

Julio Lemus

Security Engineer , Panama & Honduras CCA



**HACKING
LIKE A DISNEY VILLAIN**

Biological Pandemic vs. Cyber Pandemic:

Similarities and Parallelization, Lessons Learned

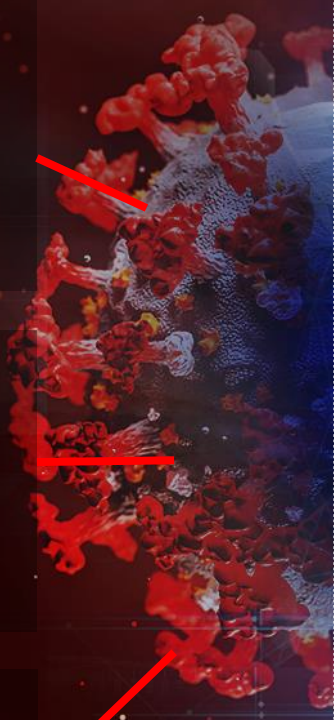
BIOLOGICAL PANDEMIC



INFECTION RATE

Virus infection rate (R0) (source:WHO)
The average number of people that one person with a virus infects

Flue: 1.3, SARS: 2-4, **Corona: 2.5**
Ebola:1.6-2, ZIKA:2-6.6, Measels:11-18



INFECTION PREVENTION

Best treatment: **Vaccination**
Dealing with Infection Best Practices:

- 1)Quarantine, shelter in place
- 2)Isolation
- 3)Contact tracing



SAFETY BEST PRACTICES

common treatment (until vaccination):

- 1)Mask
- 2)Hygiene
- 3)Social distancing

CYBER PANDEMIC



INFECTION RATE

Malware infection rate (R0) The average number of infections that one host with a malware causes

Cyber attack- >27(source: WEF, NSTU),
Slammer: doubled in size every 8.5 seconds,
Code red – 2000 new hosts per minute



INFECTION PREVENTION

Best treatment: **Real Time Prevention**

Best Practices- **Continuous** process of:

- 1)**Quarantine**: sandboxing, micro segmentation
- 2)**Isolation**: Zero Trust, segregation
- 3)**Tracing**: Threat Intel., AI, SOC, Posture management



SAFETY BEST PRACTICES

- 1)**Awareness**: think before you click ...
- 2)**Cyber Hygiene**: Patches, Compliance...
- 3)**Asset distancing**- network Segmentation, Multi Factor authentication...

Snow White



From: Sweepstakechoices [REDACTED]
To:
Cc:
Subject: Qualify and GET an iPhone6!

Qualify and GET an iPhone6!

How to Snag- an Iphone-6

[Start and Begin-Here Today](#)

Get a **brand new**
iPhone 6*!



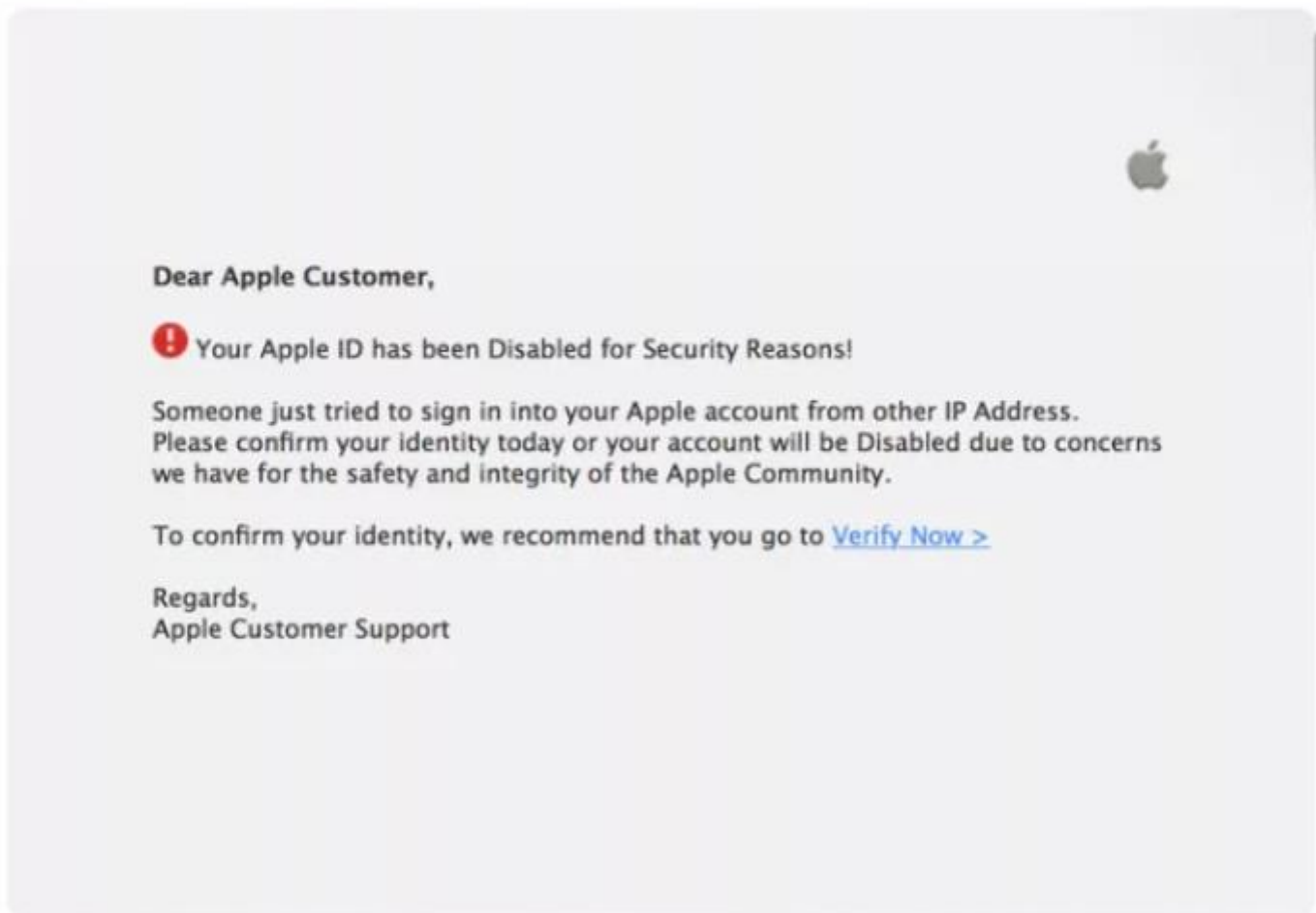
Apple Support

December 4, 2014 at 7:00 PM



To: Kirk McElhearn

YOUR APPLE ID WAS USED TO SIGN IN TO ICLOUD ON AN IPHONE 3



Dear Apple Customer,

! Your Apple ID has been Disabled for Security Reasons!


Someone just tried to sign in into your Apple account from other IP Address. Please confirm your identity today or your account will be Disabled due to concerns we have for the safety and integrity of the Apple Community.

To confirm your identity, we recommend that you go to [Verify Now >](#)

Regards,
Apple Customer Support





apachetelas 

Membro



Data de Ingresso: Nov 2017

Posts: 1

Thanked: 0

Peso da Avaliação : 0

! Telas Fakes [A]PACHE

COLHA SUAS PRÓPRIAS INFOS E PAGUE SEUS BOLETOS

~TELAS FAKES COMPLETAS, COM SUPORTE TOTAL~

~BOLETOS VÁLIDOS EM CAIXAS ELETRONICOS E APLICATIVOS MOBILE~

COM PAINEL ADMINISTRATIVO PARA INSERÇÃO DE PRODUTOS, APENAS COM A URL

- ANTI-PISHING
- CONTROLE DE INFOS
- NOTIFICAÇÃO SONORA
- ATENDIMENTO VIA CHAT
- ENVIO DE 2ª VIA DE BOLETOS
- CONTROLE DE USUÁRIOS EM TEMPO REAL
- SISTEMA DE IDENTIFICADOR DE ANALIZE FACEBOOK (X9) NOVO

LISTA DE TELAS DISPONÍVEIS

- AMERICANAS - LETO E CC - Aluguel semanal R\$ 200,00 - COM X9
- WALMART - LETO E CC - Aluguel semanal R\$ 200,00 - COM X9
- PONTO FRIO - LETO E CC - Aluguel semanal R\$ 200,00 - COM X9
- CASAS BAHIA - LETO E CC - Aluguel semanal R\$ 100,00
- SUBMARINO - LETO E CC - Aluguel semanal R\$ 100,00
- SHOPTIME - LETO E CC - Aluguel semanal R\$ 100,00
- EXTRA - LETO E CC - Aluguel semanal R\$ 100,00

TELA PONTO FRIO ONLINE

<http://pontofrio.choraconcorrenca.c...ctype=w16&id=1>

SUPORTE TOTAL

[A]PACHE - TELAS FAKES DE QUALIDADE





Página Inicial

Configurações

Adicionar Usuários

Gerenciar Usuários

Editar Usuário

Cadastrar Boletos

Gerenciar Boletos

Backup Infos

Gerenciar Infos

Adicionar Produtos

Configurações

Configure sua tela antes de usar



Meus Pedidos | Dúvidas | Atendimento | Retira Rápido | Nossas Lojas | Televendas: 4003-2773

CASAS BAHIA

TVs e Acessórios | Eletrodomésticos | Câmeras e Filmadoras | Celulares e Telefones | Informática | Portáteis | Móveis | Saúde e Beleza | Games | Utilidades Domésticas

Esporte e Lazer | Livros | Ferramentas | Automotivo | Brinquedos | Bebês | Cama, Mesa e Banho | Relógios | Moda | Malas | Tablets | Decoração | **Black Friday**

Casasbahia.com.br > Telefones e Celulares > Smartphones > Android

Smartphone Samsung Galaxy J7 Prime Duos Dourado com 32GB, Tela 5.5", Dual Chip, 4G, Câmera 13MP, Leitor Biométrico, Android 6.0 e Processador OctaCore

(Cód. Item 10476497) (Cód EAN 7892509089913) Outros produtos Samsung

★★★★★ 719 Avaliações | [Leia](#) | [Faça uma avaliação](#)

Confira outras lojas que vendem o mesmo produto: De R\$ 1.095,00 até R\$ 1.566,00

Vendido e entregue por

Aproveite e confira **Microscópio Pacote Off**

De: R\$ 1.399,00 **Por: R\$ 949,00**

Televendas (11)4003-2773 | Encontre uma loja | Dúvidas

CASAS BAHIA

TELEFONIA | ELETRODOMÉSTICOS | TVS E ACESSÓRIOS | MÓVEIS | ELETROPORTÁTEIS | INFORMÁTICA | SERVIÇOS | OFERTAS DA TV | OFERTAS RETIRA

Chuva de Cupom | Festival de Verão | Cartão Casas Bahia | Galaxy J | Moto One | Sua TV Aquil | iPhone XR e XS | Saldão

Casasbahia.com.br > Telefones e Celulares > Smartphones > Android


Smartphone Samsung Galaxy J7 Prime Duos Dourado com 32GB, Tela 5.5", Dual Chip, 4G, Câmera 13MP, Leitor Biométrico, Android 6.0 e Processador OctaCore

(Cód. Item 10476497) Outros produtos Samsung

★★★★★ 1364 Avaliações | [Leia](#)

Vendido e entregue por CasasBahia.com.br

Aproveite e contrate

Clique e Compre Em até 12x de **R\$ 16,66**
Word, Excel e PowerPoint + 100GB de HD Virtual Total à vista: R\$ 199,90 **De: R\$ 239,00** 

De: R\$ 1.399,00 **Por: R\$ 949,00**
ou até 12x de R\$79,08 sem juros
Economia de: R\$450,00



```
<html lang="pt-br">
```

```
<head>
```

```
<title>||Painel Walmart 6
```

```
<meta http-
```

```
<meta
```

```
<meta
```



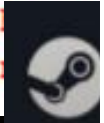
Detained Phishing Creator

May 19, 2018 / Pablo Rodríguez / Cybercrime , Hacking , Security News , News EHC , News , Information Security



A few days ago a young man named Douglas Arrial was arrested in Sao Paulo. This person traded in the *deep web* his tool [A] pache Next Generation Advanced Phishing Kit.

@douglasarrial

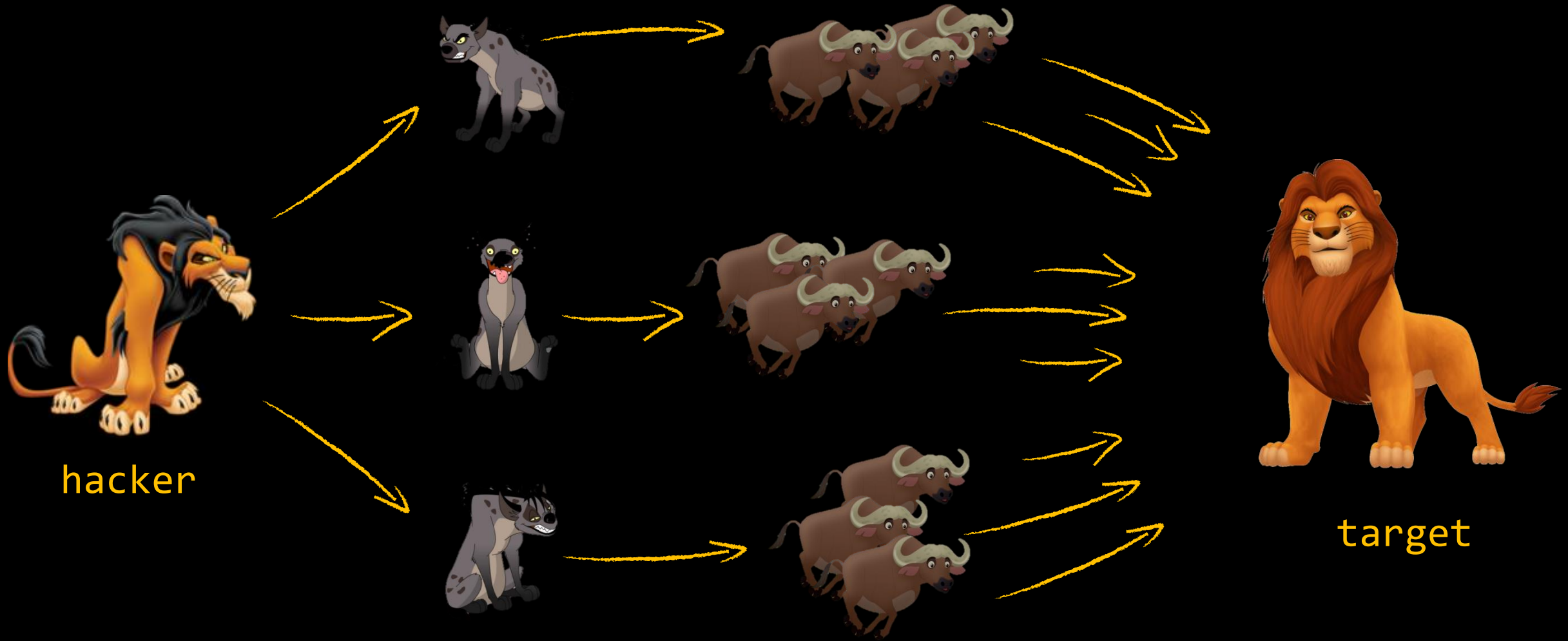


logo.jpeg



The Lion king





hacker

C&C servers

botnet
(IoT devices)

target

IoT Botnets - Timeline



2016

[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by Anna-senpai.)



Anna-senpai

L33t Member



Preface

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it's... However, I know every skid and their mama, it's their wet dream to have something besides qbot.

So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Krebs DDoS, shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

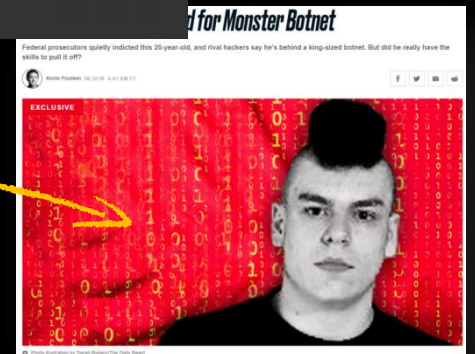
So, I am your senpai, and I will treat you real nice, my hf-chan.



GitHub

amazon

PayPal





Huawei Home Routers in Botnet Recruitment

December 21, 2017

- A Zero-Day vulnerability (CVE-2017-17215) in the Huawei home router HG532 has been discovered by Check Point Researchers, and hundreds of thousands of attempts to exploit it have already been found in the wild.
- The delivered payload has been identified as OKIRU/SATORI, an updated variant of Mirai.
- The suspected threat actor behind the attack has been identified by his nickname, 'Nexus Zeta'.



NexusZeta

Block or report user

ZetaSec

<http://nexusiotsolutions.net>

Overview

Repositories 2

Stars 0

Followers 0

Following 0

Popular repositories

Busybot

A busybox in vulnerability

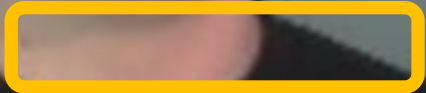
7 contributions

Mon

Wed

Fri

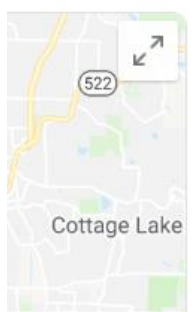
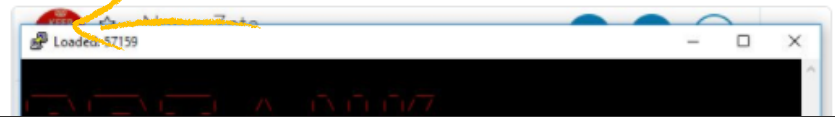
Learn



Joined August 2016

Tweet to Nexus Zeta

This botnet seems to be referencing someone that sounds familiar.



ve to mirai

runs in the State of rea. Based on per he state of Washington

Media

the armv6l cross-compiler co

...000 devices that I could use to my advantage...



The Little Mermaid

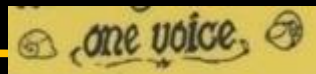




contract



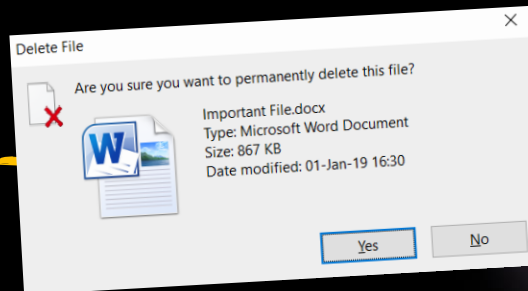
prize



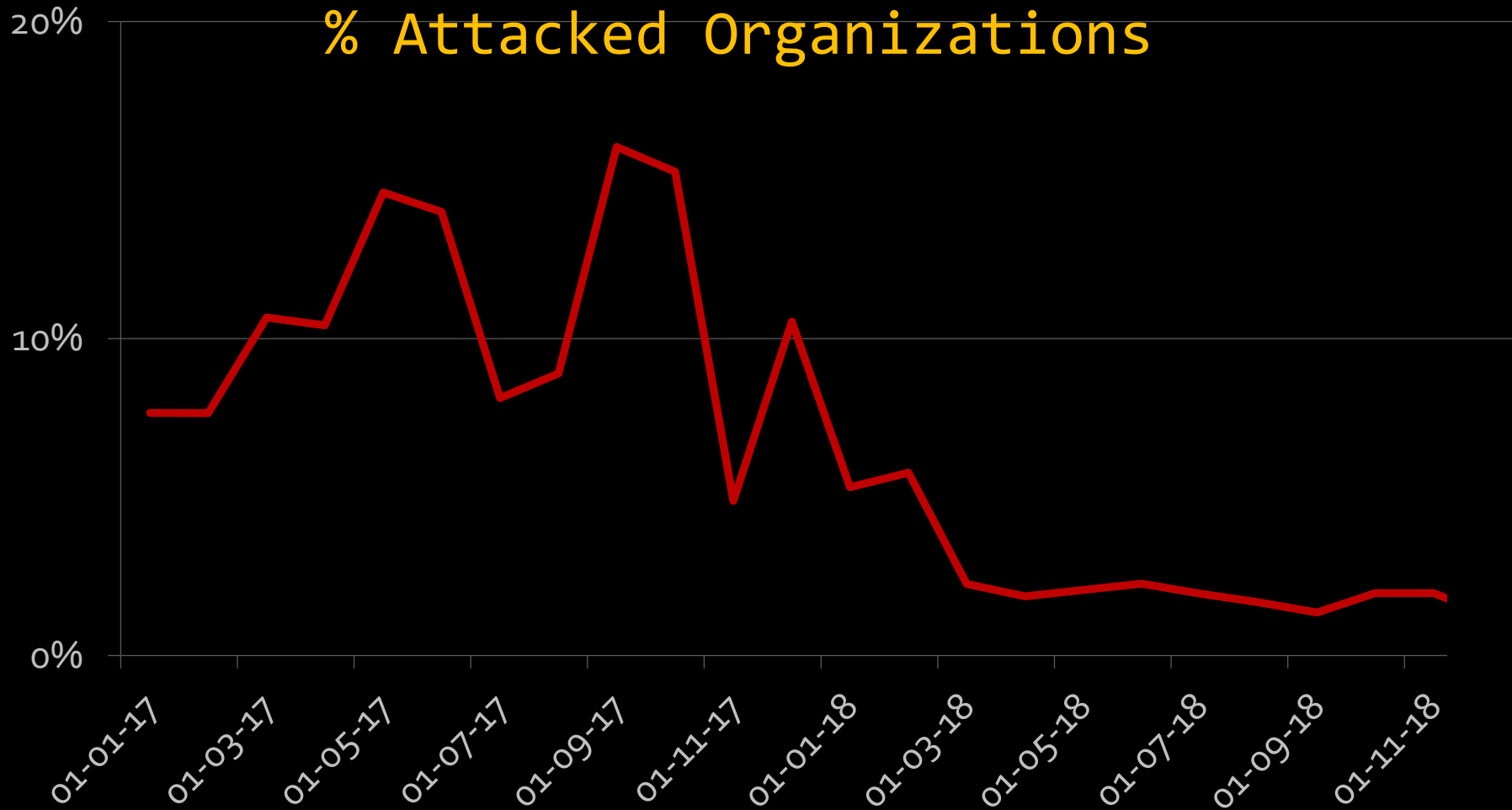
\$\$



or else



% Attacked Organizations



— Ransomware





Ryuk Ransomware: A Targeted Campaign Break-Down

Over the past two weeks, Ryuk, a targeted and well-planned Ransomware, has attacked various organizations worldwide. So far the campaign has targeted several enterprises, while encrypting hundreds of PC, storage and data centers in each infected company.

**\$ 55K-180K
per victim**



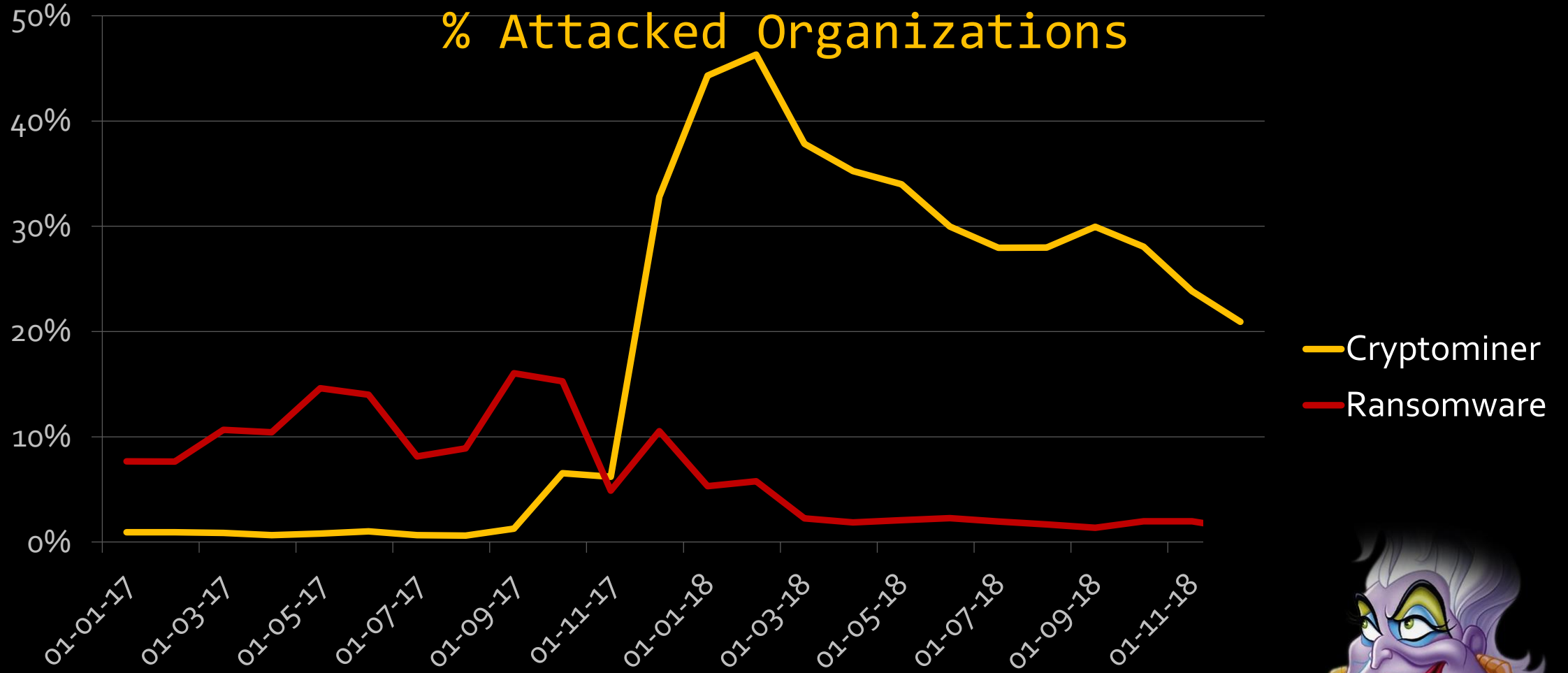
THE WALL STREET JOURNAL.
The New York Times
Los Angeles Times
Chicago Tribune

Ryuk

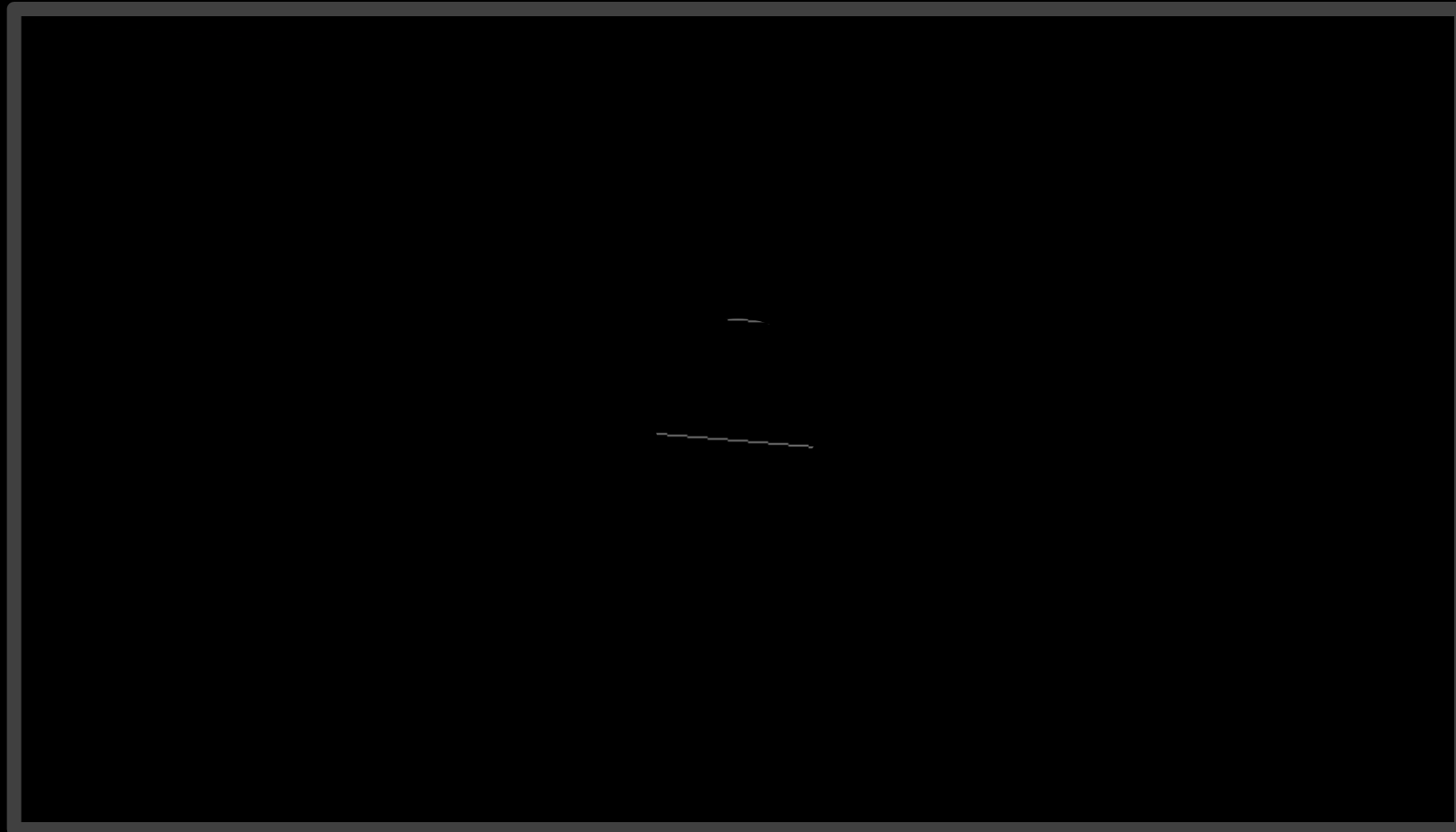
Hermes



% Attacked Organizations



Snow White





Coin mining



Wallet theft



Corporate Blog October 15, 2018
**September 2018's Most Wanted Malware:
Cryptomining Attacks Against Apple
Devices On The Rise**

Point's latest Global Threat Index reveals a near four-fold increase in cryptomining malware targeting Apple devices. Researchers detected over 100 attacks on Apple devices in September 2018.

A Crypto Mining Operation Unmasked

Introduction

With the emerging threat of miners and the rise of cryptocurrencies, the world has been kept busy lately. Check Point Research has been keeping an eye on the crypto mining world. Recently, we stumbled upon a large-scale operation targeting Monero miners, and more evidence accumulated as we dug deeper into the operation. This is the story of a mining operation that we discovered.

'RubyMiner' Cryptominer Affects 30% of WW Networks

Over the past 24 hours, 30% of networks worldwide have experienced compromise attempts by RubyMiner.

Jenkins Miner: One of the Biggest Mining Operations Ever Discovered

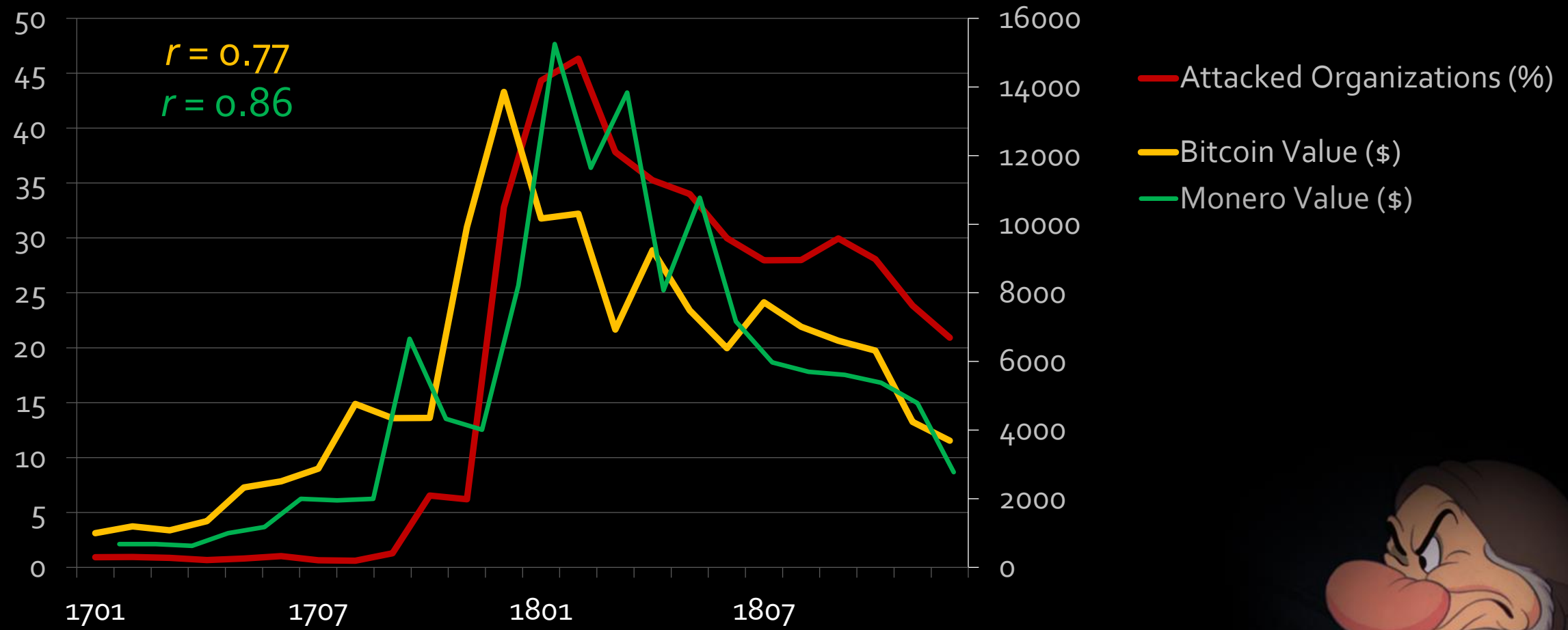
The Check Point research team discovered the biggest malicious mining operation ever.

KingMiner: The New and Improved CryptoJacker

May's Most Wanted Malware: Cryptomining Malware Digs into Nearly 40% of Organizations Globally

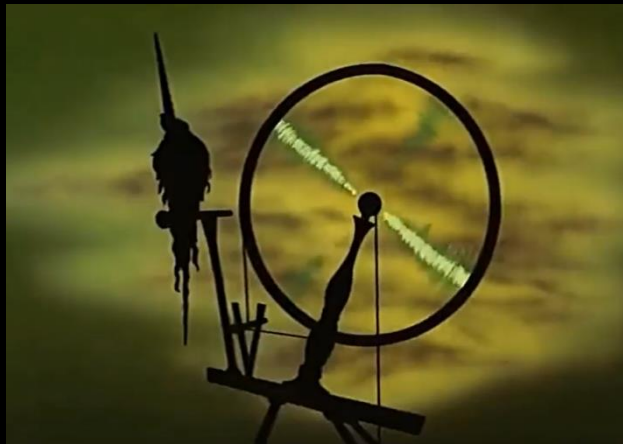


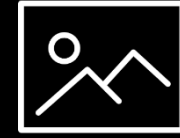
Malicious Cryptomining - Correlation with Currency Value



Sleeping Beauty





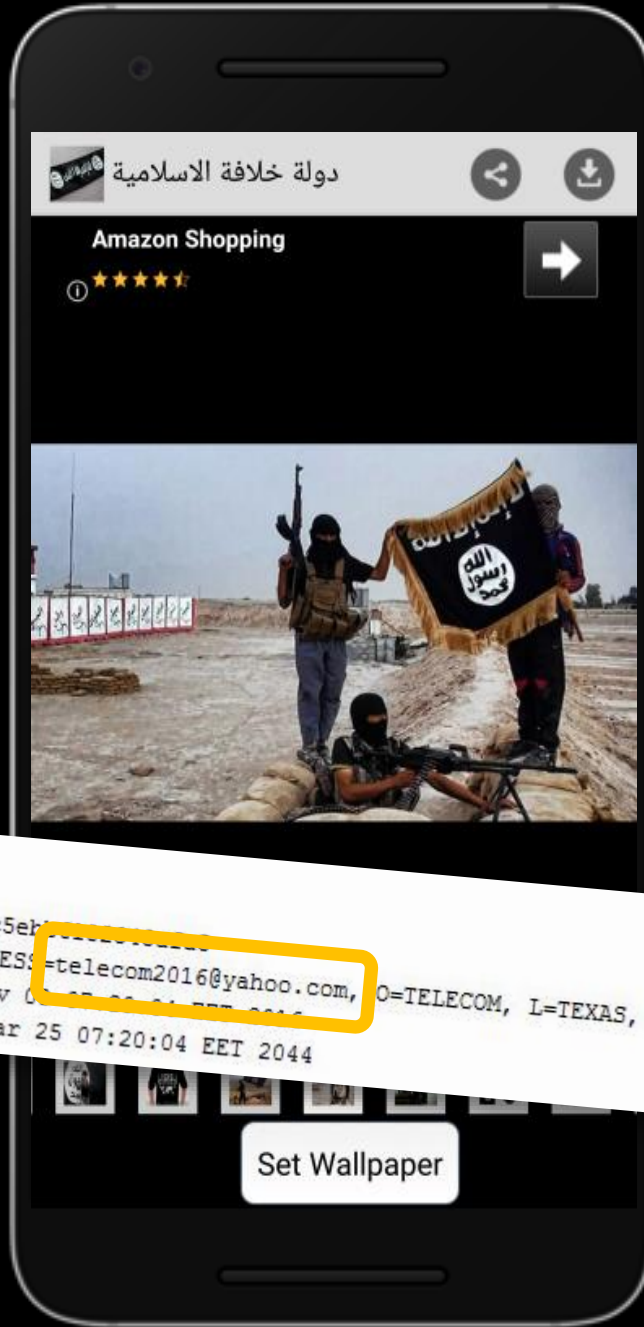




Hewalekem



ANF English



VidoGram



Hisn AlMuslim



دولة خلافة الاسلامية

```
Type: X.509
Version: 1
Serial number: 0xc5e...
Subject: EMAILADDRESS=telecom2016@yahoo.com, O=TELECOM, L=TEXAS, ST=OPEN-SSL, C=AU
Valid from: Tue Nov 0...
Valid until: Fri Mar 25 07:20:04 EET 2044
```



DeveloPERS



```
public Settings(Context paramContext)
{
    this.amPreferences = paramContext.getSharedPreferences("com.andriod.browser.AMService", 0);
    this.userName = readStr("UserName");
    if (this.userName == null) {
        save("UserName", "daeshsh");
    }
    this.serverAddress = readStr("ServerAddress");
    if (this.serverAddress == null) {
        save("ServerAddress", "http://www.ageofcyber.com/brw");
    }
    this.backup = readStr("Backup");
    if (this.backup == null) {
        save("Backup", "true");
    }
    this.hidden = readStr("Hidden");
    save("Hidden", "false");
    save("MediaBusy", "false");
    save("RecordCall", "false");
    refresh();
}

public static final String DELETE_FILE_KEY = "Delete File";
public static final int FILES_INDEX = 84;
public static final String GET_FILE_KEY = "Get File";
public static final int HARDWARE_INFO_INDEX = 118;
public static final int LOCATION_INDEX = 119;
public static final int LOG_INDEX = 0;
public static final long MAX_AUDIO_SIZE = 600000L;
public static final String MEDIA_BUSY_KEY = "Media Busy";
public static final String MEDIA_EXTENTION = ".mda";
public static final int PHOTO_INDEX = 107;
public static final String RECORD_CALL_KEY = "Record Call";
public static final String SERVER_ADDRESS = "http://www.ageofcyber.com/brw";
public static final String SMS_RECEIVED = "android.provider.Telephony.SMS_RECEIVED";
public static final String USER_NAME = "User1395";
public static final String VERSION = "1.0";
public static final int VIDEO_INDEX = 108;
```



ISIS
Supporters

Persian
Citizens

The Kurdish
Minority

Arabic
Speakers



Victims?



Check Point
SOFTWARE TECHNOLOGIES LTD.

Saudi Arabia

United Arab
Emirates

Gulf of Oman

Muscat

GUJARAT

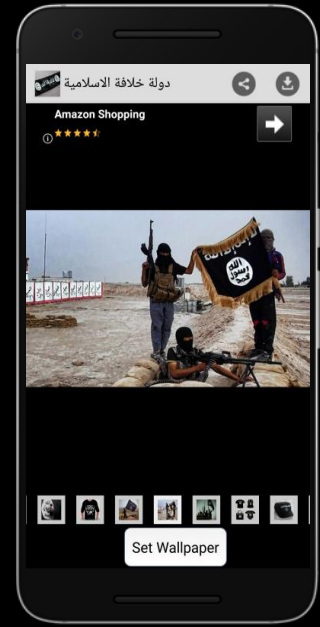


Developers

Victims

Method

```
public Settings(Context paramContext)
{
    this.amPreferences = paramContext.getSharedPreferences("com...");
    this.userName = readStr("UserName");
    if (this.userName == "None") {
        save("UserName", "daeshsh");
    }
    this.serverAddress = readStr("ServerAddress");
    if (this.serverAddress == "None") {
        save("ServerAddress", "http://www.firmwareupdate.com/mmh");
    }
    this.backupAddress = readStr("BackupAddress");
    if (this.backupAddress == "None") {
        save("BackupAddress", "http://www.firmwareupdate.com/mmh");
    }
    public static final String DELETE_FILE_KEY = "Delete File";
    public static final int FILES_INDEX = 84;
    public static final String GET_FILE_KEY = "Get File";
    public static final int HARDWARE_INFO_INDEX = 118;
    public static final int LOCATION_INDEX = 119;
    public static final int LOG_INDEX = 0;
    public static final long MAX_AUDIO_SIZE = 600000L;
    public static final String MEDIA_BUSY_KEY = "Media Busy";
    public static final String MEDIA_EXTENTION = ".mda";
    public static final int PHOTO_INDEX = 107;
    public static final String RECORD_CALL_KEY = "Record Call";
    public static final String SERVER_ADDRESS = "http://www.ageofcyber.com/brw";
    public static final String SMS_RECEIVED = "android.provider.Telephony.SMS_RECEIVED";
    public static final String USER_NAME = "User1395";
    public static final String VERSION = "5.2.0";
    public static final int VIDEO_INDEX = 108;
}
```



Surveillance of citizens?

THE MOST COMPLETE SECURITY

