# Section 2

# Cyber Threats to Businesses

# (Updated)

Stacy M. Arruda
Executive Director
FL-ISAO
Tampa, FL

*Stacy M. Arruda*

# CYBER THREATS

AG ARRUDA Group

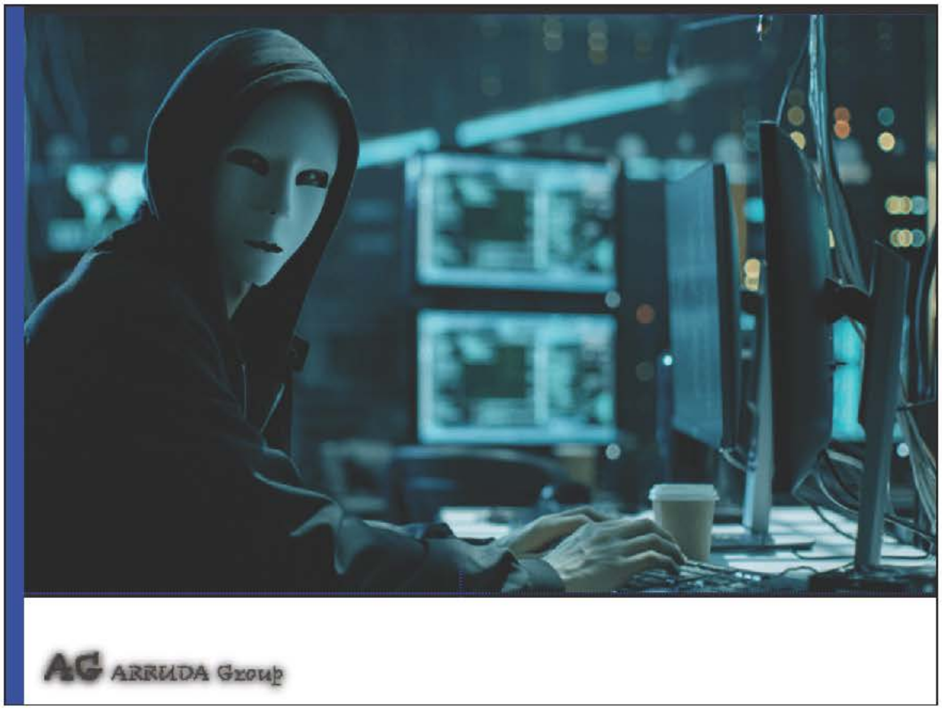
## AGENDA

- Social Media
- Actors
- Motivation
- Threats
- Mitigation

AG ARRUDA Group

SITE
SITEINTELGROUP.COM
GHOST
لااله الا الله
SCA
الله
رسول
محمد
CCA
KNT
UCC
WE ARE

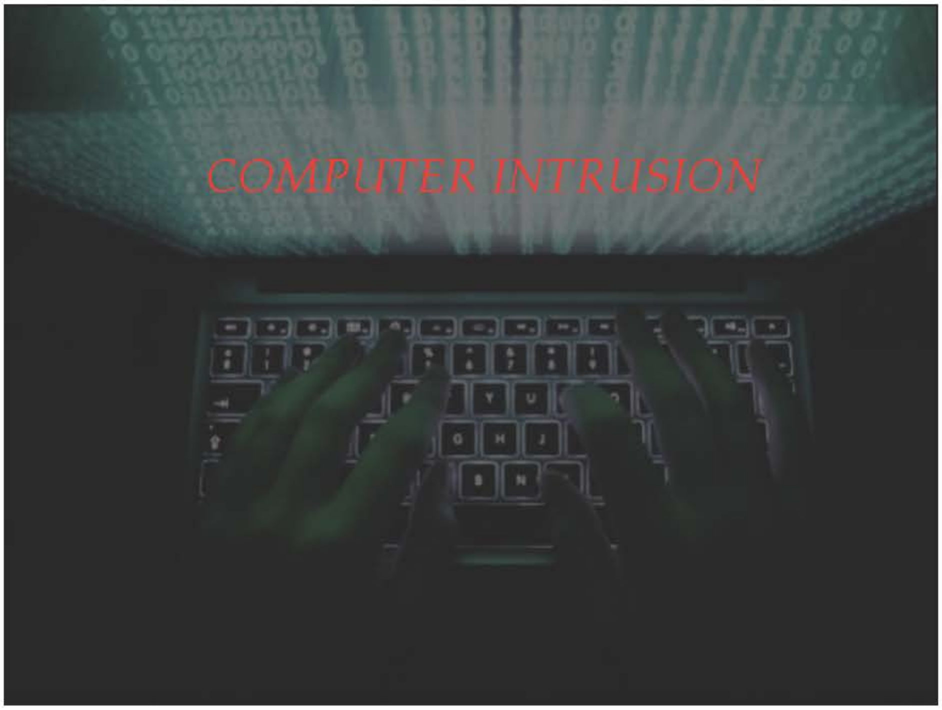
AG ARRUDA Group



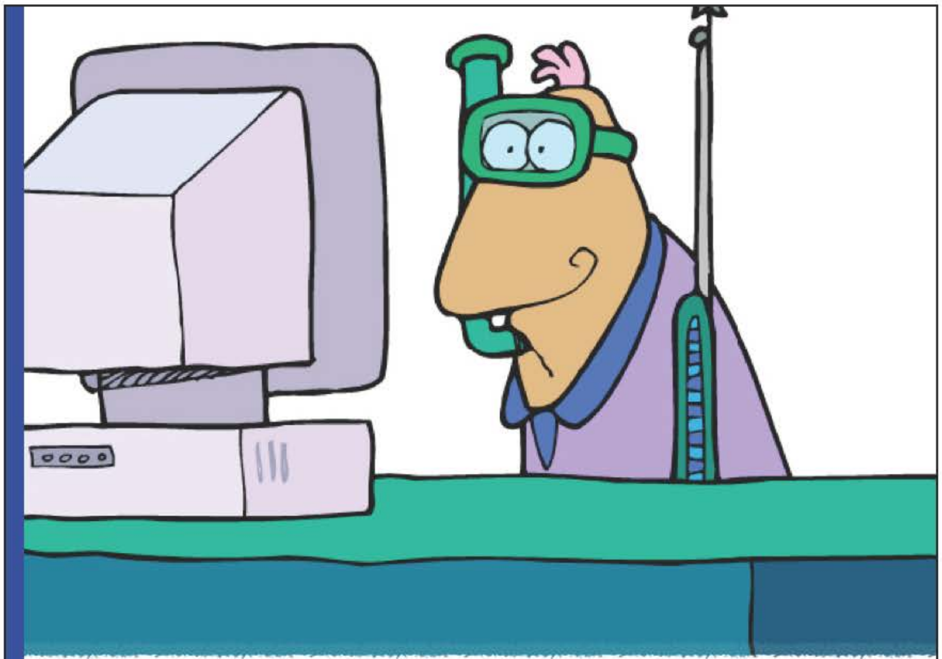
AG ARRUDA Group

# MOTIVATION

AG ARRUDA Group



## COMPUTER INTRUSION

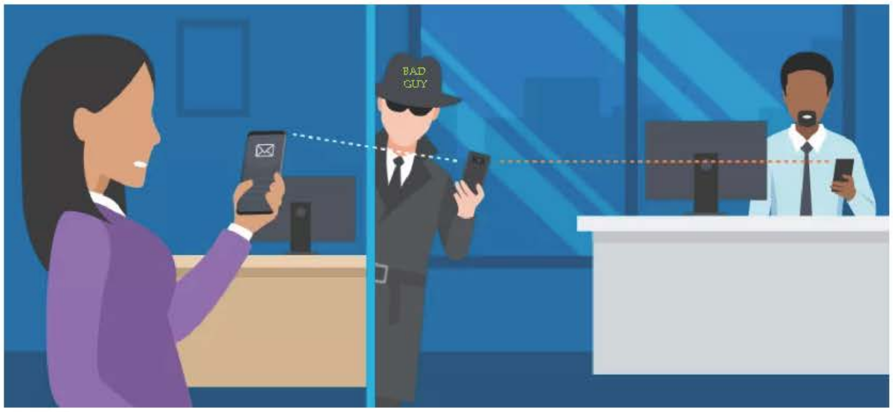


## SPEAR PHISHING

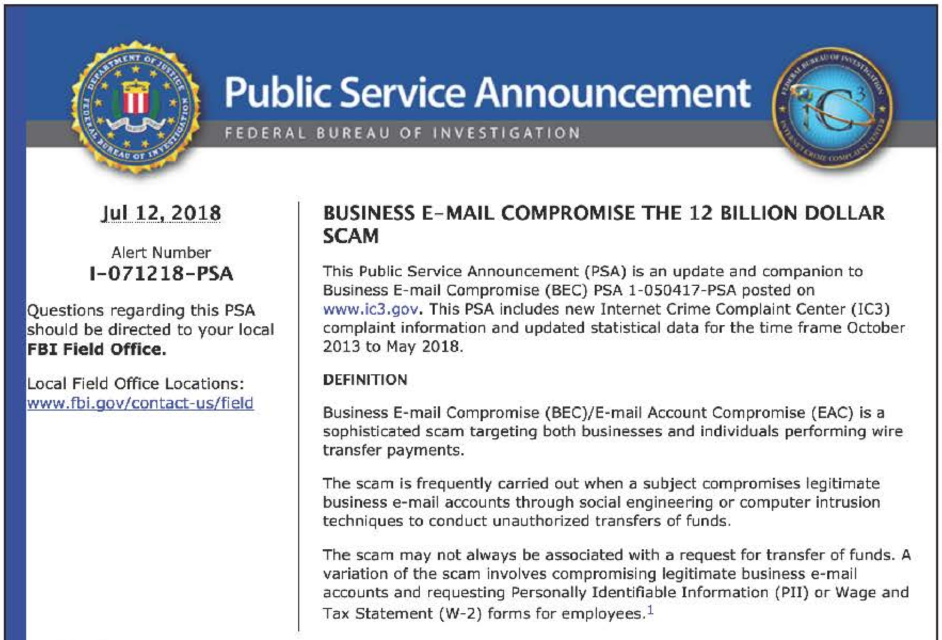
- Reconnaissance
- Craft e-mail
- Technical Subterfuge
- Trusted Source
- Network Breach

# BUSINESS E-MAIL COMPROMISE

*Man in the Middle Attack*



ARRUDA Group



## Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Jul 12, 2018

Alert Number
**I-071218-PSA**

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations:
www.fbi.gov/contact-us/field

**BUSINESS E-MAIL COMPROMISE THE 12 BILLION DOLLAR SCAM**

This Public Service Announcement (PSA) is an update and companion to Business E-mail Compromise (BEC) PSA 1-050417-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data for the time frame October 2013 to May 2018.

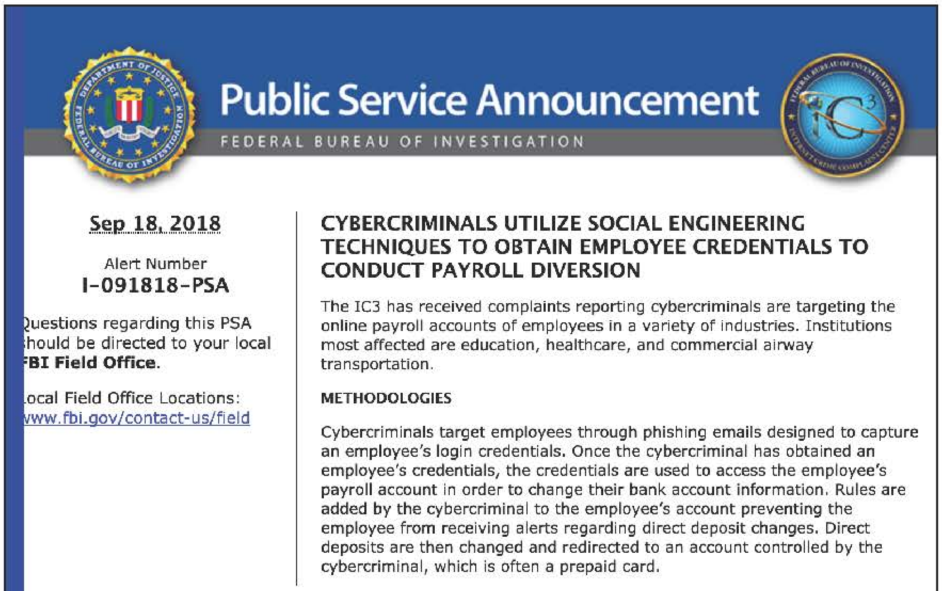
**DEFINITION**

Business E-mail Compromise (BEC)/E-mail Account Compromise (EAC) is a sophisticated scam targeting both businesses and individuals performing wire transfer payments.

The scam is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

The scam may not always be associated with a request for transfer of funds. A variation of the scam involves compromising legitimate business e-mail accounts and requesting Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms for employees.[1]

ARRUDA Group



# Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Sep 18, 2018

Alert Number
I-091818-PSA

Questions regarding this PSA should be directed to your local FBI Field Office.

Local Field Office Locations:
www.fbi.gov/contact-us/field

## CYBERCRIMINALS UTILIZE SOCIAL ENGINEERING TECHNIQUES TO OBTAIN EMPLOYEE CREDENTIALS TO CONDUCT PAYROLL DIVERSION

The IC3 has received complaints reporting cybercriminals are targeting the online payroll accounts of employees in a variety of industries. Institutions most affected are education, healthcare, and commercial airway transportation.

**METHODOLOGIES**

Cybercriminals target employees through phishing emails designed to capture an employee's login credentials. Once the cybercriminal has obtained an employee's credentials, the credentials are used to access the employee's payroll account in order to change their bank account information. Rules are added by the cybercriminal to the employee's account preventing the employee from receiving alerts regarding direct deposit changes. Direct deposits are then changed and redirected to an account controlled by the cybercriminal, which is often a prepaid card.

# RANSOMWARE/RANSOMWORM

# RANSOMWARE

AG ARRUDA Group

# CREDENTIAL STUFFING

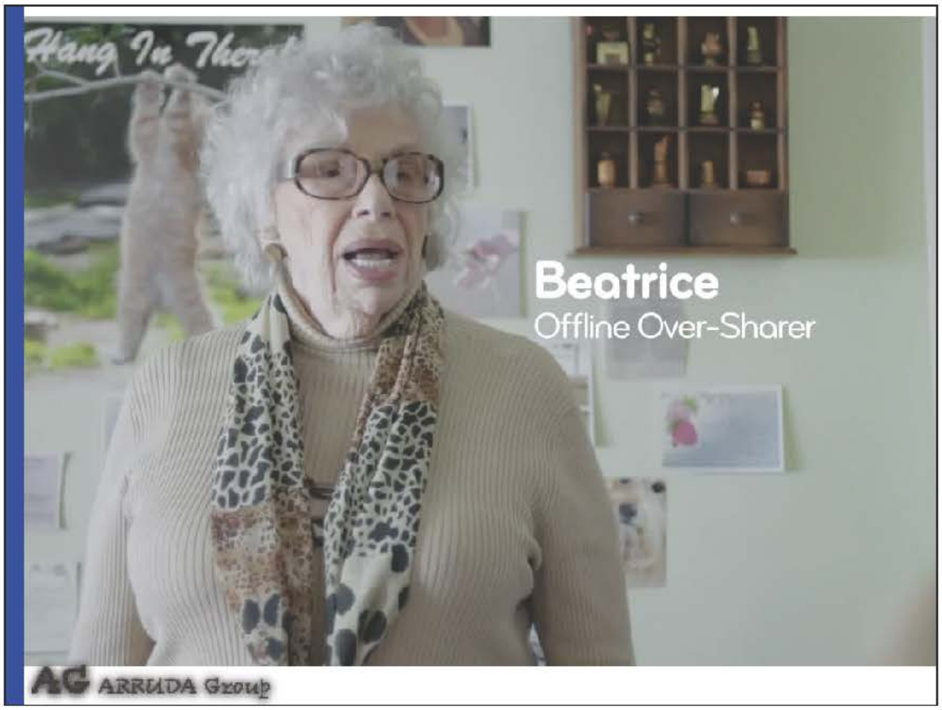
AG ARRUDA Group

# IoT

AG ARRUDA Group

# MITIGATION

AG ARRUDA Group

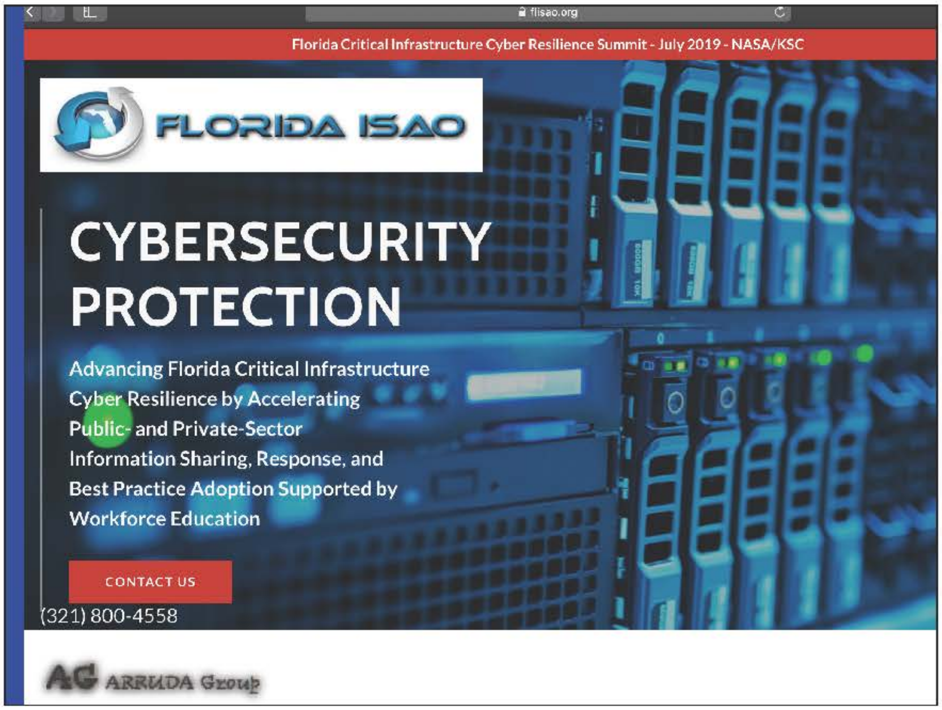


**Beatrice**
Offline Over-Sharer

AG ARRUDA Group

# INFORMATION SHARING

AG ARRUDA Group



Florida Critical Infrastructure Cyber Resilience Summit - July 2019 - NASA/KSC

FLORIDA ISAO

# CYBERSECURITY PROTECTION

Advancing Florida Critical Infrastructure Cyber Resilience by Accelerating Public- and Private-Sector Information Sharing, Response, and Best Practice Adoption Supported by Workforce Education

CONTACT US

(321) 800-4558

AG ARRUDA Group

VISION
Goals
Lead by example
SUCCESS
Vision
Teamwork

FLORIDA ISAO

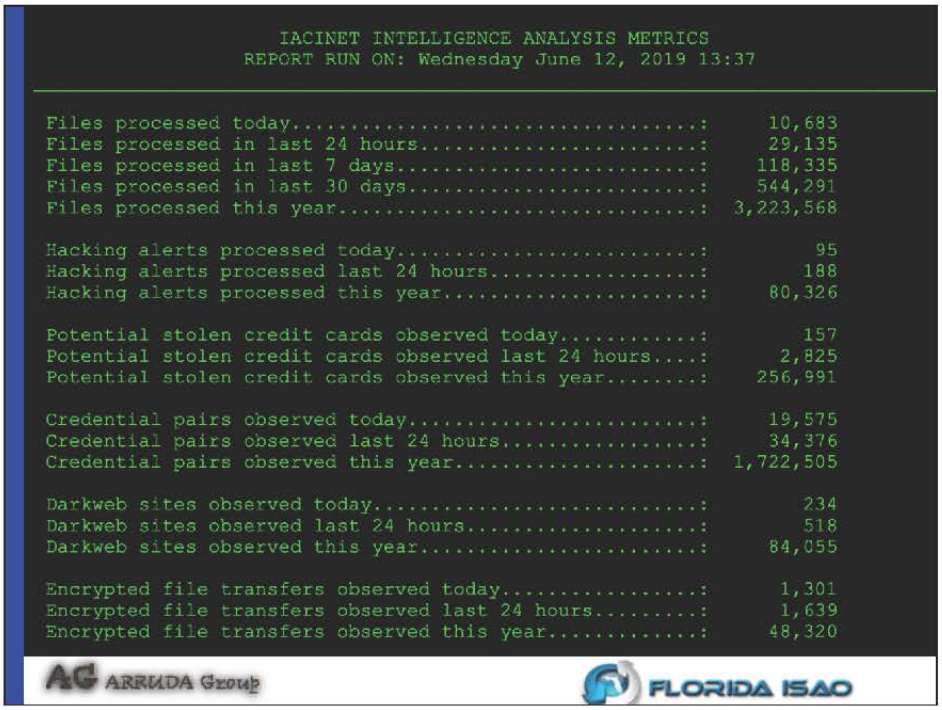
Florida ISAO Vision & Mission

## Vision

The Florida ISAO promotes information sharing through guidance, by assuring awareness of threats and providing support services supporting Florida Government and Industry reduction of cyber risks.

## Mission

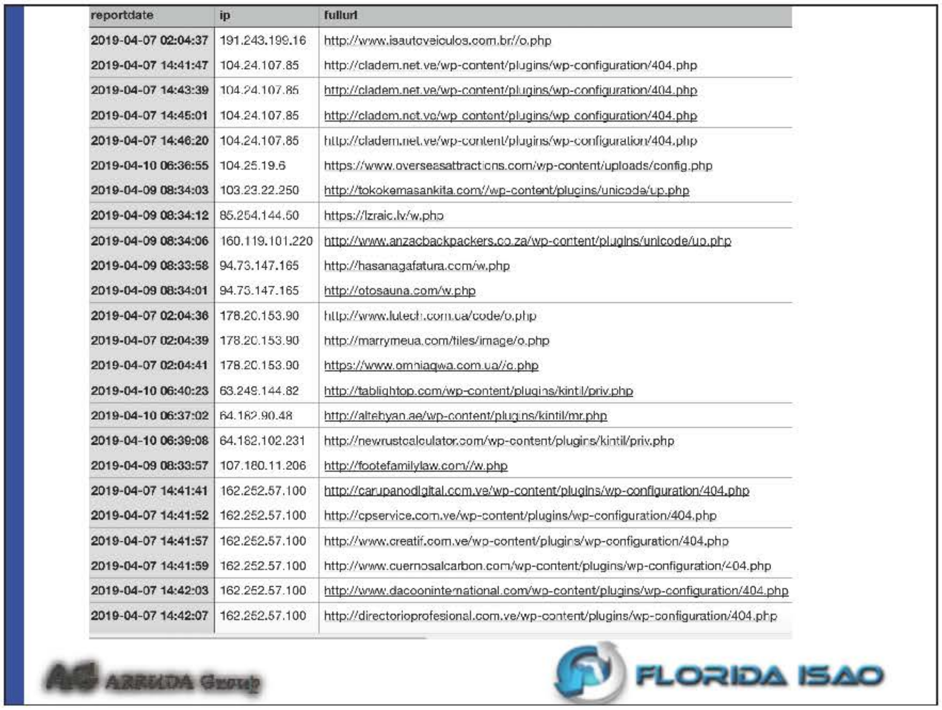
To enable advancing cyber resilience for the State of Florida's critical infrastructure sectors, sub-sectors, and other communities-of-interest via accelerating security situational awareness and defensive measures information sharing and coordinated response, supported by adoption of best practice and education.



```
                    IACINET INTELLIGENCE ANALYSIS METRICS
                 REPORT RUN ON: Wednesday June 12, 2019 13:37

Files processed today...................................:     10,683
Files processed in last 24 hours........................:     29,135
Files processed in last 7 days..........................:    118,335
Files processed in last 30 days.........................:    544,291
Files processed this year...............................:  3,223,568

Hacking alerts processed today..........................:         95
Hacking alerts processed last 24 hours..................:        188
Hacking alerts processed this year......................:     80,326

Potential stolen credit cards observed today............:        157
Potential stolen credit cards observed last 24 hours....:      2,825
Potential stolen credit cards observed this year........:    256,991

Credential pairs observed today.........................:     19,575
Credential pairs observed last 24 hours.................:     34,376
Credential pairs observed this year.....................:  1,722,505

Darkweb sites observed today............................:        234
Darkweb sites observed last 24 hours....................:        518
Darkweb sites observed this year........................:     84,055

Encrypted file transfers observed today.................:      1,301
Encrypted file transfers observed last 24 hours.........:      1,639
Encrypted file transfers observed this year.............:     48,320
```

AG ARRUDA Group

FLORIDA ISAO



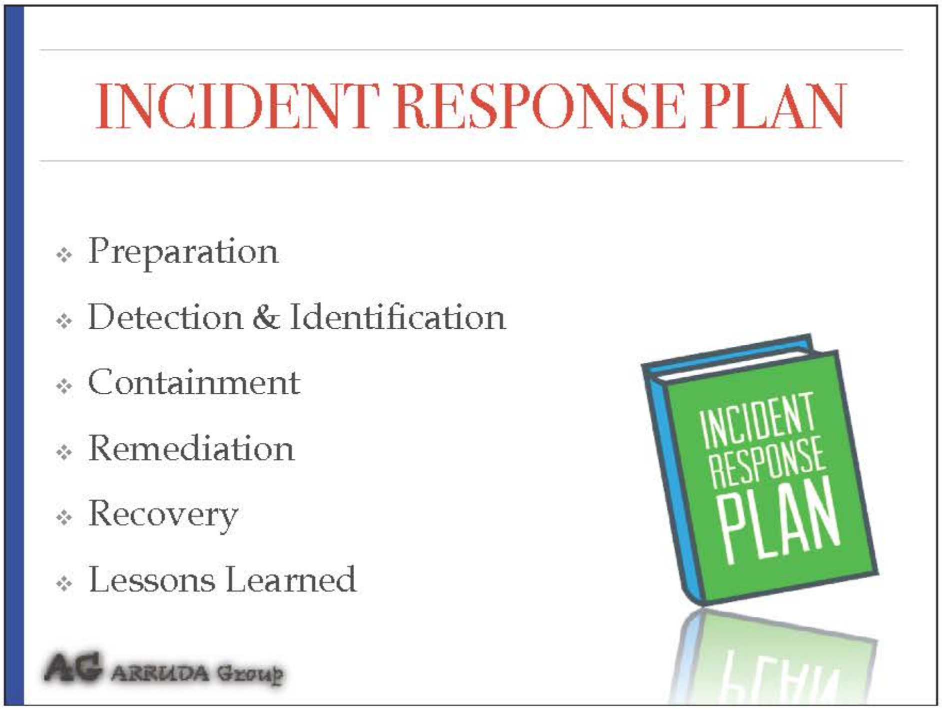
| reportdate | ip | fullurl |
|---|---|---|
| 2019-04-07 02:04:37 | 191.243.199.16 | http://www.isautoveiculos.com.br//o.php |
| 2019-04-07 14:41:47 | 104.24.107.85 | http://cladem.net.ve/wp-content/plugins/wp-configuration/404.php |
| 2019-04-07 14:43:39 | 104.24.107.85 | http://cladem.net.ve/wp-content/plugins/wp-configuration/404.php |
| 2019-04-07 14:45:01 | 104.24.107.85 | http://cladem.net.ve/wp-content/plugins/wp-configuration/404.php |
| 2019-04-07 14:46:20 | 104.24.107.85 | http://cladem.net.ve/wp-content/plugins/wp-configuration/404.php |
| 2019-04-10 06:36:55 | 104.25.19.6 | https://www.overseasattractions.com/wp-content/uploads/config.php |
| 2019-04-09 08:34:03 | 103.23.22.250 | http://tokokemasankita.com//wp-content/plugins/unicode/up.php |
| 2019-04-09 08:34:12 | 85.254.144.50 | https://lzraic.lv/w.php |
| 2019-04-09 08:34:06 | 160.119.101.220 | http://www.anzacbackpackers.co.za/wp-content/plugins/unicode/up.php |
| 2019-04-09 08:33:58 | 94.73.147.165 | http://hasanagafatura.com/w.php |
| 2019-04-09 08:34:01 | 94.73.147.165 | http://otosauna.com/w.php |
| 2019-04-07 02:04:36 | 178.20.153.90 | http://www.lutech.com.ua/code/o.php |
| 2019-04-07 02:04:39 | 178.20.153.90 | http://marrymeua.com/files/image/o.php |
| 2019-04-07 02:04:41 | 178.20.153.90 | https://www.omniaqwa.com.ua//o.php |
| 2019-04-10 06:40:23 | 63.249.144.82 | http://tablightop.com/wp-content/plugins/kintil/priv.php |
| 2019-04-10 06:37:02 | 64.182.90.48 | http://altebyan.ae/wp-content/plugins/kintil/mr.php |
| 2019-04-10 06:39:08 | 64.182.102.231 | http://newrustcalculator.com/wp-content/plugins/kintil/priv.php |
| 2019-04-09 08:33:57 | 107.180.11.206 | http://footefamilylaw.com//w.php |
| 2019-04-07 14:41:41 | 162.252.57.100 | http://carupanodigital.com.ve/wp-content/plugins/wp-configuration/404.php |
| 2019-04-07 14:41:52 | 162.252.57.100 | http://cpservice.com.ve/wp-content/plugins/wp-configuration/404.php |
| 2019-04-07 14:41:57 | 162.252.57.100 | http://www.creatif.com.ve/wp-content/plugins/wp-configuration/404.php |
| 2019-04-07 14:41:59 | 162.252.57.100 | http://www.cuernosalcarbon.com/wp-content/plugins/wp-configuration/404.php |
| 2019-04-07 14:42:03 | 162.252.57.100 | http://www.dacoointernational.com/wp-content/plugins/wp-configuration/404.php |
| 2019-04-07 14:42:07 | 162.252.57.100 | http://directorioprofesional.com.ve/wp-content/plugins/wp-configuration/404.php |

AG ARRUDA Group

FLORIDA ISAO

## MITIGATION

## Our Incident Response Plan goes something like this...

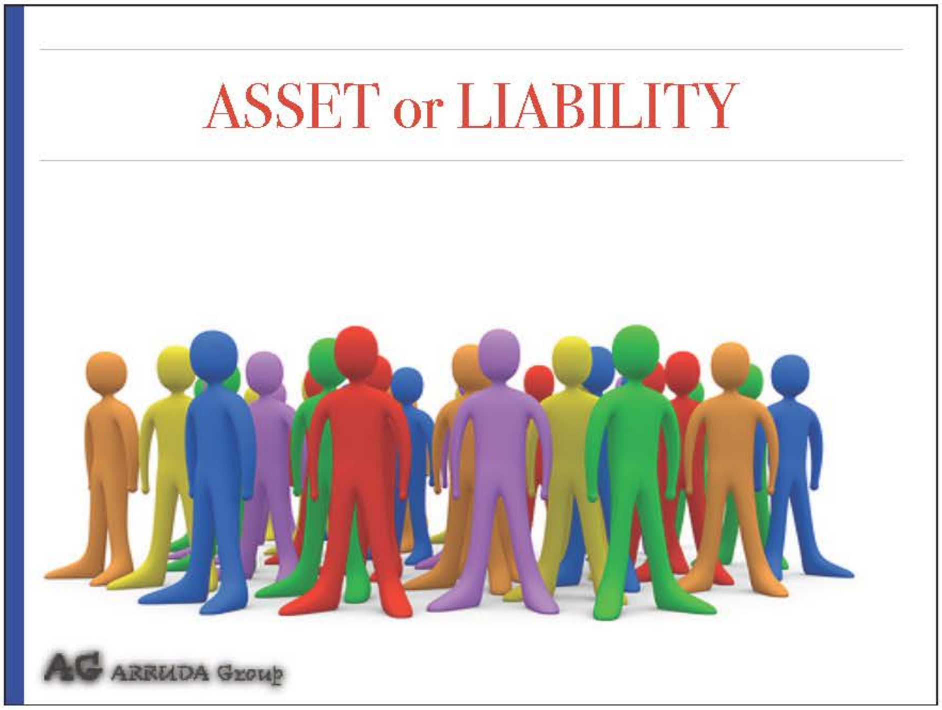


# INCIDENT RESPONSE PLAN

- Preparation
- Detection & Identification
- Containment
- Remediation
- Recovery
- Lessons Learned

INCIDENT
RESPONSE
PLAN

AG ARRUDA Group



# ASSET or LIABILITY

AG ARRUDA Group

# QUESTIONS

AG ARRUDA Group

813.382.0859
sarruda@flisao.org