
# BOLETIM DE SEGURANÇA

## Malware FrostyGoop: Ameaça contra infraestrutura crítica, explorando o protocolo Modbus

heimdall
security research
A DIVISION OF ISH

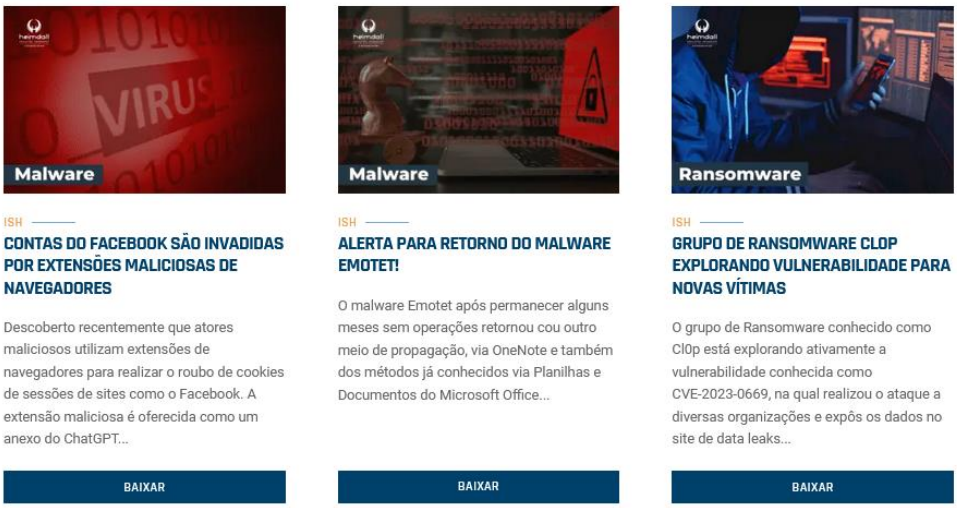
TLP: CLEAR

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 FIGURAS

# 1 SUMÁRIO EXECUTIVO

A empresa de segurança cibernética industrial Dragos divulgou na terça-feira um relatório sobre o malware **FrostyGoop**, um novo malware focado em sistemas de controle industrial (**ICS**). Este é o primeiro malware empregar comunicações **Modbus TCP** para afetar operações de tecnologia operacional (OT). O FrostyGoop foi inicialmente detectado pela Dragos em abril deste ano e tem a capacidade de interagir diretamente com ICS por meio do protocolo Modbus, amplamente utilizado em setores industriais e organizações ao redor do mundo. Isso o torna uma ameaça séria para instalações de infraestrutura crítica em diversos setores.

# 2 DETALHES SOBRE A AMEAÇA

O FrostyGoop pode interagir diretamente com o ICS usando Modbus, um protocolo ICS padrão em todos os setores industriais e organizações em todo o mundo. Ele pode ler e gravar em um dispositivo ICS contendo registros contendo entradas, saídas e configuração dados, aceita argumentos opcionais de execução de linha de comando, usa arquivos de configuração separados para especificar o destino, endereços IP e comandos Modbus e registros de saída para um console e/ou um arquivo JSON.

**Protocolo Modbus**

Modbus é um protocolo de comunicação cliente/servidor desenvolvido para controladores lógicos programáveis (PLCs) da Modicon em 1979, mas que hoje é amplamente utilizado por diversos dispositivos. Este protocolo é aberto e independente de hardware, tornando-se uma escolha popular para comunicação entre PLCs, sistemas de controle distribuído (DCS), controladores, sensores, atuadores, dispositivos de campo e interfaces. O protocolo Modbus define uma estrutura de mensagens que os controladores podem reconhecer e utilizar, independentemente do tipo de redes por meio das quais se comunicam. O protocolo especifica como cada controlador deve identificar o endereço de seu dispositivo, reconhecer uma mensagem destinada a ele, determinar a ação necessária e extrair quaisquer dados ou informações adicionais contidos na mensagem. Se uma resposta for necessária, o controlador criará e transmitirá a mensagem de resposta utilizando o protocolo Modbus.

**Capacidades ICS do malware**

Conforme análise da Dragos o malware possui as seguintes capacidades:

- Aceita argumentos opcionais de execução de linha de comando.
- Usa arquivos de configuração separados para especificar endereços IP de destino e comandos Modbus.
- Comunica-se com dispositivos ICS através do protocolo Modbus TCP.
- Envia comandos Modbus para ler ou modificar dados em dispositivos ICS.
- Registra a saída em um console ou arquivo JSON.

# 3 ARGUMENTOS OPCIONAIS ACEITOS PELO FROSTYGOOP

O malware FrostyGoop verifica se o executável está sendo executado com os argumentos necessários na linha de comando. Se não forem fornecidos argumentos, os binários encerram a execução. Embora os argumentos específicos possam variar conforme o exemplo, a funcionalidade permanece a mesma. As informações necessárias para iniciar uma conexão TCP e enviar comandos Modbus para um dispositivo ICS alvo podem ser especificadas como argumentos

de linha de comando ou contidas em um arquivo de configuração JSON separado. Os argumentos aceitos pelo FrostyGoop podem incluir dados como:

- Endereços IP especificando o dispositivo de destino com o qual se comunicar.
- Uma opção de "mode" que se correlaciona com um comando Modbus para executar no dispositivo ICS ((Read Holding Registers, Write to Single Holding Register, Write to Multiple Holding Registers).
- Um endereço de registro Modbus no dispositivo ICS de destino para enviar comandos Modbus.
- Um nome de arquivo de configuração JSON; existem dois arquivos de configuração diferentes aceitos pelo FrostyGoop, que são os seguintes:
    - Um arquivo de configuração contendo informações do dispositivo vítima, como endereço IP, comandos Modbus e endereços de registro Modbus.
    - Um arquivo de configuração contendo um horário específico para iniciar as comunicações Modbus TCP com o dispositivo vítima e vários comprimentos para atrasar a execução de comandos Modbus.
- Especificação de um nome de arquivo para salvar a saída de registro.

**Arquivo de configuração**

| Field | Description |
|---|---|
| **Code** | Modbus Command Code (i.e. '3' for Read Holding Registers, '6' for Write Single Holding Register, and '16' for Write Multiple Holding Registers) |
| **Address** | Modbus register address |
| **Count** | Quantity of registers to read or write |
| **Value** | Integer used to modify the Holding Register (used for Modbus 'write holding register' commands) |

*Figura 1 – Campos do arquivo de configuração.*

O FrostyGoop aceita um arquivo de configuração em formato JSON que contém as informações necessárias para executar comandos Modbus em um dispositivo alvo. O malware lê o arquivo, analisa os dados JSON, conecta-se ao endereço IP especificado no arquivo e envia comandos Modbus TCP para os registros indicados no arquivo de configuração. A Dragos descobriu uma amostra desse arquivo de configuração chamado 'task_test.json'. O endereço IP presente na amostra de arquivo de configuração pertence a um dispositivo de controle ENCO. Dispositivos de controle ENCO são geralmente utilizados para controle de processos em sistemas de aquecimento urbano, água quente e ventilação, monitorando parâmetros de sensores de temperatura, pressão e isolamento.

# 4 ANÁLISE DO TRÁFEGO DA REDE MODBUS

O malware inicia a comunicação com o endereço IP alvo através da porta Modbus TCP 502. Esse endereço IP pode ser especificado como um argumento durante a execução do malware ou incluído no arquivo de configuração JSON. Uma vez que a conexão é estabelecida, FrostyGoop envia comandos Modbus para o dispositivo. Após o envio dos comandos e a recepção das respostas do dispositivo alvo, os binários encerram a conexão e finalizam a execução. Os binários FrostyGoop utilizam uma biblioteca Go Modbus obtida de um repositório público no Github.

O FrostyGoop implementa três comandos Modbus:

- Command Code 3 ‘Read Holding Registers': Usado para ler o valor atualmente em uma retenção Modbus registro (ou bloco contíguo de registros de retenção).
- Command Code 6 ‘Write Single Register’: Usado para escrever um valor em um registrador de retenção.
- Command Code 16 ‘Write Multiple Holding Registers’: Usado para escrever um valor em um bloco de registros contíguos.]

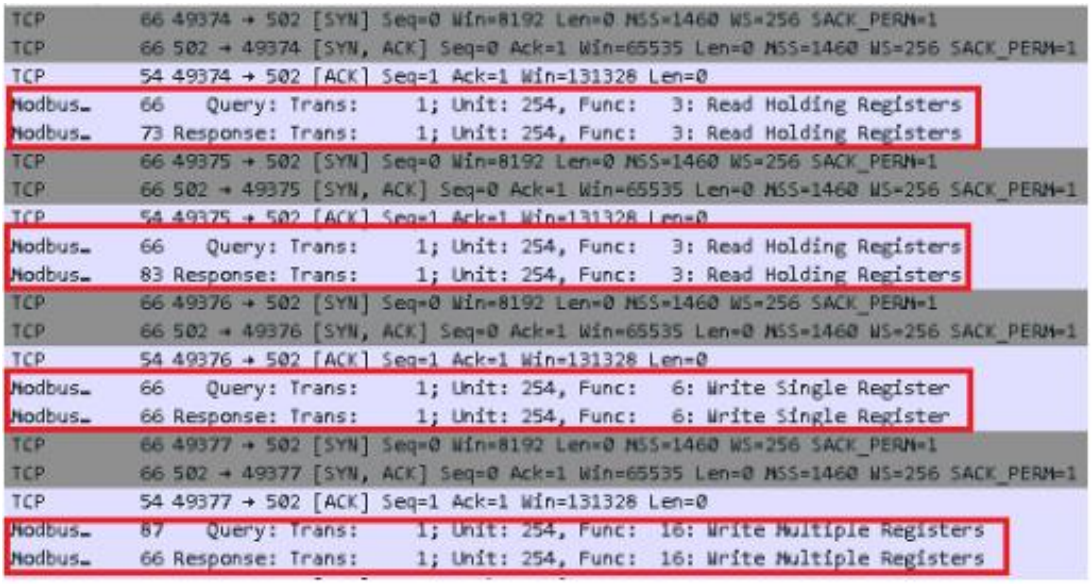



*Figura 2 – Exemplo de tráfego de rede Modbus TCP entre o FrostyGoop e um dispositivo de destino.*

# 5 REGISTROS

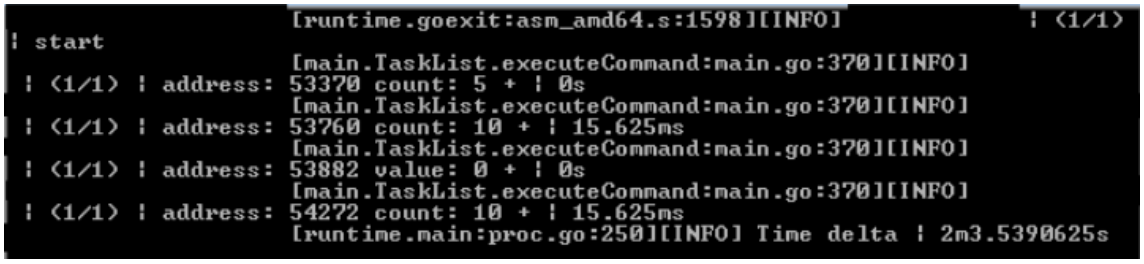



*Figura 3 – Exemplo de registro do console do FrostGoop.*

Os binários FrostyGoop registram as comunicações Modbus TCP com o endereço IP de destino em um console do Windows e em um arquivo JSON. Após a execução, FrostyGoop abre uma janela de console. Se for especificado um argumento para registro ao executar o binário, a saída é registrada em um arquivo JSON. Abaixo está um exemplo de saída para a janela do console durante as comunicações Modbus TCP com um dispositivo. Quando os binários estão prontos para iniciar as comunicações com o dispositivo de destino, eles registram a hora e a data locais, o endereço IP de destino no início das comunicações e a string 'start' na janela do console. Em seguida, quando FrostyGoop envia comandos, ele registra o registro de retenção, o número de registros, o tempo de resposta, e a resposta do dispositivo para cada comando. Se a resposta do dispositivo contiver uma exceção, FrostyGoop registra um sinal de menos. Um exemplo de quando um dispositivo enviaria uma exceção ao malware seria se o registro de retenção não existisse.

Por fim, e não menos importante, conforme os pesquisadores, a investigação apontou que os atacantes provavelmente conseguiram acessar a rede da vítima explorando uma vulnerabilidade desconhecida em um roteador **Mikrotik** exposto externamente. Os componentes da rede, como o roteador Mikrotik, quatro servidores de gerenciamento e controladores do sistema de aquecimento distrital, não estavam devidamente segmentados, o que facilitou a execução do ataque.

# 6 CONCLUSÃO

Dada a utilização generalizada de dispositivos Modbus em todo o mundo, a ampla aplicabilidade desta ameaça sublinha a necessidade urgente de necessidade de visibilidade da rede ICS e monitoramento do tráfego Modbus. Detectando e sinalizando desvios do normal comportamento e identificar padrões de ataque e comportamentos que exploram o protocolo Modbus é crucial pois isto representa um risco significativo para a integridade e funcionalidade dos dispositivos ICS, com consequências potencialmente de longo alcance para as operações industriais e segurança Pública.

# 7 REGRAS DE DETECÇÃO ANALÍTICA PARA PROTOCOLO MODBUS (ICS)

A tabela abaixo serve como referência para profissionais de segurança cibernética e administradores de sistemas de controle industrial para monitorar e responder a atividades suspeitas ou maliciosas que envolvem o protocolo Modbus.

| SID/Rule | Analytic Name | Description | Knowledge Pack |
|---|---|---|---|
| a0ddb920-0adc-4d01-9b3d-21414ef28607 | Modbus Command Force Listen Only Mode | Modbus command to put device into Force Listen Only Mode, making the device unresponsive to commands. It will only respond after power up. This can be used maliciously to effectively disable devices. | KP_Plus-7.0.X |
| f7a0af6b-fa88-4382-9232-f56525befcde | Modbus Command Restart Communications Option | Modbus command to force a device to restart, making it unresponsive until it reboots. There is some chance this could be used maliciously to disable devices. | KP_Plus-7.0.X |
| f41c99e6-cabf-46b7-9576-d2ac4676baa9 | Modbus Exception | Modbus servers send exception codes to Modbus clients when a requested operation cannot be carried out. This characterization summarizes exception codes sent from a Modbus server. | KP_Plus-6.0.X |
| e8cbde89-aa3a-4093-8064-3a8ca08fbf4c | Modbus External Comms | External device communicating with an internal asset using the Modbus protocol. This is a major security concern, as ICS devices should not be controlled outside of the OT network. | KP-2020-11 |
| 15c07ad4-5d03-4c3b-8d2d-613d5ec45217 | Modbus External Write | External device writing to an internal asset using the Modbus protocol. This is a major security concern, as ICS devices should not be controlled outside of the OT network. | KP-2020-11 |
| 3cc434cd-5086-454c-bbd4-6142b01a4623 | Modbus Write Observed for First Time | Modbus traffic with a write function code seen for the first time to a specific host. | KP-2022-009 |
| d323014b-abee-461b-a12f-641b8796070f | New ModbusTCP Detection | Monitors for new devices using the ModbusTCP protocol and generates events when activity is seen | KP-2020-11 |

*Figura 4 – Regras de detecção analíticas Modbus.*

Abaixo destacamos um resumo das colunas e do que elas representam na imagem:

**SID/Rule**: Identificador único para cada regra analítica.
**Analytic Name**: Nome da análise ou regra específica relacionada ao protocolo Modbus.
**Description**: Descrição detalhada do que cada regra faz, incluindo o comportamento malicioso ou anômalo que ela detecta.
**Knowledge Pack**: Identificador do pacote de conhecimento que inclui esta regra, indicando a versão ou o conjunto específico de regras a que pertence.

1. **a0ddb920-0adc-4d01-9b3d-21414ef28607**

**Nome**: Modbus Command Force Listen Only Mode

**Descrição**: Comando Modbus para colocar o dispositivo no modo Force Listen Only, tornando o dispositivo não responsivo a comandos até ser reiniciado. Pode ser usado maliciosamente para desativar dispositivos.

**Knowledge Pack**: KP_Plus-7.0.X

2. **f7a0af6b-fa88-4382-9232-f56255befcde**

**Nome**: Modbus Command Restart Communications Option

**Descrição**: Comando Modbus para forçar o reinício do dispositivo, tornando-o não responsivo até reiniciar. Pode ser usado maliciosamente para desativar dispositivos.

**Knowledge Pack**: KP_Plus-7.0.X

3. **f41c99e6-cabf-46b7-9576-d2ac4676baa9**

**Nome**: Modbus Exception

**Descrição**: Servidores Modbus enviam códigos de exceção para clientes Modbus quando uma operação solicitada não pode ser realizada. Resume os códigos de exceção enviados de um servidor Modbus.

**Knowledge Pack**: KP_Plus-6.0.X

4. **e8cdbe89-aa3a-4093-8064-3a8ca08fbf4c**

**Nome**: Modbus External Comms

**Descrição**: Dispositivo externo comunicando-se com um ativo interno usando o protocolo Modbus. É uma grande preocupação de segurança, pois dispositivos ICS não devem ser controlados fora da rede OT.

**Knowledge Pack**: KP-2020-11

5. **15c07d4d-5d03-4c3b-8d2d-613d5ec45217**

**Nome**: Modbus External Write

**Descrição**: Dispositivo externo escrevendo em um ativo interno usando o protocolo Modbus. É uma grande preocupação de segurança, pois dispositivos ICS não devem ser controlados fora da rede OT.

**Knowledge Pack**: KP-2020-11

6. **3cc434cd-5086-454c-bbd4-6142bd1a4623**

**Nome**: Modbus Write Observed for First Time

**Descrição**: Tráfego Modbus com um código de função de escrita visto pela primeira vez para um host específico.

**Knowledge Pack**: KP-2022-009

7. **d323014b-abee-461b-a72f-641b8796070f**

**Nome**: New ModbusTCP Detection

**Descrição**: Monitora novos dispositivos usando o protocolo ModbusTCP e gera eventos quando atividade é observada.

**Knowledge Pack**: KP-2020-11

# 8 RECOMENDAÇÕES

São elencadas abaixo pela ISH, medidas que poderão ser adotadas visando a mitigação da infecção do referido *malware*, como por exemplo:

**Arquitetura defensiva**

- Este ataque destaca a falta de segmentação de rede adequada e a presença de controladores expostos à Internet. Para combater ameaças como o FrostyGoop, uma arquitetura defensável deve ser implementada, priorizando o segmentação de ativos de rede. Isto inclui o estabelecimento de zonas industriais desmilitarizadas (DMZ), a aplicação controles rígidos de acesso entre a rede corporativa de TI e os ambientes de TO, e usando recursos físicos ou barreiras virtuais para impedir o acesso direto da Internet a sistemas críticos. Tais medidas limitariam a propagação do malware e restringir o raio de possíveis ataques cibernéticos.

**Visibilidade de monitoramento da rede ICS**

- O monitoramento contínuo do tráfego da rede TO, como as comunicações Modbus, é essencial para detectar e responder a anomalias e comportamentos de ameaça. No caso do FrostyGoop, ter um conjunto de ferramentas de monitoramento com reconhecimento de protocolo poderia ter identificado acesso não autorizado ou padrões incomuns de tráfego Modbus na porta 502, permitindo detecção e mitigação mais rápidas. Implementando uma solução de monitoramento abrangente.

**Acesso remoto seguro**

- O incidente FrostyGoop explorou vulnerabilidades associadas a pontos de acesso remoto. Acesso remoto seguro as proteções devem ser rigorosamente aplicadas para proteger contra ameaças semelhantes. Isso inclui a implantação de multifatores autenticação (MFA), garantindo que todas as conexões remotas sejam registradas e monitoradas e usando privacidade virtual redes (VPNs) para criptografar dados em trânsito. Além disso, o acesso remoto deve ser concedido mediante necessidade de utilização base com auditorias regulares para revisar direitos e privilégios de acesso.

**Resposta a incidente ICS**

- Dada a complexidade e a natureza direcionada do ataque FrostyGoop, um plano robusto de resposta a incidentes é crucial. Este plano deve incorporar respostas especializadas para ambientes de TO, uma vez que estes sistemas muitas vezes têm requisitos de continuidade operacional que substituem os sistemas de TI tradicionais. Para FrostyGoop, que diretamente interage com o ICS através de comandos Modbus, o plano de resposta deve incluir procedimentos para isolar rapidamente dispositivos

afetados, analisando o tráfego de rede em busca de comandos Modbus não autorizados e restaurando o sistema preciso. Treinamento e exercícios regulares específicos para ataques direcionados a Modbus e ICS também garantirão a preparação e gerenciamento eficaz de incidentes.

**Gestão de vulnerabilidades baseadas em risco**

- A gestão eficaz da vulnerabilidade, adaptada ao perfil de risco dos componentes do ICS, envolvendo avaliações para identificar e resolver vulnerabilidades que os adversários poderiam explorar. Mitigando vulnerabilidades de rede exploráveis, especialmente quando existem evidências de exploração ativa. Onde os patches não estão viáveis, controles compensatórios, como monitoramento aprimorado ou controles de acesso restritivos, mitigarão o riscos potenciais.

# 9 REFERÊNCIAS


- **Heimdall *by* ISH Tecnologia**
- **Report Dragos- FrostyGoop**

heimdall
security research
A DIVISION OF ISH