# The Indonesia Darknets revealed – mapping the uncharted territory of the Internet


Charles Lim, Msc., ECSA, ECSP, ECIH, CEH, CEI
(林運芫)

Honeycon 2016

13 July 2016 | GIS NTU Convention Center | Taipei, Taiwan

Indonesia Honeynet Project

SGU

# About Me


## Charles Lim, Msc., ECSA, ECSP, ECIH, CEH, CEI

Researcher – Information Security Research Group and Lecturer
Swiss German University
***Charles.lims [at] gmail.com*** *and* ***charles.lim [at] sgu.ac.id***
***http://people.sgu.ac.id/charleslim***


**I am currently doing my doctoral study in Universitas Indonesia**

**Research Interest**

- ***Malware***
- ***Intrusion Detection***
- ***Threats Intelligence***
- ***Vulnerability Analysis***
- ***Digital Forensics***
- ***Cloud Security***

**Community**

- ***Indonesia Honeynet Project - Chapter Lead***
- ***Academy CSIRT – member***
- ***Asosiasi Digital Forensik Indonesia - member***

# Agenda

- About Honeynet
- Indonesia Honeynet Project
- Building Threat Intelligence
- Research & Publications
- Statistics
- Case Study
- Conclusion

# About Honeynet

- Volunteer open source computer security research organization since 1999 (US 501c3 non-profit)

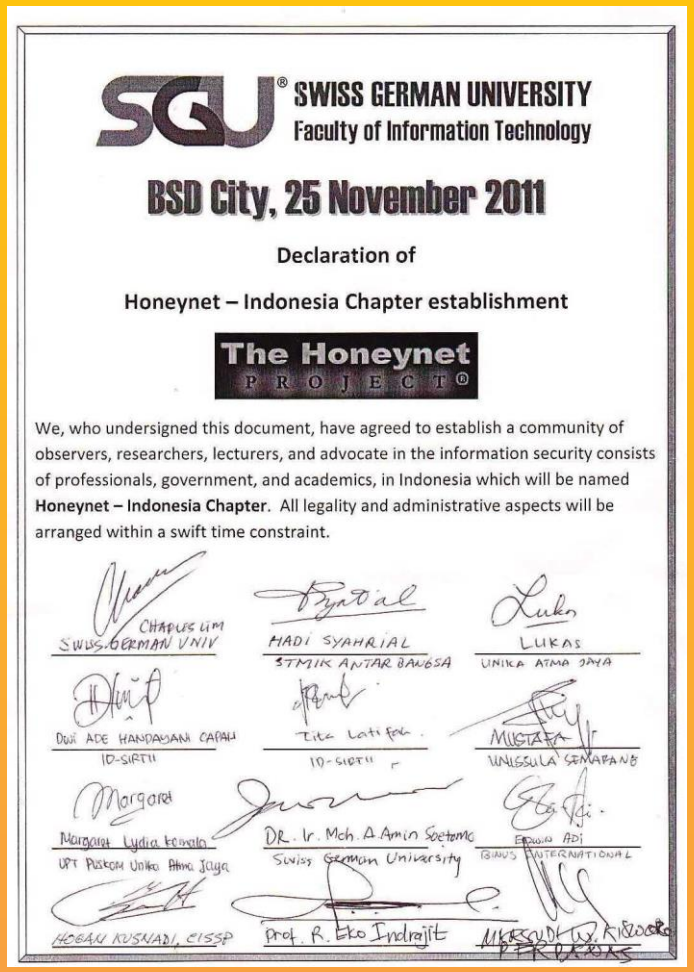
- Mission: ¨learn the tools, tactics and motives involved in computer and network attacks, and share the lessons learned¨ - http://www.honeynet.org

# About Indonesia Honeynet Project

- Mycert introduces honeypot in OIC-CERT in 2009
- Explore honeypot in 2010, due to students' interest in learning data mining on:
  - Cyber terrorism
  - Malware behavior
- Cecil (Singapore Chapter lead) introduced us to Honeynet global

# About Indonesia Honeynet Project

- 15 passionate security professionals, academicians and government officials met signed a petition in 25 November 2011
- Indonesia Chapter officially recognized 9 January 2012
- Current members: 178 (25 active members)



SWISS GERMAN UNIVERSITY
Faculty of Information Technology

**BSD City, 25 November 2011**

Declaration of

Honeynet – Indonesia Chapter establishment

The Honeynet PROJECT®

We, who undersigned this document, have agreed to establish a community of observers, researchers, lecturers, and advocate in the information security consists of professionals, government, and academics, in Indonesia which will be named **Honeynet – Indonesia Chapter**. All legality and administrative aspects will be arranged within a swift time constraint.

CHAPUS LIM — SWISS GERMAN UNIV
HADI SYAHRIAL — STMIK ANTAR BANGSA
LUKAS — UNIKA ATMA JAYA
DWI ADE HANDAYANI CAPAH — ID-SIRTII
Tita Lati Fa — ID-SIRTII
MUSTAFA Jr — UNISSULA SEMARANG
Margaret Lydia Fernala — UPT Puskom Unika Atma Jaya
DR. Ir. Mch. A Amin Soetomo — Swiss German University
EDWIN ADI — BINUS INTERNATIONAL
HOGAN KUSNADI, CISSP
Prof. R. Eko Indrajit

KOMINFO

id-SIRTII

COMPUTER SECURITY INCIDENT RESPONSE TEAM SIRT

# About Indonesia Honeynet Project

# About Indonesia Honeynet Project

- Attended Honeynet Workshop 2012
- With support from KOMINFO, we conducted yearly seminar and workshops
  - Focus on Security Awareness and Security Research
- Honeynet communities: Jakarta, Semarang, Surabaya, Yogya, Denpasar, Palembang, Lampung
- Research Topics: Incident handling, Vulnerability Analysis, Malware, Digital Forensics, Penetration Testing, Threats Intelligence

# About Indonesia Honeynet Project


Honeynet Seminar & Workshop | 10-11 Juni 2015 | Lampung, Indonesia

# Honeypots Research & Deployment

2009 → 2011 → 2013 → 2015

| Learning Period | Early Period | Growing Period | Expanding Period |
|---|---|---|---|
| Honeypot: Nepenthes | Honeypot: Nepenthes, Dionaea | Honeypot: Dionaea | Honeypot: Dionaea, Kippo, Glastopf, Honeytrap |
| Learning How to install and configure | Deployed 1st Honeypot in SGU | Target: Academic, Government, ISP | Coverage: Java, Bali, Sumatera, |
| # Honeypots deployed: None | # Honeypots deployed: 1 | # Honeypots deployed: 5 | # Honeypots deployed: 20 |
| Hardware: Client | Hardware: Simple Client and Server | Hardware: Mini PC and Server | Hardware: Raspberry Pi and Dedicated servers |

# List of contributors

- Amien H.R.
- Randy Anthony
- Michael
- Stewart
- Glenn
- Mario Marcello
- Joshua Tommy
- Andrew Japar
- Christiandi
- Kevin Kurniawan

# What is Darknets?

*Darknet – portion of routed, allocated IP space in which no active servers reside.*

***— Team CYMRU***

# What is Darknets?

| Livenet | Darknet |
| --- | --- |
| Live IP Address (used) | Unused IPs |

# Darknets and Honeypots

Goal

- To understand cyber activities in our institutions in Indonesia (Government, Education and Industry)

How

- Honeypot servers put in the unused IP address across the above organizations

# First Step – Distributing Sensors

Mini PC


Raspberry Pi

# First Step – Collecting sensors' data

Raspberry Pi

Raspberry Pi

Raspberry Pi

Repository Server

# Second Step – Analysis

Raspberry Pi

Raspberry Pi

Raspberry Pi

Repository Server

Analysis Server

# Third Step – User Experience

Raspberry Pi

Raspberry Pi

Raspberry Pi

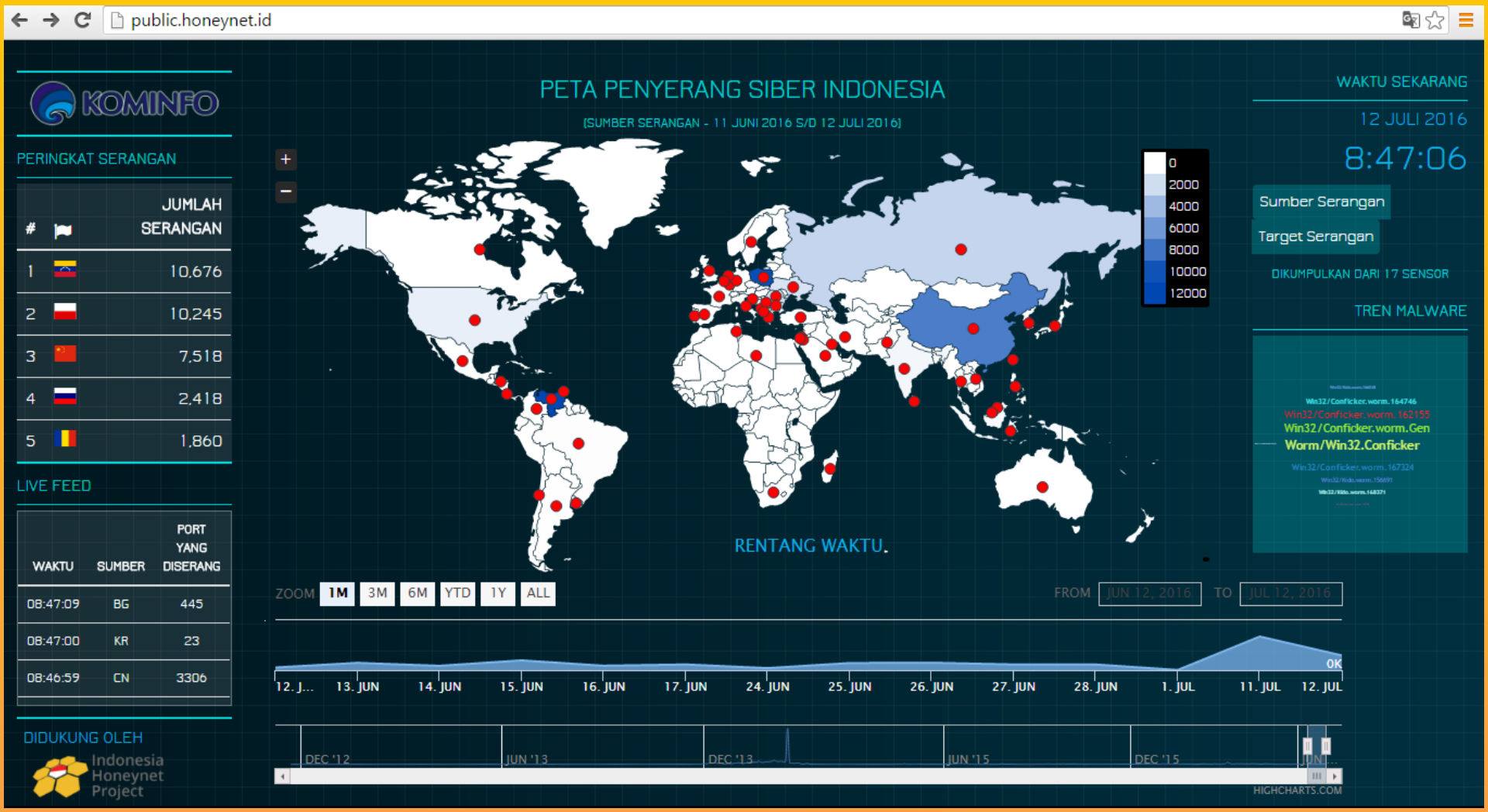
USERS

Repository Server

Analysis Server

Web Server

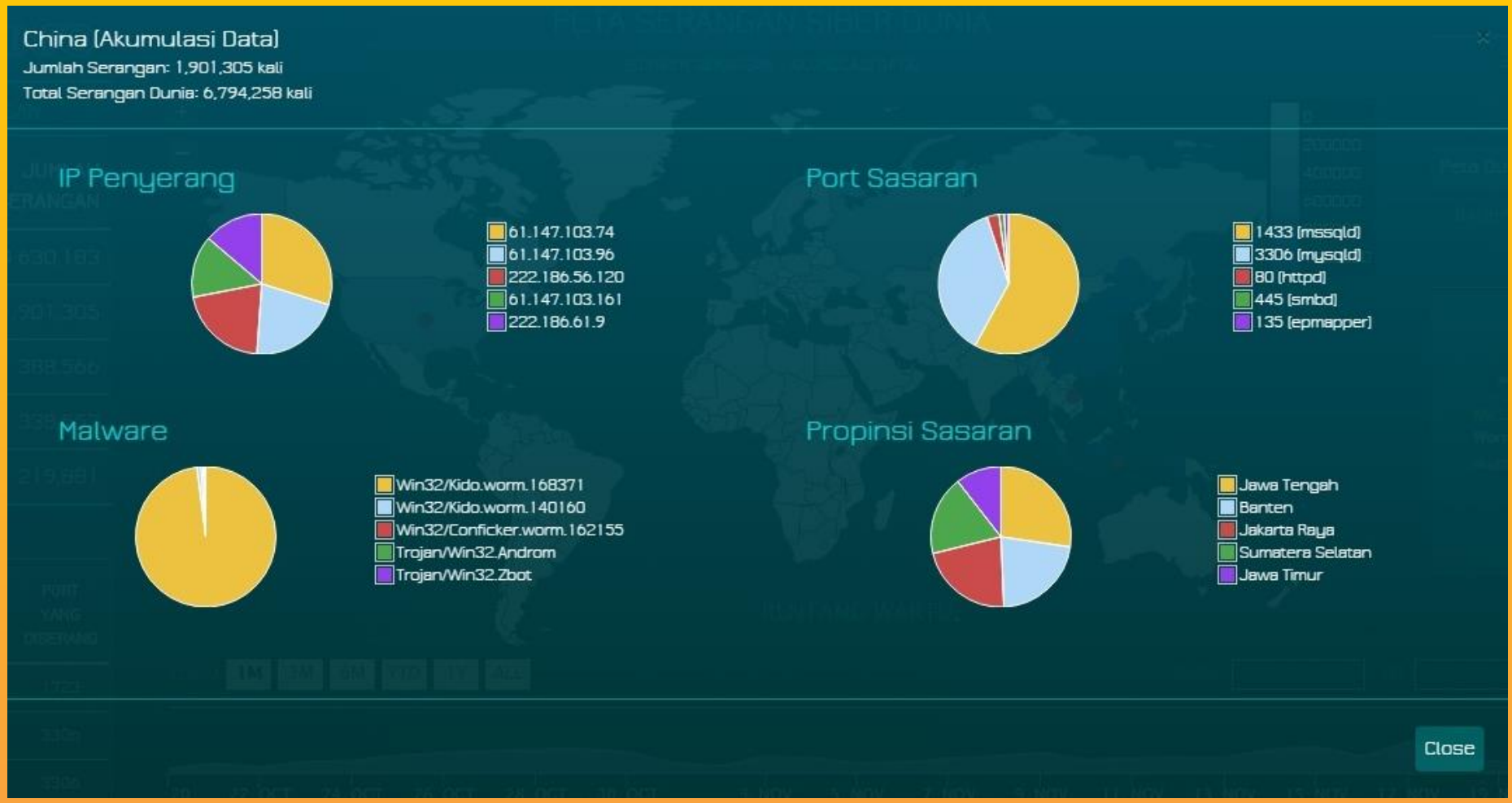
# Our Contribution




THE HONEYNET PROJECT

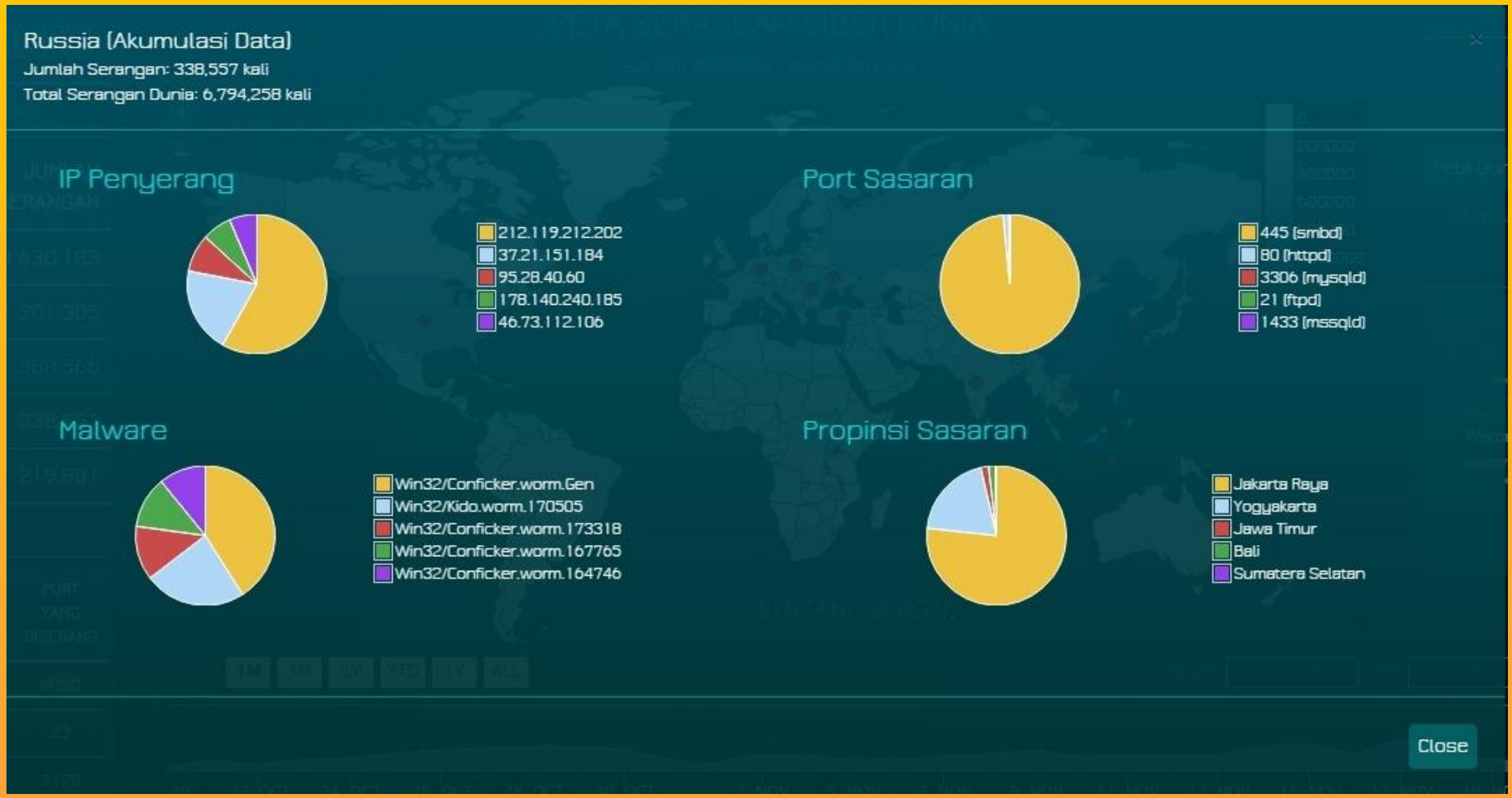
Indonesia Honeynet Project

# Our Contribution




Attacker Statistics: Attacker IP, Malware, Targeted Ports, Provinces attacked

# Our Contribution




Attacker Statistics: Attacker IP, Malware, Targeted Ports, Provinces attacked

# Our Research & Publications

2010 Second International Conference on Advances in Computing, Control, and Telecommunication Technologies

ANALYSIS OF MACHINE LEARNING TECHNIQUES USED IN BEHAVIOR-BASED MALWARE DETECTION

2010 Second International Conference on Advances in Computing, Control, and Telecommunication

IMPLEMENTATION OF INTELLIGENT SEARC USING SELF-ORGANIZING MAP FOR WEBMINI IN DOCUMENT CONTAINING INFORMATIC RELATION TO CYBER TERRORISM

2010 Second International Conference on Advances in Computing, Control, and Telecommunication Technologies

INTEGRATING DYNAMIC ANALYSIS USING CLUSTERING TECHNIQUES FOR LOCAL MALWARE IN INDONE

2014 International Conference on Information, Communication Technology and System

Development of Distributed Honeypot Using Raspberry Pi

Malware | Data Mining | Behavior Analysis | Cyber Terrorism

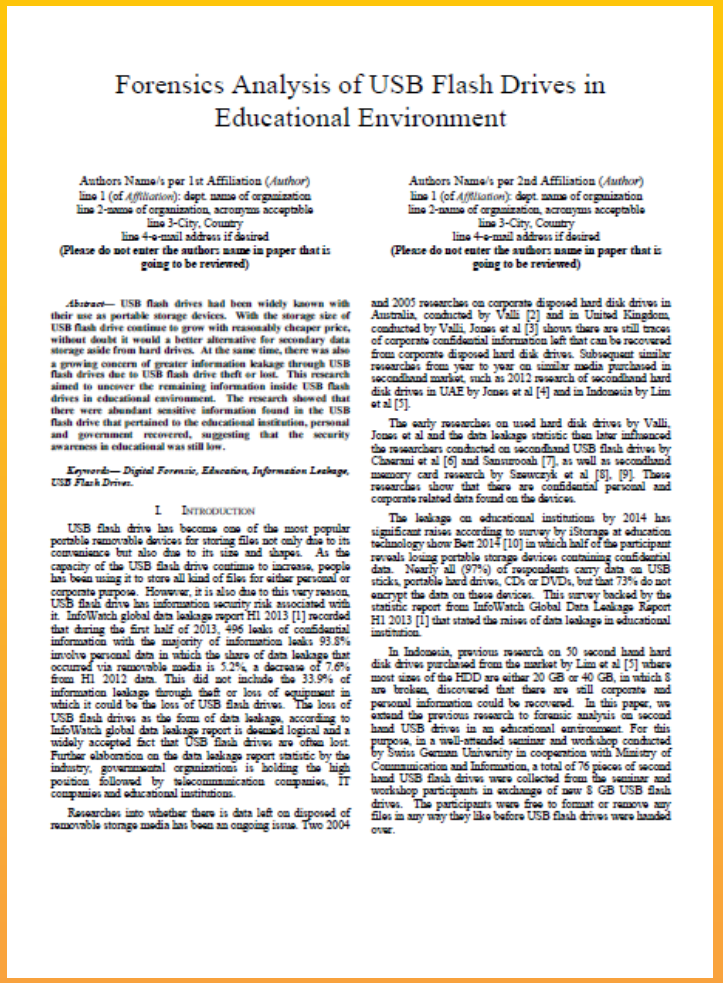
THE HONEYNET PROJECT

Indonesia Honeynet Project

# Other Research

KOMINFO

SGU



Forensics Analysis of USB Flash Drives in Educational Environment

Authors Name/s per 1st Affiliation (*Author*)
line 1 (of *Affiliation*): dept. name of organization
line 2-name of organization, acronyms acceptable
line 3-City, Country
line 4-e-mail address if desired
**(Please do not enter the authors name in paper that is going to be reviewed)**

Authors Name/s per 2nd Affiliation (*Author*)
line 1 (of *Affiliation*): dept. name of organization
line 2-name of organization, acronyms acceptable
line 3-City, Country
line 4-e-mail address if desired
**(Please do not enter the authors name in paper that is going to be reviewed)**

***Abstract*— USB flash drives had been widely known with their use as portable storage devices. With the storage size of USB flash drive continue to grow with reasonably cheaper price, without doubt it would a better alternative for secondary data storage aside from hard drives. At the same time, there was also a growing concern of greater information leakage through USB flash drives due to USB flash drive theft or lost. This research aimed to uncover the remaining information inside USB flash drives in educational environment. The research showed that there were abundant sensitive information found in the USB flash drive that pertained to the educational institution, personal and government recovered, suggesting that the security awareness in educational was still low.**

***Keywords— Digital Forensic, Education, Information Leakage, USB Flash Drives.***

## I. Introduction

USB flash drive has become one of the most popular portable removable devices for storing files not only due to its convenience but also due to its size and shapes. As the capacity of the USB flash drive continue to increase, people has been using it to store all kind of files for either personal or corporate purpose. However, it is also due to this very reason, USB flash drive has information security risk associated with it. InfoWatch global data leakage report H1 2013 [1] recorded that during the first half of 2013, 496 leaks of confidential information with the majority of information leaks 93.8% involve personal data in which the share of data leakage that occurred via removable media is 5.2%, a decrease of 7.6% from H1 2012 data. This did not include the 33.9% of information leakage through theft or loss of equipment in which it could be the loss of USB flash drives. The loss of USB flash drives as the form of data leakage, according to InfoWatch global data leakage report is deemed logical and a widely accepted fact that USB flash drives are often lost. Further elaboration on the data leakage report statistic by the industry, governmental organizations is holding the high position followed by telecommunication companies, IT companies and educational institutions.

Researches into whether there is data left on disposed of removable storage media has been an ongoing issue. Two 2004 and 2005 researches on corporate disposed hard disk drives in Australia, conducted by Valli [2] and in United Kingdom, conducted by Valli, Jones et al [3] shows there are still traces of corporate confidential information left that can be recovered from corporate disposed hard disk drives. Subsequent similar researches from year to year on similar media purchased in secondhand market, such as 2012 research of secondhand hard disk drives in UAE by Jones et al [4] and in Indonesia by Lim et al [5].

The early researches on used hard disk drives by Valli, Jones et al and the data leakage statistic then later influenced the researchers conducted on secondhand USB flash drives by Chasrani et al [6] and Sansurooah [7], as well as secondhand memory card research by Szaszyrk et al [8], [9]. These researches show that there are confidential personal and corporate related data found on the devices.

The leakage on educational institutions by 2014 has significant raises according to survey by iStorage at education technology show Bett 2014 [10] in which half of the participant reveals losing portable storage devices containing confidential data. Nearly all (97%) of respondents carry data on USB sticks, portable hard drives, CDs or DVDs, but that 73% do not encrypt the data on those devices. This survey backed by the statistic report from InfoWatch Global Data Leakage Report H1 2013 [1] that stated the raises of data leakage in educational institutions.

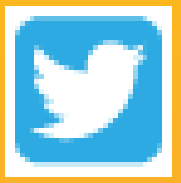
In Indonesia, previous research on 50 second hand hard disk drives purchased from the market by Lim et al [5] where most sizes of the HDD are either 20 GB or 40 GB, in which 8 are broken, discovered that there are still corporate and personal information could be recovered. In this paper, we extend the previous research to forensic analysis on second hand USB drives in an educational environment. For this purpose, in a well-attended seminar and workshop conducted by Swiss German University in cooperation with Ministry of Communication and Information, a total of 76 pieces of second hand USB flash drives were collected from the seminar and workshop participants in exchange of new 8 GB USB flash drives. The participants were free to format or remove any files in any way they like before USB flash drives were handed over.

## Second Hand USB Forensics and Publications

# Join Us

http://www.ihpcon.id

Indonesia Honeynet Project

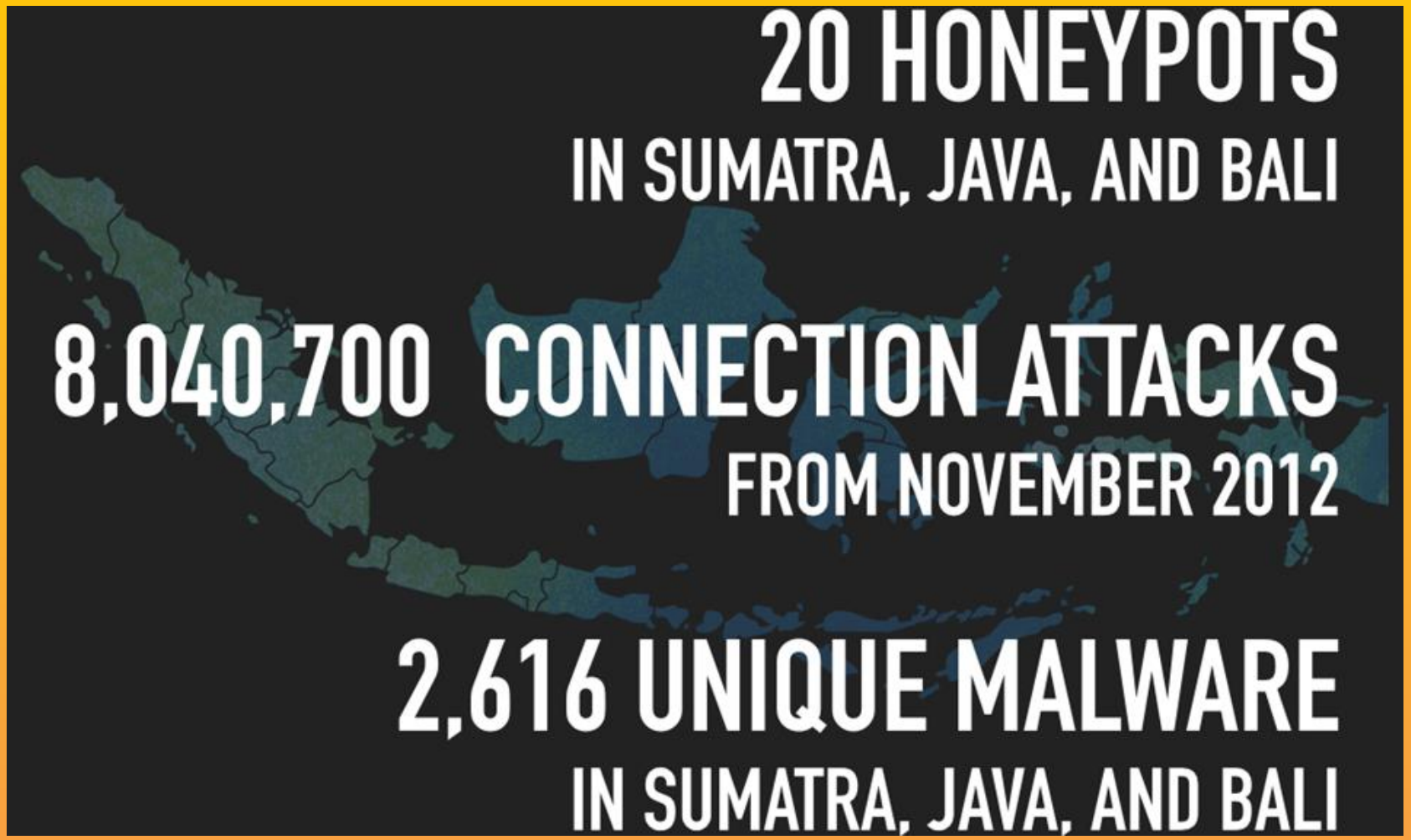


idhoneynet

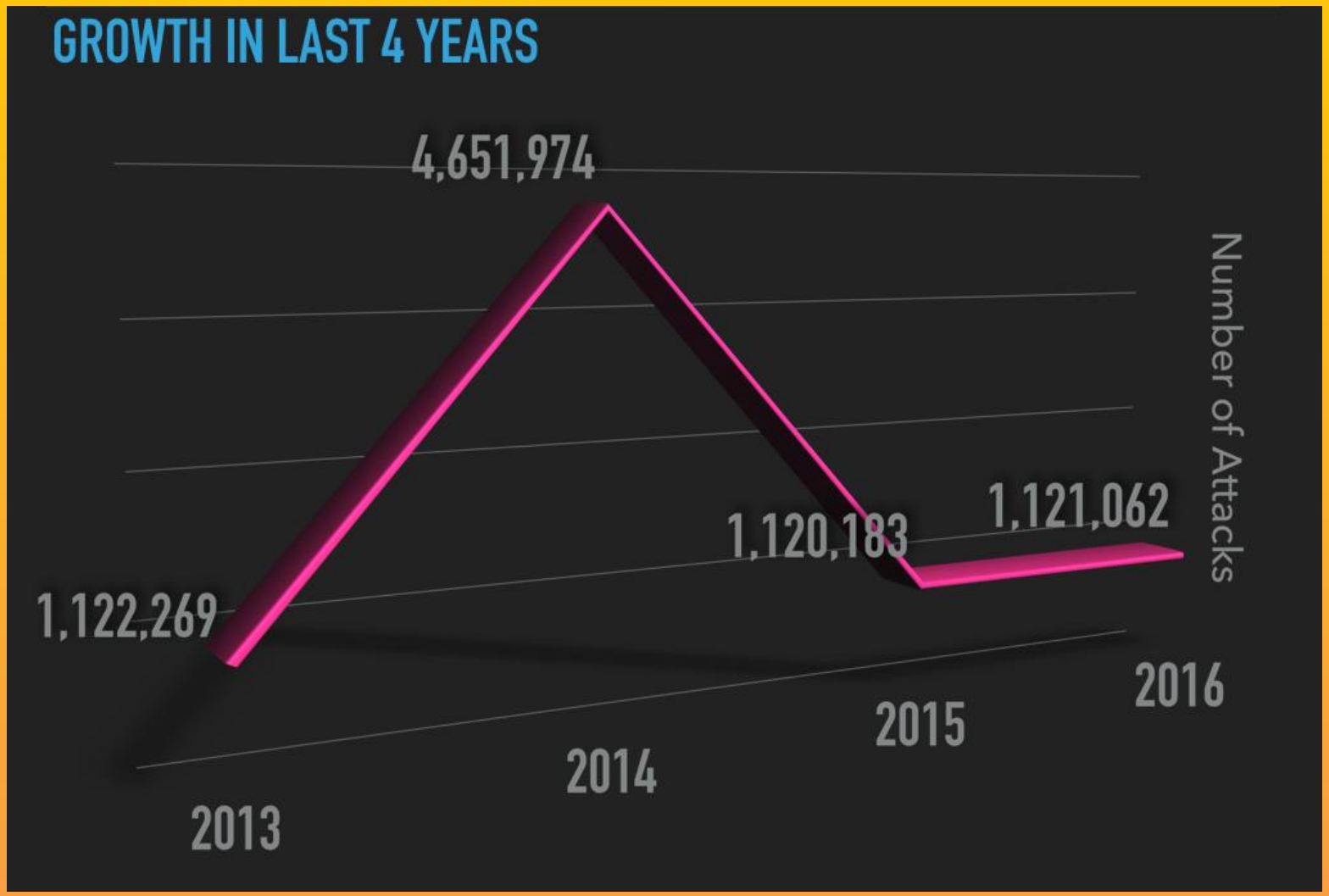
http://www.honeynet.or.id

http://groups.google.com/group/id-honeynet

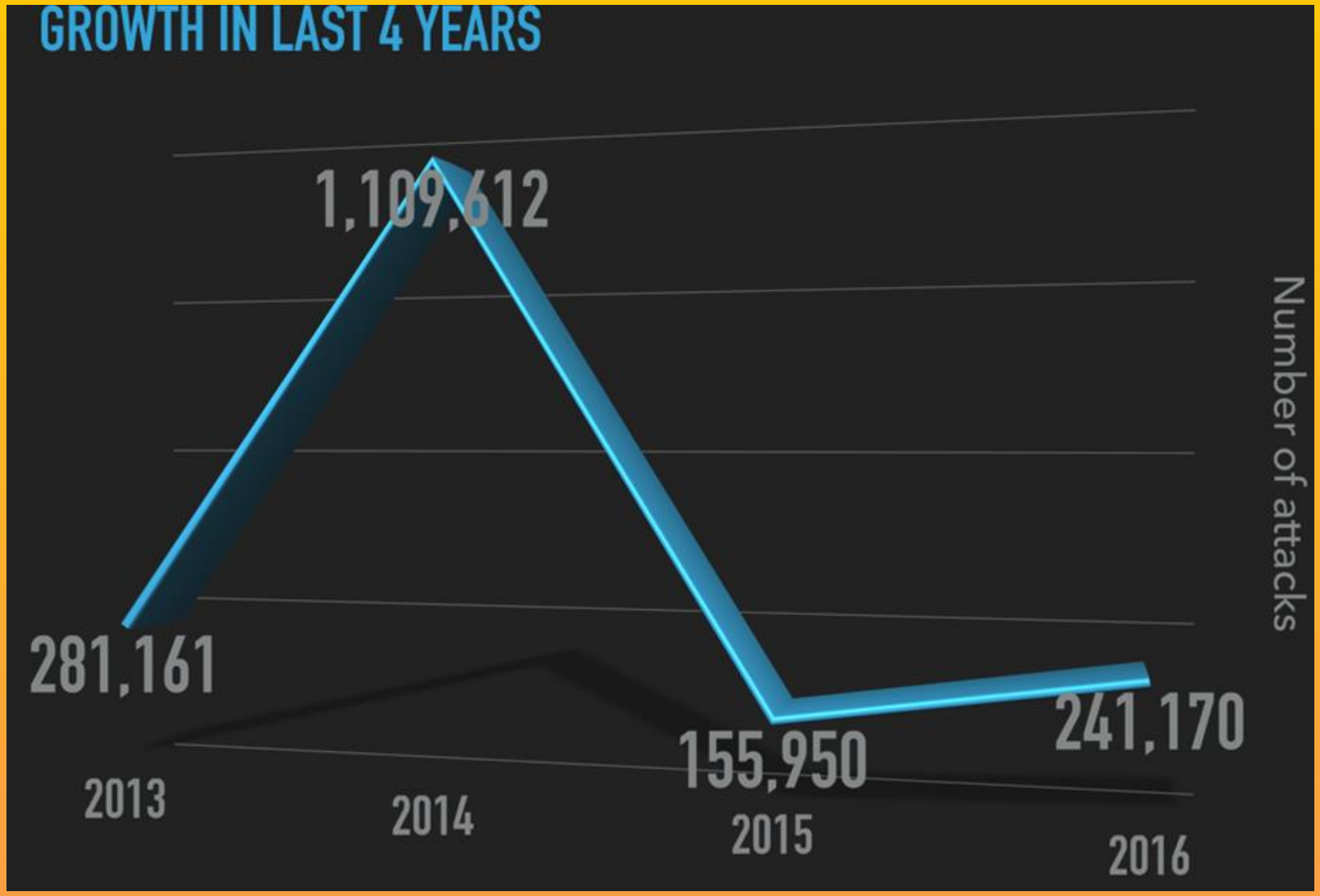
# Our Statistics



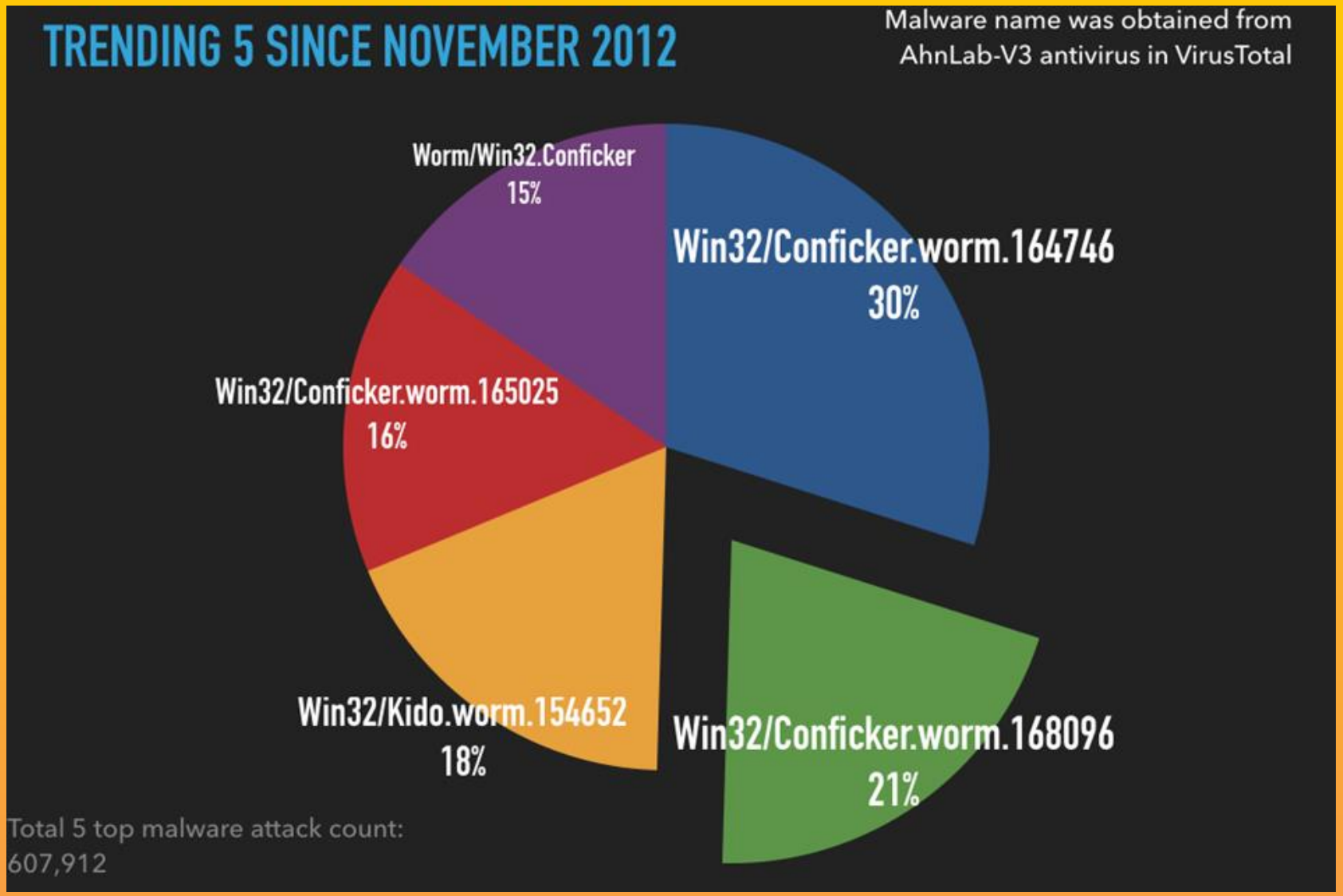
# Our Statistics



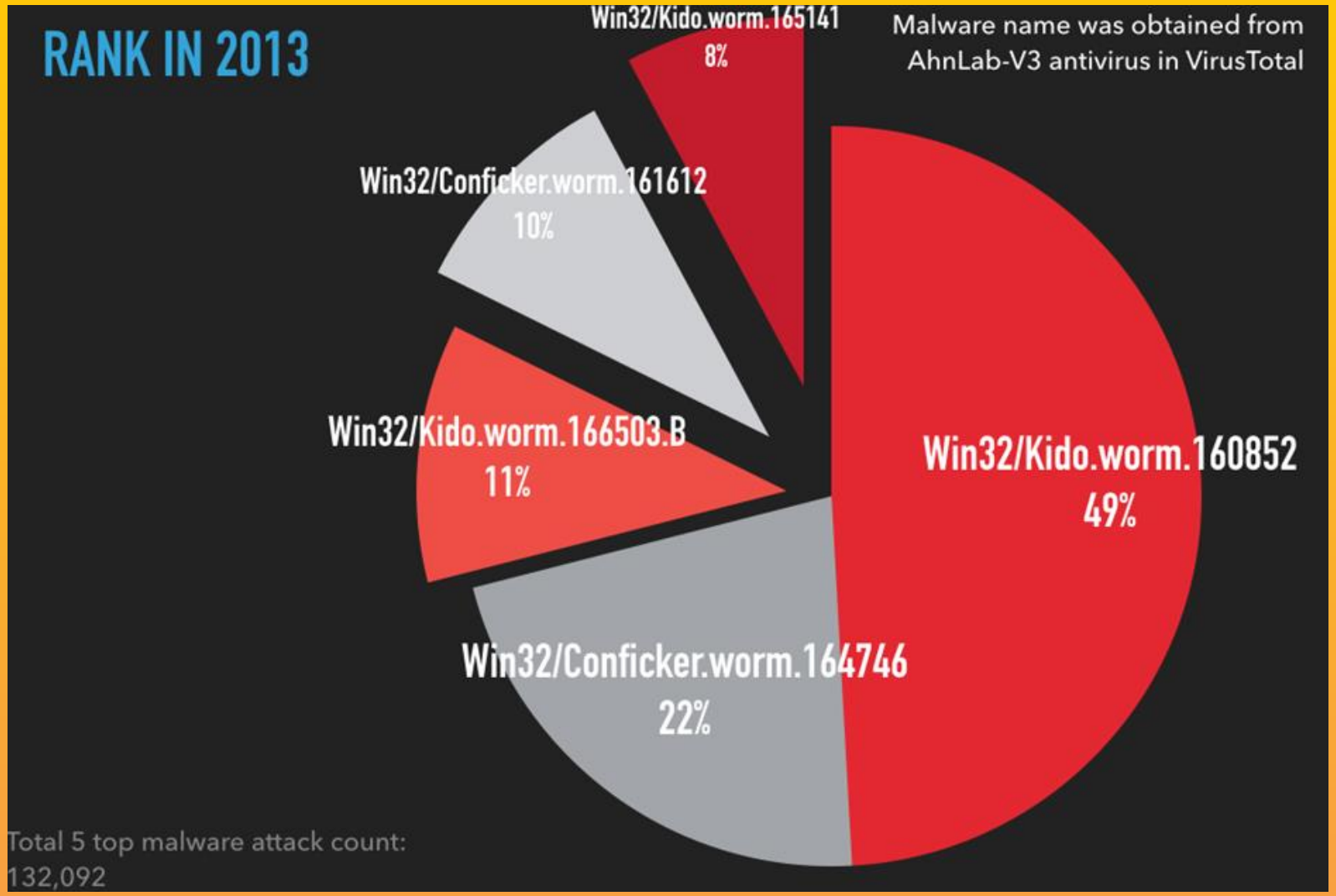
# Our Statistics (malware found)



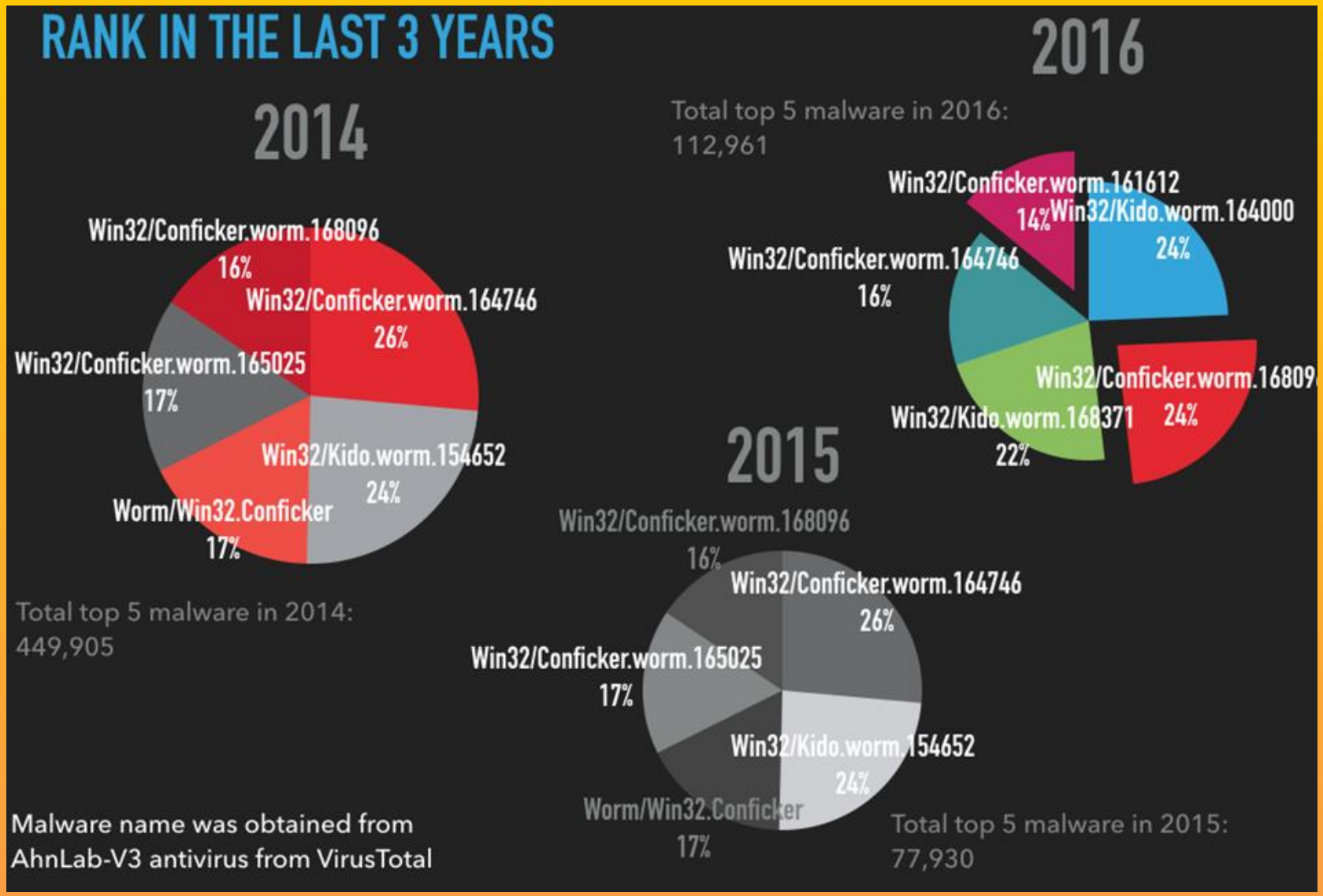
# Our Statistics



# Our Statistics



# Our Statistics



# Our Statistics (other malware)

## 2013

| Malware | Hit |
|---|---|
| Win-Trojan/Agent.22458 | 48 |
| Trojan/Win32.Zbot | 30 |
| Trojan/Win32.Androm | 23 |
| Trojan/Win32.Tepfer | 13 |
| Win-Trojan/Starman.Gen | 9 |
| Trojan/Win32.Jorik | 8 |
| Trojan/Win32.HmBlocker | 7 |
| Downloader/Win32.Dofoil | 6 |
| Worm/Win32.IRCBot | 4 |
| Win-Trojan/Agent.33128.B | 4 |

## 2014

| Malware | Hit |
|---|---|
| Win-Trojan/Agent.22458 | 123 |
| Trojan/Win32.Agent | 20 |
| Win-Trojan/Starman.Gen | 7 |
| Packed/Win32.Krap | 6 |
| Win-Trojan/Agent.33128.B | 6 |
| Win-Trojan/Xema.variant | 6 |
| Worm/Win32.IRCBot | 5 |
| Trojan/Win32.Npkon | 5 |
| Win-Trojan/Agent.40960.ZC | 4 |
| Win32/Virut.B | 1 |

Virus naming by AhnLab-V3 (Virustotal)

# Our Statistics (other malware)

**2015**

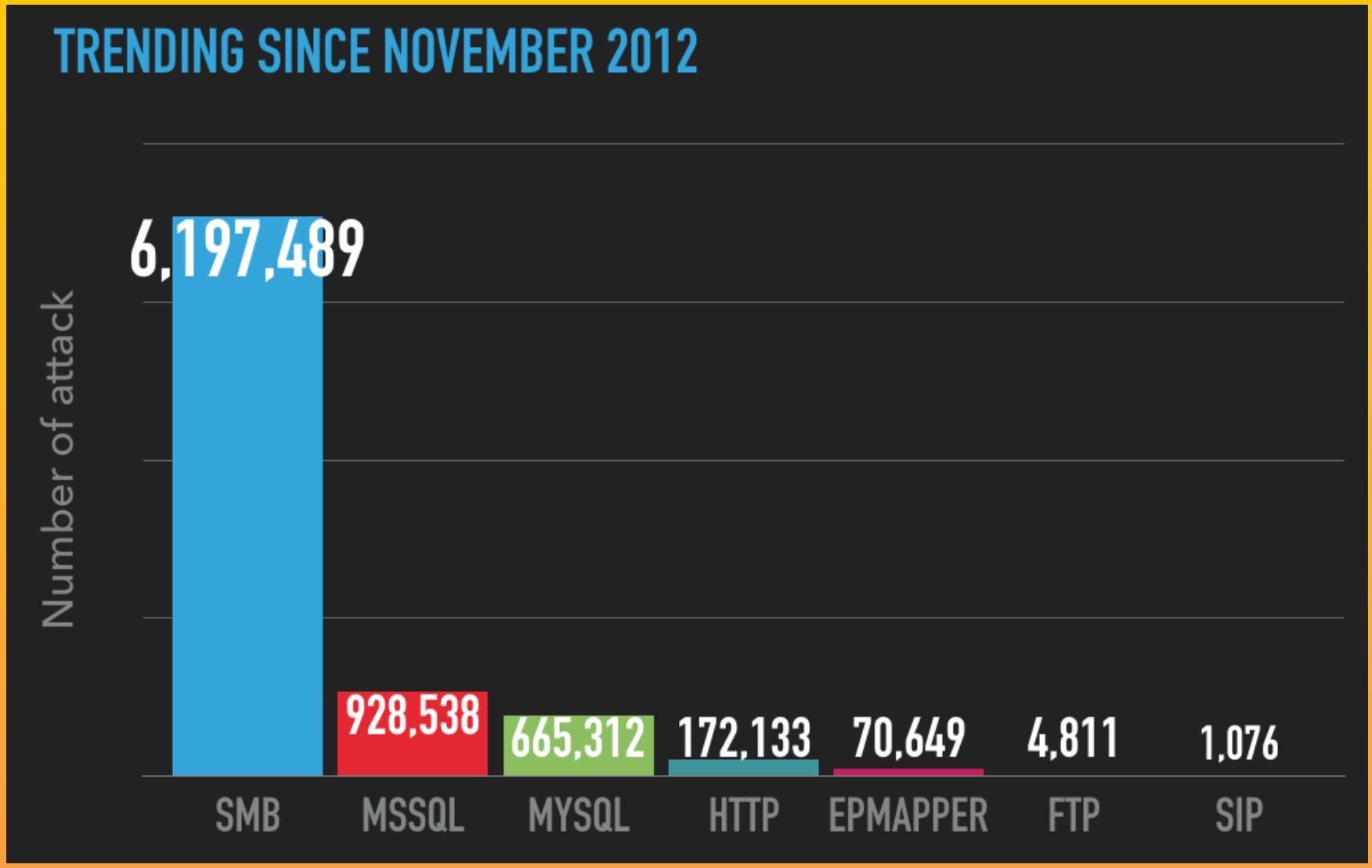
| Malware | Hit |
|---|---|
| Win-Trojan/Agent.22458 | 57 |
| Win-Trojan/Agent.33128.B | 22 |
| Trojan/Win32.Agent | 10 |
| Worm/Win32.IRCBot | 6 |
| Trojan/Win32.Npkon | 1 |
| Win-Trojan/Starman.Gen | 1 |
| Worm/Win32.Dipasik | 1 |

**2016**

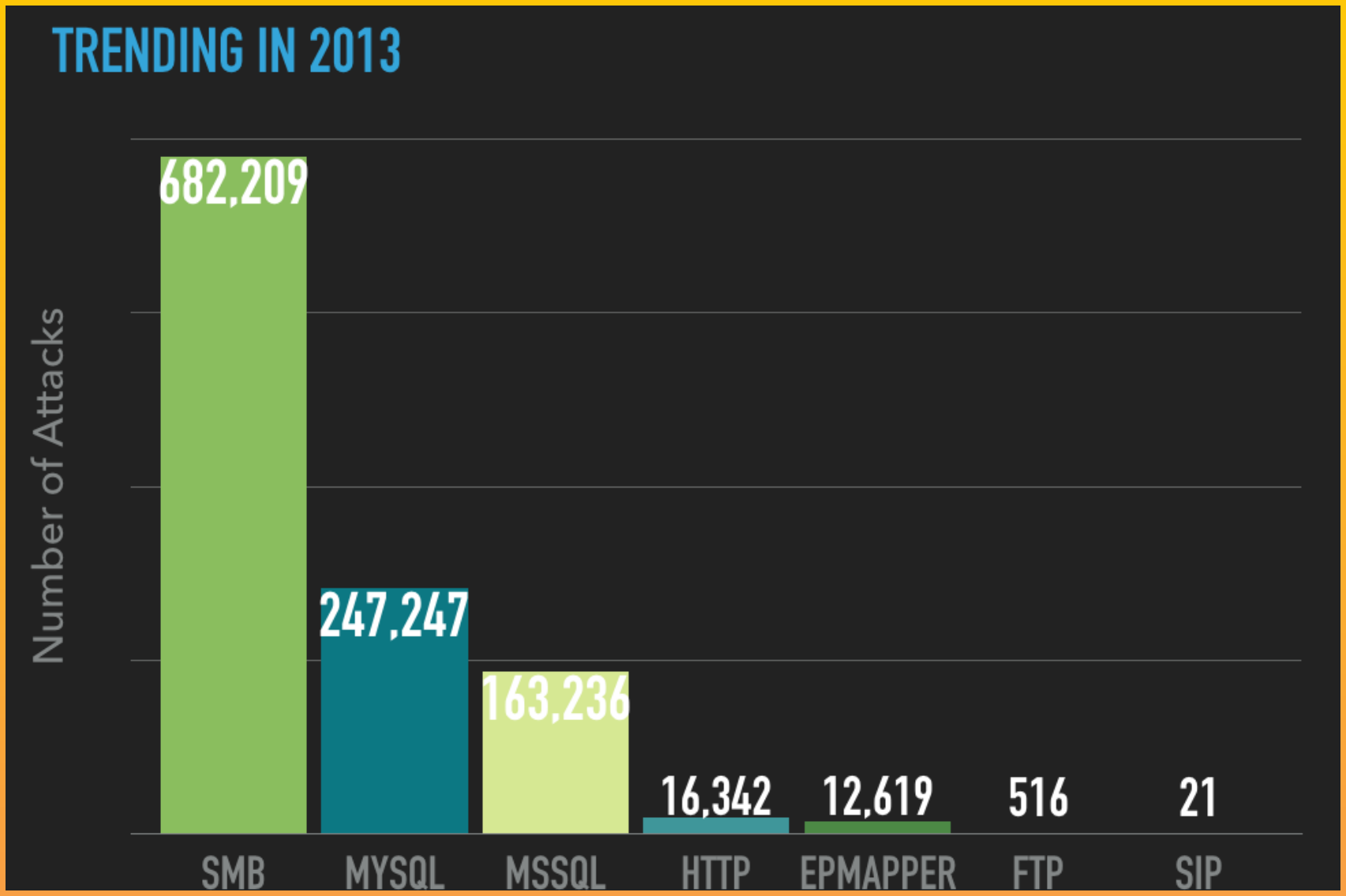
| Malware | Hit |
|---|---|
| Win-Trojan/Agent.22458 | 57 |
| Win-Trojan/Agent.33128.B | 22 |
| Trojan/Win32.Agent | 10 |
| Worm/Win32.IRCBot | 6 |
| Trojan/Win32.Npkon | 1 |
| Win-Trojan/Starman.Gen | 1 |
| Worm/Win32.Dipasik | 1 |

Virus naming by AhnLab-V3 (Virustotal)

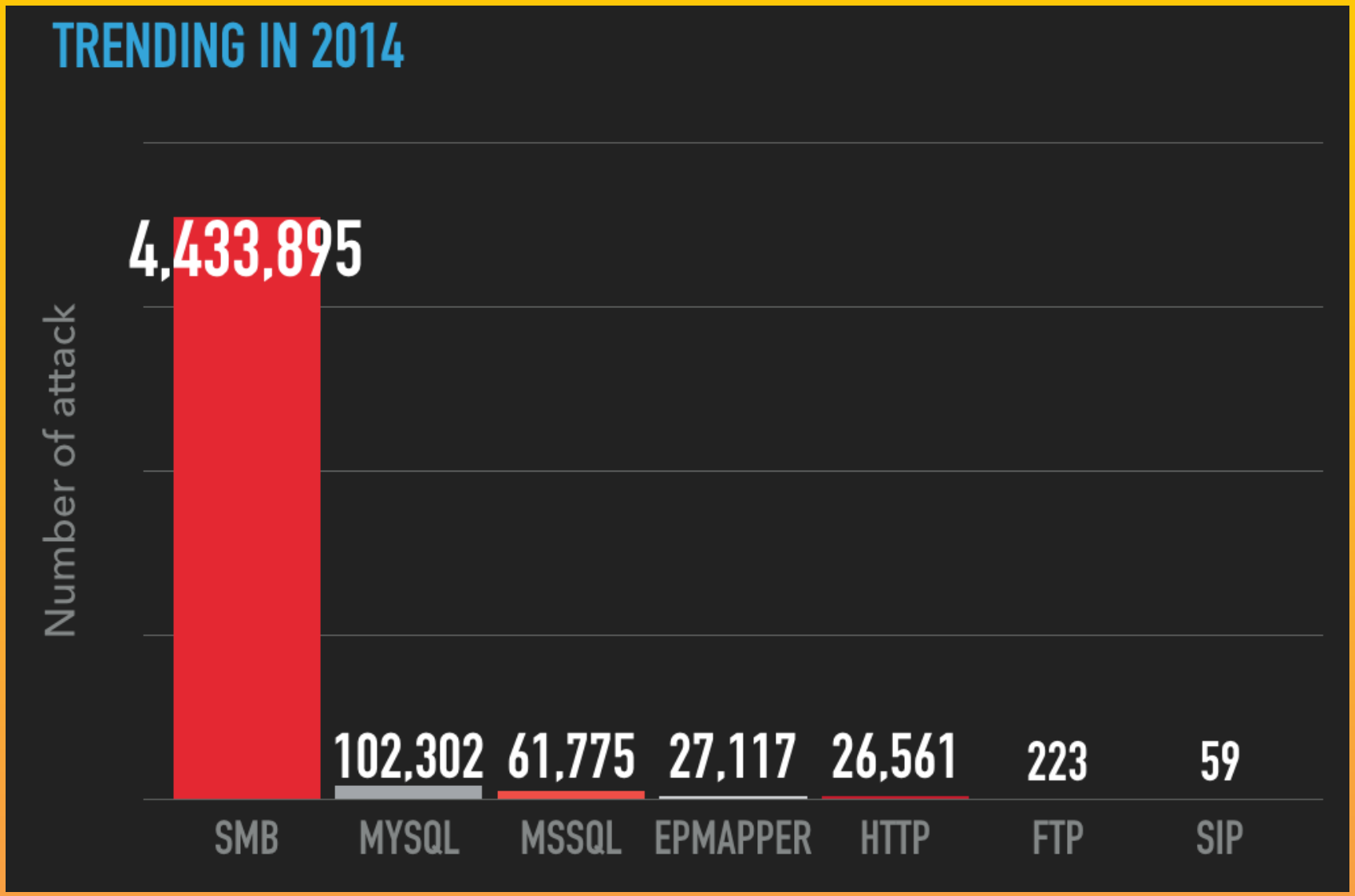
# More Statistics



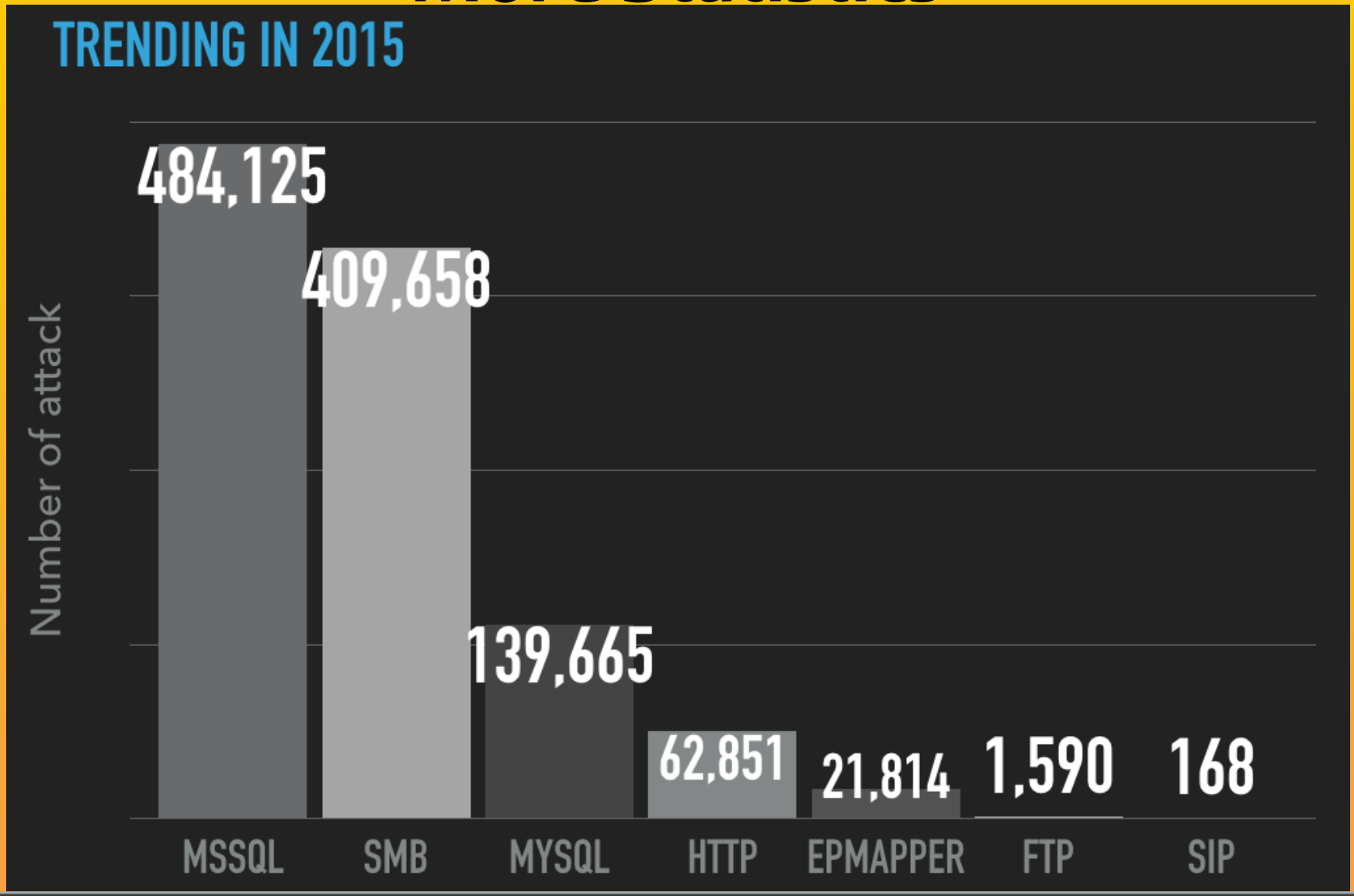
# More Statistics



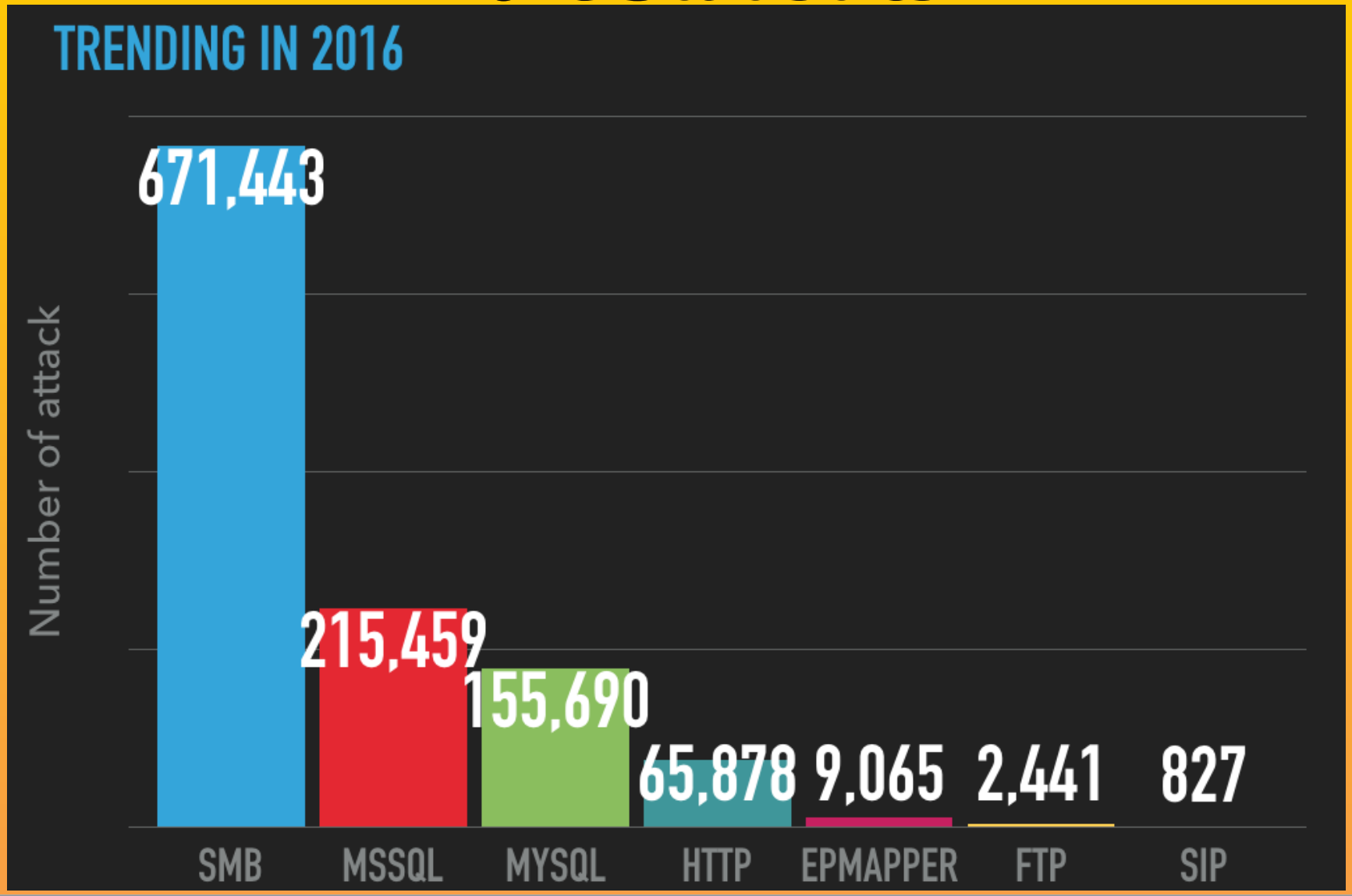
# More Statistics



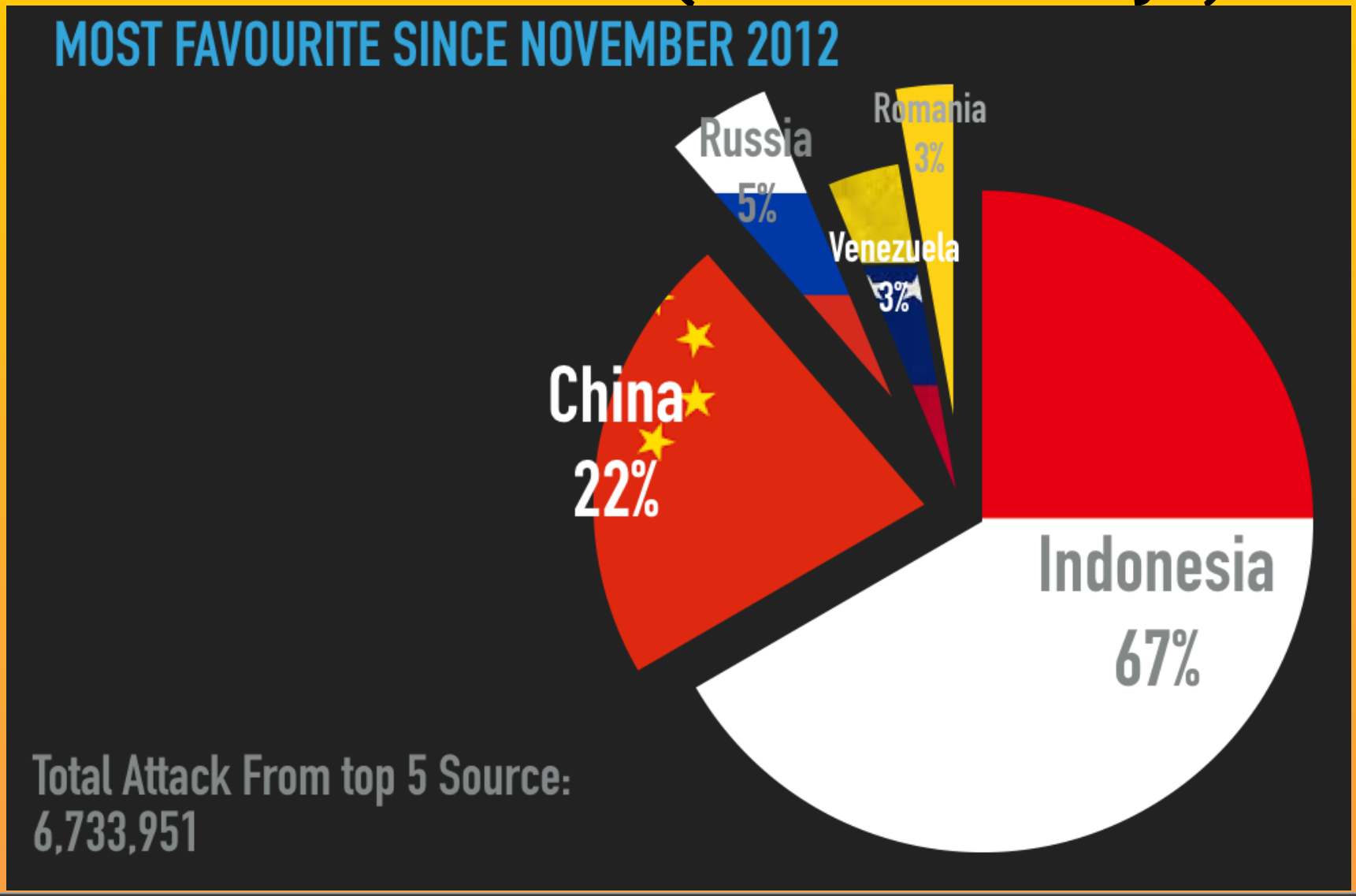
# More Statistics



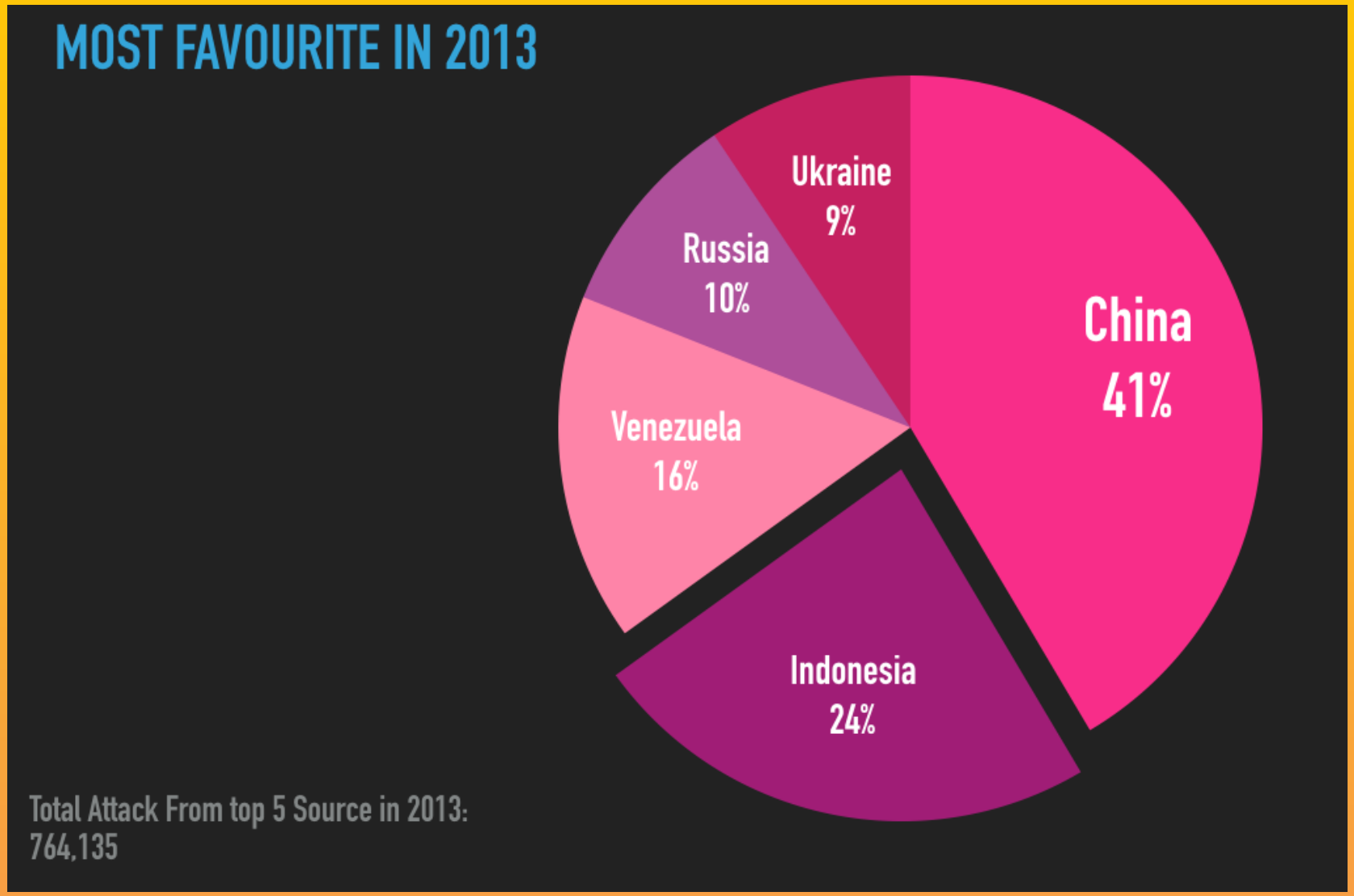
# More Statistics



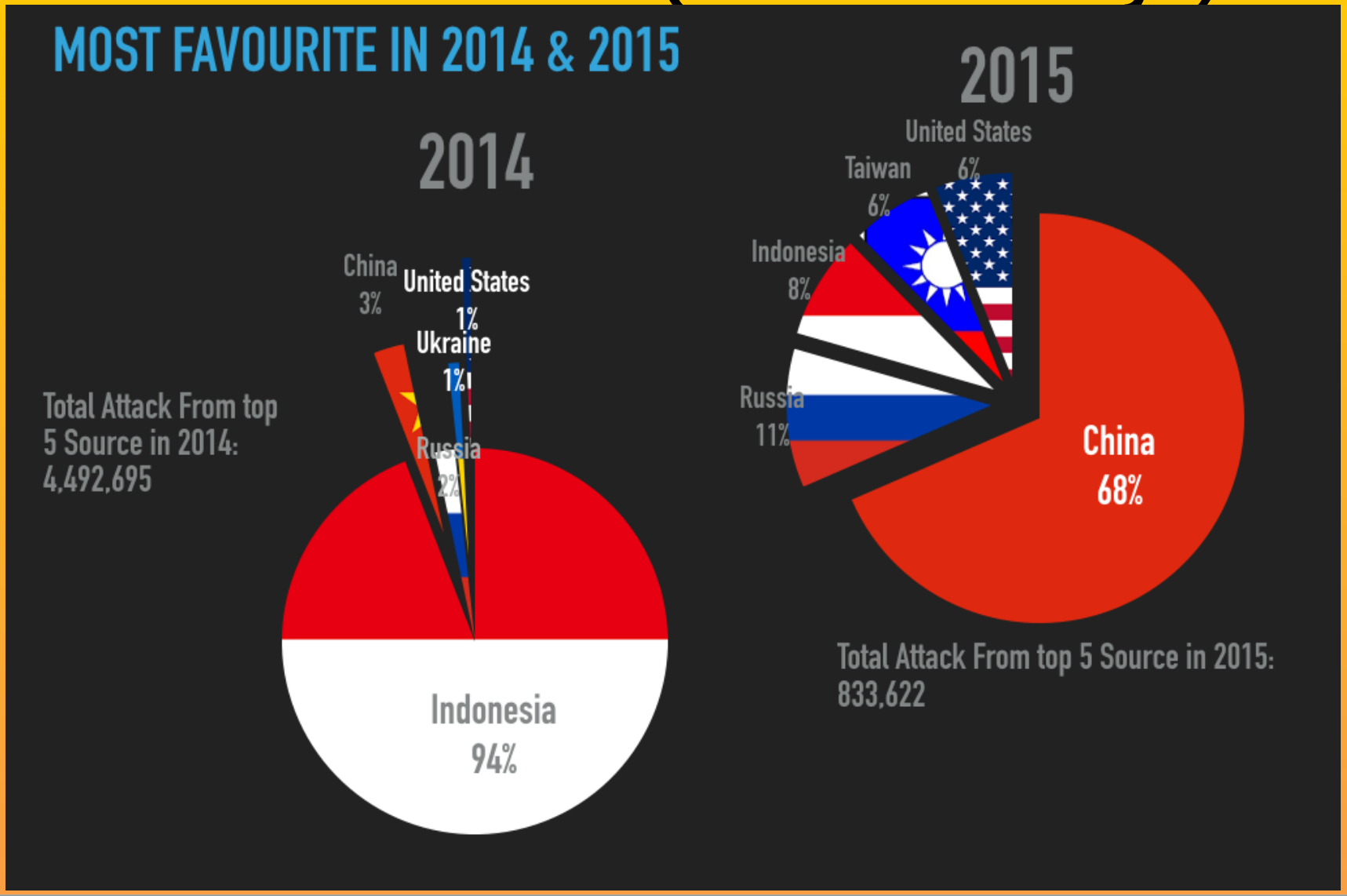
# More Statistics (who are they?)



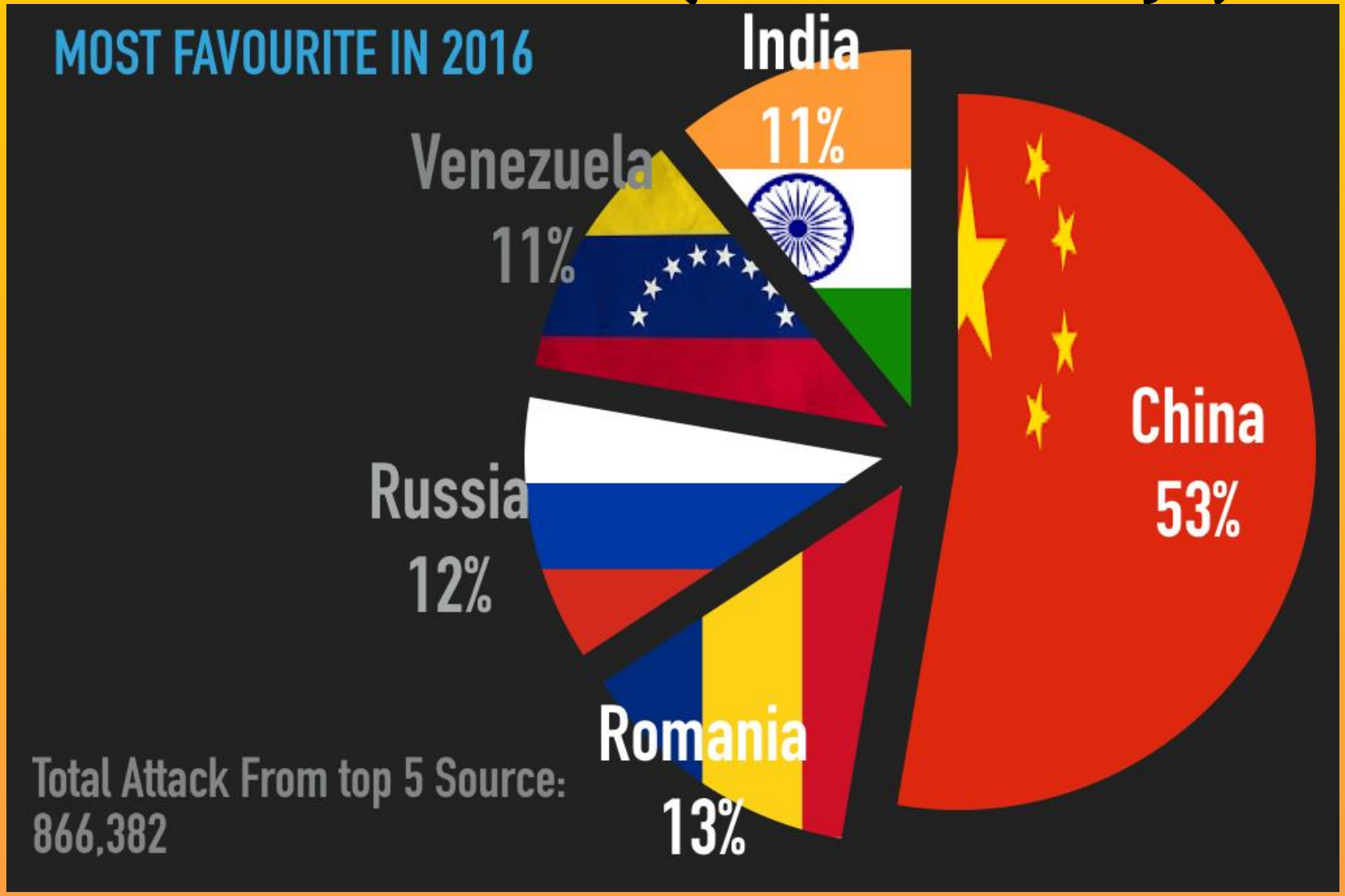
# More Statistics (who are they?)



# More Statistics (who are they?)



# More Statistics (who are they?)



# Behind the scene

- Malware Analysis
  - Automatic Static Analysis (after unpacking)
  - Automatic Behavior Analysis (Cuckoo sandbox)
- Unpacking
  - Dynamic Binary Instrumentation (DBI)
  - Recover malware code from memory dump
  - Need improvement on unpacking multi layer packed malware

# Our Current Research

- Analyzing National DNS traffic
  - Malicious Domains identification
  - Botnet Identification
  - Insider Threats
  - Anomaly Traffic Identification in medium to large ISP & Root DNS
- IDS with GPU

# Related Publications

- Joshua Tommy Juwono, Charles Lim, Alva Erwin, **A Comparative Study of Behavior Analysis Sandboxes in Malware Detection**, The 3rd International Conference on New Media 2015, Jakarta, Indonesia, 2015
- Charles Lim, Nicsen, **Mal-EVE Static Detection Model for Evasive Malware**, 10th EAI International Conference on Communications and Networking in China, Shanghai, China, 2015
- Charles Lim, Darryl Y. Sulistyan, Suryadi, and Kalamullah Ramli, **Experiences in Instrumented Binary Analysis for Malware**, The 3rd International Conference on Internet Services Technology and Information Engineering 2015 (ISTIE 2015), Bali, 2015
- Charles Lim, Meily, Nicsen, and Herry Ahmadi, **Forensics Analysis of USB Flash Drives in Educational Environment**, The 8th International Conference on Information & Communication Technology and Systems, Surabaya, 2014
- Charles Lim, and Kalamullah Ramli, **Mal-ONE: A Unified Framework for Fast and Efficient Malware Detection**, 2014 2nd International Conference on Technology, Informatics, Management, Engineering & Environment, Bandung, 2014.

# Our Future Research

- Capturing browser-based malware
- IDS with GPU
  - More optimized parallel algorithms
- Live DNS Traffic Analysis
- Android Malware Analysis

# Conclusion

- Learning takes time: 1 year to learn honeypots, 1 year to get the first honeypot running
- Our honeypots installed in academic institution, ISP, local province government
  - Challenge: installing more honeypots in these institution
- Honeypots provides opportunity for lecturer and students to perform research together

# Our Partners




















# THANK YOU

- YI LANG TSAI (蔡一郎) – Chapter Lead
- Honeynet Project – Taiwan Chapter members


- Ministry of Communication and Informatics of Republic of Indonesia


Backspace
Thank You
Page Up
Home
Page Down
Insert
Shift