TLP: CLEAR

BOLETIM DE SEGURANÇA

Exploração de vulnerabilidade em servidores PHP para injeção de minerador PacketCrypt

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 DETALHES SOBRE A AMEAÇA E EXPLORAÇÃO

Uma análise recente de malware conduzida por pesquisadores da SANS revelou informações preocupantes. Durante a investigação, foi identificado um arquivo malicioso chamado *dr0p.exe*, que era usado para baixar um segundo arquivo, denominado *pkt1.exe*, a partir do endereço IP **23.27[.]51[.]244**. De acordo com a ferramenta Shodan, esse IP está localizado nos Estados Unidos e apresenta quatro portas abertas: **22, 80, 110 e 6664**. A análise indicou que esse IP estava rodando o EvilBit Block Explorer, uma ferramenta online usada para visualizar e analisar informações da blockchain da criptomoeda EvilBit, acessível pela porta 80. 80.

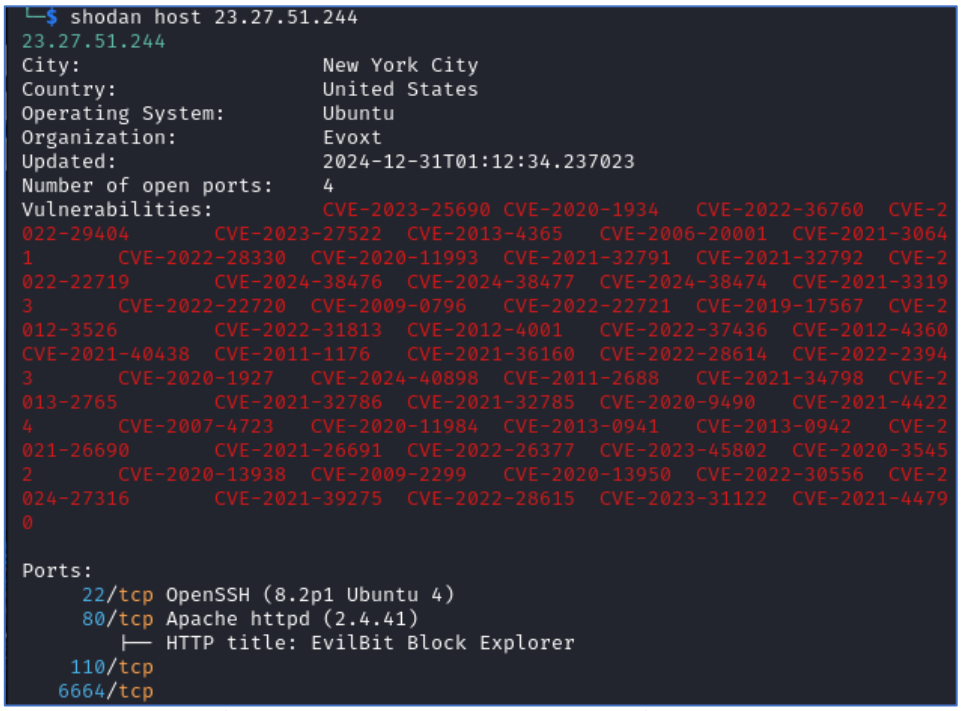

Figura 1 – Informações da consulta do IP via Shodan.

O arquivo pkt1.exe gera um executável denominado packetcrypt.exe e adiciona um endereço de carteira do PacketCrypt (PKT Classic) como argumento. Após análise utilizando o explorador de blockchain PKT Classic (PKTC), foi identificado que o titular dessa carteira minerou até o momento 5 PKTC, o que corresponde a aproximadamente 0,0021785 USDT com base nas cotações atuais.

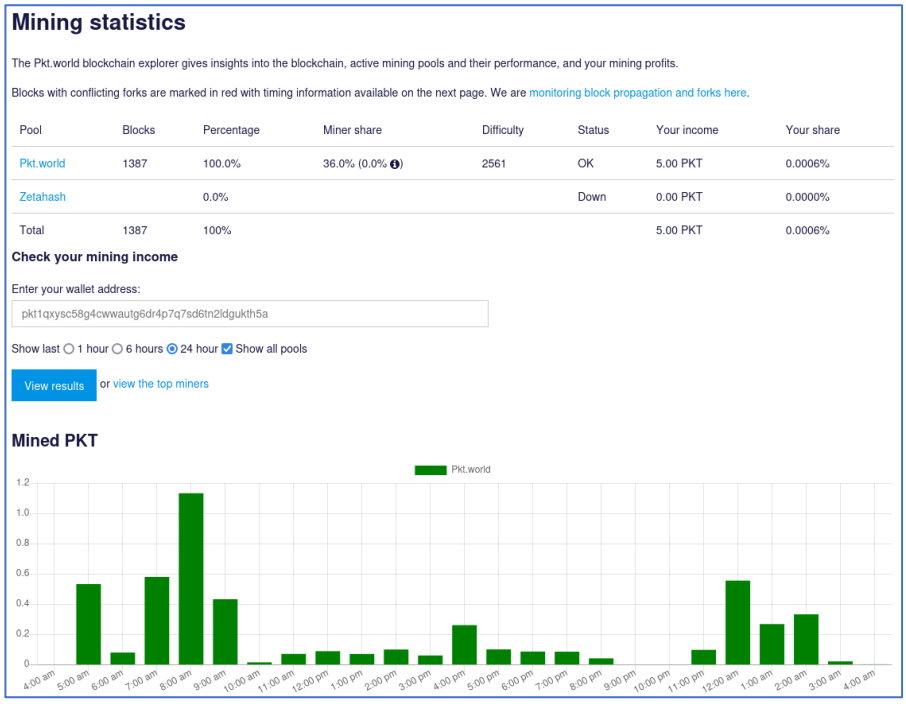

Figura 2 – Atividade da carteira PacketCrypt Classic (PKTC).

Conforme os pesquisadores, a atividade de URLs na web parece estar explorando servidores **PHP vulneráveis**, como a recente **CVE-2024-4577** php-cgi.exe, ou **servidores PHP mal configurados** que permitem acesso público irrestrito. Durante a investigação, foi notado que o projeto PacketCrypt (PKT) evoluiu de uma abordagem de *proof-of-work*, agora conhecida como PKT Classic (PKTC), para uma nova abordagem *Stake-to-Earn*, atualmente conhecida como PKT. Portanto, há uma distinção entre a criptomoeda do projeto legado (PKTC) e a iteração atual (PKT). Neste contexto, a criptomoeda minerada em servidores PHP vulneráveis é **PKTC**.

A vulnerabilidade CVE-2024-4577 categorizada como crítica, é uma falha de injeção de argumentos no PHP-CGI que pode ser explorada para obter execução remota de código (RCE). Essa vulnerabilidade ocorre devido a erros nas conversões de codificação de caracteres, afetando o recurso "Best Fit" no Windows. Quando explorada, essa falha permite que um ator malicioso passe opções para o binário PHP em execução, o que pode resultar na revelação do código-fonte de scripts, execução de código PHP arbitrário no servidor, entre outros problemas.

2 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:

Atualizar o PHP

- Atualize o PHP para as versões corrigidas: 8.3.8, 8.2.20 ou 8.1.29, conforme apropriado para o seu ambiente.

Desativar o modo CGI

- Se o modo CGI não for necessário, considere desativá-lo ou substituí-lo por alternativas mais seguras, como FastCGI, PHP-FPM ou Mod-PHP.

Revisar configurações do servidor

- Verifique se os executáveis do PHP (por exemplo, php.exe ou php-cgi.exe) não estão em diretórios acessíveis pelo servidor web, especialmente em instalações padrão do XAMPP no Windows.

Aplicar regras de firewall

- Implemente regras no firewall para bloquear solicitações maliciosas que tentem explorar a vulnerabilidade, como aquelas contendo caracteres específicos usados na exploração.

Monitorar logs de acesso

- Monitore os logs do servidor web em busca de padrões suspeitos ou tentativas de exploração, como solicitações contendo caracteres ou sequências incomuns.

Implementar um WAF

- Considere a implementação de um WAF para inspecionar e filtrar tráfego malicioso direcionado ao seu servidor PHP.

Manter backups regulares

- Garanta que backups atualizados e íntegros de seus dados e configurações estejam disponíveis para recuperação em caso de comprometimento.

3 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:	5290766026d3727c3262fd48db6db0a4
sha1:	59aec8a9c0e6f59bfee7902fbdcb6e3b9932a93b
sha256:	d078d8690446e831acc794ee2df5dfabcc5299493e7198993149e3c0c33ccb36
File name:	dr0p.exe

Indicadores do artefato	
md5:	82c7d11916fdfbf24eae6bf9200a48c9
sha1:	7d7c0517ed4f0f909258edb0f46b66fccecb8c73
sha256:	e3d0c31608917c0d7184c220d2510848f6267952c38f86926b15fb53d07bd562
File name:	pkt.exe

Indicadores do artefato	
md5:	5f6cda0f181fe14e6d395cdb50c37c41
sha1:	fadde84250ebda58f7ff880b5942d7b6acb494bb
sha256:	717fe92a00ab25cae8a46265293e3d1f25b2326ecd31406e7a2821853c64d397
File name:	PacketCryptApp.dll

Tabela 1 – Indicadores de Comprometimento

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
IP	23.27[.]51[.]244

Tabela 2 – 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.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **ISC_SANS**
- **GBHackers**
- **NVD**

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH