Cenário das Ameaças Cibernéticas em Moçambique

Fabio Assolini | Senior Security Researcher

KASPERSKY lab

Quem sou eu?

- **Fabio Assolini**

Analista Senior de Malware desde 2009

Twitter.com/Assolini

Mas nada há encoberto que não haja de ser descoberto;
nem oculto, que não haja de ser sabido.” Lucas 12:2

GREAT Global Research & Analysis Team

Marco Preuss
Director of GReAT Europe
GReAT Europe

Christian Funk
Head of GReAT, Germany
GReAT Europe

David Emm
Principal Security Researcher
GReAT Europe

Vicente Diaz
Principal Security Researcher
GReAT Europe

David Jacoby
Senior Security Researcher
GReAT Europe

Ido Naor
Senior Security Researcher
GReAT Europe

Stefan Ortloff
Security Researcher
GReAT Europe

Giampaolo Dedola
Security Researcher
GReAT Europe

Liviu Itoafa
Security Researcher
GReAT Europe

Ronan Mouchoux
Security Researcher
GReAT Europe

Jornt Van Der Wiel
Security Researcher
GReAT Europe

Costin Raiu
Director
GReAT

Dan Demeter
Security Researcher
GReAT EEMEA

Vitaly Kamluk
Director of GReAT APAC
GReAT APAC

Aleks Gostev
Chief Security Expert
GReAT APAC

Seongsu Park
Senior Security Researcher
GReAT APAC

Noushin Shabab
Senior Security Researcher
GReAT APAC

Suguru Ishimaru
Security Researcher
GReAT APAC

Wayne Lee
Junior Security Researcher
GReAT APAC

Mohamad Amin Hasbini
Senior Security Researcher
GReAT EEMEA

Ghareeb Saad Muhammad
Senior Security Researcher
GReAT EEMEA

Sergey Novikov
Deputy Director
GReAT

Yury Namestnikov
Head of GReAT Russia
GReAT Russia

Igor Soumenkov
Principal Security Researcher
GReAT Russia

Sergey Golovanov
Principal Security Researcher
GReAT Russia

Sergey Mineev
Principal Security Researcher
GReAT Russia

Sergey Belov
Principal Security Researcher
GReAT Russia

Sergey Lozhkin
Senior Security Researcher
GReAT Russia

Konstantin Zykov
Senior Security Researcher
GReAT Russia

Denis Legezo
Security Researcher
GReAT Russia

Denis Makrushin
Security Researcher
GReAT Russia

#Underground Network Monitoring #Counteracting Cyber-Espionage #Internet of Things Research #Online Banking Security

KASPERSKY lab

A Evolução das Ameaças

25 anos de desenvolvimento de novos vírus

KASPERSKY lab

O CRESCIMENTO DO MALWARE

1994

1

NOVO VIRUS
POR HORA

2006

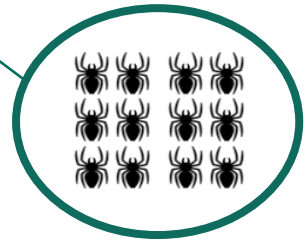
1

NOVO VIRUS
POR MINUTO

2011

1

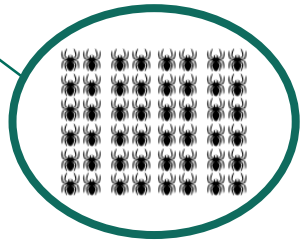
NOVO VIRUS
POR SEGUNDO



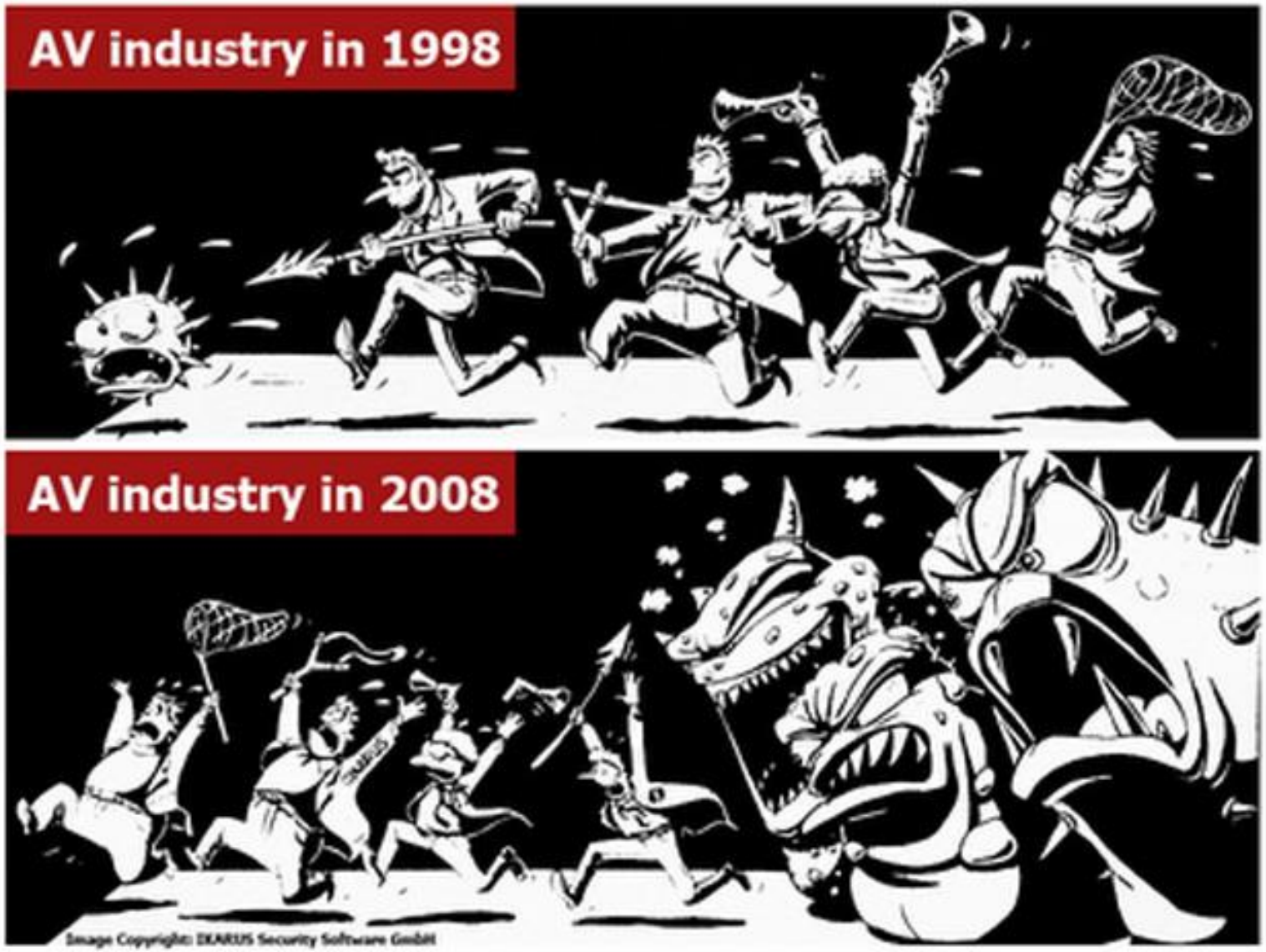
2018

310,000

NOVAS
AMOSTRAS
DIARIAS



O CRESCIMENTO DO MALWARE



COMO DETECTAMOS?

GREAT

Metadados das ameaças

Detecção automatizada

Big Data

Clusterização

Reputação e whitelisting

Automação de processos

Detecção em Nuvem

Inteligência global e local

A NATUREZA DAS AMEAÇAS

APTs

0.1%

Cyber-armas

Ataques Direcionados

9.9%

Ataques direcionados a empresas e governos

90%

Cibercrime tradicional

As ameaças em Moçambique

Dados locais

KASPERSKY lab

Moçambique – 65º país mais atacado por ameaças digitais

Moçambique – regiões mais atacadas

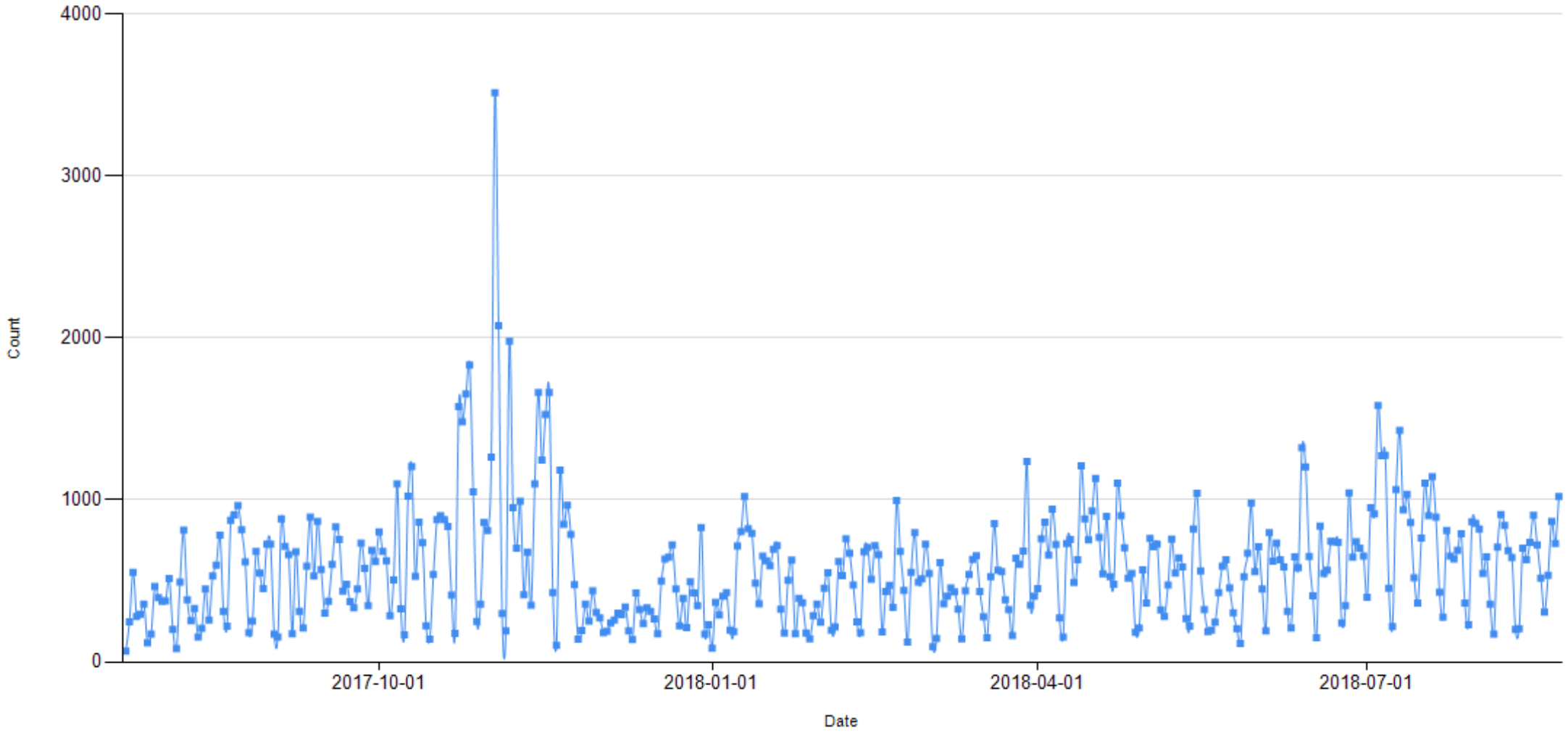
Provincias	Notificações de Ataques
Total	**1.539.098**
Maputo	1.251.295
Nampula	104.261
Sofala	46.304
Inhambane	43.995
Tete	31.292
Cabo Delgado	19.272
Zambezia	19.086
Manica	14.954
Gaza	7.835
Niassa	348

Período: 24 de Julho a 24 de Agosto 2018, considerando todos os ataques

CIBERCRIME TRADICIONAL

Ataques de Phishing

Ataques de Phishing em Moçambique – Agosto 2017 a Agosto de 2018

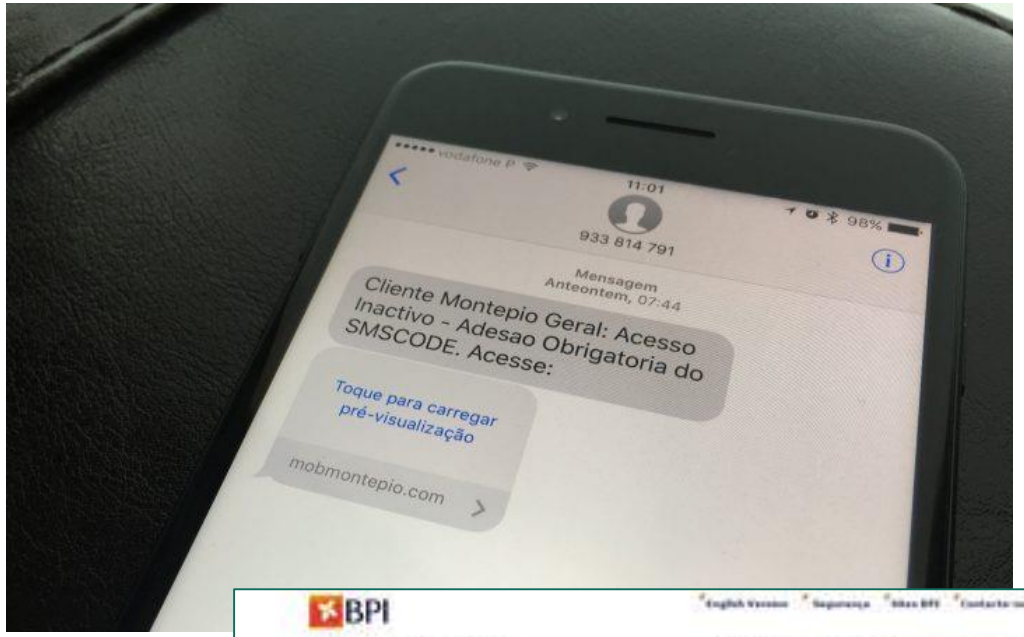


231.167 ataques em 1 ano // Média de 633 ataques por dia

KASPERSKY lab

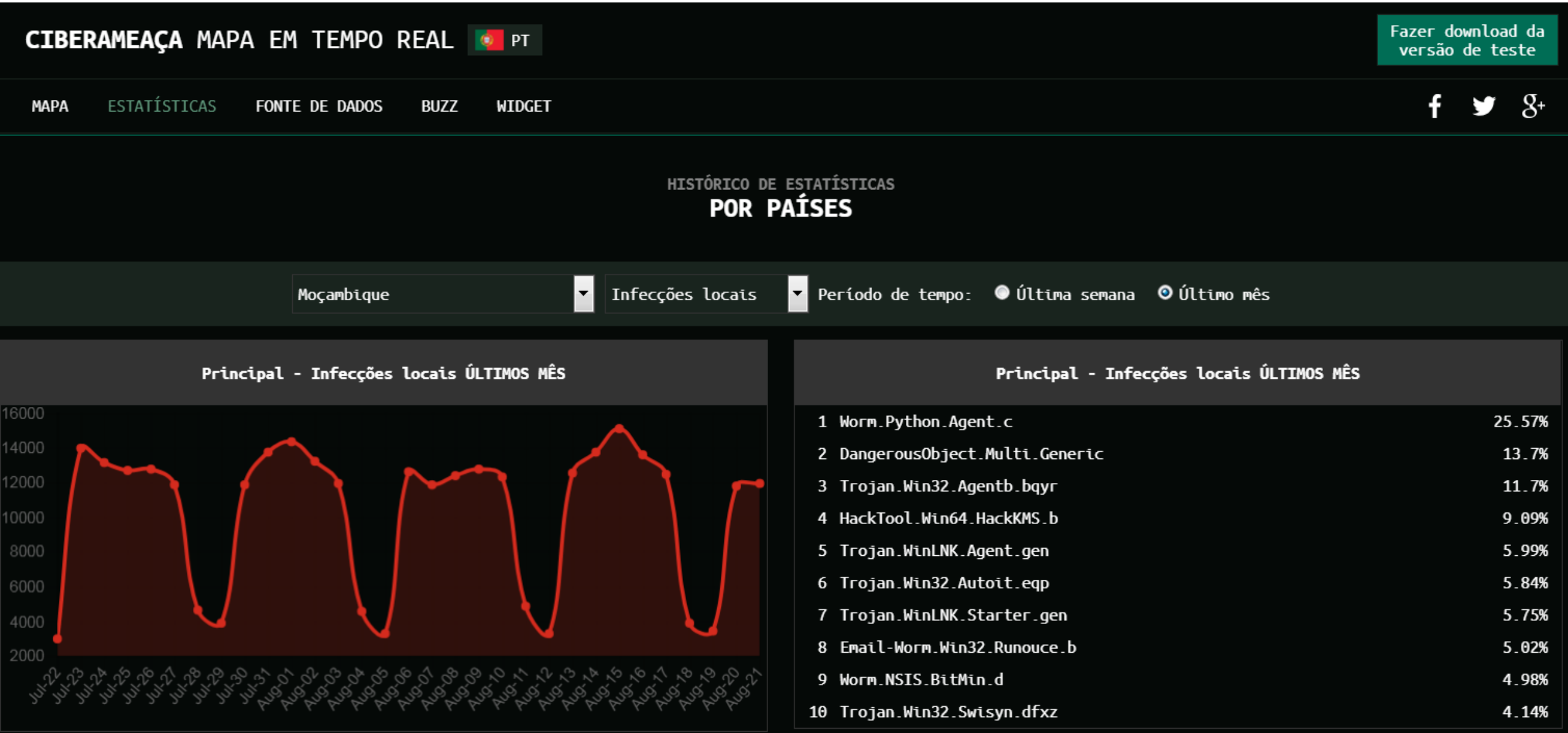
Phishing em Moçambique – onde atacam

Bancos	31,31%
Portais Globais de Internet	26,53%
Serviços Web	9,56%
Lojas on-line	8,11%
Redes Sociais	6,58%
Sistemas de Pagamento	6,09%
Online Storage	4,98%
Empresas de Telecomunicações	1,79%
Instant Messengers	1,48%
Serviços Financeiros	1,00%
Empresas de TI	0,88%
Empresas de Entrega	0,49%
Blogs	0,39%
Jogos	0,31%
Companhias Aéreas	0,22%
Midia/ Imprensa	0,09%
Governo e Impostos	0,06%
Geral	0,05%
Empresas de Taxi	0,04%
Energia	0,02%
Moedas criptográficas	0,02%
Reservas e Aluguéis	0,01%
Total	**100,00%**



Ataques de Malware

Ataques de Malware – Infecções Locais (encontradas nos computadores)



Ataques de Malware – análise por demanda

CIBERAMEAÇA MAPA EM TEMPO REAL PT

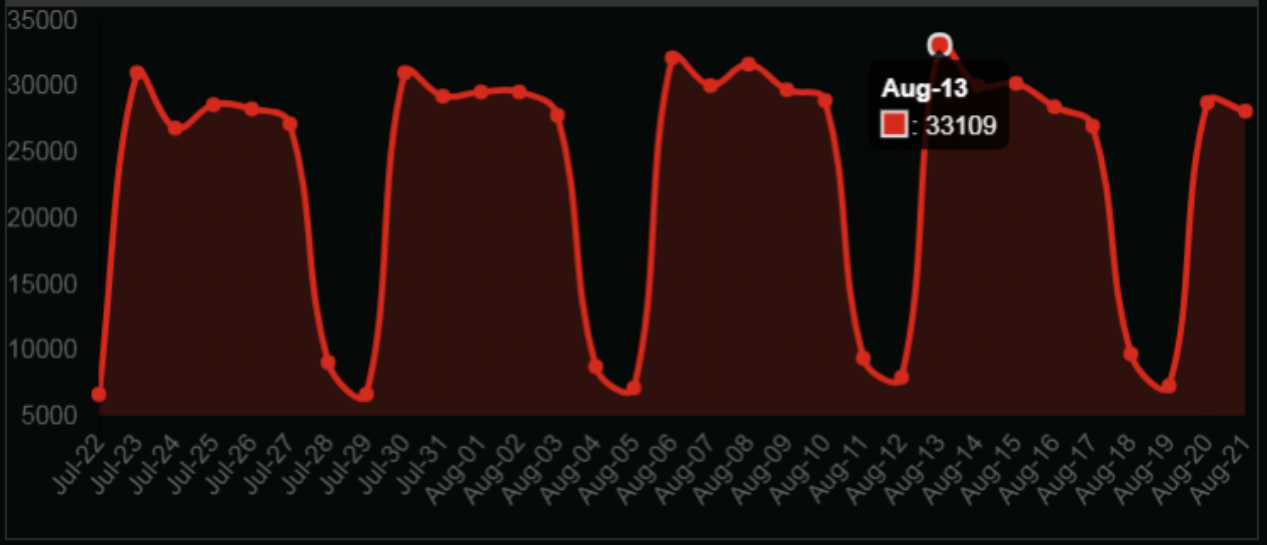
Fazer download da versão de teste

MAPA ESTATÍSTICAS FONTE DE DADOS BUZZ WIDGET

HISTÓRICO DE ESTATÍSTICAS
POR PAÍSES

Moçambique | Análise por demanda | Período de tempo: Última semana | Último mês

Principal - Análise por demanda ÚLTIMOS MÊS



Principal - Análise por demanda ÚLTIMOS MÊS

1	Worm.Python.Agent.c	12.38%
2	Trojan.Win32.Agentb.bqyr	6.11%
3	HackTool.Win64.HackKMS.b	5.54%
4	Trojan.Multi.GenAutorunReg.a	5.07%
5	Email-Worm.Win32.Runouce.b	2.57%
6	DangerousObject.Multi.Generic	2.53%
7	Trojan.Multi.Runner.d	2.49%
8	HackTool.Win32.KMSAuto.l	2.1%
9	Trojan.Win32.Adject.gen	1.86%
10	HackTool.Win32.KMSAuto.k	1.78%

Ataques de Malware – Ameaças bloqueadas em páginas de Internet

CIBERAMEAÇA MAPA EM TEMPO REAL PT

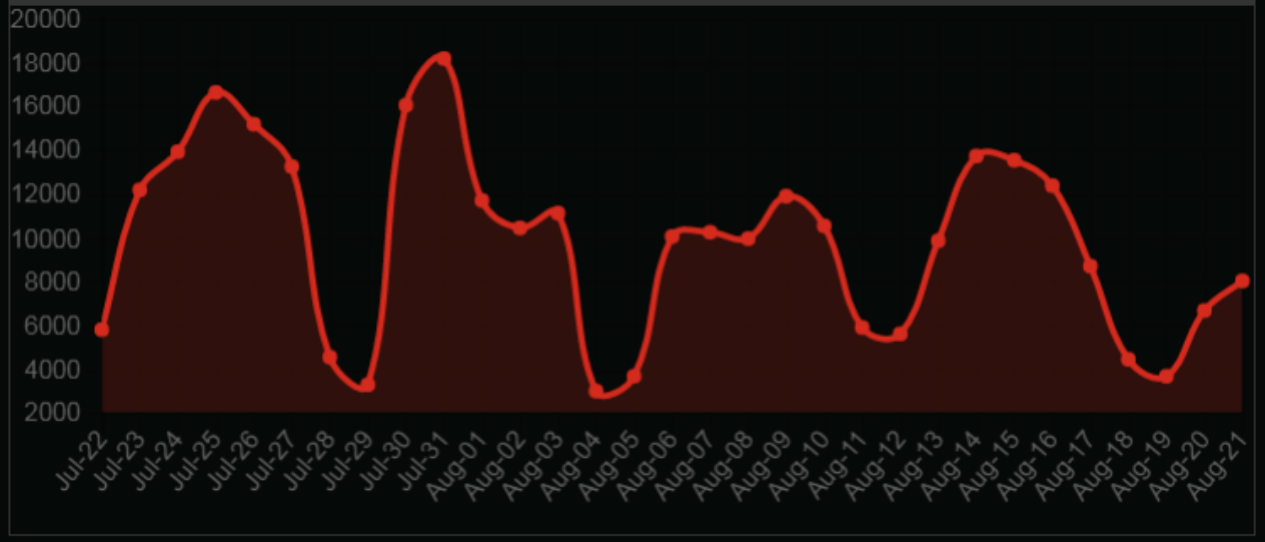
Fazer download da versão de teste

MAPA ESTATÍSTICAS FONTE DE DADOS BUZZ WIDGET

HISTÓRICO DE ESTATÍSTICAS
POR PAÍSES

Moçambique | Ameças web | Período de tempo: Última semana | Último mês

Principal - Ameças web ÚLTIMOS MÊS



Principal - Ameças web ÚLTIMOS MÊS

1	Trojan.Script.Generic	59.09%
2	Trojan.Script.Miner.gen	29.76%
3	Trojan-Clicker.HTML.Iframe.dg	3.74%
4	Backdoor.Linux.Gafgyt.co	1.97%
5	Trojan-Dropper.VBS.Agent.bp	0.55%
6	Hoax.Script.Generic	0.49%
7	Backdoor.Linux.Mirai.b	0.46%
8	Trojan.JS.Agent.eak	0.45%
9	Backdoor.Linux.Mirai.r	0.36%
10	Trojan.PHP.Agent.dr	0.32%

Ataques de Malware – bloqueios em Rede

CIBERAMEAÇA MAPA EM TEMPO REAL PT

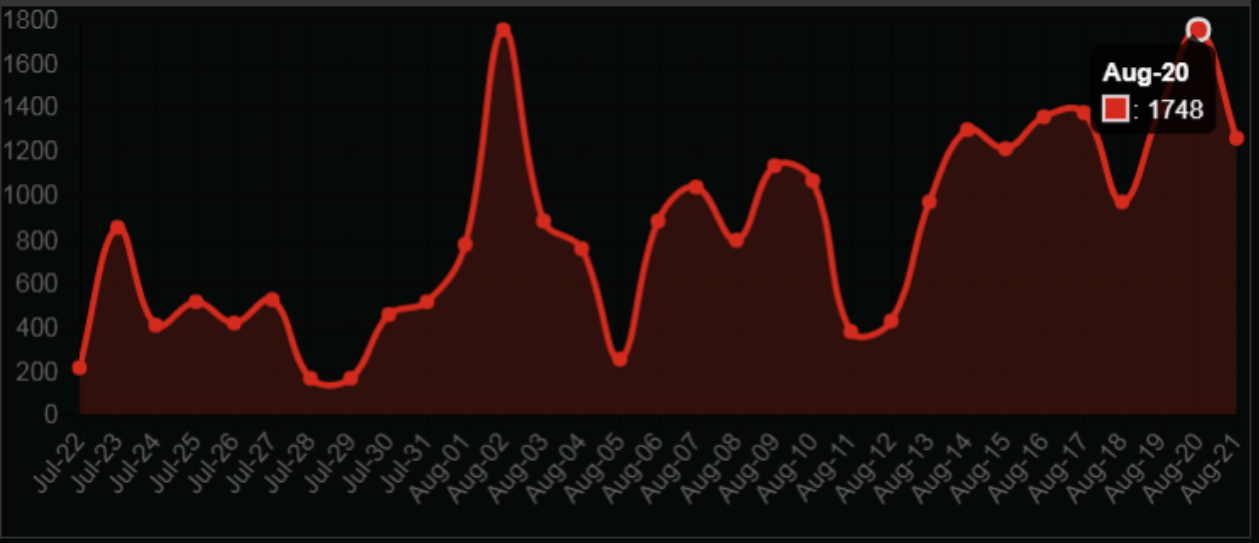
Fazer download da versão de teste

MAPA ESTATÍSTICAS FONTE DE DADOS BUZZ WIDGET

HISTÓRICO DE ESTATÍSTICAS
POR PAÍSES

Moçambique | ATAQUES À REDE | Período de tempo: Última semana Último mês

Principal - ATAQUES À REDE ÚLTIMOS MÊS



Principal - ATAQUES À REDE ÚLTIMOS MÊS

1	Intrusion.Win.MS17-010.o	27.51%
2	Bruteforce.Generic.Rdp.d	9.76%
3	Bruteforce.Generic.Rdp.a	7.17%
4	Intrusion.Win.MS17-010.e	3.42%
5	Intrusion.Win.NETAPI.buffer-overflow.exploit	2.5%
6	Intrusion.Win.CVE-2017-7269.cas.exploit	1.19%
7	Intrusion.Win.DNS.buffer-overflow.exploit	1.09%
8	Intrusion.Win.MS17-010.p	0.67%
9	Intrusion.Win.MS17-010.cf	0.44%
10	Intrusion.Win.EternalRomance.fish.leak	0.27%

Ataques de Malware – Sistemas Vulneráveis

CIBERAMEAÇA MAPA EM TEMPO REAL PT

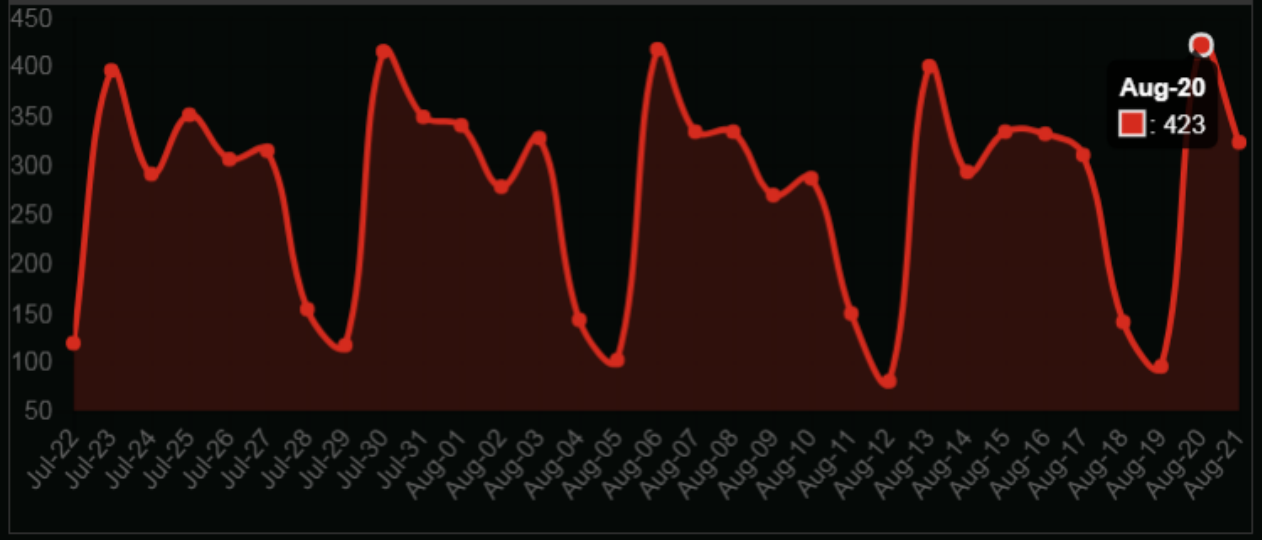
Fazer download da versão de teste

MAPA ESTATÍSTICAS FONTE DE DADOS BUZZ WIDGET

HISTÓRICO DE ESTATÍSTICAS
POR PAÍSES

Moçambique | Vulnerabilidade | Período de tempo: Última semana Último mês

Principal - Vulnerabilidade ÚLTIMOS MÊS



Principal - Vulnerabilidade ÚLTIMOS MÊS

1	Exploit.HTML.Iframe.FileDownload.cc	21.7%
2	Exploit.Win32.CVE-2017-11882.gen	18.4%
3	Exploit.AndroidOS.Lotoor.bg	10.38%
4	Exploit.AndroidOS.Psneuter.a	7.08%
5	Exploit.AndroidOS.Lotoor.bm	6.6%
6	Exploit.Script.Blocker.u	6.13%
7	Exploit.AndroidOS.Lotoor.cd	5.66%
8	Exploit.Win32.CVE-2016-7255.vho	5.66%
9	Exploit.MSOffice.CVE-2018-0802.gen	4.72%
10	Exploit.AndroidOS.Lotoor.a	1.89%

Ataques de Malware – Mensagens de SPAM

CIBERAMEAÇA MAPA EM TEMPO REAL PT

Fazer download da versão de teste

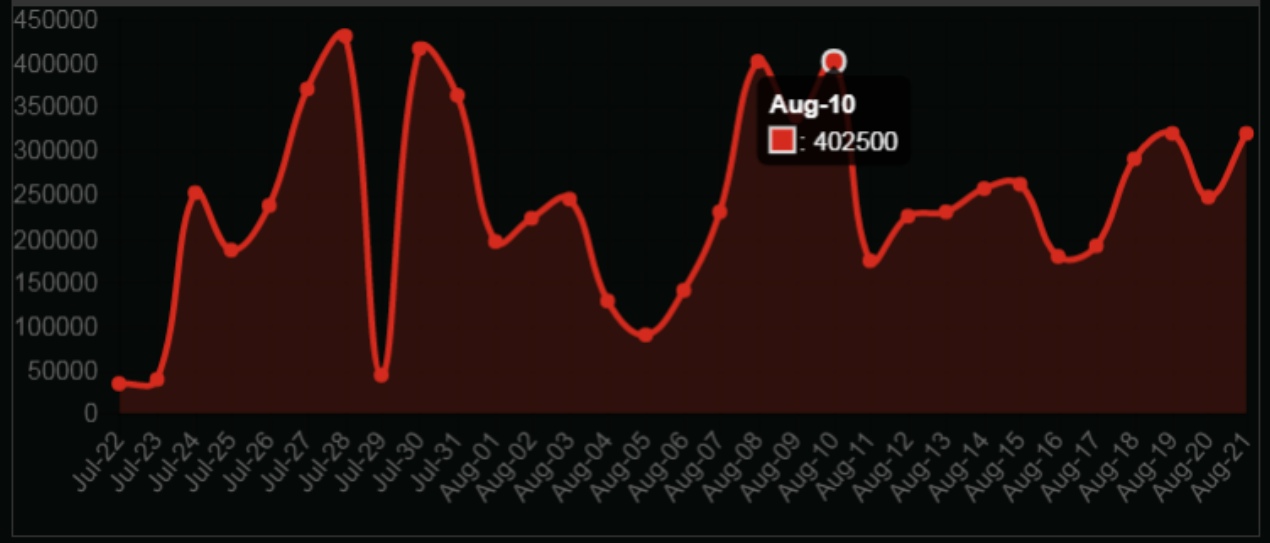
MAPA ESTATÍSTICAS FONTE DE DADOS BUZZ WIDGET

HISTÓRICO DE ESTATÍSTICAS

POR PAÍSES

Moçambique | Spam | Período de tempo: Última semana | Último mês

Principal - Spam ÚLTIMOS MÊS



Principal - Spam ÚLTIMOS MÊS

1	Shikari	70.2%
2	Analysis of Formal Attributes	20.28%
3	Linguistic Analysis	9.11%
4	Signature Analysis	0.33%
5	Enforced Anti-Spam Update Service	0.04%
6	Graphical Content Analysis	0.02%
7	Other	0.01%
8	Cloud Detection	0.01%

Ataques de Malware – E-mail infectado

CIBERAMEAÇA MAPA EM TEMPO REAL PT

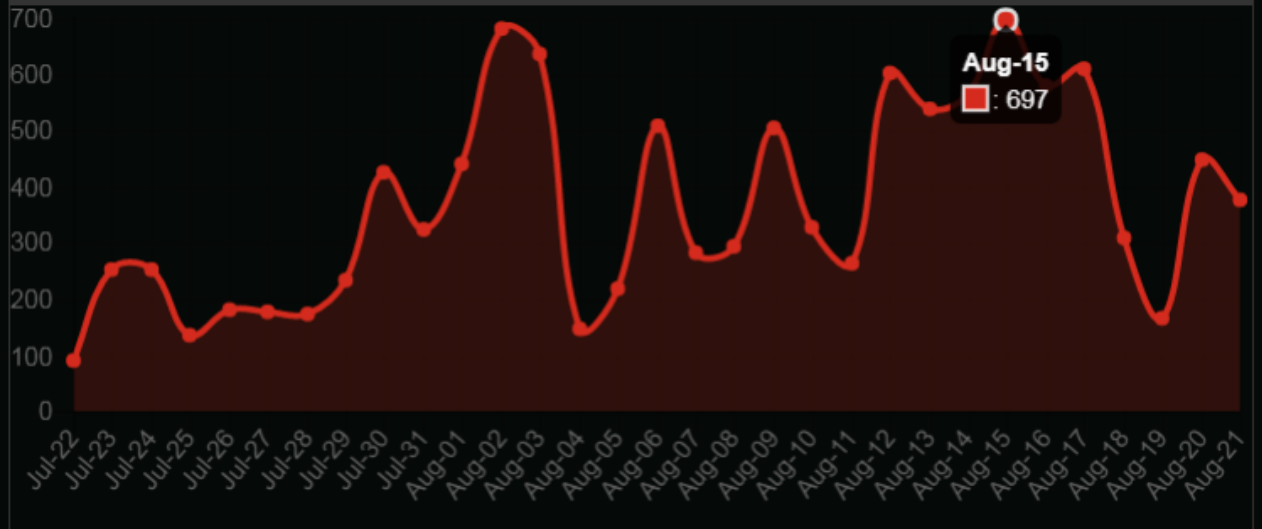
Fazer download da versão de teste

MAPA ESTATÍSTICAS FONTE DE DADOS BUZZ WIDGET

HISTÓRICO DE ESTATÍSTICAS
POR PAÍSES

Moçambique | E-mail infectado | Período de tempo: Última semana | Último mês

Principal - E-mail infectado ÚLTIMOS MÊS

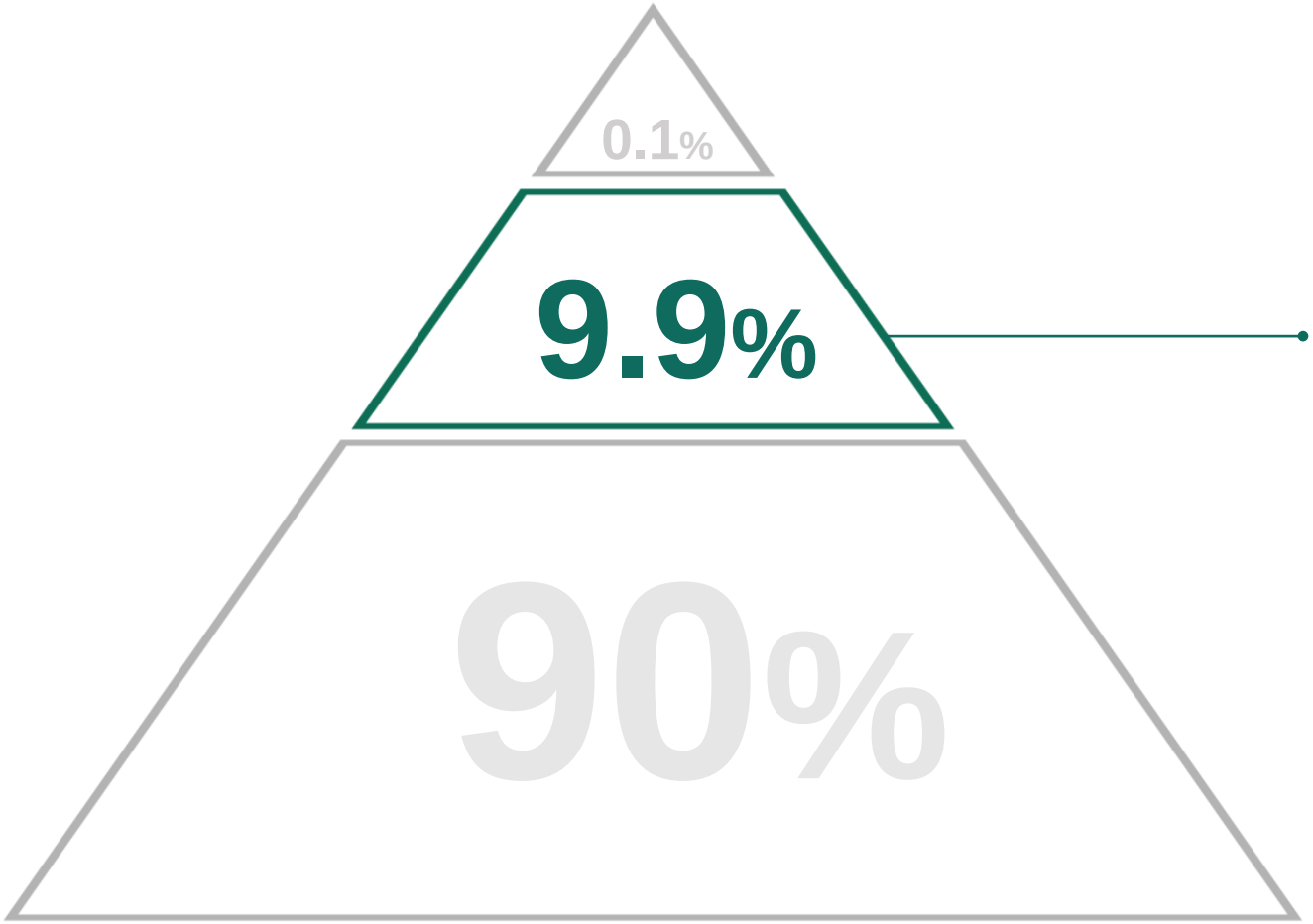


Principal - E-mail infectado ÚLTIMOS MÊS

1	Backdoor.Win32.Androm.gen	21.31%
2	Trojan-Downloader.Script.Generic	12.12%
3	Exploit.Win32.CVE-2017-11882.gen	9.44%
4	Exploit.MSOffice.CVE-2018-0802.gen	4.38%
5	Trojan-Dropper.AndroidOS.Agent.ja	2.99%
6	Trojan-Downloader.MSOffice.Agent.sb	2.99%
7	Trojan.Win32.Crypt.gen	2.57%
8	Trojan.Script.Generic	2.55%
9	Trojan.MSIL.Disfa.bqg	2.51%
10	Backdoor.Java.QRat.gen	1.86%

ATAQUES DIRECIONADOS A EMPRESAS E GOVERNOS

ESPIONAGEM E SABOTAGEM

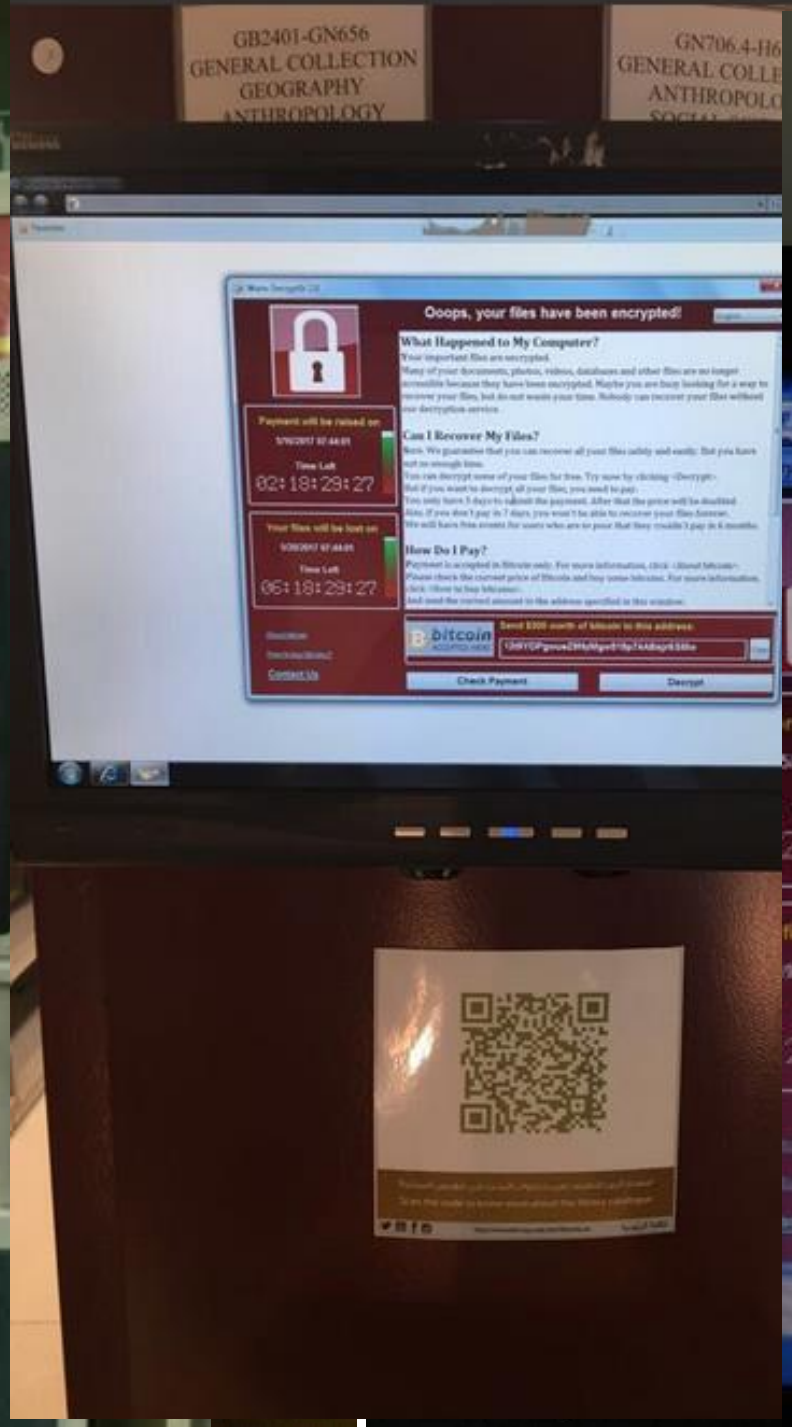


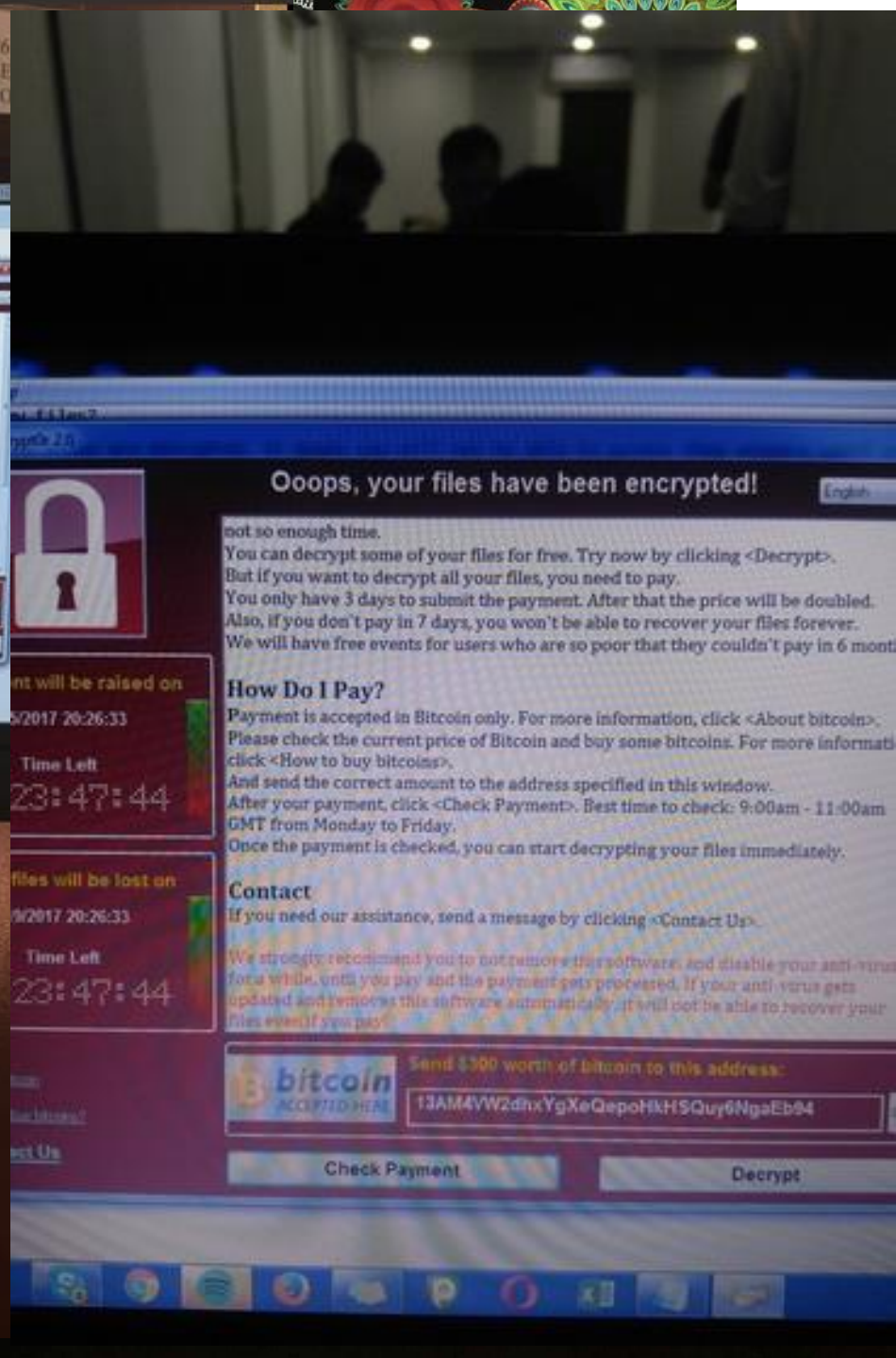
Ataques direcionados a empresas e governos para espionar ou sabotar(dinheiro não é o mais importante)

12 de Maio de 2017

Mesmo pagando não seria possível resgatar os ficheiros!

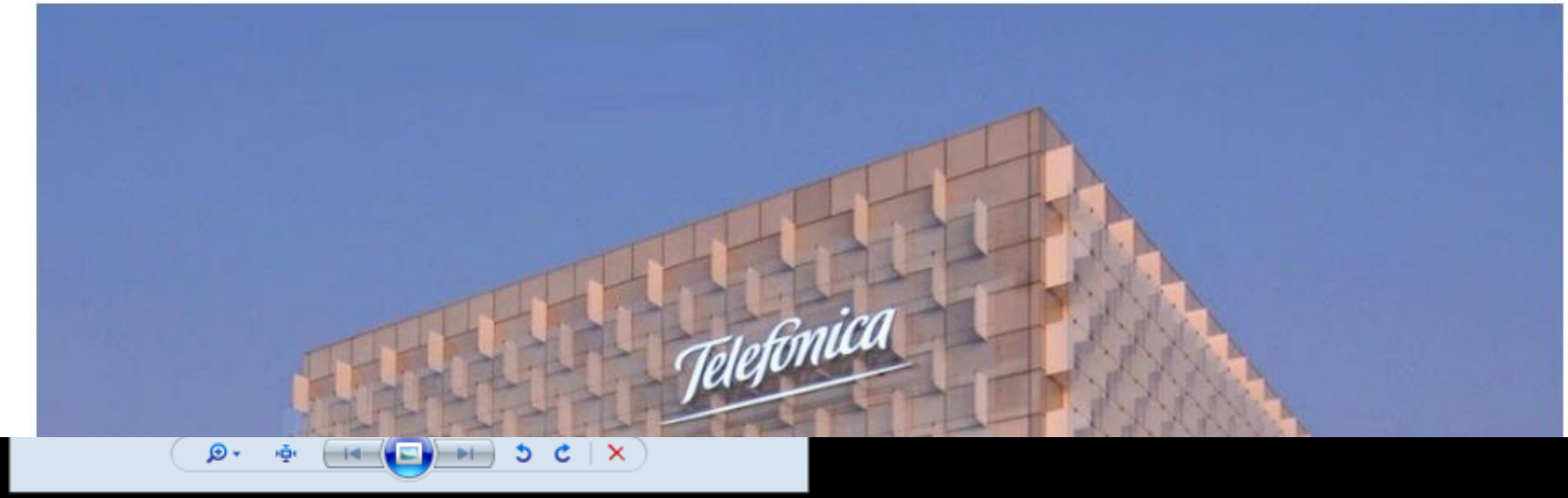

加油卡自助服务终端
中国石油


GB2401-GN656
GENERAL COLLECTION
GEOGRAPHY
ANTHROPOLOGY
Ooops, your files have been encrypted!
What Happened to My Computer?
Can I Recover My Files?
How Do I Pay?
Payment will be raised on
Time Left
02:18:29:27
Your files will be lost on
06:18:29:27
bitcoin
Check Payment
Decrypt


Ooops, your files have been encrypted!
not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 mont
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more informati
click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
GMT from Monday to Friday.
Once the payment is checked, you can start decrypting your files immediately.
Contact
If you need our assistance, send a message by clicking <Contact Us>.
We strongly recommend you to not remove this software, and disable your anti-virus
for a while, until you pay and the payment gets processed. If your anti-virus gets
updated and removes this software automatically, it will not be able to recover your
files even if you pay!
bitcoin
ACCEPTED HERE
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Check Payment
Decrypt

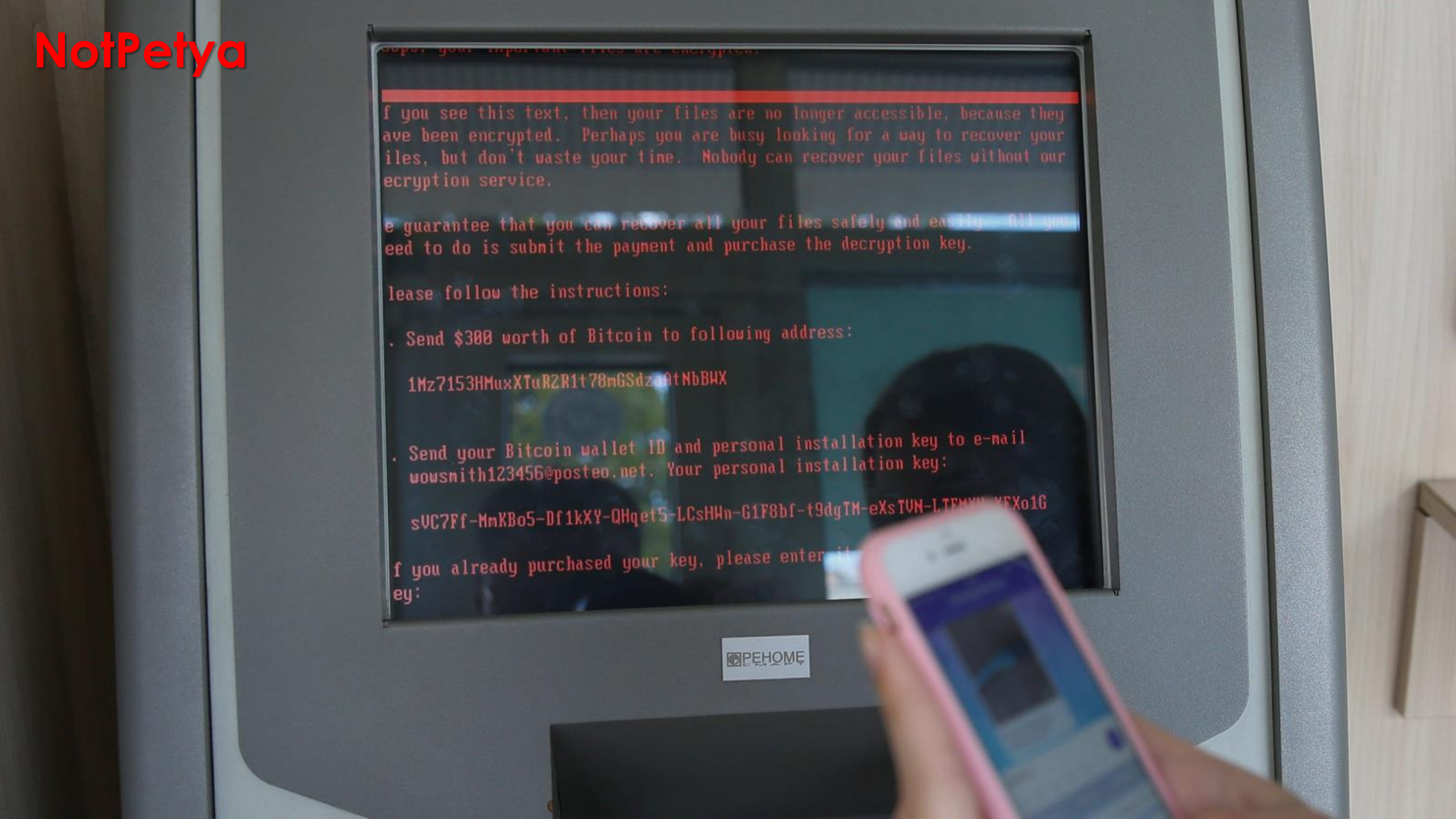
ATAQUE CIBERNÉTICO CONTRA TELEFÓNICA EN ESPAÑA

Compartir en Facebook | Compartir en Twitter | Compartir en Google+ | 82 PERSONAS COMPARTIERON



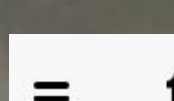
3 horas: 45.000 empresas infectadas, 74 países

NotPetya


f you see this text, then your files are no longer accessible, because they
ave been encrypted. Perhaps you are busy looking for a way to recover your
iles, but don't waste your time. Nobody can recover your files without our
ecryption service.
e guarantee that you can recover all your files safely and easily. All you
eed to do is submit the payment and purchase the decryption key.
lease follow the instructions:
. Send $300 worth of Bitcoin to following address:
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
. Send your Bitcoin wallet ID and personal installation key to e-mail
wowsmith123456@posteo.net. Your personal installation key:
sVC7Ff-MmKBo5-Df1kXY-QHqet5-LCsHWn-G1F8bf-t9dgTM-eXsTVN-
f you already purchased your key, please enter
ey:
PCHOME

threatpost Cloud Security / Malware / Vulnerabilities / Privacy

Maersk Shipping Reports $300M Loss Stemming from NotPetya Attack



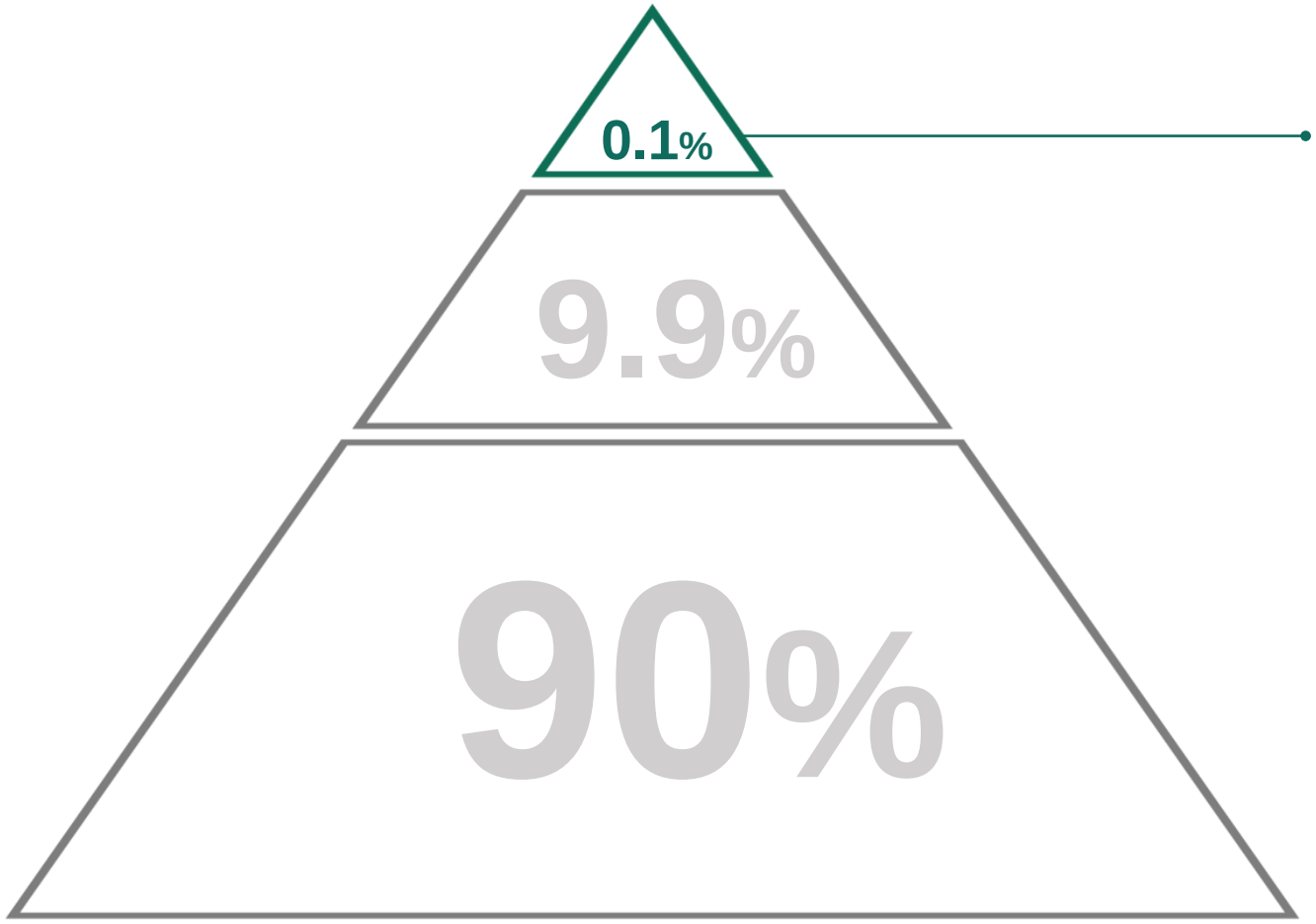
Author:
Michael Mimoso

August 16, 2017
/ 1:33 pm

2:30 minute read

CYBER-ARMAS

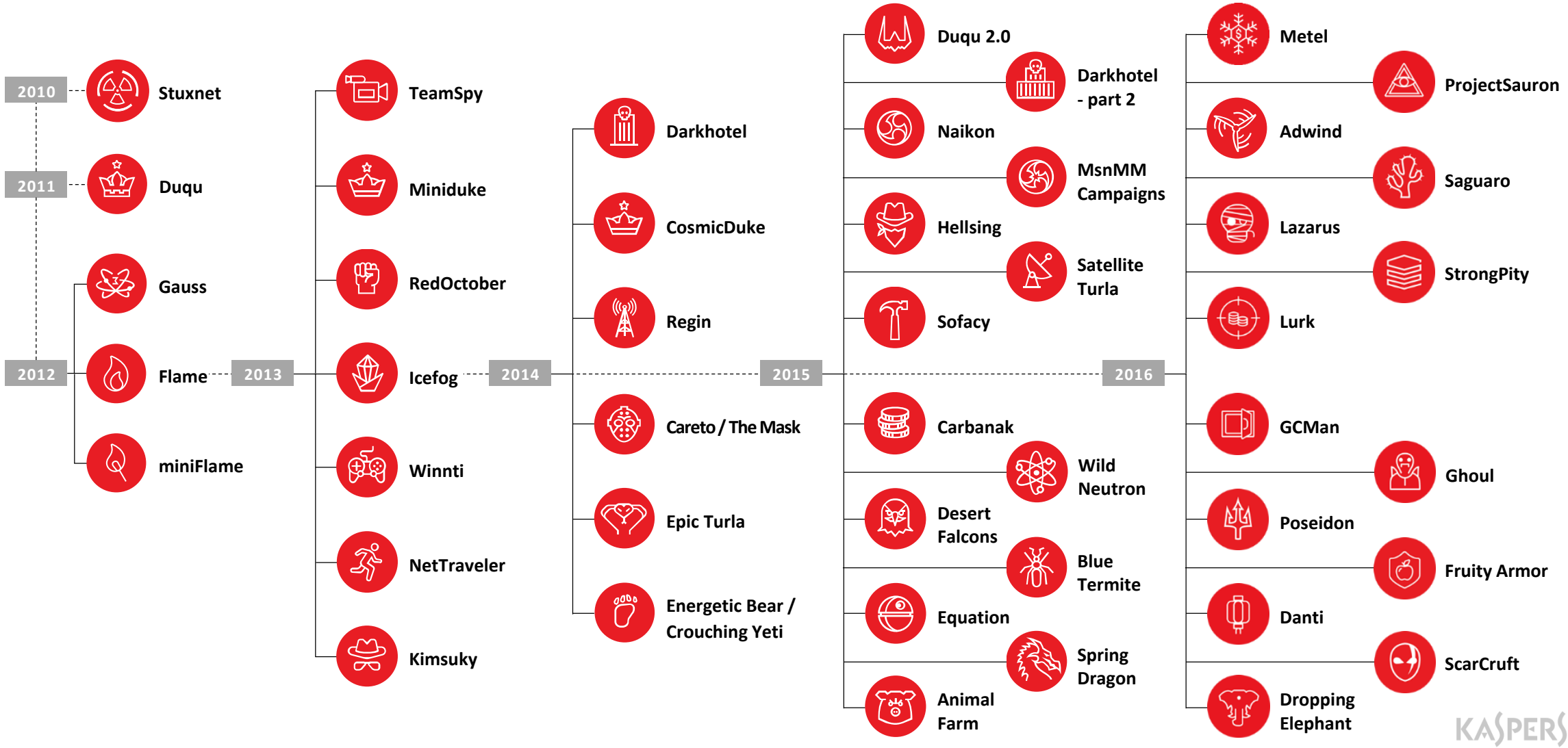
APTs



Cyber-armas

ATAQUES DIRECIONADOS – APTS

Disponiveis em https://apt.securelist.com



KASPERSKY lab

Stuxnet: 4 zero days + 1 USB encontrado no Irã e Oriente Médio

Flame: colisão de hash no Windows Update

Equation: compilação do firmware do disco duro para sobreviver a formatação

Regin: espionagem en redes telefônicas dos governos, incluso de telefones móveis através do protoloco SS7

Turla: comunicação C&C (controle e comando) usando Internet via satélite

Lazarus:
ataque aos bancos via rede SWIFT em vários países do mundo

Black Energy: ataques as redes de distribuição de energía Elétrica na Ucrânia

“Ataques como esses não chegam a Moçambique”

SECURELIST THREATS CATEGORIES TAGS STATISTICS ENCYCLOPEDIA

APT REPORTS

“Red October” Diplomatic Cyber Attacks Investigation

By GReAT on January 14, 2013. 5:00 pm

Lithuania – Embassy
Luxembourg – Gov
Mauritania – Embassy
Moldova – Gov, Military, Embassy
Morocco – Embassy
Mozambique – Embassy
Oman – Embassy
Pakistan – Embassy
Portugal – Embassy
Qatar – Embassy
Russia – Embassy, Research, Military, Nuclear/Energy
Saudi Arabia – Embassy

Campanha de espionagem contra entidades Diplomáticas, visando roubar dados sensíveis dos governos e entidades importantes ligadas as Embaixadas

“Ataques como esses não chegam a Moçambique”

Campanha de espionagem governamental que infectava a rede de hotéis onde políticos e empresarios se hospedavam

APT REPORTS

Darkhotel’s attacks in 2015

By GReAT on August 10, 2015. 12:53 pm

Darkhotel APT attacks dated 2014 and earlier are characterized by the misuse of stolen certificates, the deployment of .hta files with multiple techniques, and the use of unusual methods like the infiltration of hotel Wi-Fi to place backdoors in targets’ systems. In 2015, many of these techniques and activities remain in use. However, in addition to new variants of malicious .hta, we find new victims, .rar attachments with RTLO spearphishing, and the deployment of a 0day from Hacking Team.

The Darkhotel APT continues to spearphish targets around the world, with a wider geographic reach than its previous botnet buildout and hotel Wi-Fi attacks. Some of the targets are diplomatic or have strategic commercial interests.

The location of Darkhotel’s targets and victims in 2015:

- North Korea
- Russia
- South Korea
- Japan
- Bangladesh
- Thailand
- India
- Mozambique
- Germany

Conclusão: Como estar preparado?

- **SOCs/ CERTs/CSIRTs** tem que ser treinados!
- Abandonar as técnicas convencionais de proteção que não funcionam mais!
- Adotar novas proteções baseadas na inteligência de ameaças.
- Parceria com empresas sérias visando entender os novos ataques e impeder que aconteçam!

Na luta contra o cibercrime, os atacantes nos odeiam!

```
var     URL_DEST8 = "ca"                                        +"i"
var     URL_DEST9 = "ba"                    +"nco"  +"bra*";
var     URL_DEST10 = "bb";
var     URL_DEST11 = "mydickwinu";
var     URL_DEST12 = "ci"       +"ti"   +"b"    +"an"           +"k";
var     URL_DEST13 = "ciaa";
var     URL_DEST14 = "br"       +"a"            +"d"            +"es"
var     URL_DEST15 = "fbi3";
var     URL_DEST16 = "it"       +"a"    +"u*";
var     URL_DEST17 = "kasperskysuckers";
var     URL_DEST18 = "u"        +"n"    +"icl"  +"ass";
var     URL_DEST19 = "voegol";
var     URL_DEST20 = "tam";
var     URL_DEST21 = "sexyline31337";
var     URL_DEST22 = "vir"+             +"usto"         +"tal";
var     URL_DEST23 = "Ã§aites";
var     URL_DEST24 = "amer"     +"ican"         +"ex"   +"pr"   +"ess";
```

Na luta contra o cibercrime, os atacantes nos odeiam!

```
#
# created:
#   04/03/2014 - 12/05/2014
#
# authors:
#   We are real hacK3rs.
#
# message:
#   Fuck U, kaspeRsky!!! U never get a fresh B1ack En3rgy.
#   So, Thanks C1sco ltd for built-in backdOOrs & 0-days.
#


namespace eval CISCO {
    #
    # name:
    #   namespace CISCO
    #
    # description:
    #   object implements a set of wrappers over cisco EXEC-commands.
    #
```

OBRIGADO!
KOOXUKHURU!
KU KHENSA!

Fabio Assolini
Senior Security Researcher

KASPERSKY lab

Twitter.com/Assolini