Machete: 9 Years of Cyber Espionage Operations in Latin America

Veronica Valeros, Maria Rigaki, Kamila Babayeva, Sebastian Garcia
{valerver, rigakmar, babaykam, garciseb}@fel.cvut.cz

Stratosphere Research Laboratory, Czech Technical University
www.stratosphereips.org

A bit about us

- **Veronica Valeros (@verovaleros)**
  - Team leader of Civilsphere Project
  - Project leader of Stratosphere Research Laboratory
  - *Ask me about:* threat analysis, research, malware execution
- **Maria Rigaki (@mrigaki)**
  - PhD Student at the Czech Technical University in Prague
  - *Ask me about:* machine learning, malware analysis
- **Kamila Babayeva (@_kamifai_)**
  - Computer Science student at the Czech Technical University in Prague
  - *Ask me about:* python, network analysis, UI design, javascript
- **Sebastian Garcia (@eldracote)**
  - Director of Stratosphere, international speaker and trainer, founder of MatesLab
  - *Ask me about:* machine learning, network analysis, Stratosphere Linux IPS

Cyber espionage is understood as the act of obtaining restricted information without permission using software tools, such as malware.

Czech authorities dismantle alleged Russian cyber-espionage network

Czech officials said Russian operatives used local companies to launch cyber-attacks against foreign targets.

By Catalin Cimpanu for Zero Day | October 22, 2019 -- 13:51 GMT (14:51 BST) | Topic: Security

Chinese cyberespionage group PKPLUG uses custom and off-the-shelf tools

A previously unknown group or collective associated with China is targeting victims in Asia, possibly for geopolitical gain.

By Lucian Constantin

CSO Senior Writer, CSO | OCT 3, 2019 6:00 AM PDT

2014

APT REPORTS

“El Machete”

By GReAT on August 20, 2014. 6:30 am

CONTENTS

Introduction

Some time ago, a Kaspersky Lab customer in Latin America contacted us to say he had visited China and suspected his machine was infected with an unknown, undetected malware. While assisting the customer, we found a very interesting file

2017

Is this actor still active?

Is this a group or an individual operating the malware?

Who are the targets?

Is Machete under continuous development?

Special thanks to collaborators!

- **@malwrhunterteam**
- Special thanks to **Ross Gibb**!
- **Jakub Kroustek** (@JakubKroustek)
- **Reversing labs** (reversinglabs.com)
- **Luciano Martins** (@clucianomartins)
- **Yonathan Klijnsma** (@ydklijnsma)
- **Elnaz Babayeva** (@elnazavr)
- **Dmitry Bestuzhev** (@dimitribest)

An analysis and study of nine years of Machete cyber espionage activity.

Let’s start with Step 0:
What is Machete?

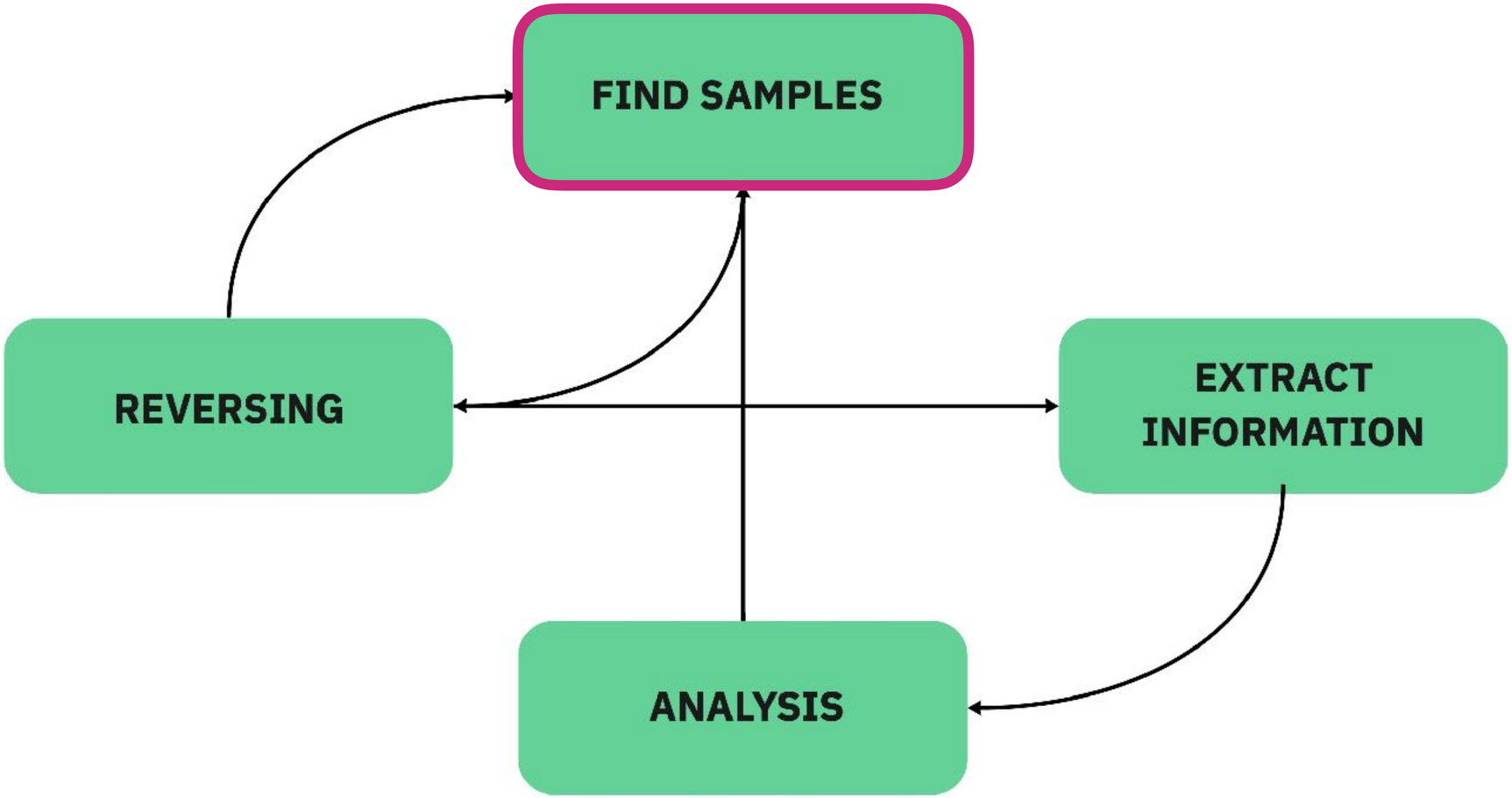
What is Machete?

Machete is also detected by some AVs as RAGUA.

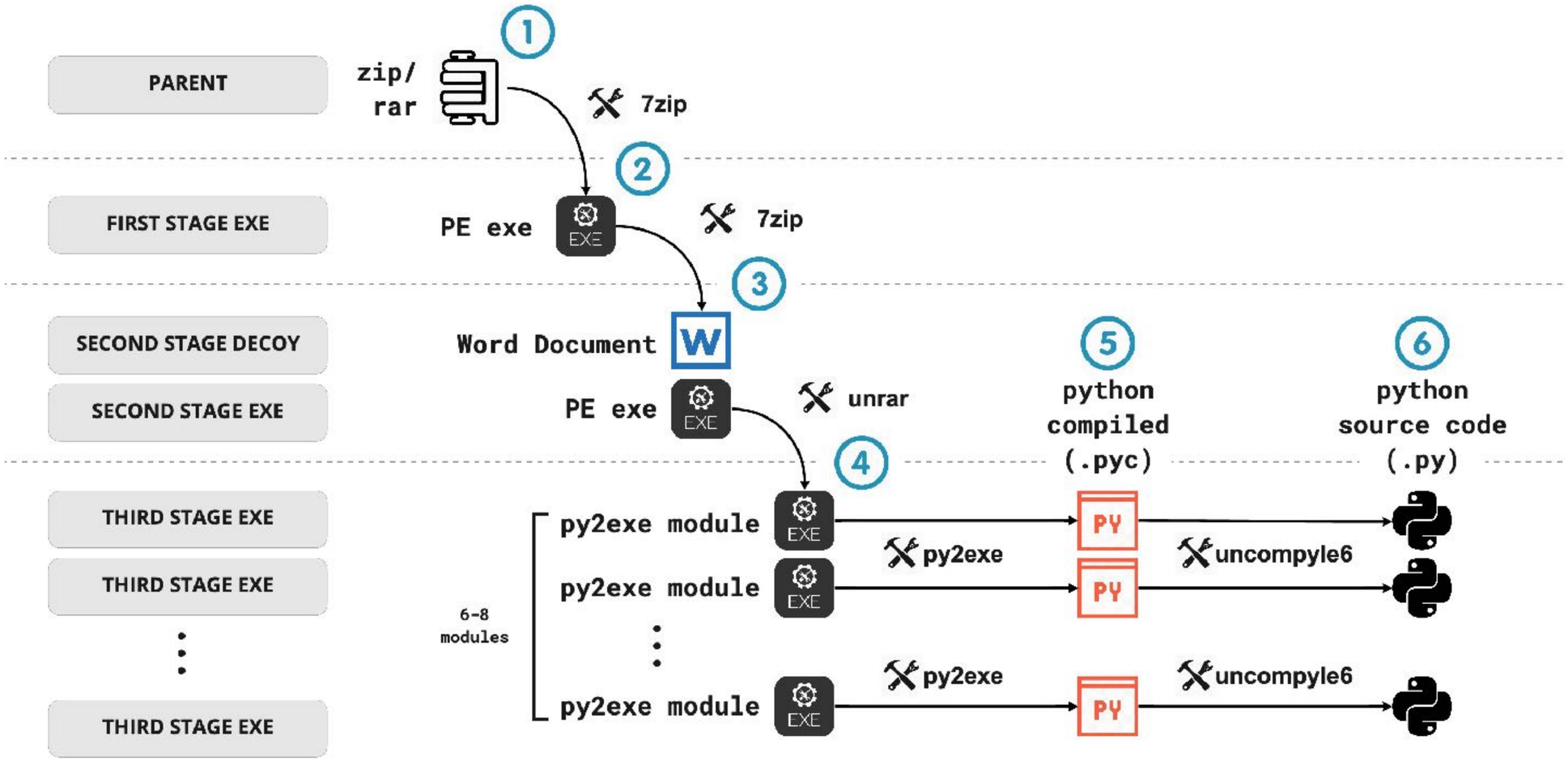
Machete is a modular python-based tool used for cyber espionage


I WANT THE DATA
AND I WANT IT MEOW
memegenerator.net

Research Methodology



Reversing Machete



Find Samples: We Wanted It All

- We searched samples in **public** and **private repositories** using Yara rules, string searches, and **OSINT-fu**.

SHA256	File Type	Type	Estimate Date	Size	Names
e0b3f89998e415ef23db7c43a0562c81443feae31de44338494020a32d19c0d6	EXE	Stage 1 - EXE		3.9M	
4f36cd8bb8ee89043d588f446e08199e6af88da43cc49b796161020853d2e90f	EXE	Stage 2 - EXE	October 11, 2012	3.3M	JavaFx.exe
048a8d6948d71f8a4d607679d1b5666818079f1a115f8279d331a372f3d2ffe6	PPT	Stage 2 - Decoy	October 10, 2012	530K	Urgente.pps
4adce69f415adaf183f775d2c8b15bb3e1d574e4ba8a39b170771fbcd85c5ad6	PY2EXE	Stage 3 - Module	October 9, 2012	587K	avwebdel.exe
8482bcedc470c04ea9dbf7a44bb09b0a294f630a0d44eccb652d198ef941d385	PY2EXE	Stage 3 - Module	October 9, 2012	848K	Javack.exe
ef5ed290fb733523efae23d16d2fc7655a9b7916bcad914c7c5ca8e22e7224fc	PY2EXE	Stage 3 - Module	October 9, 2012	737K	java.exe
9894e45330c4e5201c6cf03156a907c39d3c79642b0eb9c09c4182ec9b9395a6	PY2EXE	Stage 3 - Module	October 9, 2012	601K	JavaS.exe
20d0ca532efa6b2896f351fb6f3a8a2896a47cbe6d1547b14b8b89df1a29ea2f	PY2EXE	Stage 3 - Module	October 9, 2012	588K	javaTM.exe
edf25b9b7d64fbe84bfa9cba0463f5bc8a1c48d3b5e448b418e2f566e4fbdfbc	PY2EXE	Stage 3 - Module	October 9, 2012	587K	JavaUe.exe
586a2dad9d01b85ae6c45ac1e39201455d08518facaa27f81401cbe995a816af	PY2EXE	Stage 3 - Module	October 9, 2012	794K	UpJava.exe

Largest Collection of Samples

- **176 Total Campaigns**
- **116** Stage 1 Machete
- **155** Stage 2 Machete
- **93** Machete Decoys
- **342** Machete Modules

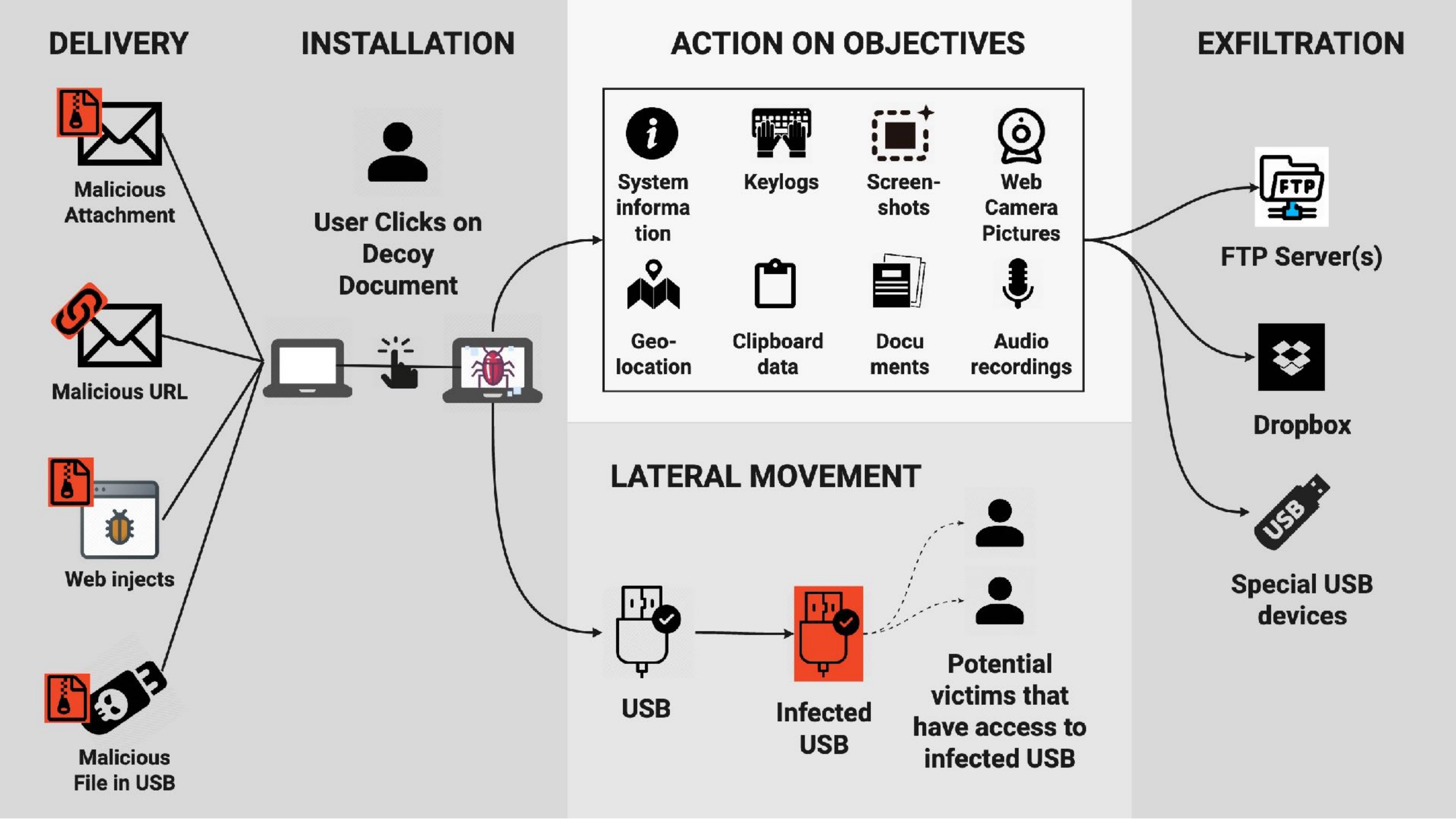
Earliest sample dated
December 2010

Latest sample dated
January 2019

Extract Information

- Python code for every module (sometimes obfuscated)
- Last modified date of Stage 3 files seems not modified
- Configuration files: FTP paths, version numbers, campaign purpose, enabled functionalities of the malware
- Command and Control servers & Operators credentials
- Encryption keys

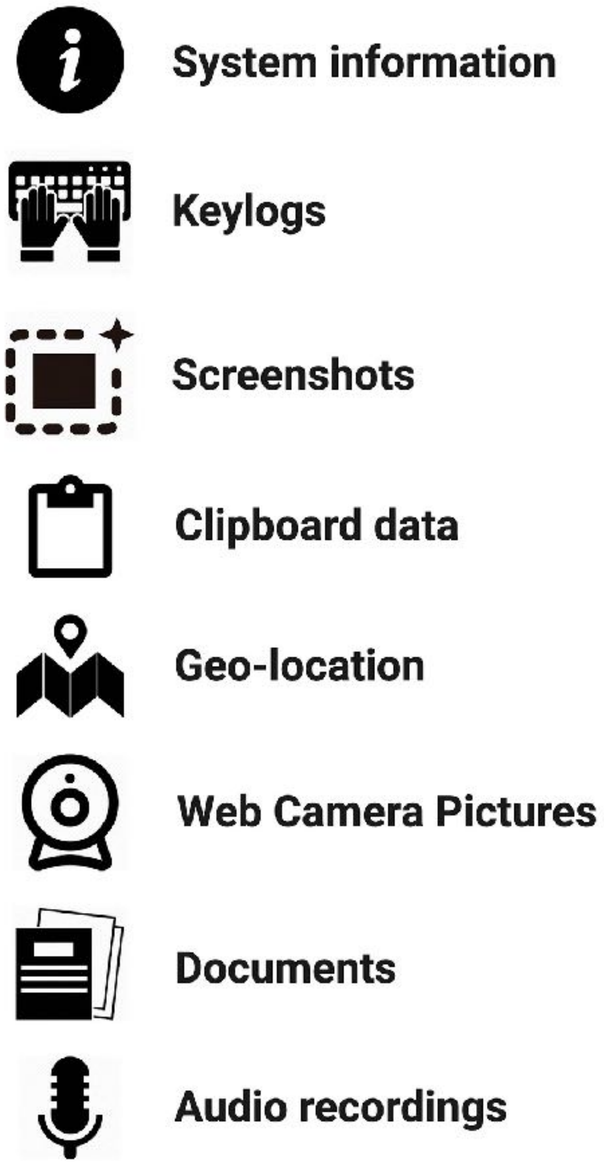
How does Machete operates?


DELIVERY
INSTALLATION
ACTION ON OBJECTIVES
EXFILTRATION
Malicious Attachment
Malicious URL
Web injects
Malicious File in USB
User Clicks on Decoy Document
System information
Keylogs
Screen-shots
Web Camera Pictures
Geo-location
Clipboard data
Documents
Audio recordings
FTP
FTP Server(s)
Dropbox
USB
Special USB devices
LATERAL MOVEMENT
USB
Infected USB
Potential victims that have access to infected USB

Delivery

Delivering a weaponized bundle to the target.

- **Spear phishing:**
  URLs, Attachments, Web Injects
- **Infected USBs:**
  file bundled with machete malware



Action on Objectives

The attacker performs the steps to achieve his actual goals inside the victim's network.

- **System information:** who the target is, device being used.
- **Geolocation:** where the target is located.
- **Keystrokes:** what the target writes.
- **Clipboard content:** what the target copies and pastes (passwords?).
- **Screen captures:** what the target is seeing on the screen (web email?).
- **Web camera captures:** who or what is in front of the computer
- **Audio:** what the victim is saying, conversations from surroundings.
- **Documents:** specific documents in the target's computer.

Lateral Movement

Move through the compromised network to find a (better) target.

- **Infect inserted USBs drives:**
  - It copies itself, including the decoy
  - Victim lured to open the infected document
  - No automatic execution so far
  - Typically used for jumping air gapped systems

FTP Server(s)

Dropbox

Special USB devices

Exfiltration

Retrieval, copy and transferring of data of interest from the victims computers.

- **288** screen captures per victim per day
- **~2000** screen captures per victim per week
- Plus keylogs, documents, clipboard data, audio, geolocation, etc.

Exfiltration

Retrieval, copy and transferring of data of interest from the victims computers.

Analysis: Versions, Infrastructure and Encryption Keys

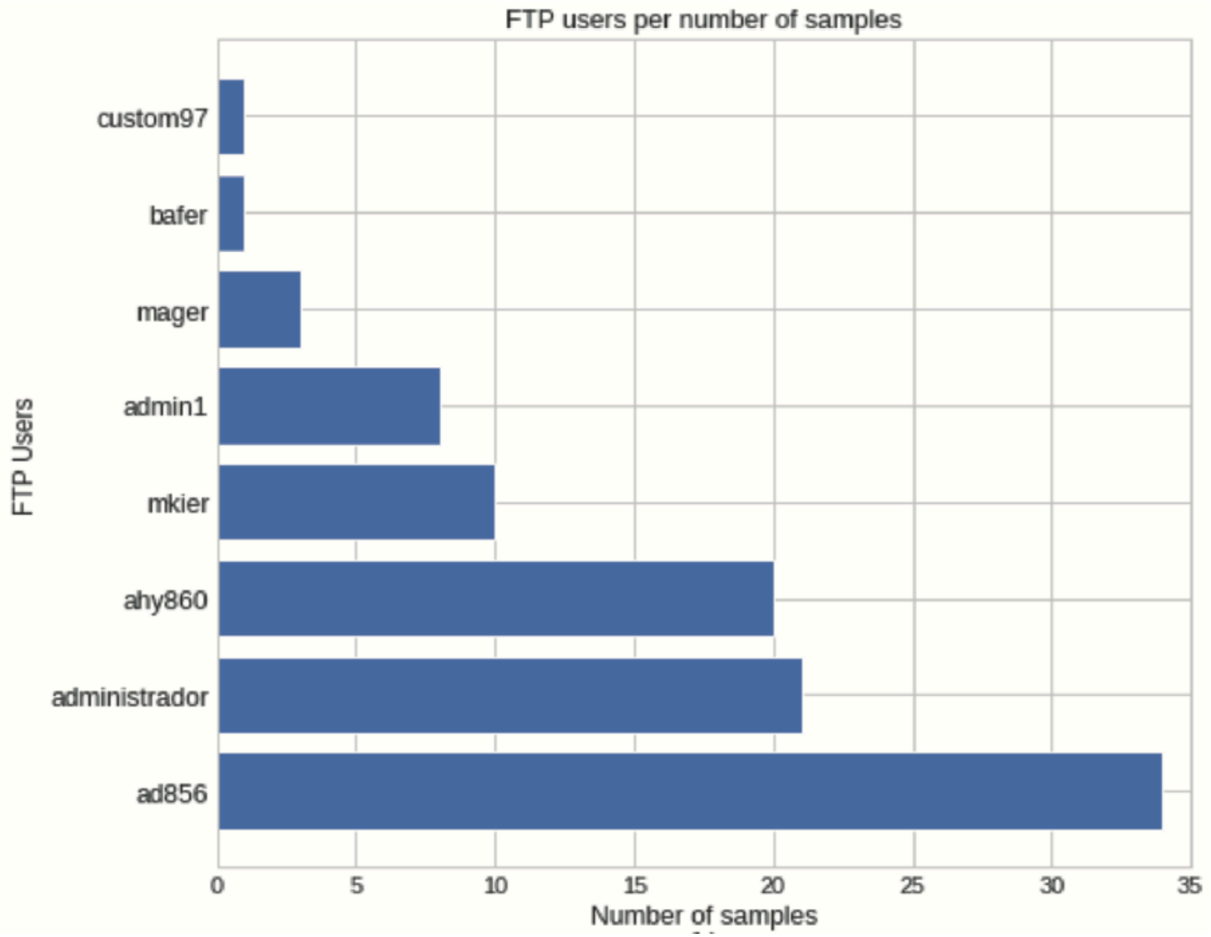
From December 2010 to January 2019

31 C&C Servers

18 FTP Users

20 FTP Passwords

6 Encryption Keys



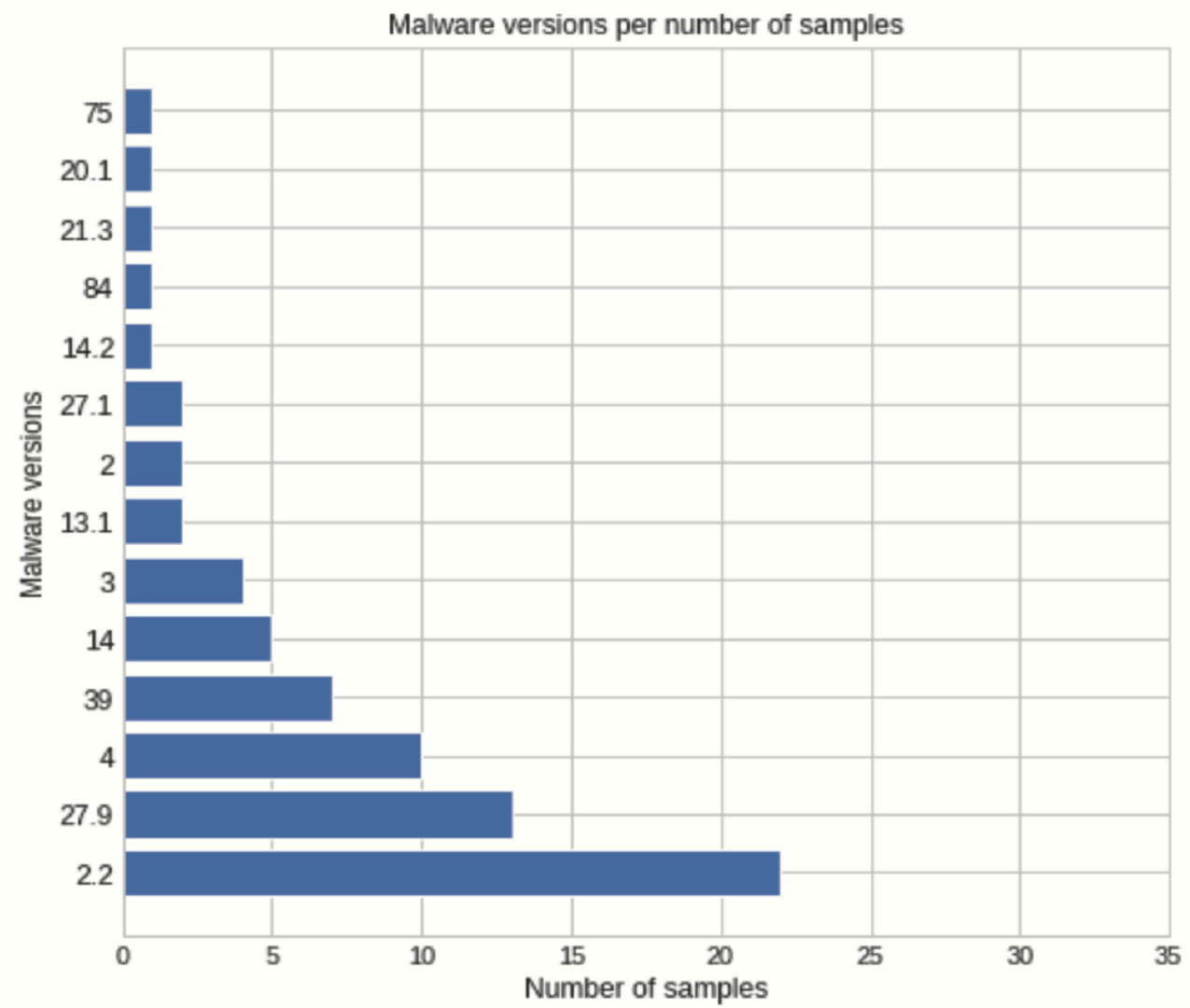
2.0 | 2.2 | 3.0 | 4.0

13.0 | 13.1 | 14.0

14.2 | 15.1 | 20.1

21.3 | 27.1 | 27.9

39.0 | 75.0 | 84.0



- Encryption keys have the same length, same structure, and seem to share password creation recipe.
- The low number of encryption keys show that the malware is likely operated by the same group.
- Attackers don’t change infrastructure often: 30 domains in 10 years.
- Heavy reuse of FTP credentials and insecure storage of them.
- Whoever had access to the samples could access the victims stolen data.
- High number of different versions suggest parallel development of the tool.

Analysis of Campaigns

From December 2010 to January 2019

Who are the targets?

Four Phases of Analysis

- First phase: noting the **type** of document (PDF, Word, JPG, etc)
- Second phase: identify the **language** used in the document
- Third phase: identify a **theme** of the documented based on content analysis (political, economic, military, etc)
- Fourth phase: identify the **main country** mentioned in the document

Jungmann verifica o funcionamento do SISFRON, em Dourados (MS)

Imprimir

Brasília, 20/01/2016 - O ministro da Defesa, Raul Jungmann, esteve nesta quinta-feira (19) em Dourados, no Mato Grosso do Sul, para acompanhar a operação do Sistema Integrado de Monitoramento de Fronteiras (SISFRON). O ministro lembrou que no ano passado foram destinados para o Sistema R$ 228 milhões, e que, para 2017, o orçamento previsto é de R$ 470 milhões. "O SISFRON é uma realidade em 600 km de fronteira, e será uma realidade nos 17 mil quilômetros, a terceira maior fronteira do mundo com 10 países vizinhos", declarou o ministro.
O projeto-piloto do SISFRON é operado na 4ª Brigada de Cavalaria Mecanizada de Dourados e abrange cerca de 650 quilômetros de fronteiras no estado, que são monitorados por radares fixos e móveis, sensores óticos, óculos de visão noturna, câmeras de longo alcance, entre outros materiais empregados. "A fronteira está distante fisicamente, mas a fronteira está perto das nossas cidades e metrópoles porque é nelas, na defesa e segurança delas, que nós vamos conseguir reduzir esta onda de criminalidade no seu início, combater as drogas, o contrabando e o descaminho. É na defesa das fronteiras que vamos assegurar a soberania do presente e do futuro e a integridade territorial".

Foto:Tereza Sobreira/MD

O ministro assistiu uma demonstração sobre o SISFRON. Militares transmitiram em tempo real ações de vigilância que ocorriam na fronteira

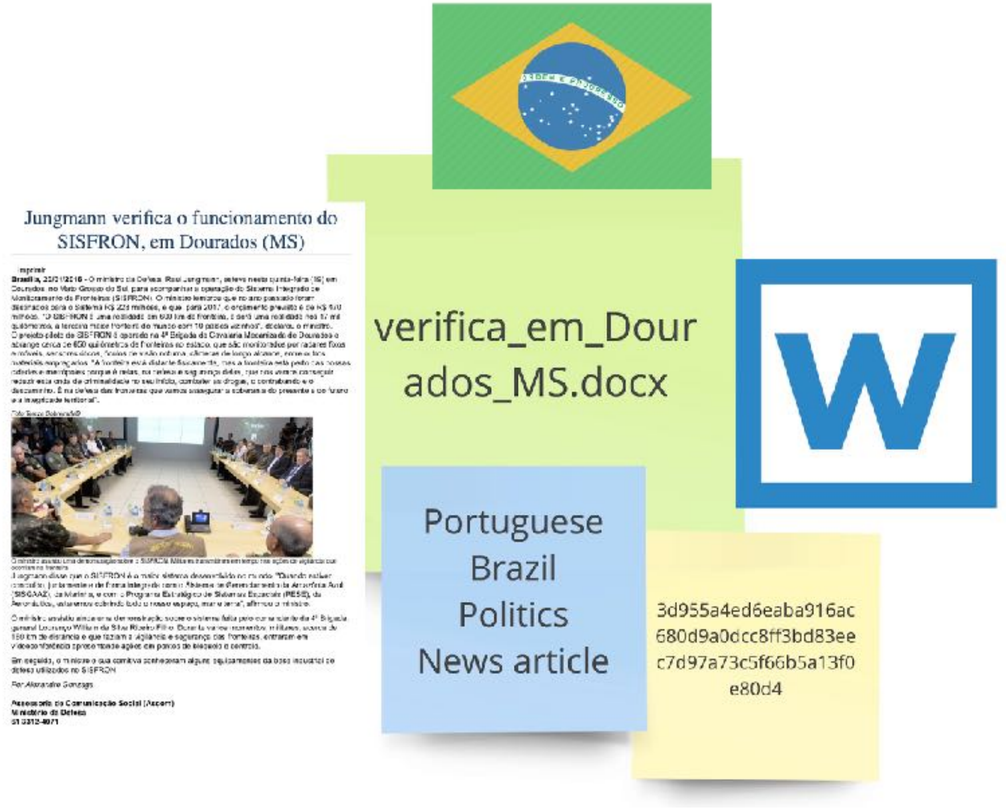
Jungmann disse que o SISFRON é o maior sistema desenvolvido no mundo. "Quando estiver concluído, juntamente e de forma integrada com o Sistema de Gerenciamento da Amazônia Azul (SISGAAZ), da Marinha, e com o Programa Estratégico de Sistemas Espaciais (PESE), da Aeronáutica, estaremos cobrindo todo o nosso espaço, mar e terra", afirmou o ministro.

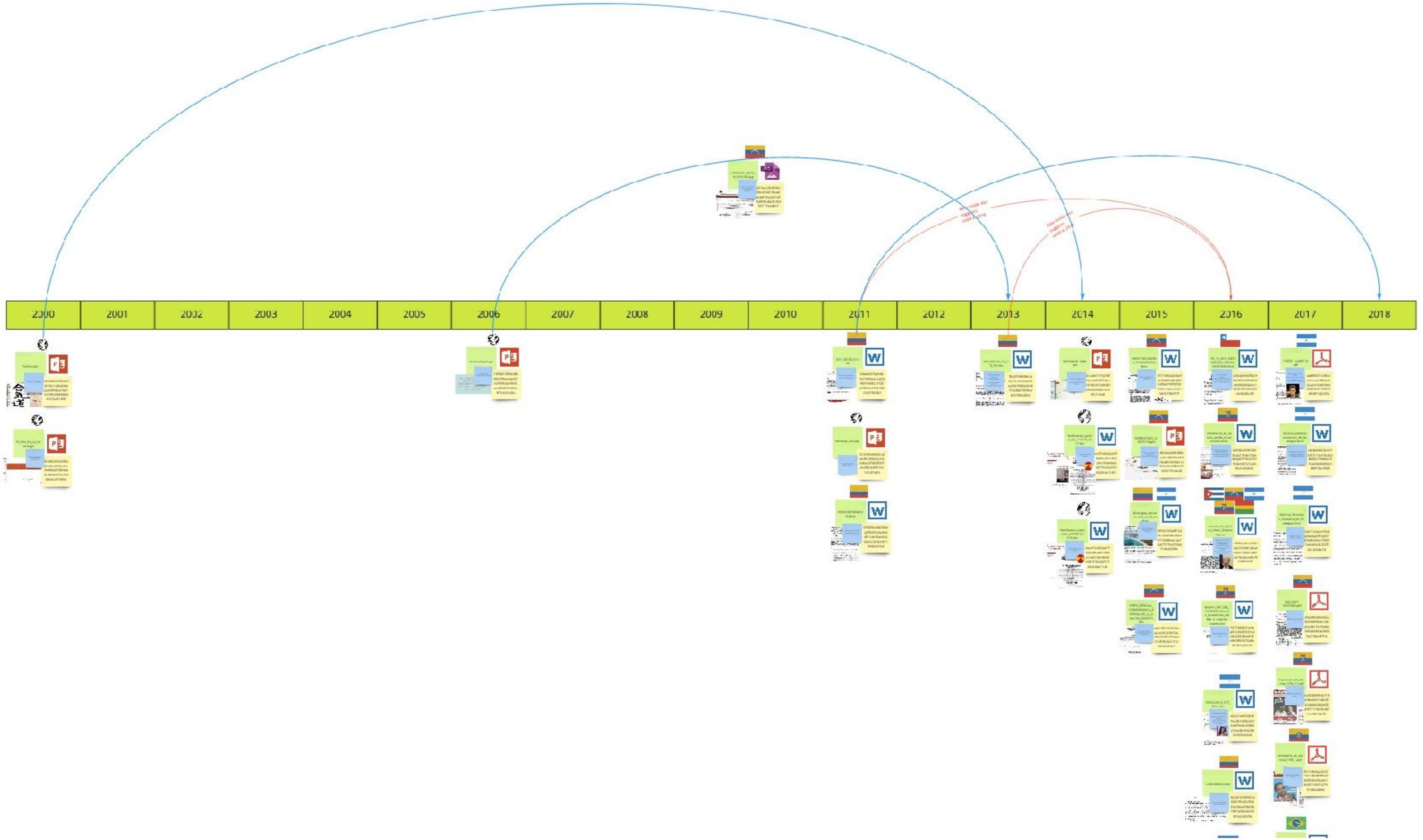
O ministro assistiu ainda uma demonstração sobre o sistema feita pelo comandante da 4ª Brigada, general Lourenço William da Silva Ribeiro Filho. Durante vários momentos, militares, acerca de 160 km de distância e que faziam a vigilância e segurança das fronteiras, entraram em vídeoconferência apresentando ações em pontos de bloqueio e controle.

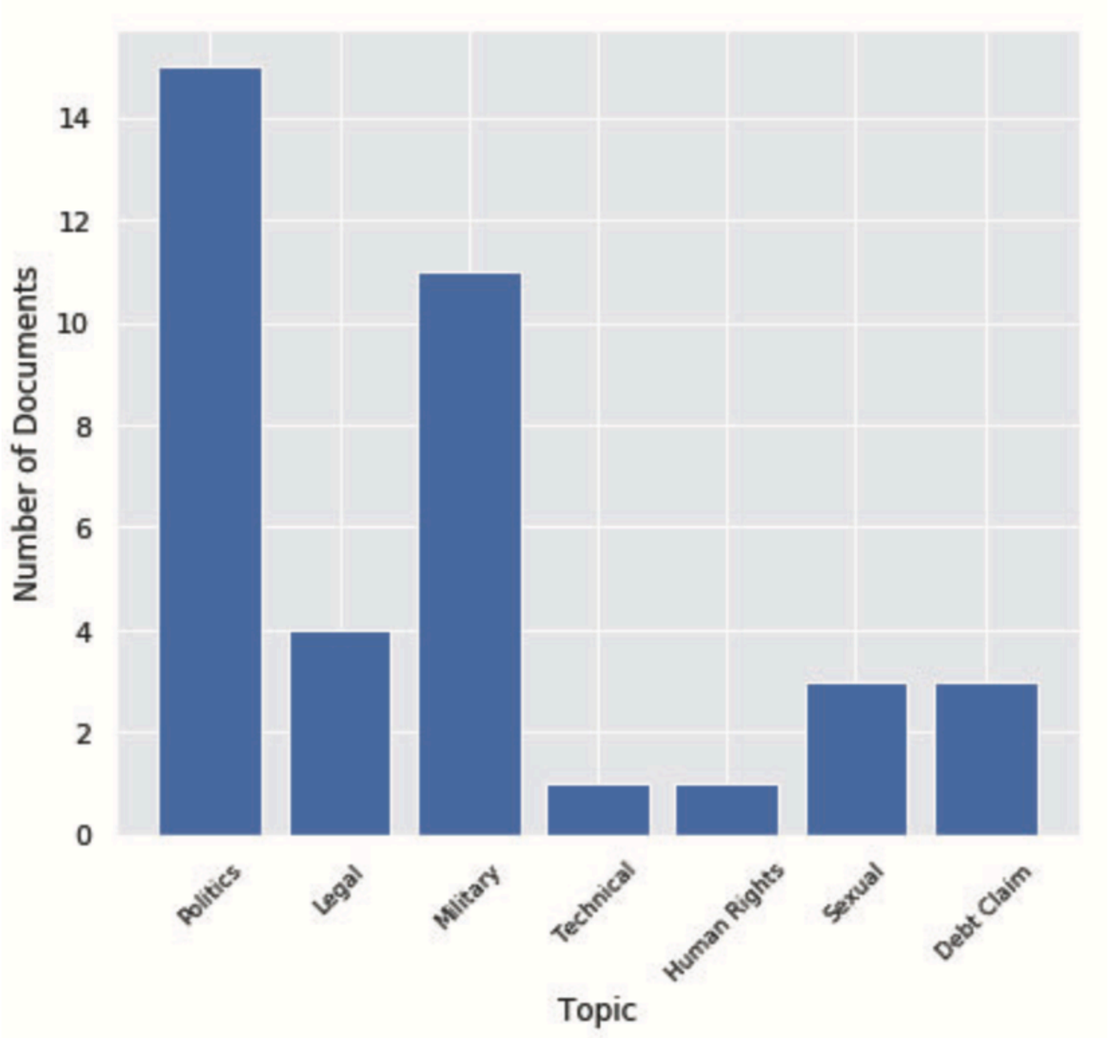
Em seguida, o ministro e sua comitiva conheceram alguns equipamentos da base industrial de defesa utilizados no SISFRON.

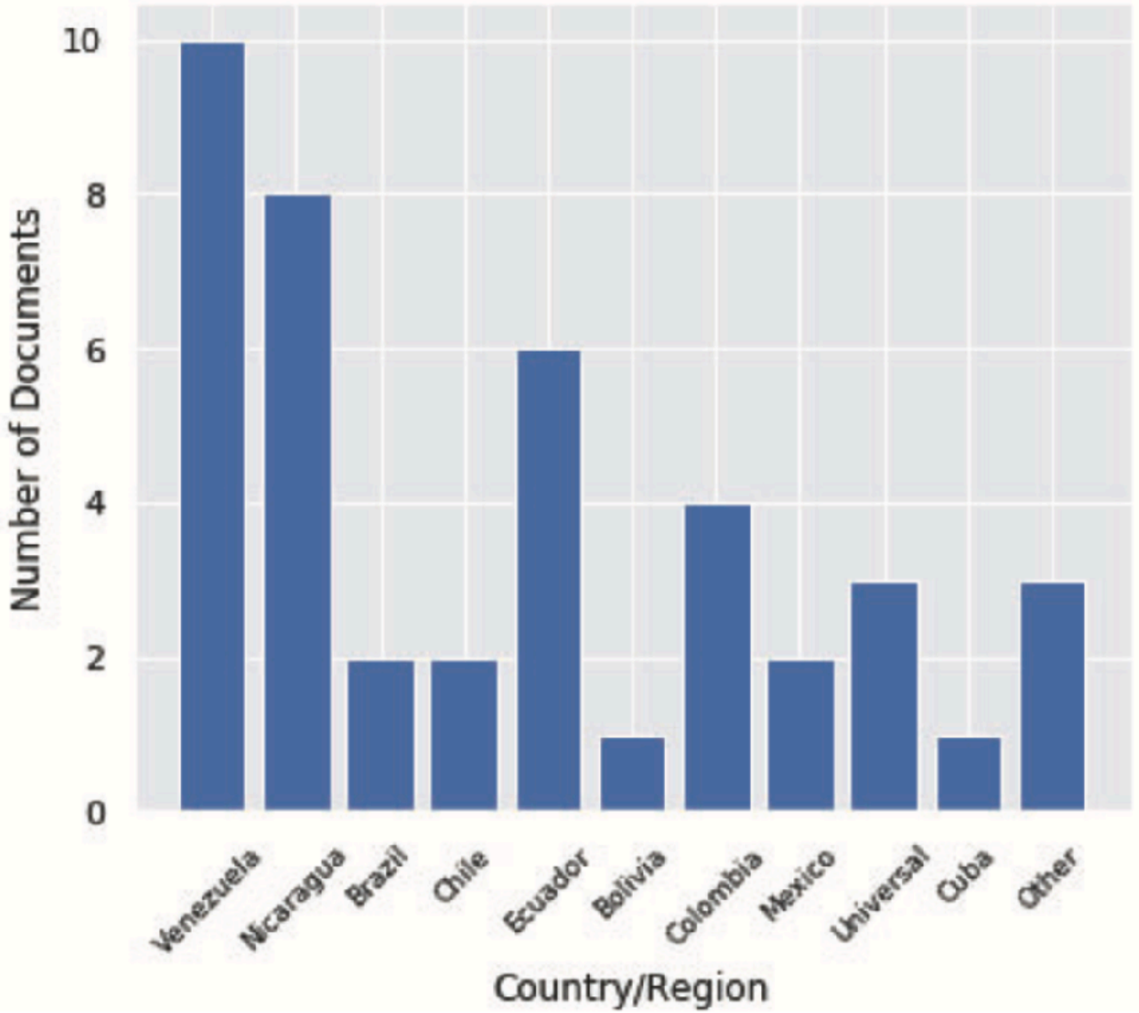
Por Alexandre Gonzaga

Assessoria de Comunicação Social (Ascom)
Ministério da Defesa
61 3312-4071




2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018


Number of Documents
0
2
4
6
8
10
12
14
Politics
Legal
Military
Technical
Human Rights
Sexual
Debt Claim
Topic


Number of Documents
0
2
4
6
8
10
Venezuela
Nicaragua
Brazil
Chile
Ecuador
Bolivia
Colombia
Mexico
Universal
Cuba
Other
Country/Region


Finland
Iceland
Norway
Russia
Canada
Poland
Kazakhstan
Mongolia
Italy
Turkey
Afghanistan
Iraq
Iran
Pakistan
India
Thailand
Indonesia
Algeria
Libya
Egypt
Saudi Arabia
Mali
Niger
Chad
Sudan
Nigeria
Ethiopia
Kenya
DR Congo
Tanzania
Angola
Namibia
Botswana
Madagascar
South Africa
Mexico
Bolivia
Chile
Argentina
North Atlantic Ocean
South Pacific Ocean
South Atlantic Ocean
Indian Ocean
Southern Ocean
Kaspersky Report 2014 Victims' locations
Cylance Report 2017 Victims' locations

Machete Evolution

From December 2010 to January 2019

- **Dec 22, 2010**: first Machete sample, 1 module, no decoy document.
- **Feb 28, 2011**: first Machete with a decoy document.
- **Mar 10, 2011**: Machete incorporates first module.
- **May 17, 2011**: first fully modular Machete (5 modules).
- **Sep 14, 2011**: Machete implements encryption using AES to encrypt user data.

- **March 21, 2013**: first versioning observed (13.0)
- **May 6, 2015**: Machete starts obfuscating the python source code.
- **Jan 24, 2017**: samples with Dropbox used for exfiltration appeared.
- **Apr 30, 2018**: number of modules reduced to 3, added a compression step, and credentials are stored encrypted.

Tracking Mistakes: Shit!

```
    keyids = {8: 'bksp', 9: 'TAB', 13: 'ENTER', 19: 'PAUSE', 20: 'BloqMayus', 27
: 'ESC', 32: 'ESPACIO', 33: 'pgup', 34: 'pgdn', 35: 'END', 36: 'HOME', 37: 'Flec
ha(Izq)', 38: 'Flecha(Arriba)', 39: 'Flecha(Dcha)', 40: 'Flecha(Abajo)', 44: 'Pr
t Scr', 45: 'INSERTAR', 46: 'DEL', 48: '0', 49: '1', 50: '2', 51: '3', 52: '4',
53: '5', 54: '6', 55: '7', 56: '8', 57: '9', 64: '@', 65: 'a', 66: 'b', 67: 'c',
 68: 'd', 69: 'e', 70: 'f', 71: 'g', 72: 'h', 73: 'i', 74: 'j', 75: 'k', 76: 'l'
, 77: 'm', 78: 'n', 79: 'o', 80: 'p', 81: 'q', 82: 'r', 83: 's', 84: 't', 85: 'u
', 86: 'v', 87: 'w', 88: 'x', 89: 'y', 90: 'z', 91: 'Win(Izq)', 92: 'Win(Dcha)',
 93: 'APPS', 96: 'Num(0)', 97: 'Num(1)', 98: 'Num(2)', 99: 'Num(3)', 100: 'Num(4
)', 101: 'Num(5)', 102: 'Num(6)', 103: 'Num(7)', 104: 'Num(8)', 105: 'Num(9)', 1
06: 'Num(*)', 107: 'Num(+)', 109: 'Num(-)', 110: 'Num(.)', 111: 'Num(/)', 112: '
F1', 113: 'F2', 114: 'F3', 115: 'F4', 116: 'F5', 117: 'F6', 118: 'F7', 119: 'F8'
, 120: 'F9', 121: 'F10', 122: 'F11', 123: 'F12', 144: 'BloqNum', 145: 'scrolloc
k', 160: 'Shitf(Izq)', 161: 'Shitf(Dcha)', 162: 'CTRL(Izq)', 163: 'CTRL(Dcha)',
164: 'ALT(Izq)', 165: 'ALT(Dcha)', 186: ';', 187: '=', 188: ',', 189: '-', 190:
'.', 191: '/', 192: '~', 219: '[', 220: '\\', 221: ']', 222: "'"}
```

Conclusions

Machete is Still an Active Threat to Latin America

- Latin America as a region has been under-researched. This needs to be fixed.
- Machete has evolved continuously almost undisturbed.
- The group behind Machete appears to have significant resources to maintain, develop and process the information collected by the espionage tool.
- Our investigation suggests that APT sophistication is directly related to the socioeconomics of the targeted regions

Thank you!

Veronica Valeros, Maria Rigaki, Kamila Babayeva, Sebastian Garcia
{valerver, rigakmar, babaykam, garciseb}@fel.cvut.cz

Stratosphere Research Laboratory, Czech Technical University
www.stratosphereips.org