UFRJ

Gatos virtuais: detectando e avaliando os impactos da mineração de criptomoedas na UFRJ

Autor: Victor R. Pires

Universidade Federal do Rio de Janeiro

Índice

- Motivação
- Mineração em infraestruturas públicas
- Problemas e propostas
- Medições dos impactos
- Descoberta de ataques de mineração
- Mitigação
- Trabalhos relacionados
- Trabalhos Futuros
- Como eu sei que não estou minerando?

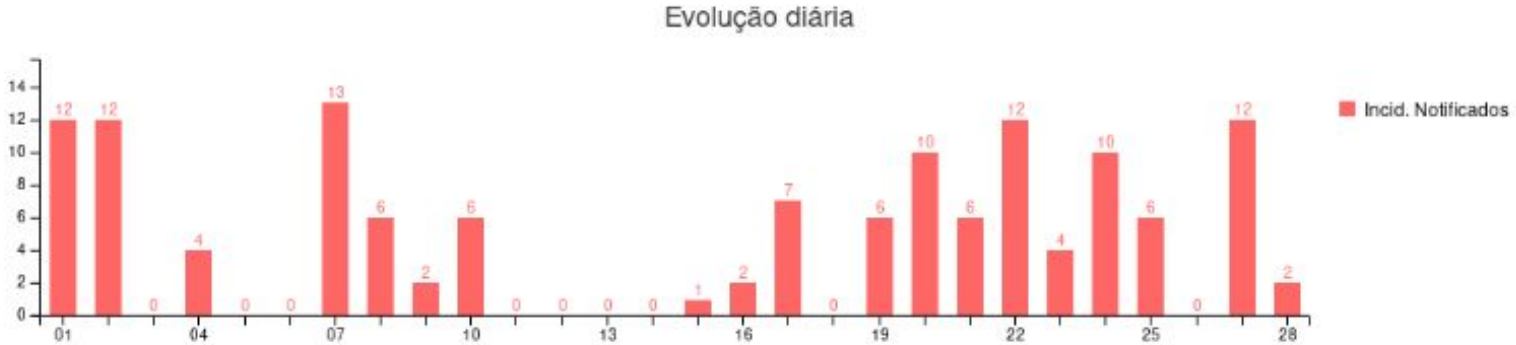
Motivação - Incidentes de segurança na UFRJ

UFRJ

- São monitorados e tratados pela Superintendência de Tecnologia da Informação - TIC
- Parceria com a RNP para a detecção de incidentes
- No ano de 2018, detectamos um novo padrão de ataque a UFRJ

LabNet

(a) janeiro de 2018



(b) fevereiro de 2018

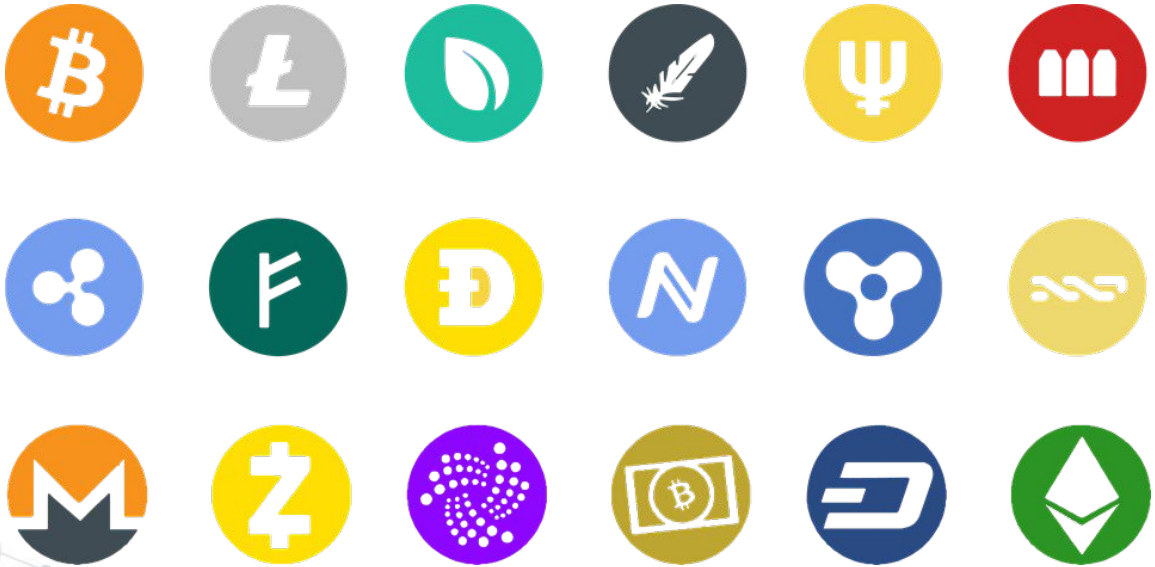
Figura 1. Número de incidentes em janeiro de e fevereiro de 2018

Motivação

- Entre janeiro e fevereiro de 2018 a UFRJ recebeu uma série de ataques de mineração de criptomoedas
  - Os ataques de mineração foram uma grande parcela dos incidentes nesse intervalo
- Esse tipo de ataque recebe o nome de *cryptojacking*
- Estimamos que uma máquina infectada concederia ao atacante valores entre R$0,2 e R$5,61 diariamente

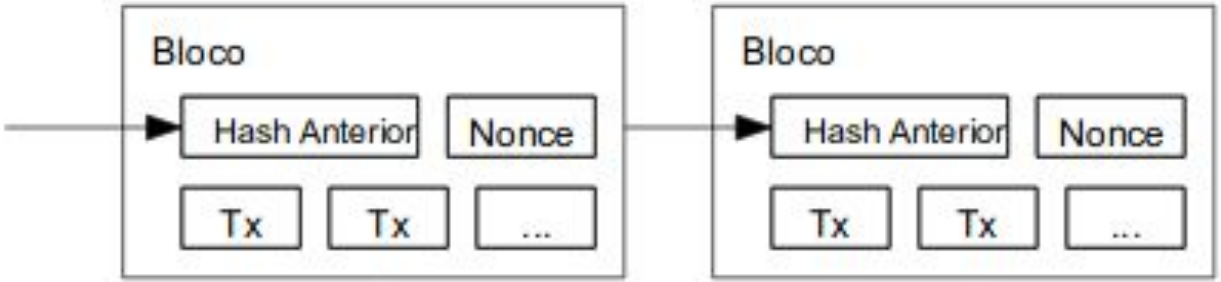
Criptomoedas

- Representam uma forma de converter energia em meio de troca



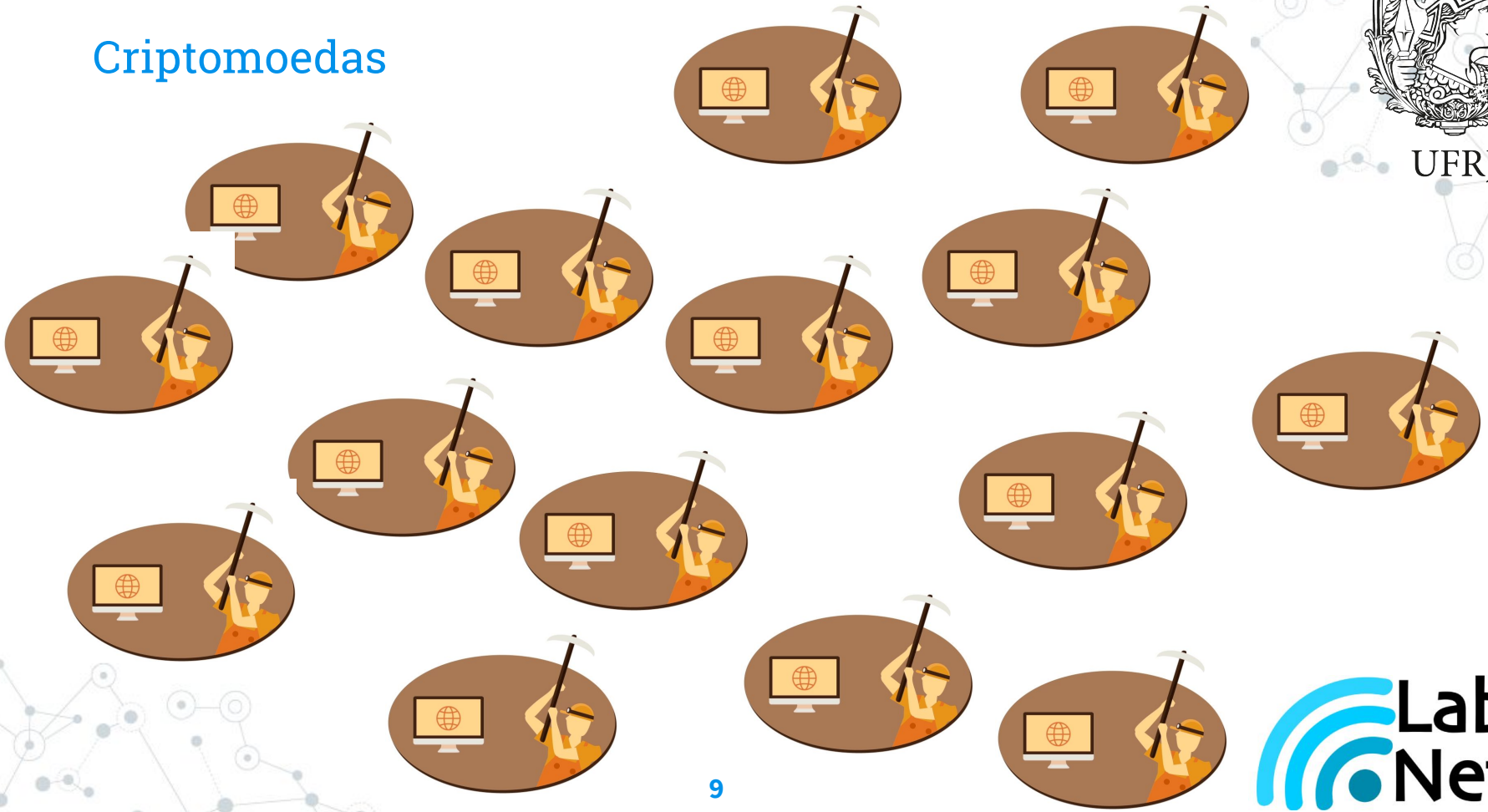
Criptomoedas

- Como uma criptomoeda funciona?



Criptomoedas

Criptomoedas



Criptomoedas


SecurityIntelligence

News Series Topics Indu

Home / Threat Research / Advanced Threats

Mirai IoT Botnet: Mining for Bitcoins?

April 10, 2017 | By **Dave McMillen** co-authored by **Michelle Alvarez** | 4 min read

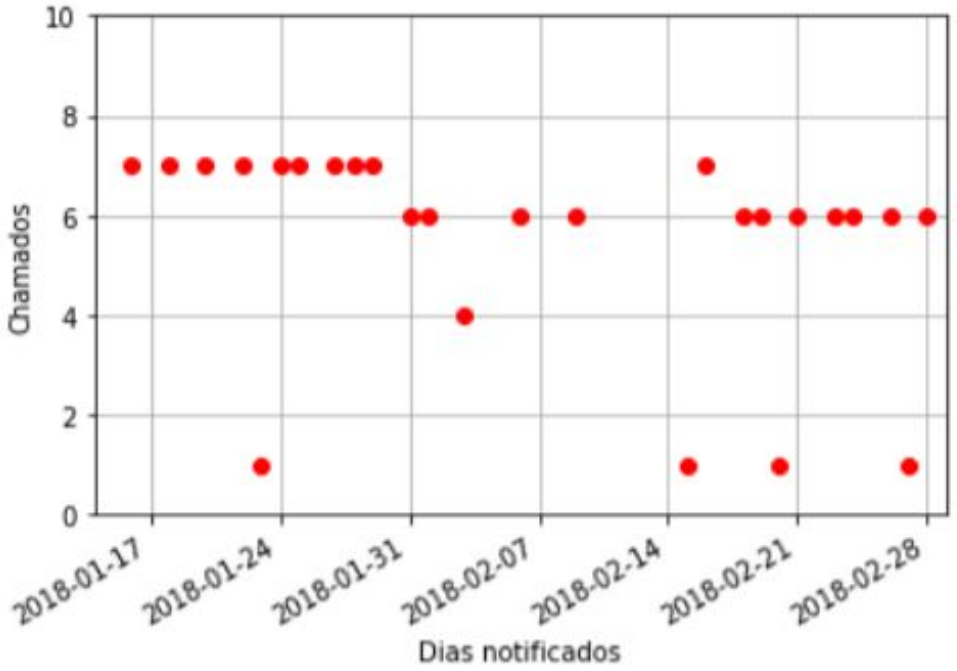


Figura 2. Número de incidentes com finalidade de mineração de criptomoedas

Mineração em infraestruturas públicas

- As infraestruturas públicas são suscetíveis a ataques de mineração devido ao fato de:
  - Usuários terem acesso às máquinas
  - Apresentarem um grande número de hosts
  - As equipes em geral serem reduzidas e/ou pouco especializadas
  - Terem energia elétrica abundante e internet
- Energia é o principal atrativo para um minerador

GATO DE ENERGIA É USADO PARA MINERAR BITCOINS EM PARAISÓPOLIS

Atividade oco do especialistas

Para evitar gasto de luz, Danilo usa ligação ilegal feita por um vizinho em Paraisópolis | Foto: Nilton Fukuda

Problema a ser tratado

1 - Como identificar ataques de mineração em infraestruturas públicas?

2 - Como medir os impactos desses ataques?

3 - Como mitigar esses ataques?

Proposta do trabalho

1 - Propomos um modelo de gasto gerados pelos gatos

2 - Propomos uma forma de detectar esses ataques

3 - Propomos uma forma de mitigar esses ataques

Contribuições do trabalho

1 - Foi descoberto que mineração ilegal de criptomoedas é prevalente

2 - Os custos e ganhos advindos da mineração ilegal foram estimados

3 - São propostas novas formas de descobrir e mitigar a mineração ilegal

Como medir os impactos desses ataques?

- A remuneração estimada do ataque foi emulada em laboratório
- As configurações de máquinas foram baseadas nos lotes que a UFRJ costuma comprar em licitações
- A escolha da simulação com Monero fez-se devido o alto número de casos dentro da UFRJ

Configuração das máquinas dos experimentos

	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 1: Configuração das máquinas para os experimentos

Estimativa dos ganhos

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 2: Resultados dos experimentos de mineração

Descoberta dos ataques de mineração

- A descoberta de ataques de mineração começa com a notificação de que uma máquina se comunica com uma *mining pool*
- Uma *mining pool* é um cluster de máquinas mineradoras
- Outra forma de descobrir é pelo tráfego anômalo da rede

Descoberta dos ataques de mineração

- Depois de descoberta a mineração, fazemos uma perícia física nas máquinas
- Em um caso particular, um funcionário da instituição era o atacante
- Em outro caso particular, a máquina era um banco de dados (que não estava em atividade) do SIGA

Mineração em infraestruturas públicas - Caso da UFRJ

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

Lab NET

Mitigação - Caso da UFRJ

UFRJ

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.

LabNet

Trabalhos relacionados

[Segura 2018], [Ruth et al. 2018], [Hong et al. 2018], [Kharraz et al. 2019], [Zimba and Wang 2018]

Descrevem que o usuário foi infectado por um *worm* ou acessou uma página com um *script* de mineração

Nesse trabalho, consideramos que o usuário tem acesso físico às máquinas e pode se tornar um atacante

Trabalhos Futuros

1. Detector automático de ataques de mineração
2. Como melhorar a detecção desses ataques
3. Monetização da mineração em benefício público
4. A prevalência de fazendas ilegais de mineração em favelas ou outras instituições e seus impactos

Como eu sei que eu não estou minerando?

1. Preste atenção no processamento do seu computador
2. Se estiver sentindo os navegadores pesados, fique atento
3. Não se engane, aplicativos de celular também podem ter mineradores

Como eu sei que eu não estou minerando?

Site do Governo de SP usou computador de visitante para minerar moeda virtual

Usado sem avisar usuários, mecanismo faz computador ficar lento e gastar mais energia. O Governo de SP tirou código e investiga o caso.

Por Helton Simões Gomes, G1

10/11/2017 13h04 · Atualizado há um ano

Como eu sei que eu não estou minerando?

ECONOMIA

BLOG DO ALTIERES ROHR

Hackers atacam roteadores MikroTik no Brasil para minerar criptomoedas na web

02/08/2018 15h22 · Atualizado há um ano

Como eu sei que eu não estou minerando?

Perguntas?

OBRIGADO

slowhusky@gmail.com