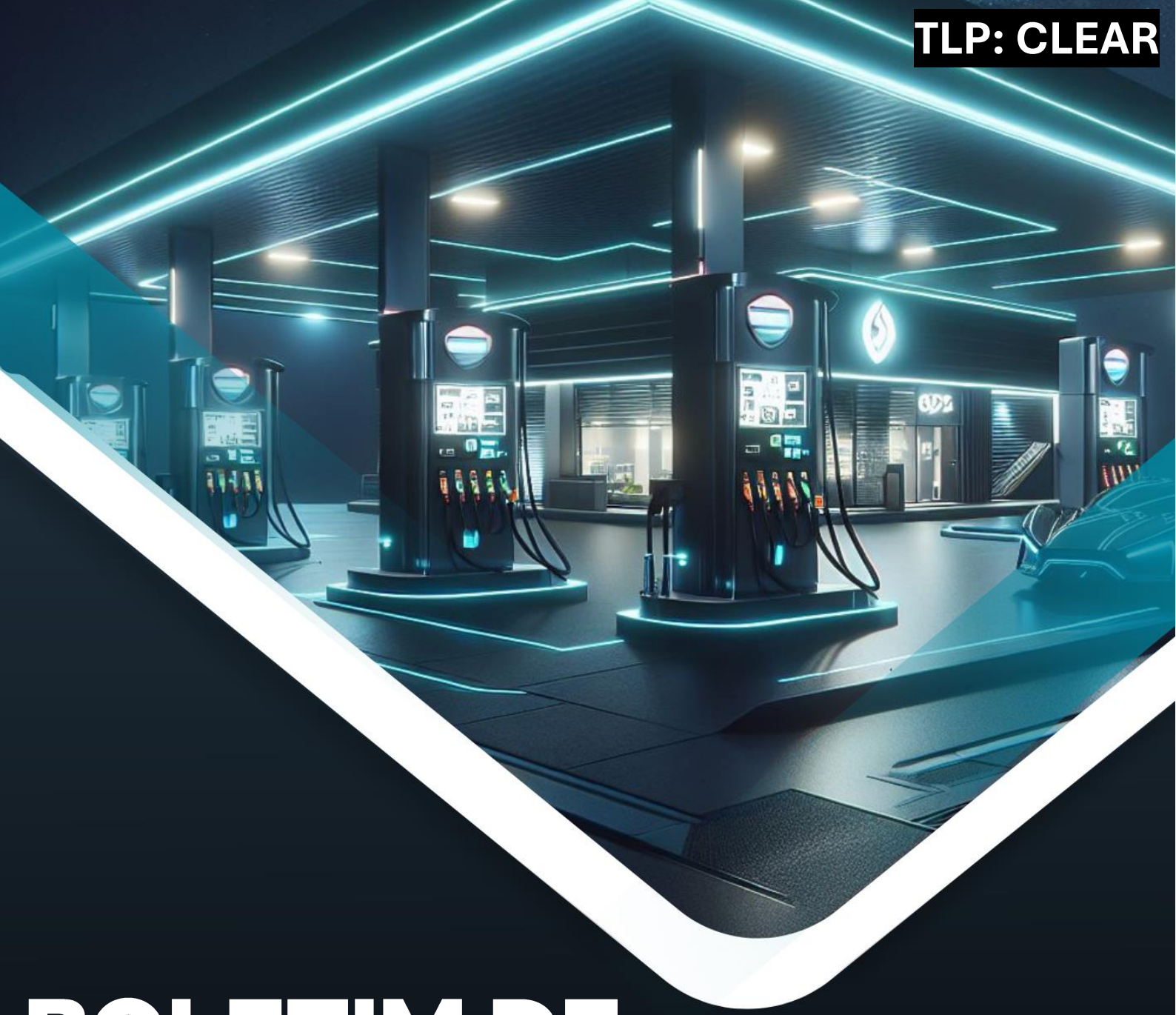
TLP: CLEAR



BOLETIM DE SEGURANÇA

IOCONTROL, novo malware com alvo de infraestruturas críticas

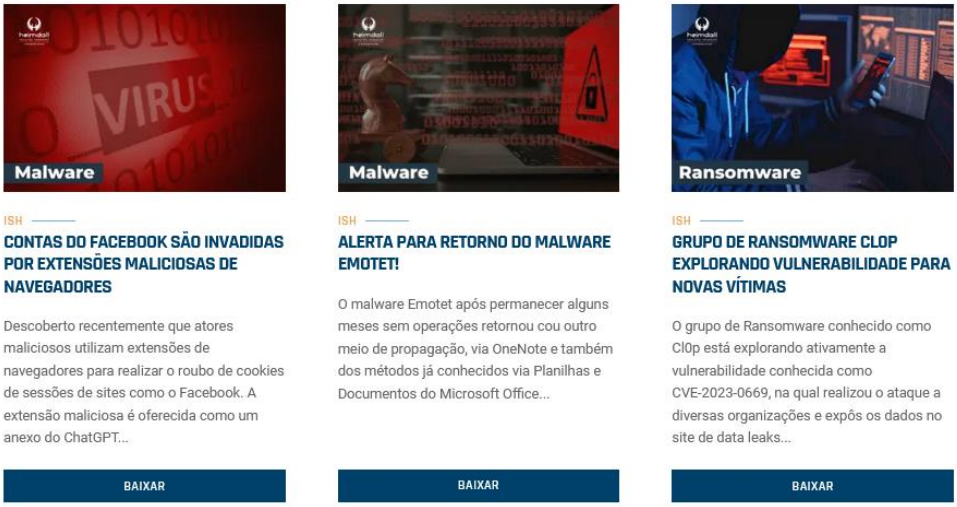
heimdall
security research

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 SUMÁRIO EXECUTIVO

Atores de ameaças iranianos estão empregando um novo malware chamado **IOCONTROL** para atacar dispositivos de Internet das Coisas (IoT) e sistemas OT/SCADA que operam em infraestruturas críticas localizadas em Israel e nos Estados Unidos. Entre os dispositivos-alvo estão roteadores, controladores lógicos programáveis (PLCs), interfaces homem-máquina (HMIs), câmeras IP, firewalls e sistemas de gerenciamento de combustível. O caráter modular do IOCONTROL permite que ele comprometa uma ampla gama de dispositivos de diferentes fabricantes, como D-Link, Hikvision, Baicells, Red Lion, Orpak, Phoenix Contact, Teltonika e Unitronics.

2 DETALHES DA AMEAÇA

Os pesquisadores que identificaram o malware IOCONTROL relatam que ele é uma arma cibernética desenvolvida por um estado-nação, com potencial para provocar interrupções graves em infraestruturas críticas. No atual cenário de tensões geopolíticas, o IOCONTROL está sendo empregado para atacar sistemas em Israel e nos Estados Unidos, incluindo plataformas de gerenciamento de combustível como Orpak e Gasboy. O malware foi associado ao grupo hacker iraniano conhecido como CyberAv3ngers, o qual já demonstrou interesse em comprometer sistemas industriais no passado. Além disso, há relatos recentes de que o grupo utiliza o ChatGPT da OpenAI para invadir PLCs, criar scripts de exploração personalizados em Bash e Python e planejar atividades pós-comprometimento.

Os ataques cibernéticos são mais uma manifestação do conflito geopolítico entre Israel e Irã. Acredita-se que o grupo conhecido como CyberAv3ngers esteja vinculado ao Comando Eletrônico Cibernético do Corpo da Guarda Revolucionária Islâmica (IRGC-CEC). Eles têm sido ativos no Telegram, divulgando capturas de tela e outras informações sobre as violações nos sistemas de combustível. Em fevereiro, o Departamento do Tesouro dos EUA impôs sanções a seis membros do IRGC-CEC associados aos CyberAv3ngers e ofereceu uma recompensa de US$ 10 milhões por informações que levem à identificação ou localização de qualquer pessoa envolvida nesses ataques.

Durante o mesmo período dos ataques às instalações de água, o grupo CyberAv3ngers afirmou no Telegram que havia comprometido 200 postos de gasolina em Israel e nos EUA, focando nos sistemas Orpak. Os hackers compartilharam capturas de tela do portal de gerenciamento dos postos afetados, além de bancos de dados contendo informações sobre os alvos e dados vazados.

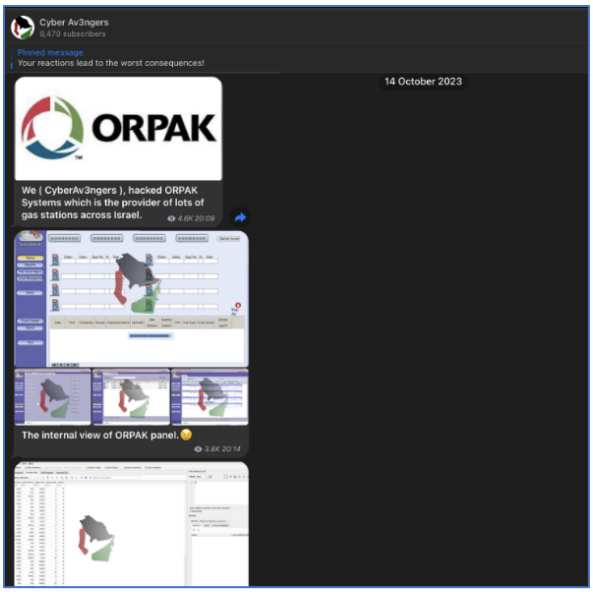


Figura 1 – Captura de tela do canal CyberAv3ngers no Telegram.

O grupo CyberAv3ngers afirmou ter invadido os sistemas da Orpak. Registros WHOIS mostram que o domínio **tylarion867mino[.]com** foi registrado em novembro de 2023, supostamente para criar uma infraestrutura de comando e controle para gerenciar dispositivos comprometidos. Em dezembro de 2023, um grupo de hackers ligado a Israel, conhecido como Gonjeshke Darande, declarou ter atacado e comprometido 70% dos postos de gasolina no Irã, alegando que a ação foi uma retaliação contra a agressão da República Islâmica e seus aliados na região.

A análise do IOCONTROL focou em dispositivos do sistema Orpak Fuel. O hash da amostra analisada é: **1b39f9b2b96a6586c4a11ab2fdbff8fdf16ba5a0ac7603149023d73f33b84498**. Ela continha um GUID interno, utilizado para identificar uma entidade vítima: **855958ce-6483-4953-8c18-3f9625d88c27**.

Ao descompactar o malware com êxito, obtive-se dois artefatos, uma seção de dados criptografados e um executável. Na análise do executável, observou-se que ele utiliza dados da seção criptografada em várias partes do código, empregando-os para diversas operações, como um caminho de arquivo e um endereço IP para conexão. Na função de descriptografia, o malware identifica o primeiro byte da configuração criptografada. Esse byte inicial determina o tamanho da configuração criptografada específica. Após ler os bytes brutos dessa configuração, o malware utiliza o esquema de descriptografia AES-256-CBC para decodificar e obter a configuração real.

```
14  data_in_1 = data_in;
15  v12 = data_size;
16  data_out_1 = data_out;
17  key = get_env("0_0");
18  iv = get_env("0_1");
19  v8 = EVP_CIPHER_CTX_new();
20  v3 = EVP_aes_256_cbc();
21  EVP_DecryptInit_ex(v8, v3, 0, key, iv);
22  EVP_DecryptUpdate(v8, data_out_1, &v7, data_in_1, v12);
23  v5 = v7;
24  EVP_DecryptFinal_ex(v8, data_out_1 + v7, &v7);
25  v6 = v5 + v7;
26  EVP_CIPHER_CTX_free(v8);
27  return v6;
```

Figura 2 – Rotina de descriptografia de configuração, pegando o par chave/IV das variáveis de ambiente.

Antes de se conectar à infraestrutura C2, o malware inicialmente instala um backdoor no dispositivo para assegurar sua persistência. Para isso, ele adiciona um novo script de inicialização em rc3.d, que será executado a cada reinicialização do dispositivo. O backdoor está localizado em /etc/rc3.d/S93InitSystemd.sh e contém o seguinte script bash:

```
trap "rm -f $iocpid" EXIT
while true; do
if ! pidof "iocontrol" > /dev/null; then
```

```
    iocontrol >/dev/null 2>&1 &
fi
    sleep 5
done
```

Tabela 1 – Script de inicialização.

Depois de converter o nome do host em um endereço IP, o malware utiliza o segundo parâmetro de configuração, 8883, como a porta para se conectar ao C2. A porta 8883 é comumente associada ao protocolo de comunicação MQTTs. Ao analisar o código mais a fundo, verificamos que o malware de fato se comunica através dessa porta.

```
37  *out_1 = 16;
38  n = sub_E0AC(v26, (int)&src);
39  memcpy(out_1 + 1, &src, n);
40  out_1[n + 1] = 0;
41  out_1[n + 2] = 4;
42  qmemcpy(&out_1[n + 3], "MQTT\x04", 5);
43  out_1[n + 8] = '\xC2';
44  strcpy(&out_1[n + 9], "\a\b");
```

Figura 3 – O malware constrói um pacote MQTT CONNECT, iniciando sua conexão MQTTs com o C2.

O MQTT é um protocolo de comunicação de rede baseado em publicação e assinatura, ideal para ambientes com largura de banda limitada ou instável, como em aplicações de Internet das Coisas (IoT). Para estabelecer a conexão, o malware emprega o MQTT 4.0, enviando três identificadores ao servidor C2: Client ID, Username e Password. O Client ID é o GUID armazenado na memória do malware, enquanto o Username e o Password são variáveis de ambiente derivadas do GUID. Esses identificadores permitem que o malware se autentique no broker MQTT.

Os comandos suportados pelo malware IOCONTROL são os seguintes:

- **Send "hello":** Relata informações detalhadas do sistema (por exemplo, nome do host, usuário atual, modelo do dispositivo) para o C2.
- **Check exec:** Confirma se o binário do malware está instalado corretamente e é executável.
- **Execute command:** Executa comandos arbitrários do sistema operacional por meio de chamadas do sistema e relata a saída.
- **Self-delete:** Remove seus próprios binários, scripts e logs para evitar a detecção.
- **Port scan:** Verifica intervalos de IP e portas especificados para identificar outros alvos em potencial.

3 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:

Mantenha o software atualizado

- Aplique regularmente atualizações e patches de software para corrigir vulnerabilidades conhecidas.

Use autenticação multifator (MFA)

- Adicione uma camada extra de segurança exigindo múltiplas formas de verificação antes de conceder acesso.

Segmente a rede

- Separe a rede em segmentos menores para limitar a movimentação lateral do malware em caso de infecção.

Monitore o tráfego de rede

- Utilize ferramentas de monitoramento para detectar atividades suspeitas e tráfego anômalo.

Implemente políticas de segurança rigorosas

- Defina e aplique políticas de segurança para controlar o acesso e o uso de dispositivos e dados.

Eduque os funcionários

- Treine os funcionários sobre práticas seguras e como reconhecer tentativas de phishing e outras ameaças.

Realize backups regulares

- Mantenha backups atualizados de todos os dados críticos e teste regularmente a restauração desses backups.

4 INDICADORES DE COMPROMETIMENTO (IOC)

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.

Indicadores do artefato	
md5:	c92e2655d115368f92e7b7de5803b7bc
sha1:	366e435a1ea0f597deb6ebe7c0c5acdb6e8b33eb
sha256:	1b39f9b2b96a6586c4a11ab2fdbff8fdf16ba5a0ac7603149023d73f33b84498
File name:	11.elf

Tabela 2 – Indicadores de Comprometimento

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
Domínio	tylarion867mino[.]com uuokhhfsdlk[.]tylarion867mino[.]com ocferda[.]com
IP	159[.]100[.]6[.]69

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.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Claroty**
- **Bleepingcomputer**

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH