Gatos virtuais: detectando e avaliando os impactos da mineração de criptomoedas em infraestrutura pública

Victor R. Pires, Felipe R. Coutinho, Daniel S. Menasché, Claudio M. de Farias

[1]Universidade Federal do Rio de Janeiro (UFRJ), Cidade Universitária – RJ – Brasil

victorpires@labnet.nce.ufrj.br, felipecoutinho@tic.ufrj.br

sadoc@dcc.ufrj.br, claudiofarias@nce.ufrj.br

Abstract. *Blockchains and cryptocurrencies represent a revolutionary way to convert energy into a medium of exchange. Today, numerous applications for blockchains and cryptocurrencies are envisioned for purposes ranging from inventory control to banking applications. Naturally, in order to mine in an economically viable way, regions where energy is plentiful and cheap, e.g., close to hydroelectric plants or in certain countries where energy production is greater than demand, are sought. The possibility of converting energy into cash, however, also opens up opportunities for a new kind of cyber attack aimed at illegally cryptocurrency mining. In this work, using data from January and February of 2018 from the Federal University of Rio de Janeiro - UFRJ, it was observed that this threat is real and it is presented a projection of the costs and gains derived from these attacks. This work also indicates ways of detection and mitigation of these attacks that were successfully implemented at UFRJ.*

Resumo. *Blockchains e criptomoedas representam uma forma revolucionária de converter energia em meio de troca. Atualmente, vislumbram-se inúmeras aplicações para blockchains e criptomoedas, para fins que variam desde o controle de inventário até aplicações bancárias. Naturalmente, para se minerar de forma economicamente viável buscam-se regiões nas quais a energia seja abundante e barata, e.g., próximas a usinas hidroelétricas ou em determinados países onde a produção de energia é maior que a demanda. A possibilidade de conversão de energia em dinheiro, no entanto, também abre oportunidades para um novo tipo de ataque cibernético que visa a mineração de criptomoedas. Nesse trabalho, usando dados de janeiro e fevereiro de 2018 da Universidade Federal do Rio de Janeiro - UFRJ, observou-se que tal ameaça é real e apresenta-se uma projeção dos custos e ganhos derivados desses ataque. Indica-se também formas de detecção e mitigação desses ataques que foram implementadas com sucesso na UFRJ.*

1. Introdução

Com a popularização das moedas virtuais, vêm também popularizando-se um novo tipo de ataque que ameaça os usuários da Internet. Tal ataque consiste no uso de CPU e memória dos usuários domésticos para fins de mineração excusa. Em 2018, foi reportado que tal tipo de ataques já era mais prevalente que ataques clássicos, como DDoS, em certas regiões dos EUA [Segura 2018].

Este trabalho é focado em uma nova classe de ataques de mineração. Os ataques previamente reportados na literatura [Segura 2018, Rüth et al. 2018, Hong et al. 2018, Kharraz et al. 2019, Zimba and Wang 2018] contavam com usuários honestos sendo explorados remotamente e possivelmente monitorados localmente. Neste trabalho, por outro lado, foi considerado usuários de infraestruturas públicas, e.g., da Universidade Federal do Rio de Janeiro - UFRJ, cujas máquinas podem ser exploradas localmente, por acesso físico às mesmas, e monitoradas remotamente, e.g., pela Diretoria de Segurança da Informação da UFRJ. Esta distinção entre o presente trabalho e os demais traz uma série de novos desafios, conforme abordado no restante deste trabalho. Para todos os fins práticos, os "gatos" nas favelas também se enquadram dentro do conceito de infraestrutura pública considerado neste trabalho, evidenciando problemas de ordem pública decorrentes de ataques de mineração no Brasil.

Como estudo de caso, neste trabalho estudou-se ação de atacantes que buscam invadir máquinas da UFRJ para executarem processos de mineração de forma distribuída, aumentando sua rentabilidade com os ataques. As infraestruturas públicas, em especial, são grandes alvos desse tipo de ataque, uma vez que possuem um grande número de *hosts*, banda de Internet e energia abundante. Este estudo tem como objetivos (a) avaliar a prevalência de ataques de mineração na UFRJ e (b) analisar os dados gerados pelos incidentes, a fim de gerar um padrão de comportamento para a detecção desse tipo de ataque.

Em resumo, as principais contribuições desse artigo são:

Foi descoberto que mineração ilegal de criptomoedas é prevalente Usando dados coletados na UFRJ, descobriu-se que a mineração ilegal de criptomoedas ocorre dentro da infraestrutura pública. Em particular, foram identificadas dezenas de tentativas de mineração da criptomoeda Monero. Vislumbrou-se que essas tentativas sejam apenas uma pequena parcela do total, e que diferentemente de ataques clássicos, que deixam um rastro nos traços de banda da rede, a mineração de criptomoedas pode ser muito difícil de detectar por envolver praticamente apenas atividade local na máquina atingida.

Os custos e ganhos advindos da mineração ilegal foram estimados Por meio de experimentos controlados em laboratório, foram quantificados os custos e ganhos advindos da mineração. Em particular, verificou-se que os custos em duas das configurações consideradas foram muito superiores aos ganhos. Tal achado pode motivar um amplo aumento no uso ilegal de recursos.

São propostas novas formas de descobrir e mitigar mineração ilegal Baseado na experiência preliminar, apresentam-se formas ingênuas de descobrir e mitigar mineração ilegal de criptomoedas. Em trabalhos futuros, pretende-se refinar tais propostas por meio de experimentos controlados e da aplicação das mesmas em ambientes reais.

O restante desse trabalho está organizado da seguinte forma: na Seção 2 são apresentados fundamentos básicos sobre criptomoedas necessários para o entendimento do restante deste artigo; na Seção 3 são contrastados os trabalhos relacionados com este trabalho, enquanto a Seção 4 apresenta a metodologia de pesquisa; as Seções 5 e 6 apresentam as principais descobertas, sobre prevalência dos ataques de mineração na UFRJ e sobre os estimados ganhos e custos decorrentes destes ataques; a Seção 7 contém uma

discussão mais ampla dos resultados onde destaca-se a Seção 7.1 que apresenta um breve resumo com ideias que foram identificadas como promissoras para mitigar os ataques discutidos neste trabalho; por fim, a Seção 8 conclui.

2. Fundamentos básicos sobre criptomoedas e ataques de mineração

Uma criptomoeda é um ativo digital projetado para funcionar como um meio de troca que usa criptografia para proteger transações financeiras, controlar a criação de unidades adicionais e verificar a transferência de ativos. O processo de geração de criptomoedas em uma rede é denominado mineração. Este processo consiste em uma máquina despender processamento para resolver um problema matemático e ser recompensada por essa resolução [Nakamoto 2008]. Todo esse processo demanda elevado consumo de energia e poder de processamento, serviços estes que precisam ter os custos reduzidos para que a mineração se torne um processo lucrativo ao minerador.

O uso de criptomoedas se tornou possível devido aos avanços tecnológicos da última década. Porém, esse uso não se restringiu somente ao apelo financeiro proposto pela tecnologia, mas também a uma série de novas abordagens usando conceitos que surgiram durante o processo, como a *blockchain*, *smartcontracs* e *distributed ledger*. As criptomoedas permitiram uma série de transações financeiras em anonimato ou com identificação dos envolvidos nessas transações dificultada.

Diferente do modelo centralizado dos sistemas bancários atuais, as criptomoedas usam controle descentralizado que funciona através da tecnologia de contabilidade distribuída, uma tecnologia que permite a realização confiável e segura de qualquer transação entre duas ou mais pessoas sem a necessidade de intermediários, através da Internet. Normalmente uma *blockchain* serve como banco de dados distribuído que guarda um registro de transações permanente e à prova de violação. A *blockchain* consiste em dois tipos de registros: transações individuais e blocos.

O processo de mineração pode ser realizado em um único computador ou utilizando um grupo destes. Na mineração *"solo"*, a recompensa gerada pelo processo de mineração depende exclusivamente da potência do computador, enquanto na mineração em *"pool"* muitos computadores mineram juntos e a potência acumulada aumenta as chances de resolução do bloco. Quando o bloco é resolvido, a recompensa é dividida proporcionalmente de acordo com a potência empregada por cada um.

2.1. Ataques de mineração

Nessa seção é apresentada uma breve introdução aos ataques de mineração, indicando seus tipos clássicos e o que foi encontrado de diferente quando foca-se em infraestruturas públicas.

2.1.1. Tipos de ataques de mineração

Um ataque de mineração consiste na infecção de um ou mais *hosts*, inserindo neles um *malware* que executa um software de mineração. Esta técnica recebe o nome de *cryptojacking* (mineração de criptomoedas utilizando recursos do computador da vítima). Atualmente, a furtividade desta técnica tem dificultado a sua detecção por parte das equipes

de segurança, especialmente pelo fato de não ser possível analisar todos os *hosts*, diante do tamanho da rede e da ausência de softwares de monitoramento instalados neles. Sendo assim, a maneira mais eficiente de identificar os ataques muitas vezes consiste na busca por tráfego anômalo na rede da instituição (vide Seção 7).

Cabe destacar que este trabalho foi focado nos usuários que intencionalmente mineram moedas virtuais em suas máquinas. Alternativamente, na literatura o foco têm sido em usuários remotos executando tal mineração indesejada. Isso se dá de duas formas: via Javascript ou via *worms*. No primeiro caso, o código de mineração é executado no *browser* e o download deste código é feito junto com o download da página desejada pelo usuário (de forma velada). Já no caso do *worm*, o código é executado de forma independente do *browser*, sendo o download feito potencialmente de forma individual. O *worm* tem capacidade de se replicar. No caso do Javascript, monitorando o uso de CPU e memória do *browser*, pode-se identificar o problema, enquanto que no caso do *worm*, precisa-se monitorar o uso de CPU e memória da máquina como um todo, pois não se sabe de antemão qual o processo que está fazendo a execução maliciosa. Discute-se em mais detalhes *cryptojacking* (tanto via Javascript quanto *worms*) na Seção 3.

2.1.2. Por que focar em infraestruturas públicas?

O problema dos ataques de mineração traz desafios adicionais em infraestruturas públicas, e.g., universidades, escolas e hospitais. Isso ocorre nas infraestruturas públicas devido aos usuários terem acesso físico às máquinas públicas. Assim, torna-se mais fácil ligar e desligar mineradores fisicamente. Para se fazer uso de máquinas de usuários domésticos, por exemplo, por meio de uma *botnet*, tais máquinas domésticas precisam conter vulnerabilidades que permitam o atacante invadir o sistema.

Uma vez que se inicia a mineração em uma máquina de uma infraestrutura pública, como ela não deixa poucos rastros na rede, pode se tornar muito difícil a detecção do comprometimento da máquina. Monitorar a rede de transmissão de dados pode não ser suficiente para identificar os ataques, que têm um aspecto fortemente local e não fazem uso de vulnerabilidades de *software*. Assim, vislumbra-se uma cooperação necessária entre as superintendências de tecnologia e as redes prestadoras de energia para que tais ataques sejam mitigados em larga escala.

3. Trabalhos relacionados

Existe uma ampla literatura sobre ataques de sequestro de mineração (*cryptojacking*) [Segura 2018, Rüth et al. 2018, Hong et al. 2018, Kharraz et al. 2019, Zimba and Wang 2018]. Nesses ataques, o usuário que tem a máquina sequestrada tipicamente acessa uma página que aparenta ser inócua mas que, de forma escondida, executa Javascript de mineração usando recursos de CPU e memória sem autorização do usuário. Alternativamente, o usuário é infectado por um *worm* que faz a mineração. Em ambos os casos, a origem do ataque é externa à máquina física. Neste trabalho, considerou-se ataques que se dão por usuários que têm acesso físico às máquinas. Embora o tema de *cryptojacking* esteja em voga, não se observou nenhum trabalho anterior que tenha analisado os riscos associados a este tipo de ataque em infraestruturas públicas, nos quais os usuários tenham acesso físico aos dispositivos.

	Trabalhos relacionados	Neste trabalho
Ponto de monitoramento (vantage point)	local (extensão do *browser*)	remoto
Vetor de acesso (access vector)	remoto	local (físico)

Tabela 1. Comparação desse trabalho com os relacionados

3.1. Novos vetores de ataque e vetores de acesso

A Tabela 1 compara os trabalhos relacionados contra o presente trabalho. Em trabalhos relacionados, os autores consideram que o *browser* de forma não intencional acessa *scripts* de mineração (vetor de acesso remoto) e que o usuário honesto tem interese em monitorar (localmente) devido a atividades suspeitas. Neste trabalho, por outro lado, assume-se que o usuário intencionalmente executa *scripts* de mineração (vetor de acesso local, físico) e que o monitoramento precisa ser remoto, e.g., *deep packet inspection* (DPI).

3.2. "Gatos" virtuais e "gatos" físicos

O problema considerado neste trabalho é particularmente complexo em países em desenvolvimento, como o Brasil, no qual temos uma significativa parcela da população acessando a rede elétrica por meio de "gatos" físicos, que potencialmente podem dar margem a "gatos" virtuais [Setti 2018, Marini 2017].

Os "gatos" virtuais descritos neste trabalho, bem como aqueles estudados na literatura de *cryptojacking*, podem ser apreciados como uma versão sofisticada dos "gatos" físicos tão comuns em favelas. "Gatos" físicos são prevalentes no Brasil [Nadaud 2012, Penin 2008] e existe uma vasta literatura sobre os mesmos. Cabe destacar que embora substanciais recursos, inclusive jurídicos, tenham sido investidos para detectar tais "gatos" físicos e removê-los, estes continuam amplamente presentes. Assim, vislumbra-se que os ataques virtuais em infraestruturas públicas, por serem mais sutis, constituem uma ameaça maior que os ataques físicos. A combinação dos dois, ou seja, ataques virtuais sobre uma infraestrutura em que existem ataques físicos, constitui o cenário mais complexo.

3.3. Ataques de *cryptojacking*

Inúmeros trabalhos recentes descrevem ataques de *cryptojacking* [Segura 2018, Rüth et al. 2018, Hong et al. 2018]. [Zimba and Wang 2018], por exemplo, descrevem um atacante que direciona a máquina vítima para uma servidor remoto e através de técnicas de escalação de privilégio (do inglês, *privilege escalation*), e transforma a máquina vítima em um recurso de mineração para o atacante. Se as mensagens trocadas pelo atacante e a vítima tiverem padrões suspeitos, e.g., de tamanho de pacotes, tempo entre pacotes ou se acessarem IPs marcados em listas negras, pode-se identificar os ataques [Kharraz et al. 2019, Kührer et al. 2014, Coinblockerlists 2018].

3.4. Detectando *cryptojacking*

Tipicamente *cryptojacking* é detectado *in browser* (ou seja, pelo próprio *browser*). O *browser* executa um monitor, que faz análises do Javascript e intercepta *crypto scripts*.

Tal monitor pode ser, por exemplo, uma extensão do *browser* (similar às extensões para economia de energia). Dois exemplos de extensões que fazem detecção de mineração indesejada são *NoCoin* [Keramidas 2018] e *MinerBlock* [Cherone and Mahon 2018].

Este trabalho considera o cenário no qual não se pode detectar o ataque a partir do *browser*, tendo em vista que o usuário da máquina intencionalmente executou o *script* de mineração (Tabela 1). Precisa-se detectar o ataque a partir da rede, e mostra-se que isso é possível, por exemplo, usando (DPI).

Alternativamente, se DPI não for viável (e.g., por os pacotes estarem criptografados com o uso de uma VPN), pode-se ainda avaliar apenas o IP origem e destino dos mesmos, e buscar por eles em listas negras [Kharraz et al. 2019, Kührer et al. 2014, Coinblockerlists 2018]. Pode-se também avaliar o tamanho dos pacotes e o tempo médio entre pacotes, na busca por padrões suspeitos. Isso possivelmente pode inclusive ser feito investigando consultas aos servidores DNS.

Caso não seja possível descobrir os ataques apenas com medições em redes, pode ser necessário monitorar remotamente a telemetria das mesmas (CPU e memória) [Avritzer et al. 2010]. Esse monitoramento pode ser feito em universidades, nos quais os computadores estão todos sob a mesma autoridade, mas não em favelas, por exemplo. Os contadores de desempenho (*performance counters* ou *performance signatures*) tipicamente são capazes de identificar atividade de mineração, que aumenta em muito o uso da CPU. Entretanto, monitorar a CPU de um número grande de máquinas pode ser desafiador. Assim, acredita-se que, em um futuro próximo, o monitoramento remoto via rede seguido pela inspeção detalhada das máquinas suspeitas, ainda será a solução mais comum, conforme considerada neste trabalho, e detalhada na seção a seguir.

4. Metodologia

A seguir, é descrita a metodologia experimental de medição da UFRJ, focada no monitoramento da prevalência de mineração nos campis, e na Seção 6 é descrita a metodologia utilizada para a realização de experimentos controlados em laboratório para averiguar ganhos e perdas decorrentes da mineração.

4.1. Sistemas de monitoramento na UFRJ

A UFRJ possui diversos sistemas de detecção de invasões e ameaças que são utilizados para prover segurança de seus alunos, docentes e funcionários. Nesse trabalho, serão utilizados os dados fornecidos por duas ferramentas utilizadas pela equipe de Segurança da Informação: *SGIS - Sistema de Gestão de Incidentes de Segurança*, fornecido pela Rede Nacional de Ensino e Pesquisa (RNP) e o sistema de gestão de tickets. O SGIS gera chamados utilizando o resultado das varreduras do tráfego de rede no PoP-RJ (Ponto de Presença da RNP no Rio de Janeiro), por onde passam quase todo o tráfego da rede acadêmica do Estado destinado à Internet. O sistema de tickets inclui chamados requisitados pelos membros da UFRJ.

4.2. Descoberta de ataques de mineração na UFRJ

A descoberta dos ataques de mineração inicia-se com a notificação de alguma irregularidade. As notificações de irregularidades na UFRJ ocorrem pelas seguintes formas, executadas em paralelo:

- notificação das instituições parceiras e órgãos de governo informando que o *host* está se comunicando com outras máquinas mineradoras infectadas;
- monitoramento de tráfego de rede da universidade verificando se o *host* está se comunicando com servidores de mineração, também conhecidos como *mining pools*;
- notificações dos usuários das máquinas indicando anomalias no comportamento do *host*.

A partir da notificação, é feita uma auditoria física nas máquinas suspeitas, para se detectar o possível vetor de ataque envolvido. Nessa auditoria, também são coletados dados sobre as configurações das máquinas envolvidas.

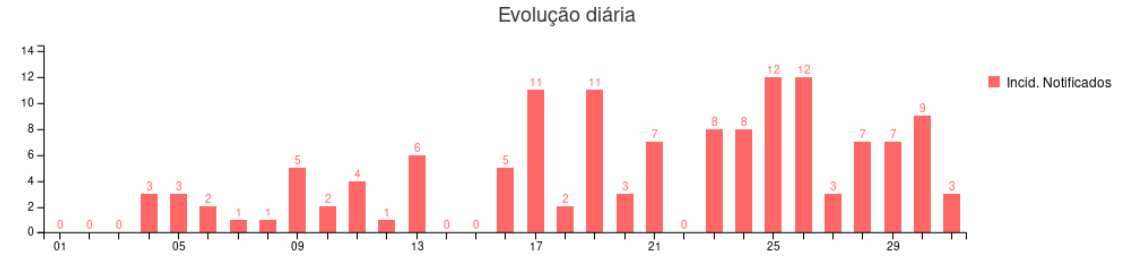
A perícia física consiste em:

1. encaminhamento físico até a máquina;
2. análise da finalidade da máquina e das conexões ativas usando `wireshark` ou `tcpdump`, em conjunto com o `netstat` (e.g., muitas conexões UDP ativas para um computador pessoal de um professor do departamento de história pode indicar suspeita de que a máquina foi comprometida);
3. análise das vulnerabilidades da máquina, sob uma visão externa, e.g., `Shodan`;
4. análise das vulnerabilidades da máquina, sob uma visão interna, e.g., usando rastreador de vulnerabilidades do Apache provida pelo `Kali Linux` caso o mesmo esteja instalado na máquina;
5. busca nas pastas da máquina (em particular, nos subdiretórios do Apache) por um arquivo (binário) que tipicamente seja usado para fins ilícitos. Este trabalho foi focado na busca por arquivos de mineração de criptomoedas, através de uma busca nos nomes de todos os arquivos da máquina pelas `strings` listadas na Tabela 2;
6. busca no `cron` do sistema por agendamento de processos de mineração, bem como no histórico do `bashrc`, pelas mesmas *strings* da Tabela 2;
7. busca no histórico de sites acessados por sites suspeitos. Por exemplo, no caso de suspeita de mineração de criptomoedas, verifica-se se existem registros de acesso a algum dos sites de mineração publicamente conhecidos, e.g., `http://btc.com`.

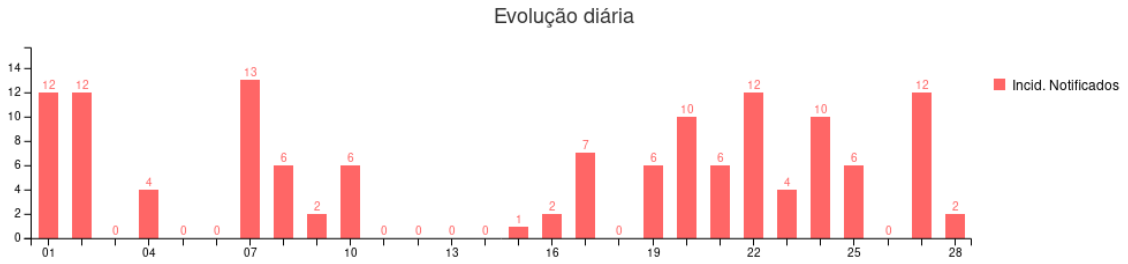
string	justificativa
miner	indica minerador
mining	indica minerador
xmr	sigla do Monero
bitcoin	na busca por Bitcoin
ethereum	na busca por Ethereum
monero	na busca por Monero, uma criptomoeda prevalente no Brasil

Tabela 2. Strings usadas na busca por mineradores de criptomoedas

Um vetor de ataque é o método pelo qual um ataque atinge seu alvo [Wu et al. 2011]. Os vetores de ataque que foram encontrados na UFRJ durante as auditorias dos ataques foram: (i) vetores epidêmicos virtuais (*worms*); (ii) vetores específicos virtuais (ataques à rede, advindos de uma conexão de Internet); (iii) vetores específicos



(a) janeiro de 2018



(b) fevereiro de 2018

Figura 1. Número de incidentes em janeiro de e fevereiro de 2018

físicos (ataques à rede, advindos de uma acesso físico aos computadores). No caso particular de mineração de criptomoedas, o acesso físico às máquinas representa um importante vetor de potencial difícil detecção.

Algums *worms* foram encontrados em casos de computadores públicos de lugares com ampla circulação de pessoas, como em laboratórios e bibliotecas. Os ataques às redes foram detectados em servidores utilizados para hospedagem de sites e armazenamento de arquivos. Já os ataques físicos foram identificados quando executados por usuários dos equipamentos, intencionalmente, para mineração em benefício próprio.

5. Prevalência da mineração ilegal

5.1. Caso estudado na UFRJ

A UFRJ foi vítima de ciberataques com a finalidade de minerar criptomoedas durante o período de janeiro até fevereiro de 2018. Em fevereiro de 2018 implementaram-se as estratégias de mitigação descritas na Seção 7.1, e desde então tem sido mais difícil identificar ataques de mineração.

Esse estudo é focado nas notificações recebidas entre 7 de janeiro e 28 de fevereiro. O estudo desses ataques foi usado para gerar as métricas do experimento de ganhos e custos estimados com a mineração. A Figura 1 reporta o número de notificações de incidentes de segurança durante o período analisado. Elas abrangem notificações de diversos tipos de ataques, incluindo DDoS, violação de direitos autorais e ataques de força bruta a `ssh`.

Na Figura 1 nota-se que existem períodos contíguos de maior atividade de notificações, por exemplo, entre 25 de janeiro de 2 de fevereiro, e entre 19 de fevereiro e 25 de fevereiro. Temos poucas notificações em outros períodos contíguos, por exemplo, entre 1 e 8 de janeiro, e entre 11 e 16 de fevereiro. O principal motivo para termos es-

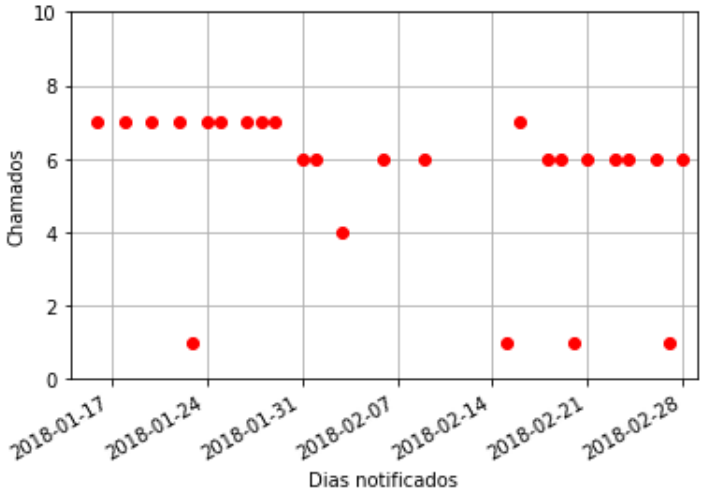


Figura 2. Número de incidentes com finalidade de mineração de criptomoedas

ses períodos contíguos relaciona-se ao fato de que, quando um ataque ocorre, o atacante que passou pelo *firewall* muitas vezes consegue comprometer várias máquinas. Quando o problema é mitigado, volta-se para uma fase de calmaria.

Desses incidentes notificados, foram reconhecidos como ataques de mineração 144 casos. As datas das notificações destes casos estão reportadas na Figura 2. As notificações são diárias e são geradas pelo *script* que pega informações do *backbone* e faz *deep packet inspection*. O *script* é executado ao longo do dia e após o fim do dia, esse recomeça a contagem das notificações. Isto explica porque, em quase todos os dias, o número de notificações variou entre 7 e 6. Provavelmente os dispositivos comprometidos e os usuários executando mineração eram sempre os mesmos, e sua atividade diária gerou em torno de 7 notificações predizíveis por dia (e.g., na comunicação entre o usuário e a central de mineração). Cabe destacar que em alguns dias, como por exemplo, no dia 27 de janeiro (sábado) não houve comunicação devido a rede da UFRJ ser instável nos fins de semana, quando ocorre à manutenção nesta.

Em determinados dias, por exemplo, no dia 24 de janeiro, tivemos uma baixa no número de notificações que, em seguida, aumentou no dia 25 de janeiro. Isto deve-se ao fato de que no dia 24 de janeiro o problema da mineração foi sanado provisoriamente, reinstalando-se algumas máquinas do sistema. Entretanto, o problema retornou porque o vetor de ataque ainda estava ativo e reiniciou suas atividades no dia 25 de janeiro. A seguir, será descrito em mais detalhes um dos episódios ocorridos neste período.

Episódio de mineração Bitcoin: Em uma unidade da UFRJ, identificou-se computadores minerando Bitcoin. A partir do histórico de navegação do *browser*, constatou-se que um usuário havia acessado sites de *mining pools*. Dentre eles, destacaram-se os sites `http://btc.com` e `http://f2pool.com`. Nesses sites, o usuário faz login com sua conta e basta deixar o computador ligado para arrecadar recursos de mineração. Por descuido, o usuário deixou um arquivo com um rastro de seu login e senhas de mineração na máquina. Com as credenciais de acesso às *pools*, foi possível identificar os instantes de início e fim de cada atividade de mineração.

	Configuração 1	Configuração 2	Configuração 3
Processador	Intel Pentium Dual Core	Intel Core i3	Intel Core i5
Núcleos	02	02	04
Memória RAM	04 Gb	04 Gb	04 Gb

Tabela 3. Configurações de máquinas usadas em nossos experimentos

Cabe destacar que a notificação do evento acima alertou a equipe de segurança para tomar as iniciativas anteriormente ditas, foi gerada pelo fato de ter ocorrido acesso ao site da *mining pool*, que por sua vez gerou tráfego suspeito. Isto ocorreu pelo descuido do usuário ao fazer a mineração. Caso a mineração fosse cuidadosamente executada a fim de produzir o mínimo de interações com o restante da rede, acredita-se que teria sido mais difícil detectar a atividade suspeita.

Dentre as moedas virtuais mais mineradas na UFRJ, destacaram-se o Bitcoin e o Monero.

Bitcoin: O Bitcoin foi a primeira moeda virtual a ser adotada em larga escala, o que justifica sua prevalência na UFRJ. O Bitcoin funciona como um lastro para as outras criptomoedas e já existem inúmeros programas simples para minerar Bitcoin em qualquer plataforma (Linux, MacOS, Android e Windows, nas mais diversas versões).

Monero: O Monero [Andersen 2014] proporciona aos seus usuários níveis de privacidade maiores que aqueles oferecidos pelo Bitcoin. Além disso, ele também provê as facilidades em termos de *software* de mineração para *script kiddies*. Por esses motivos, muitos mineradores têm adotado o Monero como criptomoeda de primeira escolha, conforme identificado nas medições.

6. Ganhos e custos estimados com a mineração

A seguir, apresentam-se resultados obtidos com experimentos controlados em laboratório para estimar os ganhos e custos associados à mineração na UFRJ. Em particular, emulam-se as configurações das máquinas que descobriram-se estarem minerando, entre janeiro e feveiro de 2018, conforme descrito anteriormente na Seção 5.

6.1. Ambiente do experimento controlado

Consideram-se três configurações que correspondem às máquinas mineradoras de Monero e Bitcoin encontradas na UFRJ (vide Seção 5). Não é surpreendente que tais configurações siguam padrões encontrados em computadores nos diversos setores da instituição, visto que as compras de equipamentos são feitas em lotes. Assim, as configurações também capturam de forma mais ampla os potenciais ganhos e custos de mineração na UFRJ como um todo. A Tabela 3 resume as configurações.

O experimento contou com 3 máquinas. Para cada configuração apresentada na Tabela 3, considera-se uma máquina mineradora, que passou o período do experimento minerando. Os *hosts* executam o sistema operacional Linux Ubuntu 16.04 e o *software* de monitoramento de consumo de energia *PowerTOP*. O software de mineração escolhido foi o *MinerGate*, que minera a moeda virtual Monero (vide Seção 5). Para fins de coleta de dados da rede (monitoramento de fluxos de rede) utilizou-se o *NFDump* (*netflow*) e para visualizar os fluxos foi usado o *NFsen* e *RRD Graphics*.

***Hashing power* (frequência de mineração)**			
Descrição	**Config. 1**	**Config. 2**	**Config. 3**
Hashing por *host* (r)	85 H/s	88 H/s	177 H/s
Hashing total, assumindo $N = 3$ ($R = Nr$)	255 H/s	264 H/s	531 H/s
Consumo de energia			
Consumo energético por *host* (e)	21 W/h	38 W/h	40 W/h
Consumo energético total em KW por dia, assumindo $N = 3$ ($NE = 24 \times 10^{-3} Ne$)	1,512 KW	2,736 KW	2,880 KW
Custo total, assumindo $N = 3$ ($C = NEc$)	R$ 0,92	R$ 1,67	R$ 1,76
Ganhos totais com 1/100 de pool fee[1]			
Total minerado (XMR) em 24 horas	0,0001563	0,0001618	0,003254
Ganho total (G) em reais	R$ 0,27	R$ 0,28	R$ 5,61

Tabela 4. Custos e ganhos totais de mineração de Monero com 3 *hosts* e as respectivas configurações (vide Tabela 3) (conforme Fig. 2, houve uma média de três *hosts* ativos minerando na UFRJ em janeiro e fevereiro de 2018).

6.2. Resultados experimentais

A Tabela 4 ilustra os custos e ganhos associados à mineração de Monero na infraestrutura típica da UFRJ, utilizando cada configuração apresentada na Tabela 3.

Seja N o número de *hosts* minerando ao longo do período de observação, para cada uma das configurações. Neste trabalho, considera-se $N = 3$. Optou-se por utilizar este valor pelo fato de que, na média observou-se em torno de 3 incidentes de mineração durante o período observado entre janeiro e fevereiro de 2018 (vide Seção 5).

Cabe destacar que no experimento minerou-se apenas via CPU. Em geral, pode-se minerar via CPU e GPU. Entretanto, como as máquinas da UFRJ em geral não possuem GPU, optou-se pela primeira opção.

A mineração ocorreu durante o período de dois meses. Porém, em alguns dias do experimento, ocorreram falhas no fornecimento de energia elétrica e de conectividade com a internet. Assim, optou-se por apresentar uma amostra de 24 horas, onde, além de demonstrar dados íntegros, torna mais fácil a compreensão do trabalho. Seja $r^{(j)}$ o poder de *hashing* de cada máquina, na configuração j e ***H/s*** representando *hashes por segundo*. Nas medições reportou-se $r^{(1)} = 85$ H/s , $r^{(2)} = 88$ H/s e $r^{(3)} = 177$ H/s, respectivamente. O poder de *hashing* total é dado por $R^{(j)}$ no sistema j, $j = 1, 2, 3$, $R^{(j)} = Nr^{(j)}$.

O ganho diário correspondente ao poder de *hashing* reportado acima, com os 3 *hosts*, é dado por $G^{(1)} = R\$\ 0{,}27$, $G^{(2)} = R\$\ 0{,}28$ e $G^{(3)} = R\$\ 5{,}61$, nas configurações 1, 2 e 3 respectivamente. Para a obtenção de tais valores, foi utilizada a cotação média do Monero em reais no período de estudo. Embora o poder de *hash* da configuração 3 seja de aproximadamente o dobro daquele reportado nas configurações 1 e 2, fatores aleatorios inerentes à mineração causaram um ganho relativo muito superior na configuração 3, no estudo de caso considerado. Nas configurações 1 e 2 os ganhos esperados são pequenos comparados com os gastos energéticos e custos monetários, conforme indicado a seguir.

Para estimar o gasto energético por *host*, mediu-se o consumo energético das

[1]Taxas de utilização da moeda

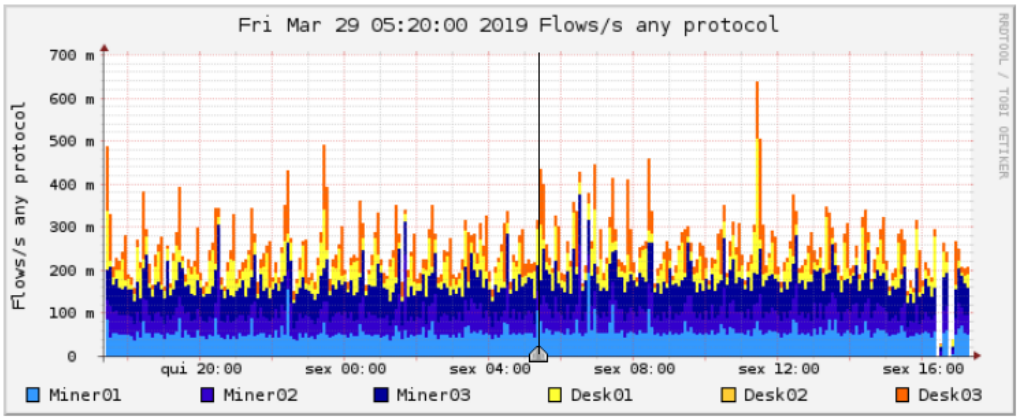


Figura 3. Tráfego total dos *hosts* no experimento

máquinas. Os valores medidos por máquina foram $e^{(1)} = 21$ W/h, $e^{(2)} = 38$ W/h e $e^{(3)} = 40$ W/h, para as configurações 1, 2 e 3, respectivamente. Multiplicando pelo número de *hosts* ativos, e pelo custo de energia[1] obtemos o custo total estimado por dia, $C^{(j)} = 0,024e^{(j)}Nc = E^{(j)}Nc$, onde o custo c é medido em reais por KW e o consumo de energia E em KW por dia.

Até então, não foram levados em consideração os padrões de rede associados à mineração no experimento controlado, nem os custos de rede subjacentes. Para uma análise preliminar sobre aspectos de rede são consideradas, além das 3 máquinas mencionadas até então, mais 3 máquinas, com as mesmas configurações. Tais máquinas adicionais são máquinas *baseline*, que executam aplicações de um *desktop* de uso geral, e que não fazem mineração. Um dos propósitos é contrastar o uso de rede das máquinas correspondentes (Figura 3).

Conforme indicado na Figura 3, o padrão de tráfego dos *hosts* que estão realizando a mineração é inferior ao dos *hosts* executando atividades padrões de equipamentos da UFRJ. Este fato corrobora a ideia de que é mais desafiador identificar ataques de mineração remotamente, conforme considerado neste trabalho, em comparação com uma detecção local no *browser*, usando ferramentas do tipo *mine blockers* [Cherone and Mahon 2018] (vide Tabela 1).

7. Discussão

Nesta seção, são discutidos aspectos mais amplos relacionados ao trabalho, alguns dos quais são fruto de pesquisa corrente ou de trabalhos futuros.

7.1. Mitigação de ataques de mineração: um estudo de caso na UFRJ

Para mitigar os ataques sofridos pelas máquinas, foi definida uma política de atuação constituída pelos seguintes passos: (1) Restauração de *backups* não comprometidos, caso existam; (2) Remoção de *worms* e *malwares*; (3) Bloqueio dos IPs de *mining pools* e de sites de mineradoras. Adotando a política acima, a partir de março de 2018, identificou-se que o número de casos reportados de mineração na UFRJ diminuiu significativamente. A inserção de sanções legais na política de segurança da informação também poderia reduzir este tipo de incidente.

[1]Custo / KW- Jan.2018 - R$ 0,61 - Valor informado no site da companhia fornecedora.

7.2. Identificação automática de mineração

Como forma de identificar automaticamente os ataques de mineração considerados neste artigo, é imperativo que o sistema de IDS esteja preparado para detectar o comportamento de *malwares* voltados a mineração. Em trabalhos futuros, pretende-se elaborar um estudo baseado nos padrões do tráfego de rede encontrados, a fim de que sejam identificadas as comunidades ilegais de mineração. Cabe destacar que tais medidas de identificação automática de mineração estão fora do escopo da maioria dos trabalhos relacionados, tendo em vista que os mesmos assumem que pode-se monitorar o uso de CPU e memória das máquinas potencialmente comprometidas, tornando assim o monitoramento da rede, muito mais difícil, desnecessário (vide Tabela 1). A identificação automatizada de mineração nas conexões realizadas através de VPNs *(Virtual Private Networks)* também traz seus seus próprios desafios, a serem tratados em trabalhos futuros.

7.3. Monetização da mineração em benefício público

A monetização da mineração, em benefício da própria UFRJ, é potencialmente promissora. Uma vez que a universidade tem períodos de baixa movimentação ou ociosos, o que faz com que os recursos sejam subutilizados, pode-se considerar a mineração durante esses períodos.

Cabe destacar que a monetização da mineração, tanto para universidades quanto para usuários domésticos, é promissora mas não-trivial. Existe ampla oportunidade para se monetizar a mineração em infraestruturas privadas ou públicas. Entretanto, esta monetização envolve prever o valor das criptomoedas e o excedente de energia com o qual cada instituição pode contar a priori.

Em residências domésticas em inúmeras cidades do Brasil, por exemplo, existe um consumo mínimo de energia associado ao valor básico mínimo da conta de luz. Em residências nas quais não se alcance esse limite, é possível monetizar o excedente. Alternativamente, em órgãos públicos o custo da conta varia em faixas, e é importante que a mineração legal ocorra dentro das faixas de interesse.

8. Considerações finais

Ataques de mineração vêm se popularizando pelo fato de serem fáceis de implementar e potencialmente gerarem recursos financeiros que possam ser convertidos em qualquer tipo de bens. Tais ataques, por sua vez, consistem em uma ameaça à estabilidade das próprias criptomoedas. Afinal, se os ataques se tornarem muito prevalentes, pode haver mais incentivo para que as mesmas sejam banidas de inúmeros países, diminuindo seu valor. Se o valor das moedas for reduzido a zero, os ataques de mineração perderão seu propósito. Portanto, em prol da estabilidade da Internet e das criptomoedas, é fundamental o reconhecimento da prevalência destes ataques, e o domínio das formas de mitigá-los.

Neste trabalho apresentou-se medições que indicam que ataques de mineração ocorreram na UFRJ. Em particular, foi indicado que Bitcoin e Monero foram as duas moedas mais mineradas. Em seguida, apresentou-se resultados de um experimento controlado indicando os ganhos e custos desta mineração no campus universitário, em janeiro e fevereiro de 2018. Finalmente, indicou-se também formas de mitigar estes ataques, que foram aplicadas na UFRJ.

Acredita-se que este trabalho abre portas para inúmeros desenvolvimentos futuros. Em particular, no Brasil o problema dos "gatos" nas favelas pode ser uma porta de entrada para o novo problema dos "gatos" virtuais. Medições que permitam avaliar a prevalência deste tipo de ataque são primordiais, e precisam ser feitas em colaboração entre as empresas de prestação de serviços de energia e de comunicação.

Referências

Andersen, D. (2014). Mining money with monero and cpu vector intrinsics. https://da-data.blogspot.com/2014/08/minting-money-with-monero-and-cpu.html.

Avritzer, A., Tanikella, R., James, K., Cole, R. G., and Weyuker, E. (2010). Monitoring for security intrusion using performance signatures. In *WOSP/SIPEW Conf. Performance engineering*, pages 93–104. ACM.

Cherone, L. and Mahon, P. (2018). Minerblock extension. https://tinyurl.com/minerblock.

Coinblockerlists (2018). Coinblockerlists. https://github.com/ZeroDot1/CoinBlockerLists.

Hong, G., Yang, Z., and Yang, S. (2018). How you get shot in the back: A systematical study about cryptojacking in the real world. In *ACM SIGSAC Computer and Comm. Security*, pages 1701–1713.

Keramidas, R. (2018). No coin. https://github.com/keraf/NoCoin/blob/master/src/js/background.js.

Kharraz, A., Ma, Z., Murley, P., Lever, C., and Mason, J. (2019). Outguard: Detecting in-browser covert cryptocurrency mining in the wild. *The Web Conference (WWW)*.

Kührer, M., Rossow, C., and Holz, T. (2014). Paint it black: Evaluating the effectiveness of malware blacklists. In *Advances in Intrusion Detection*, pages 1–21. Springer.

Marini, T. (2017). Gato de energia é usado para minerar bitcoins em Paraisópolis. *Estadão*.

Nadaud, G. C. A. (2012). Acesso à energia elétrica de populaçoes urbanas de baixa renda: o caso das favelas do Rio de Janeiro. *UFRJ/COPPE/Progr. Planej. Energético*.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Computers*.

Penin, C. (2008). Combat, prevention and optimization of commercial losses of power.

Rüth, J., Zimmermann, T., Wolsing, K., and Hohlfeld, O. (2018). Digging into browser-based crypto mining. In *IMC*, pages 70–76. ACM.

Segura, J. (2018). The state of malicious cryptomining. https://tinyurl.com/maliccry.

Setti, R. (2018). Febre de bitcoins cria uma nova indústria de 'mineradores'. *O Globo*.

Wu, Z., Ou, Y., and Liu, Y. (2011). A taxonomy of network and computer attacks based on responses. *Info. Technology, Computer Engineering and Managm. Sciences*, page 4.

Zimba, A. and Wang, Z. (2018). Crypto mining attacks in information systems: An emerging threat to cyber security. *Journal of Computer Information Systems*, page 13.