização de serviços legítimos como Dropbox e TryCloudflare para hospedar e distribuir componentes maliciosos aumenta a eficácia da campanha, pois dificulta a detecção por soluções de segurança. Conforme informado em análises, o malware executa diversas ações maliciosas:

Uso de serviços legítimos para evasão

- Os atacantes utilizam dropbox e trycloudflare para hospedar e distribuir arquivos maliciosos, dificultando a detecção por soluções de segurança.

Execução de código remoto e exfiltração de dados

- O asyncrat permite acesso remoto, captura de tela, registro de teclas digitadas e extração de arquivos, possibilitando espionagem e roubo de credenciais.

Persistência e furtividade

- A ameaça opera de forma assíncrona, garantindo que comandos maliciosos sejam executados sem interrupção das atividades do sistema, dificultando sua detecção.

Uso de scripts em python para infecção

- A cadeia de infecção começa com scripts python disfarçados, permitindo que o malware se espalhe e comprometa o sistema antes da ativação do trojan.

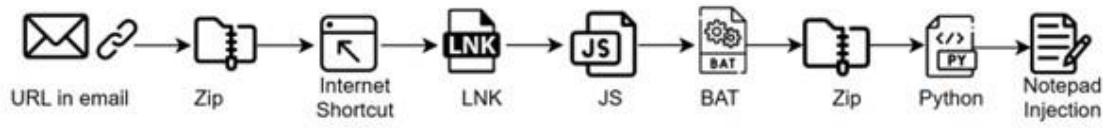


Figura 1 – Cadeia de ataque do AsyncRAT.

Conforme já mencionado, os agentes da ameaça utilizaram o TryCloudflare como um canal para distribuir cargas maliciosas do AsyncRAT, aproveitando-se da infraestrutura legítima desse serviço para ocultar o tráfego e dificultar a detecção. Nessas campanhas, os alvos principais eram usuários corporativos que, ao interagir com links de phishing, eram redirecionados para arquivos hospedados no Dropbox contendo scripts Python maliciosos. Durante o processo de infecção, a execução desses scripts permitia o download e a instalação do AsyncRAT, concedendo aos atacantes acesso remoto e persistente aos sistemas comprometidos. Além disso, a campanha se beneficiava de técnicas de ofuscação e do uso de serviços amplamente confiáveis, como armazenamento em nuvem e túneis de proxy, para enganar os mecanismos de segurança e induzir as vítimas a acreditarem na legitimidade dos arquivos maliciosos antes de executá-los.

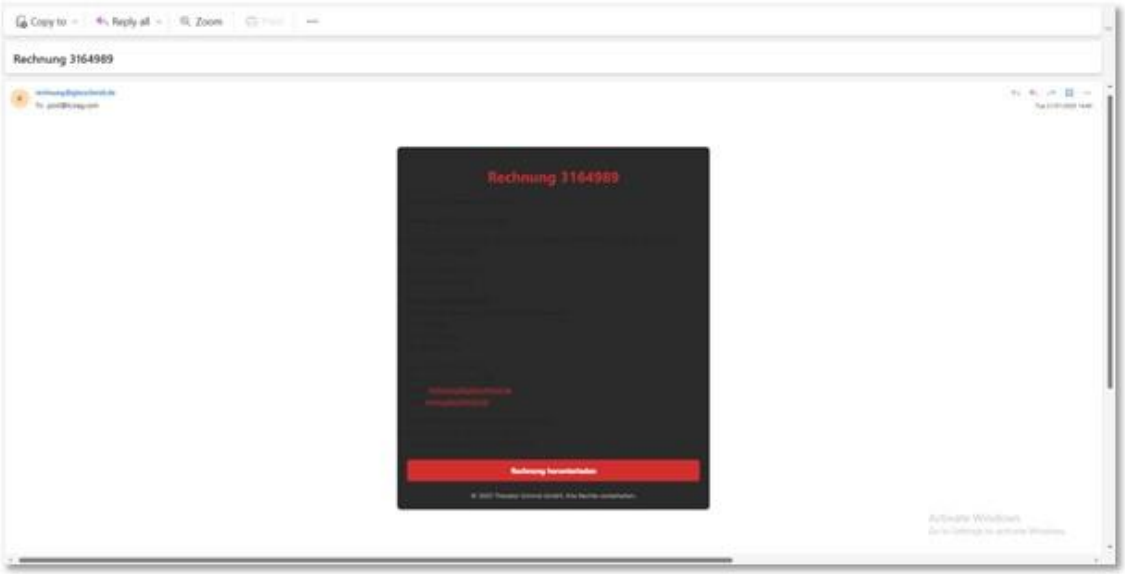


Figura 2 – E-mail de phishing AsyncRAT.

A ameaça representada pelo AsyncRAT Reloaded é altamente sofisticada e demanda atenção por parte das organizações, especialmente aquelas que dependem de ambientes baseados em nuvem e ferramentas de colaboração remota. Suas capacidades avançadas de acesso remoto, captura de credenciais e exfiltração de dados, combinadas com uma distribuição furtiva via serviços legítimos, tornam essa ameaça uma preocupação crítica. As organizações devem adotar medidas proativas de segurança, como restrição de execução de scripts não assinados, monitoramento de tráfego anômalo e reforço de autenticação multifator (MFA). Além disso, a capacitação dos funcionários sobre riscos de phishing e engenharia social é essencial para reduzir as chances de comprometimento.

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
Initial Access	T1566.001: Phishing: Spearphishing Attachment	Os atacantes enviam e-mails de phishing contendo links para arquivos ZIP maliciosos hospedados no Dropbox. Quando o destinatário clica no link, um arquivo ZIP é baixado, contendo um arquivo de atalho da internet no formato .URL.
Execution	T1204.002: User Execution: Malicious File	Ao abrir o arquivo .URL, o usuário inicia uma cadeia de downloads e execuções de arquivos maliciosos, incluindo arquivos .LNK, .JS e .BAT, que culminam na execução de scripts Python que instalam o AsyncRAT.
Defense Evasion	T1070.004: Indicator Removal on Host: File Deletion	Os scripts maliciosos podem excluir arquivos temporários ou evidências de sua presença para dificultar a detecção.
Defense Evasion	T1562.001: Impair Defenses: Disable or Modify Tools	Os atacantes podem desativar ou modificar ferramentas de segurança no sistema comprometido para evitar a detecção.
Persistence	T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	O AsyncRAT pode se configurar para iniciar automaticamente através de chaves de registro ou pastas de inicialização, garantindo persistência no sistema infectado.
Command and Control	T1105: Ingress Tool Transfer	Os atacantes utilizam serviços legítimos como Dropbox e TryCloudflare para transferir ferramentas e cargas maliciosas para o sistema da vítima.
Command and Control	T1071.001: Application Layer Protocol: Web Protocols	O AsyncRAT se comunica com seus servidores de comando e controle (C2) usando protocolos web, facilitando a exfiltração de dados e o recebimento de comandos.

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 da referida *ameaça*, como por exemplo:

Implementar autenticação multifator (MFA)

- A ativação da mfa reduz a possibilidade de comprometimento de contas caso credenciais sejam roubadas pelo malware.

Restringir execução de scripts não assinados

- Bloquear a execução de arquivos .js, .bat e .lnk de fontes desconhecidas impede a ativação da cadeia de infecção.

Monitorar acessos e tráfego anômalo

- Identificar conexões suspeitas para domínios do trycloudflare e outras infraestruturas maliciosas ajuda a detectar atividades incomuns.

Treinar funcionários contra phishing

- Conscientização sobre ataques de engenharia social reduz a probabilidade de que usuários interajam com e-mails e links maliciosos.

Reforçar políticas de segurança de e-mail

- Implementar filtros avançados, como dmarc, spf e dkim, dificulta a entrega de e-mails de phishing com links maliciosos.

Utilizar soluções de detecção e resposta (EDR)

- Ferramentas EDR avançadas ajudam a identificar e conter a execução do asyncrat antes que ele comprometa o sistema.

Bloquear downloads de fontes não verificadas

- Impedir downloads automáticos de arquivos do dropbox e outros serviços em nuvem reduz o risco de execução inadvertida de malware.

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:	1c2e6b9e143c1f41cf65600238c14980
sha1:	0aa1b8fba8d7bd19a0064edfdf86c027da253644
sha256:	7f7a5acf4507d48c8bc390ccdaea5df5cdbae014f1c1903e89603a92a2812030
File name:	RE-002.pdf.lnk

Indicadores do artefato	
md5:	1f621e5ba1138932edddb275f97b8244
sha1:	659ecdeb19b8e49be61fe41e8796d1215272b16e
sha256:	d7b1c6b33c34c2c154f2a084c7c3b71b01b50143e301fd87ab27e2ce67e3dc2b
File name:	ll.js

Indicadores do artefato	
md5:	ef30409462adb50d1966becdfd5a4347
sha1:	cd61de9e4003ba568ae76f064935addb106a6d6d
sha256:	50a72cee1a6be26102903c4e9e9450c66e8121f7e1f85541bbfab0edd0225338
File name:	cq.bat.txt

Tabela 2 – Indicadores de Comprometimento

5.2 INDICADORES DE URL, IPS E DOMÍNIOS

Indicadores de URL, IPs e Domínios	
URL	hxxps[:]//inventory-card-thumbzilla-ip[.]trycloudflare[.]com/DE/ hxxps[:]//mercy-synopsis-notify-motels[.]trycloudflare[.]com/ma[.]zip hxxp[:]//sufficiently-points-est-minimize[.]trycloudflare[.]com/ma[.]zip
IP	62[.]60[.]190[.]141 62[.]60[.]190[.]196

Tabela 3 – Indicadores de Comprometimento 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**
- **Forcepoint**
- **Thehackernews**

7 AUTORES

- **Leonardo Oliveira**

heimdall
security research
A DIVISION OF ISH