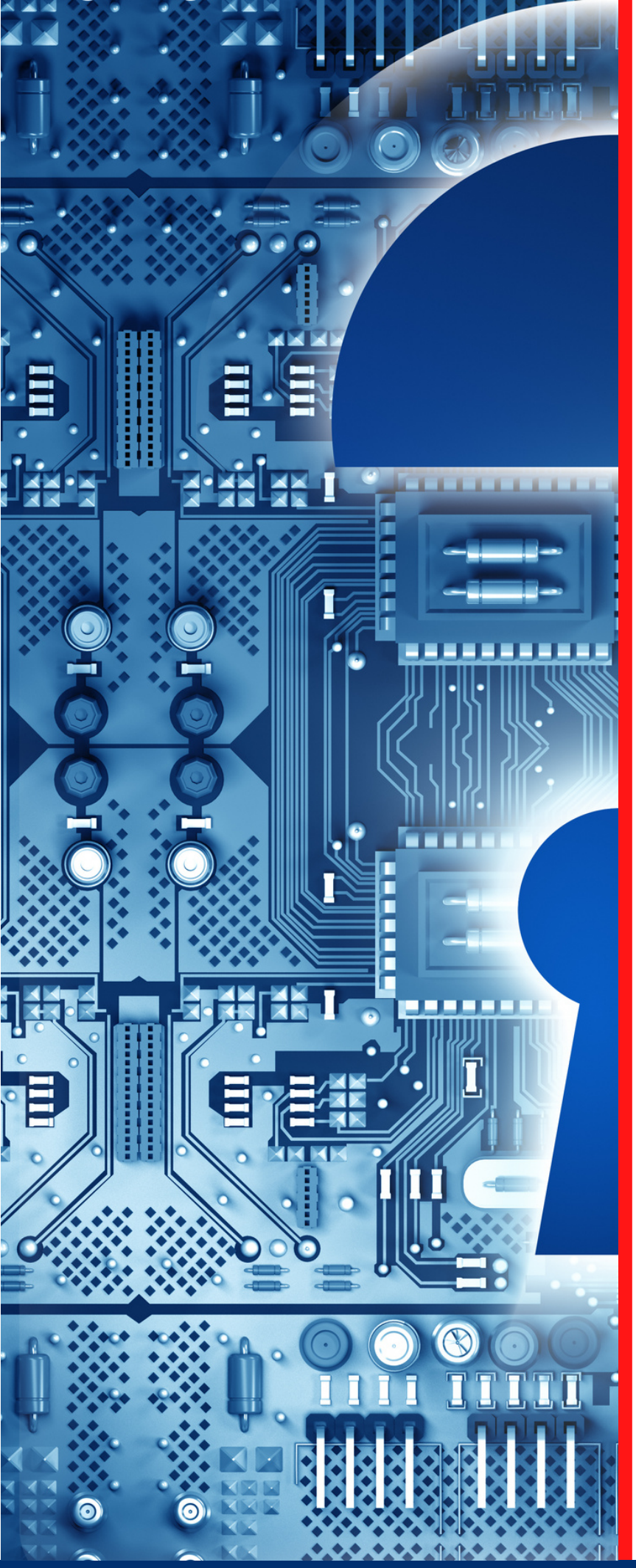


OSIC

ORIENTAÇÃO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

02/2023

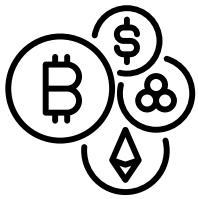
Abuso com Mineração de Criptoativos em Infraestruturas (*Cryptojacking*).

Textos: João Alberto Muniz Gaspar
Diagramação: Douglas Rocha de Oliveira
Produção: Secretaria de Segurança da Informação e Cibernética

Espaço cibernético inclusivo, seguro, estável, acessível e pacífico.

TLP:CLEAR

Criptomoeda



A criptomoeda é um ativo financeiro digital que utiliza criptografia e tecnologia *blockchain* para[1] garantir a realização de transações.

A mineração de criptomoedas, ou criptomineração, é o processo utilizado para conquistar o ativo e tem como objetivo verificar e incluir as transações de criptoativos na *blockchain*, que é o banco de dados que registra as movimentações dos usuários.

A popularidade e o aumento do uso de criptomoedas começou a chamar tanta atenção que desenvolveram uma nova forma de abuso chamada *Cryptojacking*.

Cryptojacking

O *cryptojacking*, ou *malware* de criptomineração, é um ataque que coopta os recursos de computação do alvo para minerar criptomoedas, como bitcoin e Ethereum. Esse *malware* usa a capacidade de processamento da Unidade Central de Processamento (CPU) do dispositivo, por vezes, usa a *Graphics Processing Unit* (GPU), comum nas placas de vídeos utilizadas por gamers, para realizar cálculos matemáticos complexos que resultam em longas sequências alfanuméricas, intituladas de *hashes*.

Existem muitos métodos diferentes para instalar o *Cryptojacking* em um dispositivo, sendo os mais tradicionais:

[2] A ameaça abusa de sítio eletrônico, também em anúncios, com injeção de *script*. A infecção ocorre quando a vítima visita o site ou o clica no anúncio infectado, este ato executa o *script* automaticamente com o armazenamento do código malicioso no dispositivo do usuário; e

Engenharia social, em particular o *phishing*, em que o alvo é induzido a clicar em *link* que executa o código para implantar o *script* de criptomineração em seu dispositivo.

Recentemente, há relatos de outros métodos como:

A exploração de vulnerabilidades, em que se destaca a biblioteca Log4J, que permitem a execução de código no equipamento vulnerável. Em diversos casos, a mesma vulnerabilidade permite ao atacante realizar movimentação lateral, tendo acesso a outros dispositivos da rede e os infectando com o *cryptojacking*; e

Utilização de abusos na cadeia de suprimentos (*Suply Chain*) de *software* semeando repositórios de código-fonte aberto com pacotes e bibliotecas maliciosos que contêm *scripts* de *cryptojacking* incorporados em seus códigos.

Independentemente do mecanismo de entrega, a detecção do *malware* é difícil, pois o código do *cryptojacking* funciona em segundo plano e as vítimas inocentes continuam utilizando seus sistemas normalmente.

Os sinais geralmente relacionados com *cryptojacking* são:

- perda de desempenho do dispositivo;
- atrasos na execução de processos;
- aquecimento anormal da CPU ou da GPU, podendo ocorrer o superaquecimento similar a um *overclock*;[3]
- incremento no consumo de energia do dispositivo afetado; e
- aumento incomum do tráfego de rede.

Uma das maneiras de distinguir a criptomineração do processamento legítimo é monitorar a rede em busca de conexões externas desconhecidas e com longa duração. Além disso, bons pacotes anti*malware* usam algoritmos de *machine learning*[4] para entender os comportamentos na rede, permitindo que ela reconheça os sinais de criptomineração, como quando uma conexão de saída é feita para enviar a moeda digital ao invasor ou quando protocolos de criptomineração são usados.

Sugestões

Como ações protetivas contra os ataques de criptomineração, o Departamento de Segurança da Informação (DSI) sugere:

- no caso de ataques executados em navegador, o processo de mineração é interrompido com o fechamento da guia do navegador;
- instalar *antimalware* com proteção de *endpoint*[5] capaz de detectar criptomineradores;

- manter o filtro da *web* atualizado;
- gerenciar *plugins*[6] e extensões do navegador para minimizar o risco de execução de *scripts*; e
- aplicar *patches* e *updates*[7] de segurança nos equipamentos.

Por fim, orienta-se executar uma configuração de ativos que favoreça a segurança, observando a proteção básica dos equipamentos, que inclui aplicação de *patches*, desativação de serviços não utilizados e limitação de rastros externos para minimizar o risco de ataques baseados em equipamentos de rede.

Recomenda-se, ainda, a leitura das orientações contidas no sítio eletrônico abaixo:

https://www.cisa.gov/tips/st18-002

TLP:CLEAR

Informações complementares

1. ***Blockchain:*** *a* tecnologia *blockchain* é um livro contábil que faz o registro de transações de criptomoedas, de forma que esse registro seja confiável e imutável.
2. ***Script*****:** é um conjunto de instruções para que uma função seja executada em determinado aplicativo.
3. ***Overclock:*** o *overclock* é um método usado para aumentar o desempenho de um componente do computador além dos padrões de fábrica. Essa é uma prática bem comum entre usuários mais experientes.
4. ***Machine learning*****:** pode ser traduzido como aprendizado de máquina ou aprendizagem de máquina, esse é um conceito associado à inteligência artificial, ela treina computadores para realizarem atividades como seres humanos. Grandes exemplos disso são o reconhecimento de fala, a identificação de imagens, o reconhecimento facial ou de expressões faciais, entre outros.
5. ***Endpoint:*** um *endpoint* é qualquer dispositivo que seja, fisicamente, um "ponto final" em uma rede, por essa razão têm esse nome. *Notebook*, *desktops*, *smartphones*, *tablets*, servidores e ambientes virtuais podem ser considerados *endpoints*.
6. ***Plugin:*** *plugins* são adições complementares ou alterações de *software* que permitem a personalização de programas de computador, aplicativos e navegadores da *web*, bem como a personalização do conteúdo oferecido pelos *sites*.
7. ***Patches/updates:*** são programas de computador criados para atualizar ou corrigir um *software* de forma a melhorar sua usabilidade ou performance.