BOLETIM DE SEGURANÇA

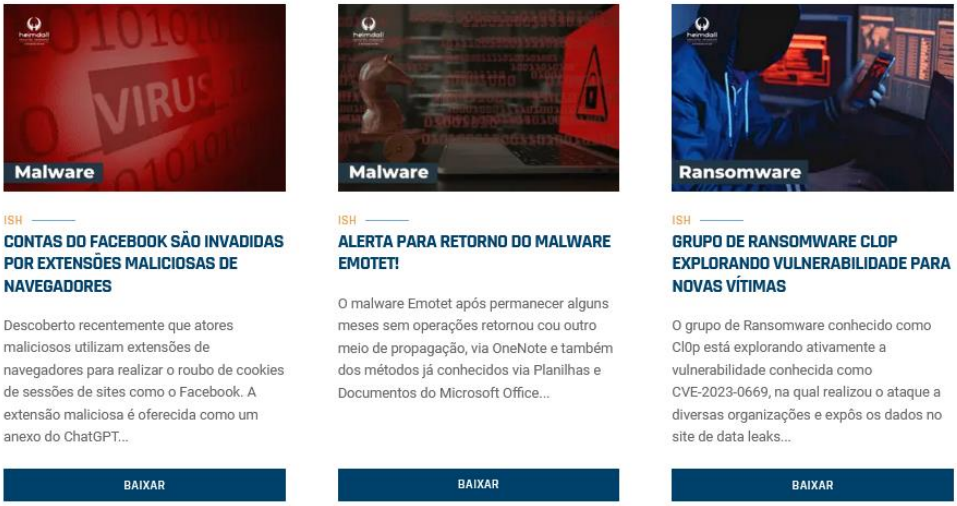
Malware PondRAT escondido em pacotes Python tem como alvo desenvolvedores de software

heimdall
security research
A DIVISION OF ISH

TLP: CLEAR

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 da Unit 42 identificaram uma campanha ativa que utiliza pacotes Python contaminados para distribuir backdoors em sistemas Linux e macOS. Esses pacotes, denominados PondRAT, são versões mais leves do POOLRAT, um conhecido RAT (Remote Administration Tool) associado ao grupo de ameaças Gleaming Pisces. A campanha visa desenvolvedores de software, utilizando pacotes Python infectados para infiltrar sistemas e instalar backdoors.

2 INFORMAÇÕES SOBRE A AMEAÇA

Gleaming Pisces, também conhecido como Citrine Sleet e distribuidor do AppleJeus, é um grupo de ameaças financeiras ligado à Coreia do Norte, ativo desde 2018. Este grupo, associado ao Reconnaissance General Bureau (RGB) da Coreia do Norte, é notório por seus ataques sofisticados, especialmente contra a indústria de criptomoedas.

Em campanhas anteriores, o Gleaming Pisces utilizou software falso de negociação de criptomoedas para comprometer sistemas em várias plataformas. Durante a investigação da campanha de pacotes Python envenenados, analisamos o Linux RAT entregue como carga útil final e foram encontradas semelhanças significativas com o malware macOS usado em uma campanha anterior do AppleJeus, relatada pela CISA e orquestrada pelo Gleaming Pisces.

As semelhanças incluem:

- Estruturas de código sobrepostas
- Nomes de funções e chaves de criptografia idênticos
- Fluxos de execução semelhantes

Essa família foi nomeada como RAT de PondRAT. Análises posteriores revelaram que o PondRAT compartilha muitas características com o POOLRAT, outro macOS RAT do arsenal do Gleaming Pisces. Com base nessas descobertas, atribuímos a campanha de pacotes Python envenenados ao Gleaming Pisces.

Ao rastrear a atividade recente do Gleaming Pisces, foram encontrados pacotes Python envenenados carregados no PyPI por várias personas falsas maliciosas. Esses pacotes implementaram uma cadeia de infecção evasiva para evitar a detecção e, eventualmente, baixaram um Linux RAT nos endpoints infectados. A VIPYR Security e a Qihoo 360 relataram essa atividade, envolvendo pacotes Python como:

- real-ids (versões 0.0.3 - 0.0.5)
- coloredtxt (versão 0.0.2)
- beautifultext (versão 0.0.1)
- minisound (versão 0.0.2)

Concluiu-se que, embora a Qihoo 360 também tenha relatado atividades relacionadas ao Windows, essas parecem ser separadas das campanhas do Linux e macOS. Avaliou-se que a atividade relatada pela Qihoo 360 foi realizada por um agente de ameaça diferente, em contraste com as campanhas do Linux e macOS conectadas ao Gleaming Pisces.

A cadeia de infecção inclui pacotes Python envenenados que decodificam e executam código malicioso. Após a instalação e carregamento do pacote malicioso pelo Python, um código malicioso executa comandos bash para baixar o RAT, modificar suas permissões e executá-lo.

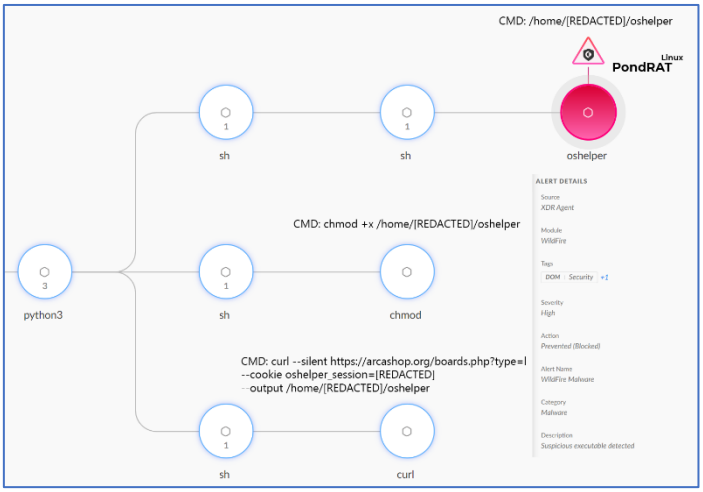


Figura 1 – Cadeia de infecção e a prevenção do PondRAT.

Durante a análise de códigos semelhantes ao PondRAT, foram identificados outros malwares. Essa descoberta também se baseou em pesquisas anteriores e na atribuição ao grupo Gleaming Pisces. A Figura 2 a seguir apresenta um resumo dessas similaridades.

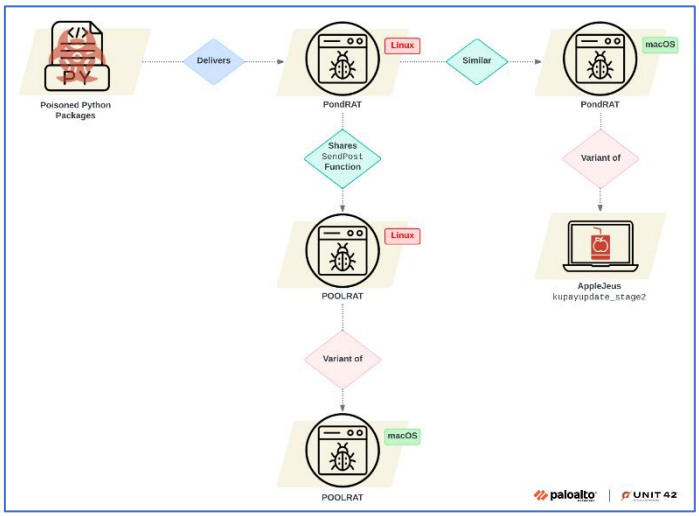


Figura 2 – Semelhanças entre o PondRAT e outros malwares anteriormente atribuídos ao Gleaming Pisces.

Recentemente, a VIPYR Security publicou uma pesquisa onde analisou o código de um Linux RAT (SHA256: 973f7939ea03fd2c9663dafc21bb968f56ed1b9a56b0284acf73c3ee141c053c). Esse RAT era desconhecido na época, mas agora foi identificado como a variante Linux do PondRAT. Os operadores do Gleaming Pisces não alteraram o código, mantendo os nomes das funções como originalmente definidos pelo agente da ameaça.

Ao examinar a função principal deste RAT, foram identificadas chamadas para duas funções distintas: FConnectProxy e AcceptRequest.

- FConnectProxy: Responsável por gerenciar a conexão com o servidor C2, configurando o URI e os parâmetros das requisições HTTP.
- AcceptRequest: Analisa e descriptografa comandos do servidor C2, sendo responsável por receber e executar comandos dos operadores remotos.

Em 2021, a CISA relatou uma nova onda de ataques AppleJeus, denominada Kupay Wallet. Durante essa onda, foi identificado um macOS RAT chamado kupayupdate_stage2 (SHA256: 91eaf215be336eae983d069de16630cc3580e222c427f785e0da312d0692d0fd), utilizado como carga útil final.

Na análise do kupayupdate_stage2 para macOS, observou-se que as funções do malware também não foram removidas. A análise do código revelou várias similaridades com o RAT Linux, incluindo os nomes das funções FConnectProxy e AcceptRequest, além de um fluxo de execução de código semelhante.

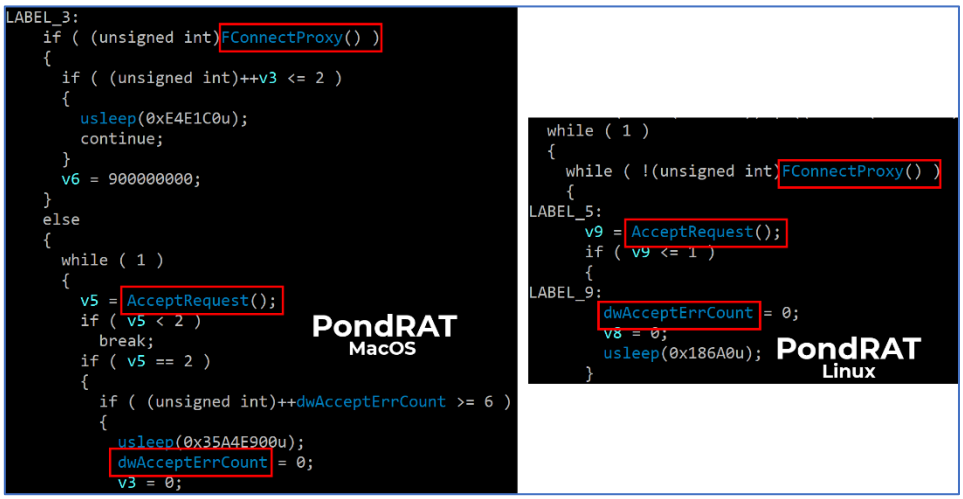


Figura 3 – Nomes de métodos e similaridades de fluxo de execução do novo Linux RAT.

Após as descobertas mencionadas, verificou-se mais amostras da variante macOS do PondRAT, que utilizavam a mesma chave de criptografia. Foi identificado uma amostra macOS previamente associada à campanha de pacotes Python envenenados e um outro RAT macOS vinculado ao AppleJeus.

Ao analisar essas novas amostras do macOS, que compartilhavam a mesma chave de criptografia, descobriu-se que uma delas, um arquivo binário Mach-O multiarquitetura (SHA256: bfd74b4a1b413fa785a49ca4a9c0594441a3e01983fc7f86125376fdbd4acf6b), estava utilizando a mesma infraestrutura que a variante Linux do PondRAT.

Os arquivos binários multi-arch para macOS suportam tanto arquiteturas Intel quanto ARM. Este exemplo específico continha dois binários Mach-O adicionais, compilados para x64 e ARM, conforme esperado.

Os dois binários descartados compartilhavam o mesmo código (nomes de função e chave de criptografia) com kupayupdate_stage2, assim como a variante Linux do PondRAT. Com base nas semelhanças de código e no nome compartilhado, os_helper, concluiu-se que ele também foi distribuído como o payload final da campanha de pacotes Python envenenados. Além disso, essas variantes do macOS utilizaram o mesmo servidor de comando e controle (C2), jdkgradle[.]com, que a variante Linux.

Figura 4 – Execução do malware os_helper macOS.

As novas variantes do POOLRAT para Linux (SHA256: 5c907b722c53a5be256dc5f96b755bc9e0b032cc30973a52d984d4174bace456 e SHA256: f3b0da965a4050ab00fce727bb31e0f889a9c05d68d777a8068cfc15a71d3703) apresentam várias semelhanças notáveis com a versão para macOS (prtspool). A análise indica que essas variantes são, na verdade, versões do POOLRAT para macOS, e não um novo tipo de malware.

Tanto as versões para Linux quanto para macOS utilizam uma estrutura de função idêntica para carregar suas configurações, com nomes de métodos e funcionalidades muito semelhantes. Além disso, os nomes dos métodos em ambas as variantes são surpreendentemente parecidos, e as strings são quase idênticas. Por fim, o mecanismo que lida com comandos do C2 é praticamente o mesmo.

Figura 5 – Comparação da função LoadConfig entre POOLRAT para macOS e POOLRAT para Linux.

Durante a análise das amostras do PondRAT, identificamos que o manipulador de comandos apresenta semelhanças com o POOLRAT. O PondRAT possui um conjunto básico de comandos que permitem ao invasor realizar as seguintes ações:

- Carregar e baixar arquivos
- Verificar o status de um implante para confirmar sua atividade
- Instruir o implante a pausar operações por um período determinado (“sleep”)
- Executar comandos (com a opção de recuperar ou não a saída)

Dado que a funcionalidade do PondRAT é semelhante, mas mais restrita em comparação ao POOLRAT, concluímos que o PondRAT é uma versão mais leve do POOLRAT. A Tabela 1 a seguir compara os comandos implementados no POOLRAT e no PondRAT.

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:

Verifique a origem dos pacotes

- Sempre baixe pacotes Python de fontes confiáveis e verifique a autenticidade antes de instalar. Evite pacotes de fontes desconhecidas ou não verificadas.

Use software antivírus atualizado

- Mantenha seu software antivírus e antimalware sempre atualizados para detectar e bloquear ameaças conhecidas, incluindo variantes do PondRAT.

Implemente firewalls robustos

- Configure firewalls para monitorar e controlar o tráfego de rede, bloqueando acessos não autorizados e atividades suspeitas.

Eduque sua equipe

- Treine desenvolvedores e funcionários sobre os riscos de segurança cibernética e as melhores práticas para evitar a instalação de software malicioso.

Monitore atividades de rede

- Utilize ferramentas de monitoramento de rede para detectar comportamentos anômalos que possam indicar a presença de malware.

Realize auditorias de segurança regulares

- Faça auditorias de segurança periódicas para identificar e corrigir vulnerabilidades em seus sistemas e redes.

Utilize autenticação multifator (MFA)

- Implemente MFA para adicionar uma camada extra de segurança ao acessar sistemas e dados sensíveis.

4 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:	33c9a47debdb07824c6c51e13740bdfe
sha1:	7b6e6487b803bbe85d7466b89da51a269fa4fc29
sha256:	973f7939ea03fd2c9663dafc21bb968f56ed1b9a56b0284acf73c3ee141c053c
File name:	local_file.exe

Indicadores de compromisso do artefato	
md5:	b62c912de846e743effdf7e5654a7605
sha1:	8027c1d1ac0fd7d40ee850119c6d4501fbe75eab
sha256:	0b5db31e47b0dccfdec46e74c0e70c6a1684768dbacc9eacbb4fd2ef851994c7
File name:	localfile~.x64

Indicadores de compromisso do artefato	
md5:	f50c83a4147b86cdb20cc1fbae458865
sha1:	8a030a03570134cee4659b1b1f666f6f48c27fa5
sha256:	3c8dbfcbb4fccbaf924f9a650a04cb4715f4a58d51ef49cc75bfcef0ac258a3e
File name:	localfile~.arm64

Indicadores de compromisso do artefato	
md5:	05957d98a75c04597649295dc846682d
sha1:	676537b0f7707feae0130bbcbdc881f5b4eb3f03
sha256:	bfd74b4a1b413fa785a49ca4a9c0594441a3e01983fc7f86125376fdbd4acf6b
File name:	os_helper

Indicadores de compromisso do artefato	
md5:	4c66950d791ff5d39d53ffcd0b52a64d
sha1:	dd5bb0609b92163d8834a37a517885ce0b512938
sha256:	5c907b722c53a5be256dc5f96b755bc9e0b032cc30973a52d984d4174bace456
File name:	5c907b722c53a5be256dc5f96b755bc9e0b032cc30973a52d984d4174bace456.bin.sample

Indicadores de compromisso do artefato	
md5:	ce35c935dcc9d55b2c79945bac77dc8e
sha1:	720e6abf3befb585164450325246fe9cb000268f
sha256:	cbf4cfa2d3c3fb04fe349161e051a8cf9b6a29f8af0c3d93db953e5b5dc39c86
File name:	cbf4cfa2d3c3fb04fe349161e051a8cf9b6a29f8af0c3d93db953e5b5dc39c86.dylib

Tabela 1 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	www.talesseries[.]com/write.php rgedista[.]com/sfxl.php
Domínio	rebelthumb[.]rede jdkgradle[.]com

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.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **UNIT42**
- **Thehackernews**

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH