El timo del CEO y otras historias del cibercrimen

whoami

Alfredo Reino

@areino

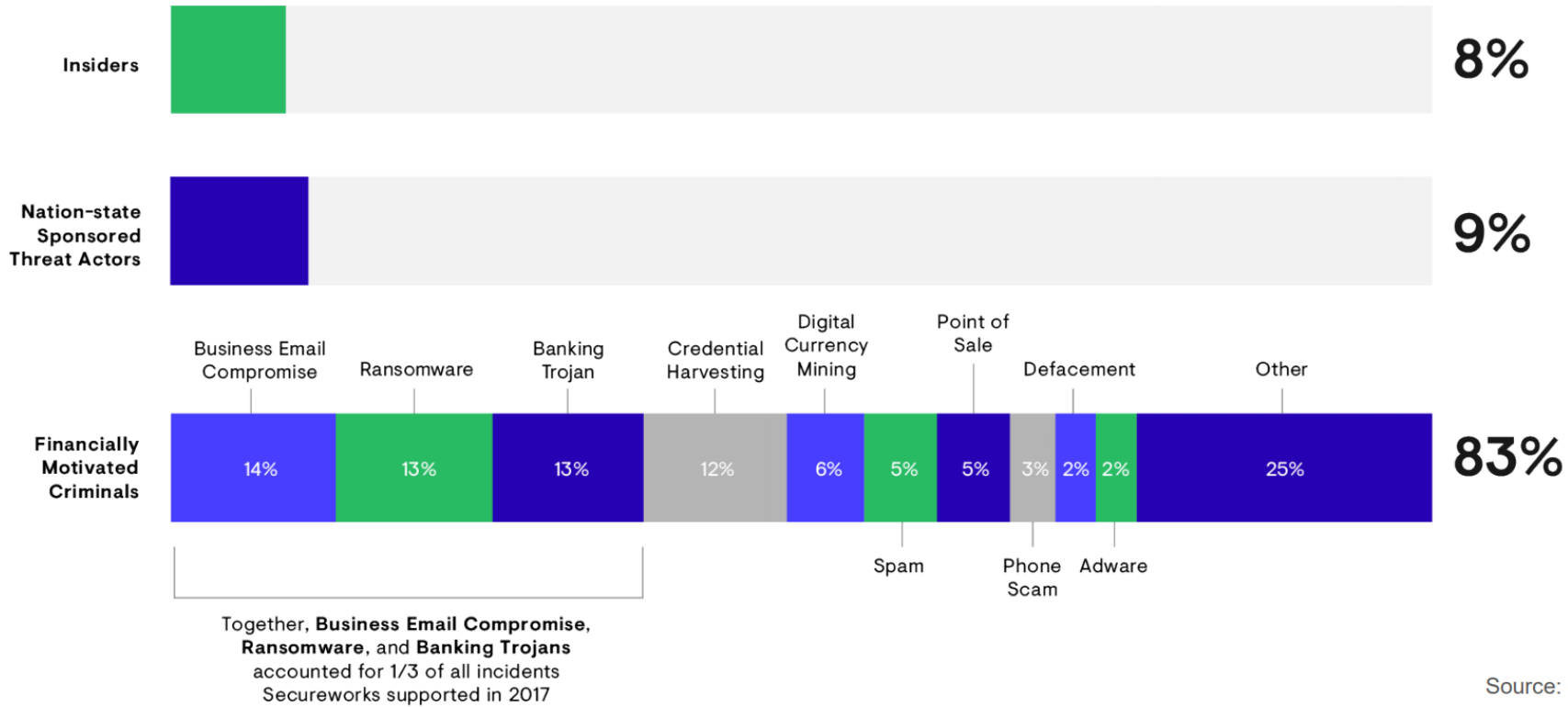
Solutions Principal EMEA en Secureworks

(antes Accenture, Verizon, Symantec, Roche, etc.)

Profesor Adjunto en Master de Ciberseguridad en IE

CISSP, ISSMP, CCSK, CISM, CEH, GCFA, AWS Architect, etc.

Hack0n



Source: Secureworks

SUCESOS ›

La EMT de Valencia sufre una rocambolesca estafa de cuatro millones de euros

Una directiva transfiere la suma a una cuenta externa tras ser víctima presuntamente del fraude del CEO

66

IGNACIO ZAFRA

Valencia - 28 SEP 2019 - 13:42 CEST

DELINCUENCIA INFORMÁTICA

Tres detenidos por estafar 10 millones con el 'fraude al CEO'

Los ladrones suplantaban la identidad de un responsable para pedir transferencias a sus cuentas

El Periódico
Martes, 22/10/2019 - 17:16

0

Hack0n

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

May 04, 2017

Alert Number
I-050417-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
E-MAIL ACCOUNT COMPROMISE
THE 5 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update to Business E-mail Compromise (BEC) PSAs 1-012215-PSA, 1-082715a-PSA and I-061416-PSA, all of which are posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data as of December 31, 2016.

DEFINITION
Business E-mail Compromise (BEC) is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The E-mail Account Compromise (EAC) component of BEC targets individuals that perform wire transfer payments.

The techniques used in the BEC/EAC scam have become increasingly similar,

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.

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

September 10, 2019

Alert Number

I-091019-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 EMAIL COMPROMISE THE $26 BILLION SCAM

This Public Service Announcement is an update and companion piece to Business Email Compromise PSA 1-071218-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to July 2019.

DEFINITION

Business Email Compromise/Email Account Compromise (BEC/EAC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests.

The scam is frequently carried out when a subject compromises legitimate business or personal email accounts through social engineering or computer

Perfecto ,

Estamos en este momento efectuando una operación financiera en relación con una adquisición de empresa.
En esta etapa, esta operación debe permanecer estrictamente confidencial, y te obliga no hablar de esto con nadie de momento en la empresa que sea por teléfono o de viva voz.

El anunció legal de esta adquisición tendrá lugar el 30 de enero de 2017 en nuestras instalaciones y en presencia de toda la administración implicadas.

Vas a ser mi contacto con el fin de finalizar esta transacción, que es tan importante para nuestra empresa.

¿Cuáles son los saldos bancarios?

Cordialmente

Source: https://www.incibe.es/protege-tu-empresa/avisos-seguridad/fraude-del-ceo

01 Attacker scans the seller's email account(s)- for high-value transactions in the preorder phase (i.e., a buyer has asked for a quote.)

02 Attacker sets up a redirect rule in the seller's email to hijack future emails from the buyer.

03 Buyer sends a purchase order (PO) to the seller, and the PO is redirected to the attacker.

04 Attacker "clones" the buyer's email (using a similar but misspelled domain) and forwards the PO to seller, establishing a man-in-the-middle (MITM) compromise.

05 Seller replies to "buyer" (the cloned email address controlled by attacker) with an invoice containing payment instructions.

06 Attacker modifies the bank payment destination in the invoice and forwards the modified invoice to the buyer.

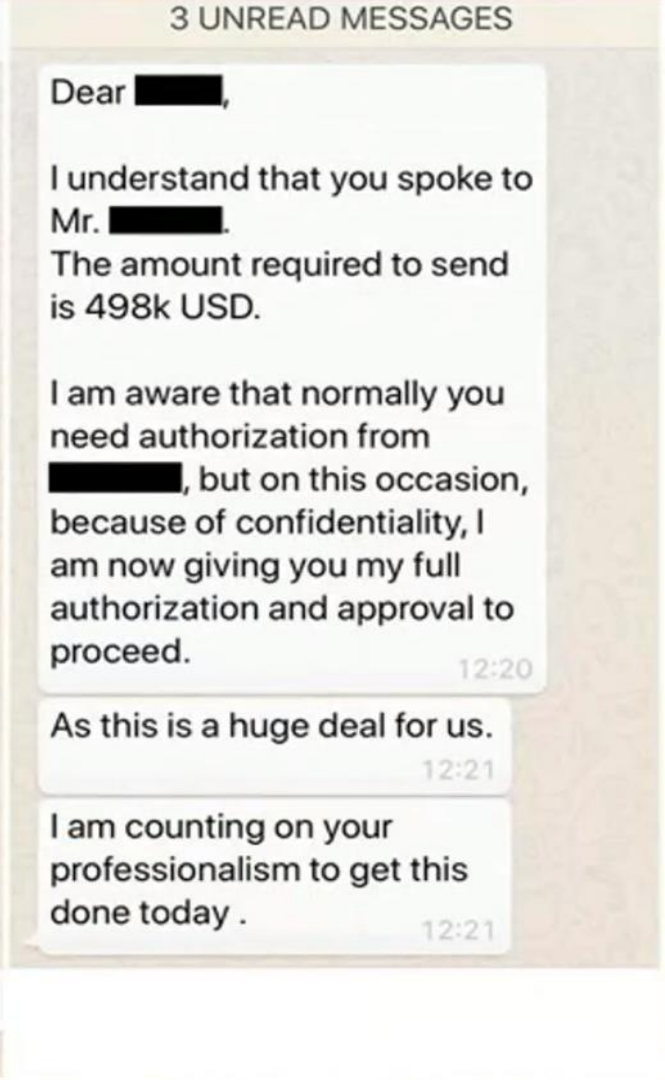
07 Buyer wires money to attacker-controlled bank account.

08 Seller's email is compromised by phishing or malware.


WhatsApp Messenger
Version 2.16.13
© 2010-2016 WhatsApp Inc.
All rights reserved.
LICENSES


3
[redacted]
typing...
Hi [redacted], how are you?
Are you 0available?
We need to discuss a confidential acquisition which I am currently engaged in. I am just going over a few details with my Lawyer first.
Can I call you shortly? 11:18
Hi [redacted] 11:19
For sure I am available 11:19
Ok noted thanks 11:30
I will contact you shortly 11:34
I just hung up with my Lawyer.
According to the NDA, all exchanges regarding this acquisition need to be monitored and filed.
Because of an internal audit, I need you to take care of a


3
[redacted]
typing...
payment on my my behalf from your entity in order to secure the bid.
Can I count on you? 11:49
Of course 11:49
Yes 11:49
Very well [redacted] 11:52
Please contact my lawyer Mr. [redacted] now, and follow his instructions.
He will give you a brief overview. 11:54
[redacted] mobile:
+44 [redacted] 11:55
Ok 11:55
I am calling him r
11:56


3 UNREAD MESSAGES
Dear [redacted],
I understand that you spoke to Mr. [redacted].
The amount required to send is 498k USD.
I am aware that normally you need authorization from [redacted], but on this occasion, because of confidentiality, I am now giving you my full authorization and approval to proceed. 12:20
As this is a huge deal for us. 12:21
I am counting on your professionalism to get this done today . 12:21

Forget email: Scammers use CEO voice 'deepfakes' to con workers into wiring cash

AI-generated audio was used to trick a CEO into wiring $243,000 to a scammer's bank account.

Criminals are using AI-generated audio to impersonate a CEO's voice and con subordinates into transferring funds to a scammer's account.

So-called deepfake voice attacks could be the next frontier in a scam that's cost US businesses almost $2bn over the past two years using fraudulent email.

The Wall Street Journal reports that the CEO of an unnamed UK-based energy company thought he was talking on the phone with his boss, the CEO of the German parent company, who'd asked him to urgently transfer €220,000 ($243,000) to a Hungarian supplier.

SEE: 10 tips for new cybersecurity pros (free PDF)

However, the UK CEO was in fact taking instructions from a scammer who'd used AI-powered voice technology to impersonate the German CEO. It's the voice equivalent of deepfake videos that are causing alarm for their potential to manipulate public opinion and cause social discord.

contacted by an individual using the name [illegible] in or about

10. DRUNZ contacted Company B using the email address Daniel.Drunz@navy-mil.us and identified himself as a U.S. Navy contracting official. Beginning in or about August 2016, DRUNZ provided Company B with documents that DRUNZ represented were a U.S. Navy contract bearing contract number N65236-16-D-0093. This contract called for Company B to sell DRUNZ highly sensitive communications interception equipment listed on the United States Munitions List ("USML") and therefore controlled for export under the International Trafficking in Arms Regulations ("ITAR"). Specifically, according to Company B, many of these commodities are controlled under the USML Category XI. Multiple items that were acquired by this criminal organization via the fraud scheme are so highly restricted that, according to Company B, even a photograph of the item is considered controlled under the ITAR as their existence is not public knowledge.

Source: United States District Court for the District of Maryland

THREAT ANALYSIS

Wire Wire: A West African Cyber Threat

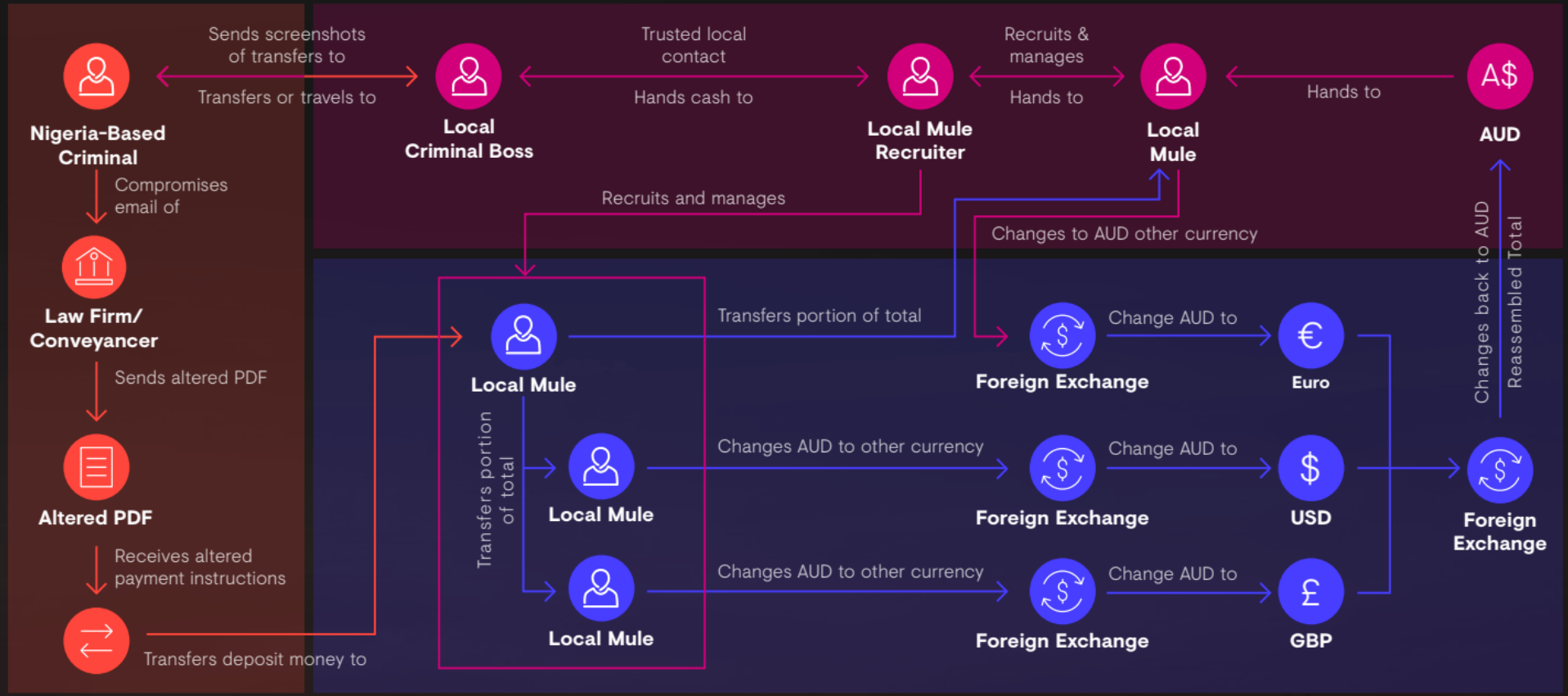
THURSDAY, AUGUST 4, 2016

- **Author:** Joe Stewart and James Bettke, SecureWorks® Counter Threat Unit™ Threat Intelligence

Summary

"Nigerian prince" and "419" scams have plagued victims for decades and transitioned to the Internet in the 1990s. There are many variations and names for these scams, which originated in Nigeria. The scammers refer to their trade using the terms "yahoo yahoo" or "G-work," calling themselves "yahoo-yahoo boys," "yahoo boiz," or "G-boys." However, the simple con man fraud practiced by many West African-based threat actors is being replaced by a new crime they refer to as "wire-wire," "waya-waya," or "the new G-work." These terms have not entered the mainstream lexicon as of this publication and are not well-defined, but SecureWorks® Counter Threat Unit™ (CTU) research indicates that they refer to the evolution of low-level con games into more sophisticated and conventional cybercrime that is compromising businesses around the world. The businesses range in size and span industries from machinery manufacturers to countertop material manufacturers to chemical companies. The cybercriminals use spearphishing and malware to gain direct access to organizations' computers to facilitate the theft of large sums of money without the victim's knowledge.

A Facebook search for "wire-wire" reveals numerous groups and users operating in the open. They advertise their services or offer training courses about wire-wire to would-be criminals. Multiple social media platforms have a wealth of information about individual threat actors, but meticulous research is necessary to understand how these thefts are being accomplished.


Nigeria-Based Criminal
Sends screenshots of transfers to
Transfers or travels to
Local Criminal Boss
Trusted local contact
Hands cash to
Local Mule Recruiter
Recruits & manages
Hands to
Local Mule
Hands to
A$
AUD
Compromises email of
Law Firm/ Conveyancer
Sends altered PDF
Altered PDF
Receives altered payment instructions
Transfers deposit money to
Recruits and manages
Changes to AUD other currency
Changes back to AUD
Reassembled Total
Local Mule
Transfers portion of total
Foreign Exchange
Change AUD to
Euro
Transfers portion of total
Local Mule
Changes AUD to other currency
Foreign Exchange
Change AUD to
USD
Foreign Exchange
Local Mule
Changes AUD to other currency
Foreign Exchange
Change AUD to
GBP

Diverse Roles

Job descriptions for the underground

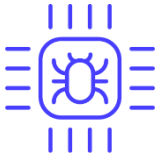
Malware Authors

Inject Writers

Exploit Kit Load Vendor

Network and System

Data Processing Specialists



Network Exploitation Specialists

Service Providers

Recruiters

Money Mules

Hack0n

YOUR COMPUTER AND FILES AE ENCRYPTED

$125 WITHIN 24 HOURS. $199 AFTER 24 HOURS

OPERATING SYSTEM AND FILES DELETED AFTER 72 HOURS

----------WRITE THIS INFORMATION DOWN----------

Email: supportfile@yandex.com

The same information is on your desktop called
Payment_Instructions

Ransom Id: 6754844

BTC Address: 1HxkJ3vz2tvpcHgdt9yyY4XivdY9jKkcZH

IF YOU LOOSE THIS INFO YOU WILL NOT BE ABLE TO CONTACT US

----------WRITE THIS INFORMATION DOWN----------

Your computer files have been crypted and moved to a hidden encrypted partition on your computer.
Without the decryption password you will not get them back.
No matter what you do the files will not re-appear and be decrypted until you pay.

Once payment is received you will get the decryption password and simple instructions to restore all your files and computer to normal instantly. Email us if you need assistance or have paid.

Email: supportfile@yandex.com

DO NOT LOOSE THE CONTACT INFO

Online Banking Malware

Cyber heists can be highly targeted

Banking Trojans

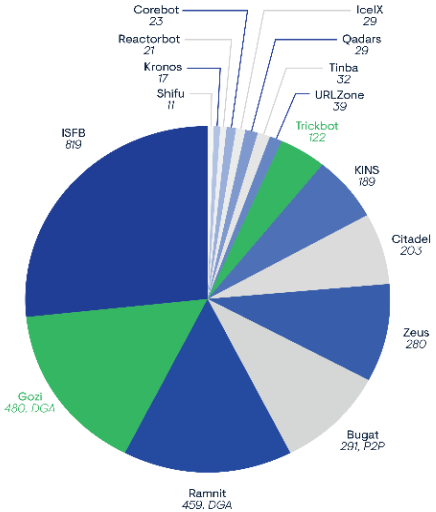
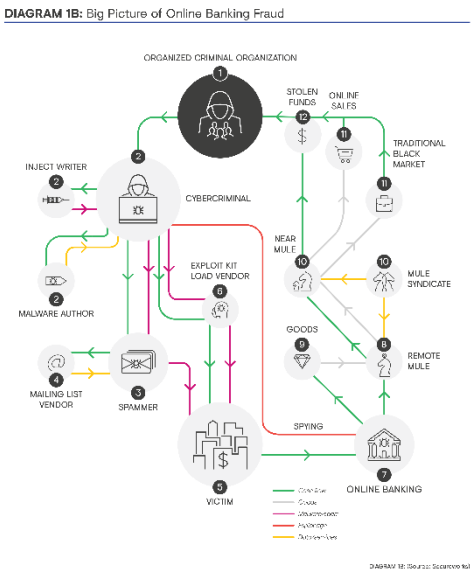


FIGURE 6: *Unique banking trojan configurations extracted April 2016 – April 2017*

Online Banking



ATM Theft

FIGURE 10: *Cobalt gang headline*

FIGURE 11: *ATM malware sales post*

Hack0n

Cybercrime Business Operations

Generating and maximizing revenue

“Yakuza” — Japan

- May 2016
- Blank ATM Cards — stolen card data from a South African bank
- 11 convenience stores
- 3 hours

¥11.4M from ATMs

“Avalanche” network — Ukraine

- November 2016
- Phishing attacks, DDoS attacks, malware distribution and cross-border money movement
- Victims in 180 countries

$100s of millions

Hack0n

Nation-State Cyber Activity and Cybercrime

Blurred lines of cybercriminals

NICKEL GLADSTONE (AKA Lazarus Group) — North Korea

- January 2016
- Compromised Bangladesh central bank

$81M USD

CTU researchers assess with moderate confidence that the **NICKEL GLADSTONE group** poses an ongoing and credible threat to global banking networks.

Observaciones

- **Empresas de todos los tamaños**
  - Pico de incidencia los lunes
- **Objetivo ideal son industrias con pagos grandes ocasionales entre gente que no se conoce**
  - Industrias con cadena de suministro complejas (fabricación, tecnología, etc.)
  - Compraventa de viviendas (el países anglosajones)
- **Métodos**
  - Reconocimiento previo (redes sociales, documentos públicos, etc)
  - Robo de credenciales (phishing, etc.)
  - Sistema de email comprometido (malware/RAT/etc.)
  - Reglas de reenvío de correo
  - Suplantación con dominios engañosos

Recomendaciones (1/4)

- **Autenticación fuerte (2FA/MFA) para webmail**

- **Alerta de correos con dominios recién registrados**
  - Listas DNSRBL como Day Old Bread (DOB)
    http://support-intelligence.com/dob/

- **Deshabilitación de reenvío fuera de la organización**
  - Revisión periódica de reglas de reenvío existentes

Recomendaciones (2/4)

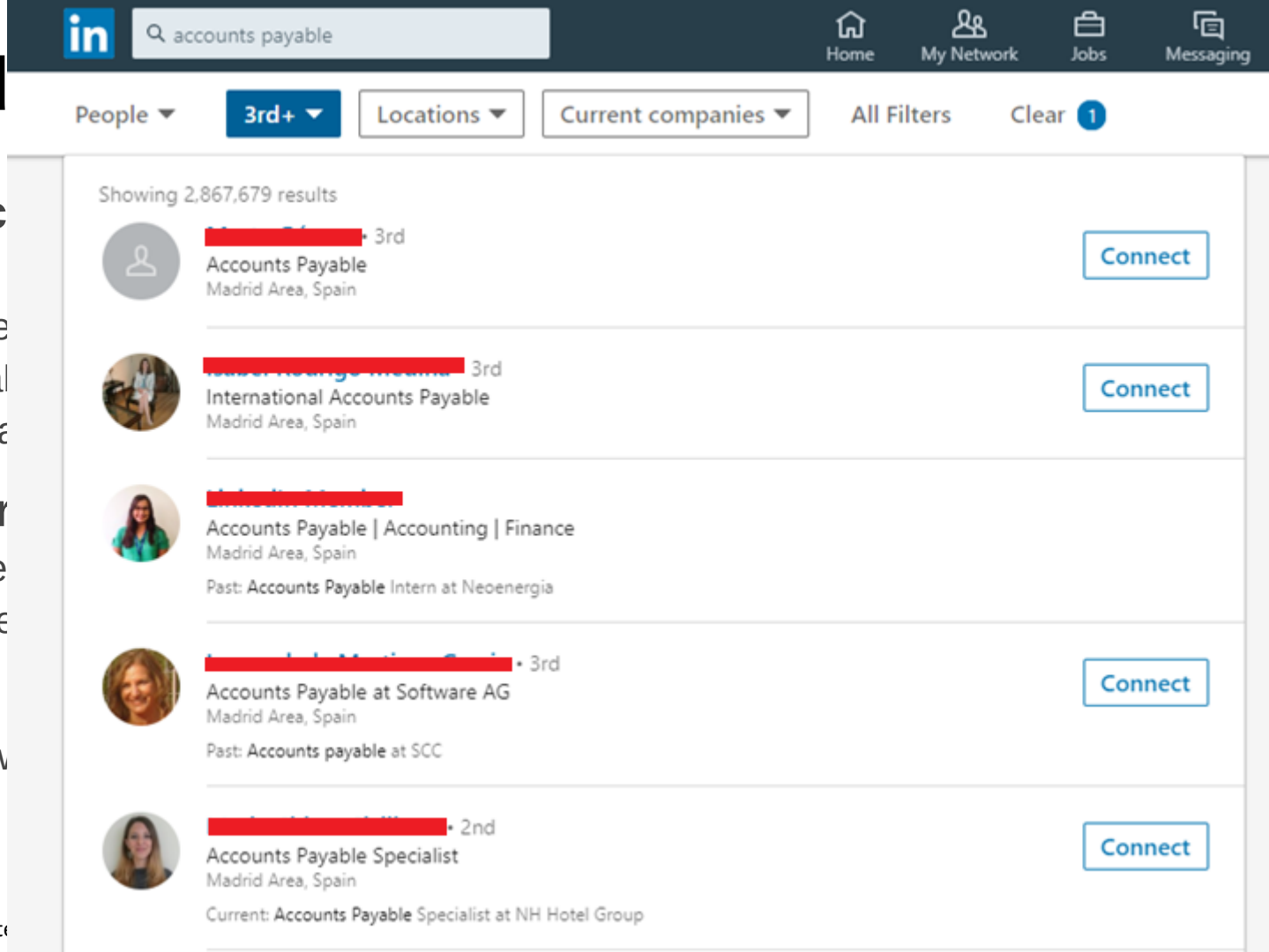
- **Habilitación de “auditing” en los buzones**

```
Get-Mailbox -RecipientTypeDetails UserMailbox, SharedMailbox -ResultSize Unlimited -Filter
{AuditEnabled -eq  $False } | Set-Mailbox -AuditEnabled $True
```

- **Monitorización en SIEM/MSSP de**
  - Intentos de logon fallidos
  - Acceso de acceso a cuentas de correo desde países inusuales
  - Alertas de actividad sospechosa de O365/CAS/etc

Recomend

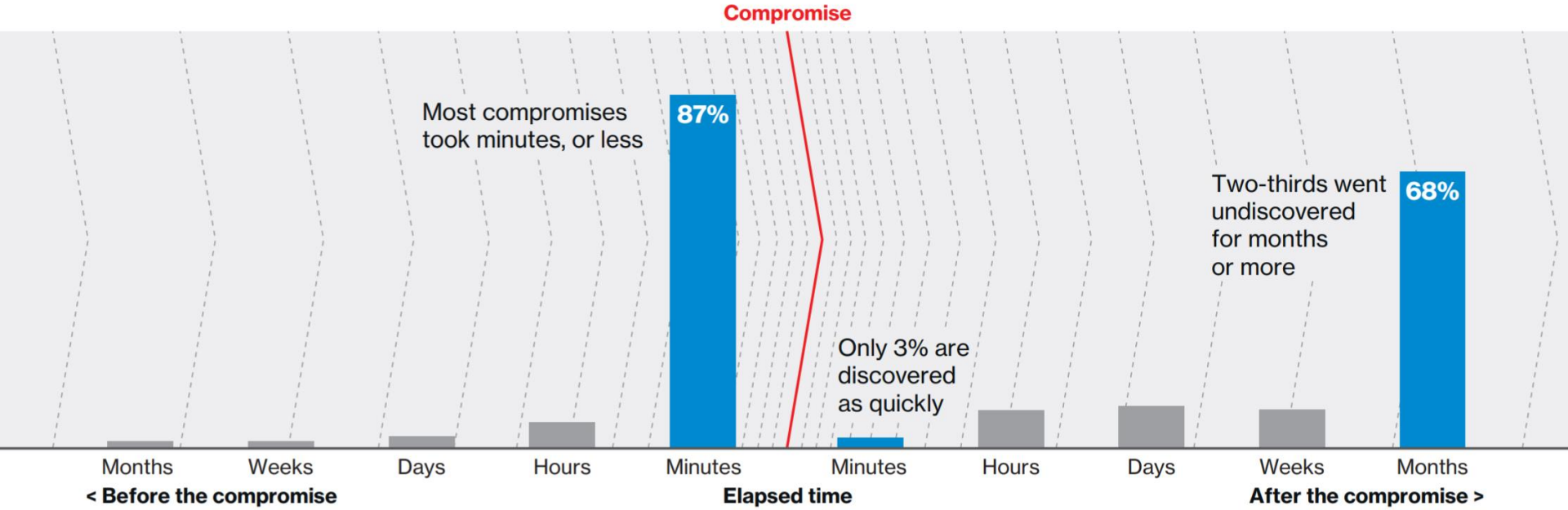
- **Formación y c**
  social
  - Suplantación de
  - Dominios no hal
  - Apelaciones a la
- **Revisión de pr**
  - Comprobacione
  - Aprobaciones re
- **Limitación de**
  - FB, LinkedIn, Tv



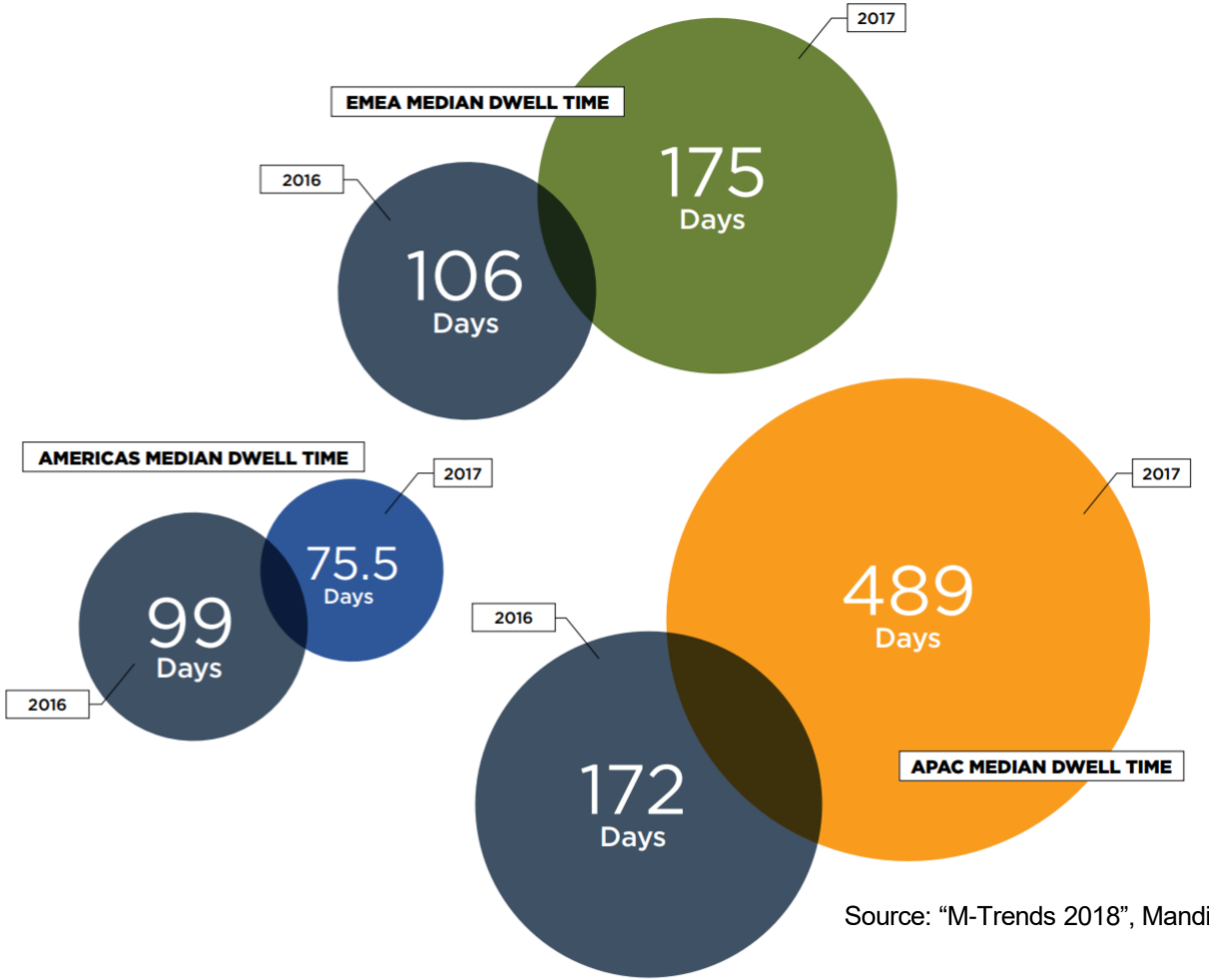
Recomendaciones (4/4)

- **Medidas de seguridad BÁSICAS**
  - AV, seguridad perimetral, actualizaciones de seguridad
  - MONITORIZACIÓN CONTINUA

- **Respuesta a Incidentes**
  - Incluir escenario de BEC en Plan de Respuesta a Incidentes
  - Tener contactos de finanzas, bancos, etc. a mano.
  - Ejercicios sobre el tablero incluyendo gerencia (“Gold Team” Tabletop Exercise/TTX)



Source: “DBIR 2018”, Verizon



Source: “M-Trends 2018”, Mandiant

"My dear, here we must run as fast as we can, just to stay in place. And if you wish to go anywhere you must run twice as fast as that."

— Lewis Carroll, *Alice in Wonderland*