



BOLETIM DE SEGURANÇA

Exploração de vulnerabilidade em servidores PHP para
injeção de minerador PacketCrypt

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



ISH

CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR



ISH

ALERTA PARA RETORNO DO MALWARE EMOTET!

O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR



ISH

GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS

O grupo de Ransomware conhecido como CLOP está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

SUMÁRIO

1	Detalhes sobre a ameaça e exploração.....	5
2	Recomendações.....	7
3	Indicadores de Comprometimento (IoC).....	8
4	Referências	9
5	Autores.....	9

LISTA DE TABELAS

Tabela 1 – Indicadores de Comprometimento.	8
Tabela 2 – Indicadores de Comprometimento de Rede.	8

LISTA DE FIGURAS

Figura 1 – Informações da consulta do IP via Shodan.	5
Figura 2 – Atividade da carteira PacketCrypt Classic (PKTC).	6

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.

```
└─$ shodan host 23.27.51.244
23.27.51.244
City:                New York City
Country:             United States
Operating System:   Ubuntu
Organization:       Evoxt
Updated:            2024-12-31T01:12:34.237023
Number of open ports: 4
Vulnerabilities:    CVE-2023-25690 CVE-2020-1934 CVE-2022-36760 CVE-2
022-29404 CVE-2023-27522 CVE-2013-4365 CVE-2006-20001 CVE-2021-3064
1 CVE-2022-28330 CVE-2020-11993 CVE-2021-32791 CVE-2021-32792 CVE-2
022-22719 CVE-2024-38476 CVE-2024-38477 CVE-2024-38474 CVE-2021-3319
3 CVE-2022-22720 CVE-2009-0796 CVE-2022-22721 CVE-2019-17567 CVE-2
012-3526 CVE-2022-31813 CVE-2012-4001 CVE-2022-37436 CVE-2012-4360
CVE-2021-40438 CVE-2011-1176 CVE-2021-36160 CVE-2022-28614 CVE-2022-2394
3 CVE-2020-1927 CVE-2024-40898 CVE-2011-2688 CVE-2021-34798 CVE-2
013-2765 CVE-2021-32786 CVE-2021-32785 CVE-2020-9490 CVE-2021-4422
4 CVE-2007-4723 CVE-2020-11984 CVE-2013-0941 CVE-2013-0942 CVE-2
021-26690 CVE-2021-26691 CVE-2022-26377 CVE-2023-45802 CVE-2020-3545
2 CVE-2020-13938 CVE-2009-2299 CVE-2020-13950 CVE-2022-30556 CVE-2
024-27316 CVE-2021-39275 CVE-2022-28615 CVE-2023-31122 CVE-2021-4479
0

Ports:
22/tcp OpenSSH (8.2p1 Ubuntu 4)
80/tcp Apache httpd (2.4.41)
    └─ HTTP title: EvilBit Block Explorer
110/tcp
6664/tcp
```

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.

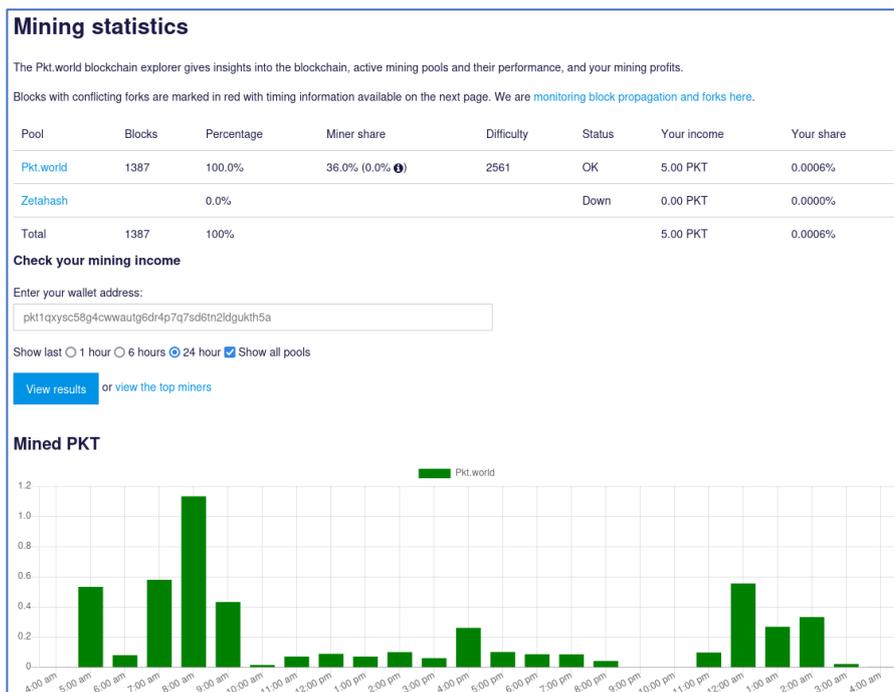


Figura 2 – Atividade da carteira PacketCrypt Classic (PKTC).

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