TLP: CLEAR

BOLETIM DE SEGURANÇA

Nova campanha com TorNet Backdoor e outros malwares

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

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:

- *Instituições financeiras*
- *Empresas de manufatura*
- *Empresas de logística*
- *Tecnologia e serviços de TI*
- *Setor governamental*
- *Organizações públicas*
- *Setor de saúde*
- *Setor de educação e pesquisa*

2.2 IMPACTO FINANCEIRO POTENCIAL

- *Roubo de dados sensíveis e propriedade intelectual*
- *Interrupção das operações comerciais*
- *Custos associados à resposta a incidentes e remediação*
- *Danos à reputação da empresa*
- *Multas e penalidades por não conformidade*
- *Fraudes e perdas financeiras diretas*
- *Danos à reputação e perda de clientes*
- *Extorsão e ransomware como consequência*

2.3 OBJETIVO DA AMEAÇA

O objetivo da ameaça é obter acesso não autorizado a sistemas corporativos e exfiltrar informações sensíveis para fins financeiros e de espionagem. A abordagem visa **fraudar empresas, interromper operações e causar prejuízos financeiros às vítimas**.

3 TÁTICO

3.1 INFORMAÇÕES SOBRE A AMEAÇA

A ameaça identificada pela Cisco utiliza **e-mails de phishing** como vetor inicial, enviando anexos maliciosos no formato **“.tgz”** que contêm arquivos executáveis camuflados. Quando abertos, esses arquivos ativam um **loader .NET**, responsável por baixar e executar o malware **PureCrypter**, que atua como distribuidor de payloads adicionais. Entre os principais malwares entregues estão o **Agent Tesla e o Snake Keylogger**, utilizados para capturar credenciais e registrar atividades do usuário. Além disso, um **novo backdoor chamado TorNet** foi identificado, operando dentro da rede TOR para dificultar a detecção e monitoramento por soluções de segurança. O **backdoor TorNet** permite aos atacantes manter acesso persistente ao sistema infectado, receber comandos remotamente e executar cargas maliciosas diretamente na memória do dispositivo, evitando rastros em disco. A comunicação C2 via **rede TOR** dificulta a interceptação do tráfego, tornando a remoção da ameaça mais complexa. Os atacantes exploram essas técnicas para exfiltrar dados, realizar movimentação lateral e até implantar **ransomware** em fases futuras do ataque. O impacto potencial inclui **roubo de informações financeiras e corporativas, interrupção operacional e danos à reputação** das empresas afetadas.

3.2 OPERAÇÃO E CAPACIDADE DA AMEAÇA

O backdoor TorNet possui capacidades de se conectar à máquina da vítima à rede TOR para comunicações C2 furtivas, recebendo e executando assemblies .NET arbitrários na memória da vítima, permitindo a execução de código malicioso adicional sem deixar rastros no disco, o malware executa diversas ações maliciosas:

Persistência

- Criação de uma tarefa agendada no Windows para manter o acesso, incluindo em endpoints com bateria fraca.

Evasão de detecção

- Desconexão da máquina da vítima da rede antes de implantar o payload e reconexão posterior, evitando a detecção por soluções antimalware baseadas em nuvem.

Comunicação segura

- Uso da rede TOR para comunicações C2, dificultando a interceptação e análise do tráfego.

As intrusões identificadas têm início por meio de e-mails de phishing, que servem como vetor primário de infecção. O agente de ameaça se disfarça de

instituições financeiras e empresas dos setores de manufatura e logística, enviando falsos comprovantes de transferência bancária e recibos de pedidos fraudulentos. A maioria dessas mensagens está escrita em polonês e alemão, sugerindo que o alvo principal são usuários desses países. No entanto, também foram identificadas amostras em inglês, indicando uma possível ampliação do alcance da campanha. Com base no conteúdo dos e-mails e nos nomes dos arquivos anexados, avalia-se com confiança média que o motivador principal do agente é financeiro.

Os e-mails maliciosos contêm anexos com a extensão ".tgz", demonstrando o uso do GZIP para compactar um arquivo TAR que abriga o malware. Essa técnica tem como objetivo mascarar o verdadeiro conteúdo do anexo e evitar detecções por soluções de segurança de e-mail. Ao descompactar o arquivo, a vítima acaba executando o código malicioso, permitindo que o invasor obtenha acesso ao sistema e inicie a infecção.

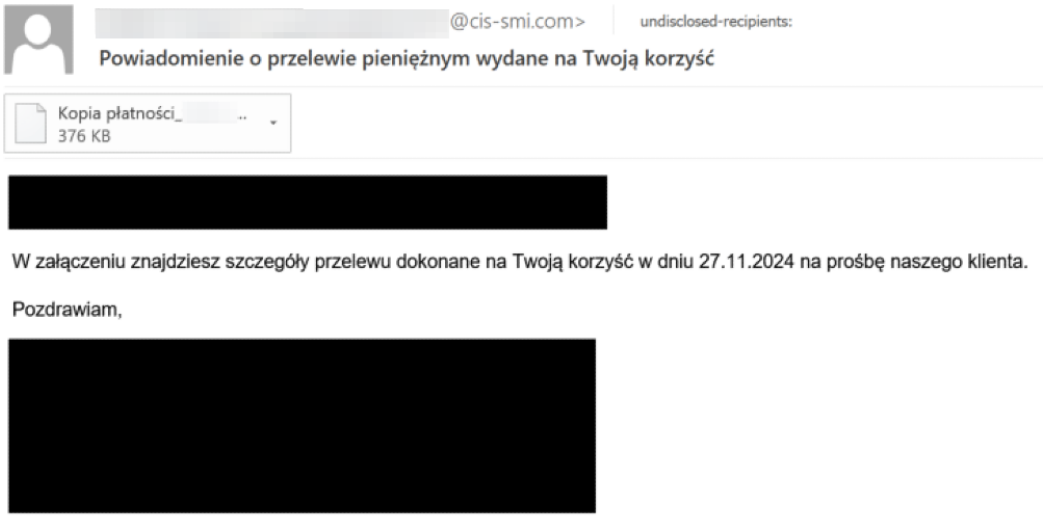

Figura 1 – Exemplo de e-mail de phishing em polonês.

Figura 2 – Exemplo de e-mail de phishing em alemão.

Quando a vítima abre o anexo de e-mail compactado, descompacta manualmente os arquivos e executa o carregador .NET, o sistema é instruído a baixar o malware PureCrypter criptografado a partir de um servidor comprometido. O loader então descriptografa e executa o PureCrypter diretamente na memória, evitando a criação de arquivos no disco e dificultando a detecção por soluções de segurança.

Em algumas das intrusões observadas nesta campanha, o PureCrypter também instala e executa o backdoor TorNet. Esse backdoor estabelece comunicação com o servidor de comando e controle (C2) e conecta a máquina comprometida à rede TOR, ocultando o tráfego malicioso. Além disso, ele possui a capacidade de baixar e executar dinamicamente assemblies .NET na memória da vítima, expandindo as possibilidades de ataque e facilitando a introdução de novas cargas maliciosas no ambiente infectado.

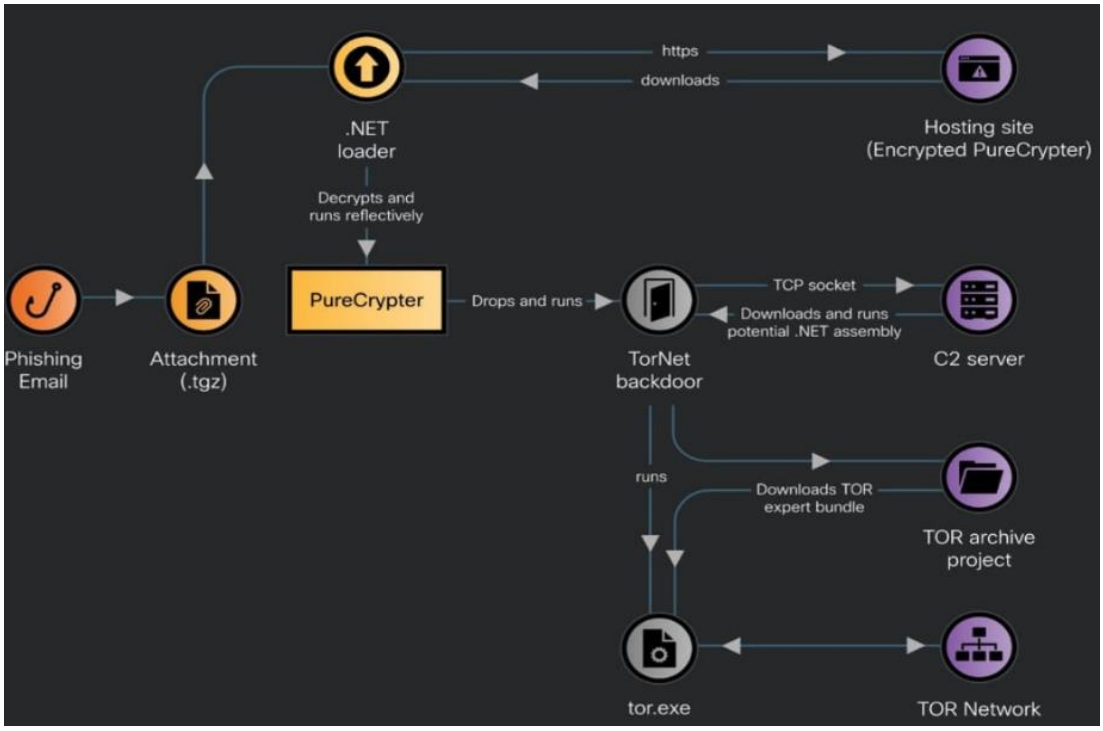

Figura 3 – Fluxo de ataque da ameaça.

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 invasores utilizam e-mails de phishing com anexos maliciosos para enganar os usuários e induzi-los a executar o malware.
Execution	T1204.002 - User Execution: Malicious File	A execução do malware depende da ação do usuário ao abrir manualmente o anexo malicioso recebido por e-mail.
Execution	T1053.005 - Scheduled Task/Job: Scheduled Task	Os atacantes criam tarefas agendadas no Windows para manter a persistência no sistema comprometido, garantindo que o malware seja executado mesmo após reinicializações.

Defense Evasion	T1562.001 - Impair Defenses: Disable or Modify Tools	Os invasores desconectam a máquina da vítima da rede antes de implantar o payload e a reconectam posteriormente, evitando a detecção por soluções de segurança baseadas em nuvem.
Command and Control	T1090.003 - Proxy: Multi-hop Proxy	O backdoor TorNet conecta a máquina da vítima à rede TOR para estabelecer comunicações de comando e controle (C2) de forma furtiva, dificultando a detecção e rastreamento.

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:

Treinamento e conscientização sobre phishing

- Realizar treinamentos periódicos para funcionários, ensinando-os a reconhecer e-mails suspeitos, principalmente aqueles com anexos de formatos incomuns como ".tgz".
- Simular campanhas de phishing para reforçar boas práticas de segurança.

Filtragem e bloqueio de e-mails maliciosos

- Implementar filtros avançados de e-mail para detectar anexos maliciosos e bloquear mensagens suspeitas.
- Configurar políticas de DMARC, DKIM e SPF para evitar spoofing de e-mails.

Restrições de execução de arquivos e macros

- Configurar políticas de segurança para bloquear a execução de arquivos desconhecidos e restringir a execução de macros em documentos recebidos por e-mail.
- Desativar a execução automática de arquivos compactados baixados da internet.

Monitoramento de atividades e detecção de anomalias

- Implementar soluções de EDR (Endpoint Detection and Response) para detectar e bloquear atividades suspeitas, como criação de tarefas agendadas incomuns.
- Monitorar acessos à rede TOR e comunicações com servidores suspeitos.

Restrição de downloads e execução de arquivos em .NET

- Configurar restrições para impedir a execução automática de arquivos baixados de fontes não confiáveis.
- Monitorar o uso do .NET Loader, já que é um vetor utilizado para carregar o PureCrypter diretamente na memória.

Segmentação de rede e controle de comunicação C2

- Implementar segmentação de rede para evitar a movimentação lateral de malwares.
- Monitorar e restringir conexões de saída para a rede TOR e servidores suspeitos.

Atualizações e políticas de patching

- Manter sistemas operacionais, navegadores e softwares de segurança sempre atualizados para reduzir vetores de ataque.
- Aplicar patches de segurança regularmente para mitigar vulnerabilidades que possam ser exploradas em futuras campanhas maliciosas.

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:	904b3876526c1f765c93b330d229a1a2
sha1:	8abe037a0b7589f5e802c5e4a397d5252d3fcfb7
sha256:	9d33726fc1d39fdc0426c70ed0cfb515e15f50d39c46d8ff38025b4faf8811dc
File name:	Nkzhwtuma.exe

Indicadores do artefato	
md5:	904b3876526c1f765c93b330d229a1a2
sha1:	8abe037a0b7589f5e802c5e4a397d5252d3fcfb7
sha256:	9d33726fc1d39fdc0426c70ed0cfb515e15f50d39c46d8ff38025b4faf8811dc
File name:	Nkzhwtuma.exe

Indicadores do artefato	
md5:	4f304e815ea78124d44f1bf77f3b611c
sha1:	bc3afdb81424a106f3d75869e9a5019c8575d075
sha256:	75d2d368d735fca2bad0155510cb4a927f7f246ea72299395990027264056521
File name:	Lbpcok.exe

Tabela 2 – Indicadores de Comprometimento

5.2 INDICADORES DE URL, IPS E DOMÍNIOS

Indicadores de URL, IPs e Domínios	
URL	hxxps[://]sanel[.]net[.]pl hxxps[://]cud-senegal[.]org
Domínio	Italzformendinggallores[.]duckdns[.]org humblecrazeforeal8897[.]accesscam[.]org sertiscoppersail432[.]freeddns[.]org moristaetdfertal9002[.]ddnsgeek[.]com paradoncalleke5689[.]camdvr[.]org greeslieforreallcul5672[.]casacam[.]net blissfulzeroooooos690[.]ddnsfree[.]com www.blissfulzeroooooos690[.]ddnsfree[.]com

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**
- **Talos**
- **MITRE ATT&CK**
- **Thehackernews**

7 AUTORES

- **Leonardo Oliveira**

heimdall
security research
A DIVISION OF ISH