BOLETIM DE SEGURANÇA

Servidores Linux são alvos de Malware em campanha de espionagem.

heimdall
security research
A DIVISION OF ISH

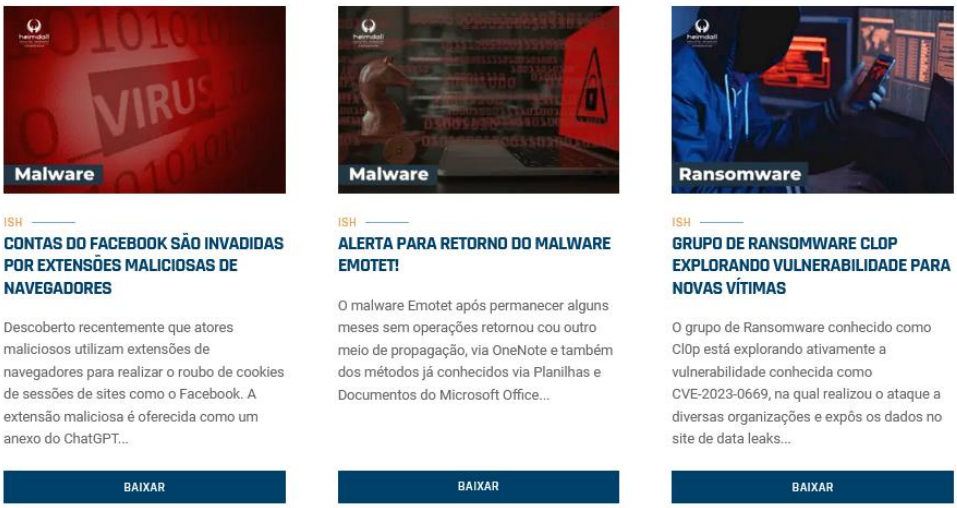
TLP: CLEAR

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 TABELAS

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Pesquisadores de segurança da Kaspersky observaram que uma versão Linux do DinodasRAT, também conhecido como XDealer, estaria realizando ataques em sistemas Red Hat e Ubuntu. Acredita-se que essa variante do malware esteja em operação desde 2022. Embora a primeira versão do DinodasRAT tenha sido identificada em 2021, a variante Linux não foi publicamente descrita.

2 INFORMAÇÃO SOBRE A AMEAÇA

O DinodasRAT, é um backdoor multiplataforma codificado em C++ com uma gama de funcionalidades. Este RAT possibilita que um ator malicioso monitore e obtenha dados sigilosos do computador alvo. Uma versão Windows do malware foi empregada em ataques a instituições governamentais na Guiana, sendo documentada pela ESET sob o nome de Operação Jacana. Em outubro de 2023, após a divulgação da ESET, identificamos uma nova versão Linux do DinodasRAT. Indícios nas amostras sugerem que esta versão (V10, segundo a nomenclatura dos invasores) pode ter iniciado suas operações em 2022. Contudo, a primeira variante Linux conhecida (V7), ainda não descrita publicamente, data de 2021.

O DinodasRAT Linux visa principalmente as distribuições Linux baseadas em Red Hat e Ubuntu. Na sua primeira execução, ele gera um arquivo oculto no mesmo diretório do executável, que segue o padrão ".[executable_name].mu". Este arquivo atua como um mutex, assegurando que apenas uma instância do implante seja executada e que ela só prossiga se a criação deste arquivo for bem-sucedida.

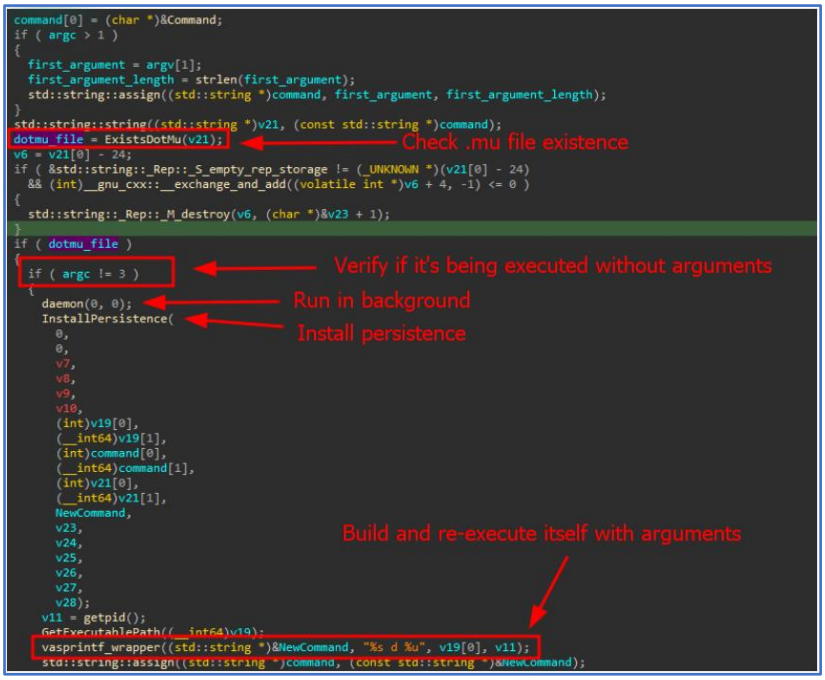


Figura 1 – Código principal do backdoor.

O backdoor, ao ser ativado, segue um processo de três etapas para estabelecer persistência, inicialmente, é executado sem argumentos, o que o leva a operar em segundo plano, acionando a função “**daemon**” do Linux, em seguida, busca estabelecer sua permanência no sistema comprometido, utilizando scripts de inicialização *SystemV* ou *SystemD* e por fim, ele se executa novamente, desta vez com o ID do processo pai (**PPID**) como argumento. Isso resulta na criação de um novo processo (filho) que prossegue com a infecção backdoor, enquanto o processo pai permanece em espera.

O backdoor, antes de se conectar ao servidor C2, recolhe informações da máquina infectada e do tempo de infecção para criar um identificador único (**UID**) para o dispositivo da vítima. Curiosamente, os atacantes não usam dados do usuário para gerar este UID. O UID geralmente contém a data da infecção, Hash MD5 da saída do comando *dmidecode* (relatório detalhado do hardware do sistema infectado), número aleatório como ID, versão do backdoor.

O UID tem o formato: **Linux_{DATE}_{HASH}_{RAND_NUM}_{VERSION}.**

Depois, a implantação armazena todas as informações locais sobre o ID da vítima, nível de privilégio e outros detalhes relevantes num arquivo oculto chamado "/etc/.netc.conf". Este arquivo de perfil contém os metadados atualmente coletados do backdoor. Se o arquivo não existir, o Dinodas o criará, seguindo a estrutura Seção e Chave:Valor. A implantação também garante que qualquer acesso a este arquivo ou a si mesmo (ao ler seu próprio caminho de arquivo) não atualize o tempo de "acesso" na estrutura estatística, que contém o carimbo de data/hora de acesso de um arquivo específico no sistema de arquivos. Isso é feito usando o comando "touch" com o parâmetro "-d" para modificar esses metadados.

A versão DinodasRAT Linux utiliza as duas versões dos gerenciadores de serviços Linux (Systemd e SystemV) para estabelecer persistência num sistema afetado. Quando o malware é iniciado, uma função é chamada para determinar o tipo de distribuição Linux que a vítima está usando. Atualmente, existem dois tipos de distros que o implante tem como alvo com base em suas leituras de "/proc/version" - RedHat e Ubuntu 16/18. No entanto, o malware pode infectar qualquer distribuição que suporte qualquer uma das versões acima dos gerenciadores de serviços do sistema. Assim que o sistema for reconhecido, ele instala um script de inicialização adequado que fornece persistência para o RAT. Este script é executado assim que a configuração da rede é concluída e inicia o backdoor.

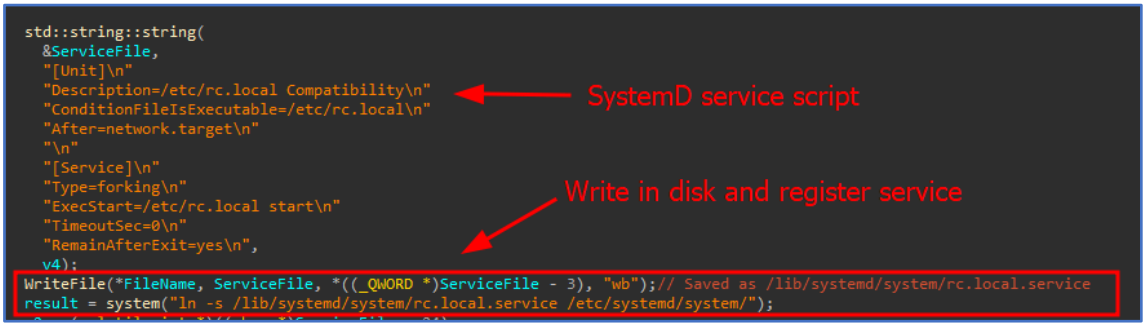


Figura 2 – Registro de serviço SystemD.

Para sistemas baseados em RedHat e Ubuntu, os scripts de inicialização de serviço são usados para verificar a persistência e a presença do binário chkconfig. Isso indica que a inicialização é realizada com SysV, não com Systemd. Se o chkconfig não estiver presente, o implante abrirá ou criará o arquivo de script "/etc/rc.d/rc.local" e se anexará à sequência de execução que ativa o backdoor durante a inicialização do sistema. Se o chkconfig estiver presente, a rota SysV é assumida e o malware cria scripts de persistência em "/etc/init.d".

A comunicação do DinodasRAT na versão Linux com o C2 é idêntica à versão Windows. A conexão é estabelecida através de TCP ou UDP. O domínio C2 está embutido no código binário.

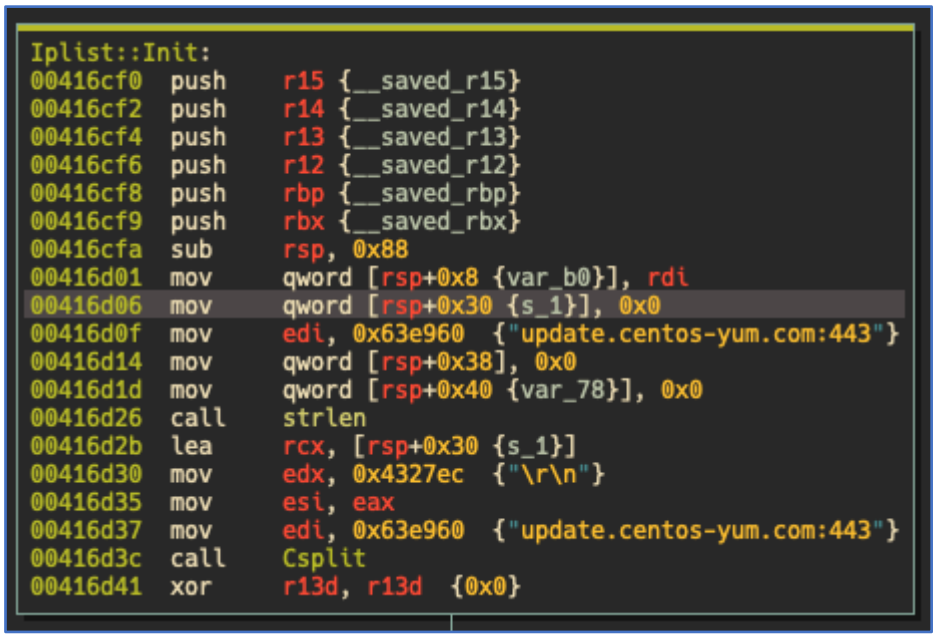


Figura 3 – O servidor e a porta C2 codificados.

O DinodasRAT tem um tempo programado para enviar dados de volta ao C2, mas esse tempo não é constante para todos os usuários ou conexões. Se o usuário que executa o implante for root (EUID = 0), o implante envia as informações de volta ao C2 imediatamente. No entanto, se o usuário não for superusuário e a configuração estiver definida como checkroot, o implante aguardará dois minutos para uma espera "curta" (padrão) e 10 horas para uma espera "longa". A espera "longa" é ativada quando há uma conexão remota com o servidor infectado

originada de um dos IPs configurados no C2. Para se comunicar com o servidor C2 e transmitir qualquer dado, a inserção segue uma estrutura de pacotes de rede com diversos campos.

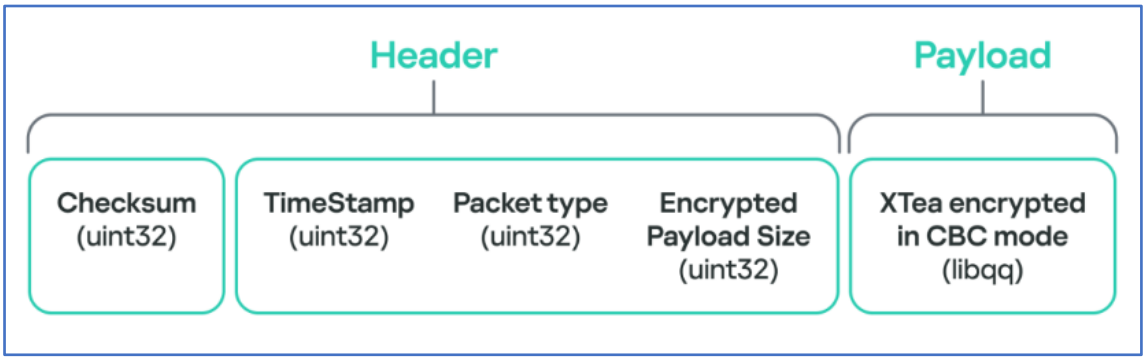


Figura 4 – Versão simplificada do pacote de rede.

A versão Linux do DinodasRAT mantém as mesmas características de criptografia da versão Windows. Ele usa funções da biblioteca **libqq qq_crypt** do Pidgin para criptografar e descriptografar a comunicação entre o implante e o C2, além da criptografia de dados. Essa biblioteca emprega o *Tiny Encryption Algorithm* (**TEA**) no modo CBC para codificar e decodificar os dados, facilitando a portabilidade entre as plataformas. Além disso, o implante Linux utiliza duas das mesmas chaves presentes na versão Windows.

```
For C2 encryption:   A1 A1 18 AA 10 F0 FA 16 06 71 B3 08 AA AF 31 A1
For name encryption: A0 21 A1 FA 18 E0 C1 30 1F 9F C0 A1 A0 A6 6F B1
```

Figura 5 – Característica de encriptação.

No momento da análise, a infraestrutura que suporta as versões Linux do DinodasRAT estava ativa e operacional. Foi descoberto um endereço IP que está associado aos domínios C2 para as variantes Windows e Linux. O DinodasRAT para Windows utiliza o domínio **update.microsoft-settings[.]com**, que é mapeado para o endereço IP **199.231.211[.]19**. Curiosamente, este mesmo endereço IP também está vinculado ao domínio **update.centos-yum[.]com**, que segue o mesmo padrão de subdomínio e domínio de atualização do sistema operacional.

Domain	IP	First seen	ASN	Registrar
update.centos-yum[.]com	199.231.211[.]19	May 4, 2022	18978	Name.com, Inc.

Figura 6 – Domínio associado ao C2.

3 CONCLUSÃO

Em 2023, a ESET revelou a Operação Jacana, uma campanha direcionada a usuários do Windows. Durante o monitoramento contínuo, descobriu-se que os operadores Jacana conseguem infectar a infraestrutura Linux com uma nova variante do DinodasRAT, antes desconhecida e não detectada. O código e os indicadores de comprometimento da rede são semelhantes aos exemplos do Windows descritos pela ESET. O backdoor é totalmente funcional, permitindo ao operador controle total sobre a máquina infectada, possibilitando a exfiltração de dados e a espionagem.

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:

Monitoramento

- O DinodasRAT é capaz de monitorar e coletar dados sobre atividades do usuário, configurações do sistema e processos em execução1. Portanto, é importante monitorar regularmente as atividades do sistema.

Prevenção de execução múltipla

- O DinodasRAT cria um arquivo oculto no diretório onde reside seu binário, que atua como um mutex para evitar a execução de múltiplas instâncias no dispositivo infectado. Portanto, é crucial verificar a existência de tais arquivos ocultos.

Persistência

- O malware define persistência no computador usando scripts de inicialização SystemV ou SystemD. Assim, é importante verificar regularmente esses scripts de inicialização.

Comunicação com o servidor C2

- A comunicação com o servidor C2 ocorre via TCP ou UDP, enquanto o malware utiliza o Tiny Encryption Algorithm (TEA) no modo CBC. Portanto, é essencial monitorar o tráfego de rede para detectar qualquer comunicação suspeita.

Atualizações de malware

- O DinodasRAT pode baixar novas versões do malware que potencialmente incorporam melhorias e recursos adicionais. Assim, é importante manter todos os sistemas de detecção de malware atualizados.

Limpeza

- O DinodasRAT pode desinstalar-se e apagar todos os vestígios de sua atividade. Portanto, é crucial ter um sistema robusto de backup e recuperação.

5 INDICADORES DE COMPROMISSOS

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 Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de compromisso do artefato	
md5:	b202e37174ae70834f887d53fb84cb60
sha1:	b769731b6e5983dd07fc19ca4b531c70b16479fd
sha256:	3d93b8954ed1441516302681674f4989bd0f20232ac2b211f4b601af0fcfc13b
File name:	ntfsys

Indicadores de compromisso do artefato	
md5:	decd6b94792a22119e1b5a1ed99e8961
sha1:	fd2cb41c5495fff1b21ba267e374062ce509a320
sha256:	bf830191215e0c8db207ea320d8e795990cf6b3e6698932e6e0c9c0588fc9eff
File name:	bf830191215e0c8db20_browsing7ea320d8e795990cf6b3e6698932e6e0c9c0588fc9effXxX5Elf.elf

Indicadores de compromisso do artefato	
md5:	8138f1af1dc51cde924aa2360f12d650
sha1:	74b1da190d670fa4c207afb0fbca4d7df701538a
sha256:	15412d1a6b7f79fad45bcd32cf82f9d651d9ccca082f98a0cca3ad5335284e45
File name:	15412d1a6b7f79fad45bcd32cf82f9d651d9ccca082f98a0cca3ad5335284e45.elf

Indicadores de compromisso do artefato	
md5:	4cd25a82c0651e543d42389c14dd86f6
sha1:	6d4dc35c0d70a8ca90b87c39e644db36ce29e232
sha256:	98b5b4f96d4e1a9a6e170a4b2740ce1a1dfc411ada238e42a5954e66559a5541
File name:	98b5b4f96d4e1a9a6e170a4b2740ce1a1dfc411ada238e42a5954e66559a5541.elf

Indicadores de compromisso do artefato	
md5:	20b4ac6be041b72862e1645953a951eb
sha1:	dd5f99687aa953b422f27035b13398bcdf8e0401
sha256:	a2c3073fa5587f8a70d7def7fd8355e1f6d20eb906c3cd4df8c744826cb81d91
File name:	a2c3073fa5587f8a70d7def7fd8355e1f6d20eb906c3cd4df8c744826cb81d91.elf

Indicadores de compromisso do artefato	
md5:	e7417613dde54377fbddff96f9ba8819
sha1:	b0b8fb71e2abc17d5d0ef358c1c16e9a4223483c
sha256:	ebdf3d3e0867b29e66d8b7570be4e6619c64fae7e1fbd052be387f736c980c8e
File name:	ntfsys.so6

Indicadores de compromisso do artefato	
md5:	f1cf940f9e64edbd21f30249926c7e03
sha1:	8f6840d7b6b43d37293fc37c1636132b5934876b
sha256:	6302acdfce30cec5e9167ff7905800a6220c7dda495c0aae1f4594c7263a29b2
File name:	6302acdfce30cec5e9167ff7905800a6220c7dda495c0aae1f4594c7263a29b2.elf

Indicadores de compromisso do artefato	
md5:	8138f1af1dc51cde924aa2360f12d650
sha1:	74b1da190d670fa4c207afb0fbca4d7df701538a
sha256:	15412d1a6b7f79fad45bcd32cf82f9d651d9ccca082f98a0cca3ad5335284e45
File name:	15412d1a6b7f79fad45bcd32cf82f9d651d9ccca082f98a0cca3ad5335284e45.elf

Indicadores de compromisso do artefato	
md5:	decd6b94792a22119e1b5a1ed99e8961
sha1:	fd2cb41c5495fff1b21ba267e374062ce509a320
sha256:	bf830191215e0c8db207ea320d8e795990cf6b3e6698932e6e0c9c0588fc9eff
File name:	bf830191215e0c8db20_browsing7ea320d8e795990cf6b3e6698932e6e0c9c0588fc9effXxX5Elf.elf

Tabela 1 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
Domínio	update.centos-yum[.]com
IP	199.231.211.19

Tabela 2 – Indicadores de Compromissos 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**
- **Kaspersky**
- **Bleepingcomputer**

heimdall
security research
A DIVISION OF ISH