CyberThreat Landscape

v2018

San Diego Society for Information Management (SIM)

May 23, 2018

SIM

AGENDA

FBI update | Our role/responsibility | Why to partner...

- FBI 101 cont.
- CyberThreat landscape
- Incident Response
- IT = Cybersecurity
- Threat Intelligence
- Questions

SIM WHERE IT LEADERS CONNECT

The mission of the FBI is to protect the American people and uphold the constitution of the United States

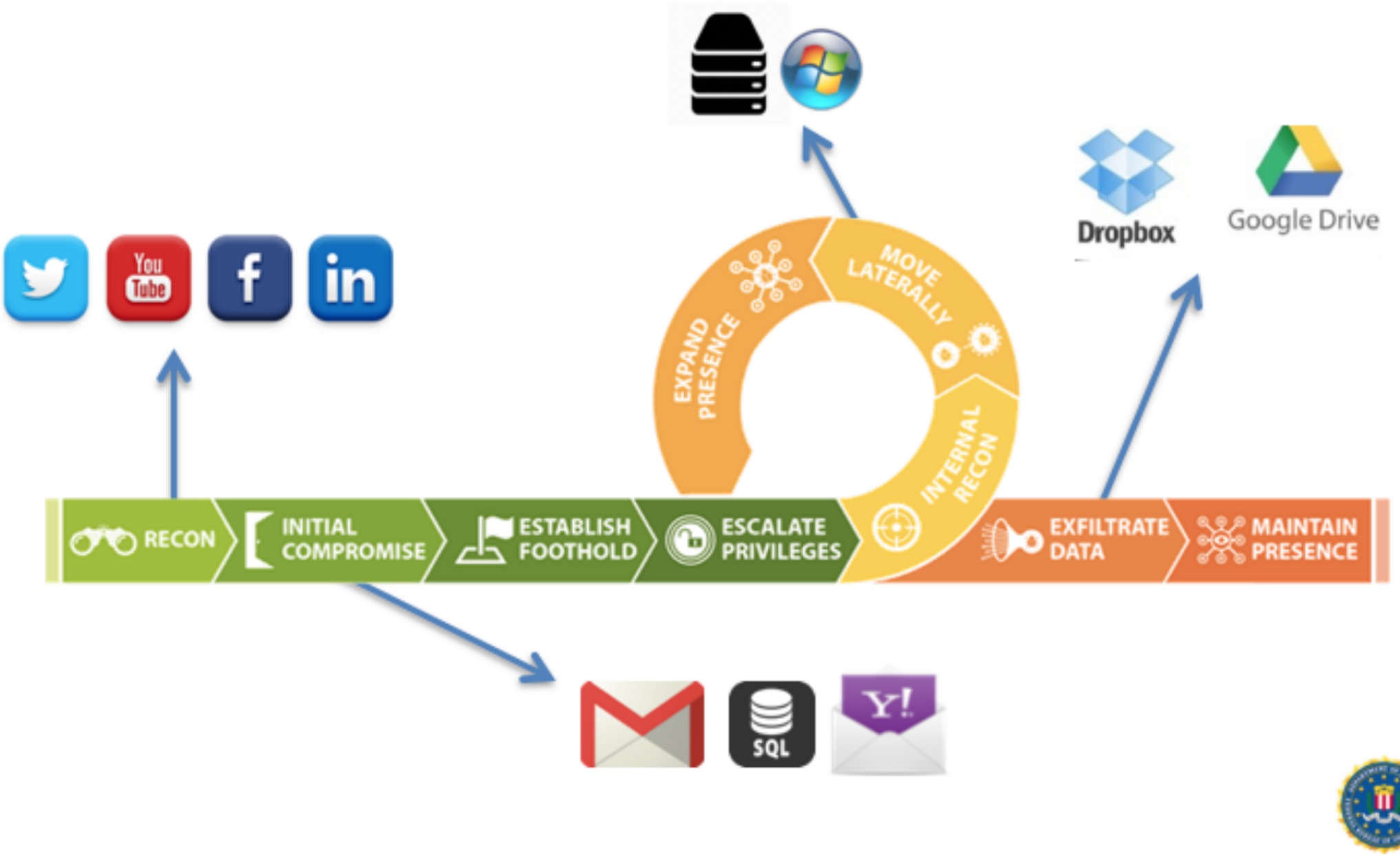
1. Protect nation from terrorism

2. Protect nation from counterintellignce threat

3. Protect nation from cyber-based attack(s)

...


FBI CYBER DIVISION
IDENTIFY • PURSUE • DEFEAT


Dropbox
Google Drive
EXPAND PRESENCE
MOVE LATERALLY
INTERNAL RECON
RECON
INITIAL COMPROMISE
ESTABLISH FOOTHOLD
ESCALATE PRIVILEGES
EXFILTRATE DATA
MAINTAIN PRESENCE
SQL

2016-2020

CHINA´S FIVE-YEAR PLAN

BEFORE THE STORM

- ID your crown jewels
- Ensure IT is part of Cyber Incident Response Plan
- Have 'authorization to monitor' in place
    - employee use agreements, banner'ing
- Educate ALL staff
    - EM, General Counsel, end-users
- Have 'Cyber Incident Response Plan' - dynamic document

OH S#*!T MOMENT

- Assess: ID computer, port, outgoing destination, etc.
- Isolate: affected computers, network segment, etc.
- Collect: images, logs, timeline, etc.
- Notify: internal chain, law enforcement, DHS, downstream victims

FBI RESPONSE

- Contact is made (proactive vs. reactive)
- 'Low-key' SA and CS response (telephonic and/or in-person)
- Meeting with ALL involved (witnesses, IT, security, legal)
- Log collection (firewall, DNS, event, RDP, web access, etc.)
- Victim server image if possible
- Constant communication

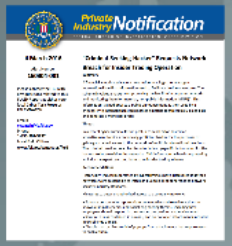
// There is NO CybersecurITy w/out IT .

WHERE
IT
LEADERS
CONNECT

CISO Academy

COLLABORATION / PARTNERSHIPS

// we have too much intel to NOT share...



// 'We must share until it's uncomfortable' - SAC Brown

THREAT INTELLIGENCE

TLP: GREEN

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

26 February 2016

Alert Number

M-000069-BT

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information please contact **FBI CYWATCH immediately.**

Email:

cywatch@ic.fbi.gov

Phone:

1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This FLASH has been released **TLP: GREEN**: The information in this product is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share this information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

Summary

The FBI is providing the following information with HIGH confidence:

This document is an update to Flash alert M-000054-BT, dated April 3, 2015, Flash alert M-000058-BT, dated April 30, 2015 and M-000066-BT, dated November 3, 2015. Since September 2012, approximately 50 U.S. financial institutions have been targeted in over 350 separate DDoS attacks with varying effects. The botnets used in the attacks, identified as "Brobot" and "Kamikaze/Toxin" consist of compromised high bandwidth webservers with vulnerable content management systems (CMS). The compromised bots are infected through a vulnerable CMS account. Once the account is accessed, attack scripts are uploaded to a hidden directory on the associated web site.

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

4 March 2016

Alert Number
160304-001

Please contact the FBI with any questions related to this FLASH Report at either your local **Cyber Task Force** or **FBI CYWATCH**.

Email:
cywatch@ic.fbi.gov
Phone:
1-855-292-3937
Local Field Offices:
www.fbi.gov/contact-us/field

"Criminal-Seeking-Hacker" Requests Network Breach for Insider Trading Operation

Summary

A financially motivated cyber crime insider trading scheme targets international law firm information used to facilitate business ventures. The scheme involves a hacker compromising the law firm's computer networks and monitoring them for material, non-public information (MNPI)[1]. This information, gained prior to a public announcement, is then used by a criminal with international stock market expertise to strategically place bids and generate a monetary profit.

Threat

In a recent cyber criminal forum post, a criminal actor posted an advertisement to hire a technically proficient hacker for the purposes of gaining sustained access to the networks of multiple international law firms. The criminal provided search criteria for industry-specific information for the hackers to locate within the networks. This information when interpreted by an industry expert can contribute to an insider trading scheme.

Recommendations

Historically, industries targeted by cybercriminals have discovered that their networks were susceptible to intrusion due to lack of adherence to network security industry standards.

Measures to deter unauthorized access to a company network:

- Educate personnel on appropriate preventative and reactive actions to known criminal schemes and social engineering threats, including how employees should respond in their respective position and environment.
- Scrutinize links contained in e-mails, and do not open attachments included in unsolicited e-mails.
- Disable macros. Be careful of pop-ups from attachments that require users to enable them.

InfraGard

Partnership for Protection

Welcome John Caruthers Logout

HOME | PUBLICATIONS | COLLABORATION | RESOURCES | SETTINGS

WELCOME TO INFRAGARD

DOWNLOAD MEMBERSHIP CARD

INBOX (139 NEW)

NEWS

GENERAL INFORMATION

MY CALENDAR

FORUMS

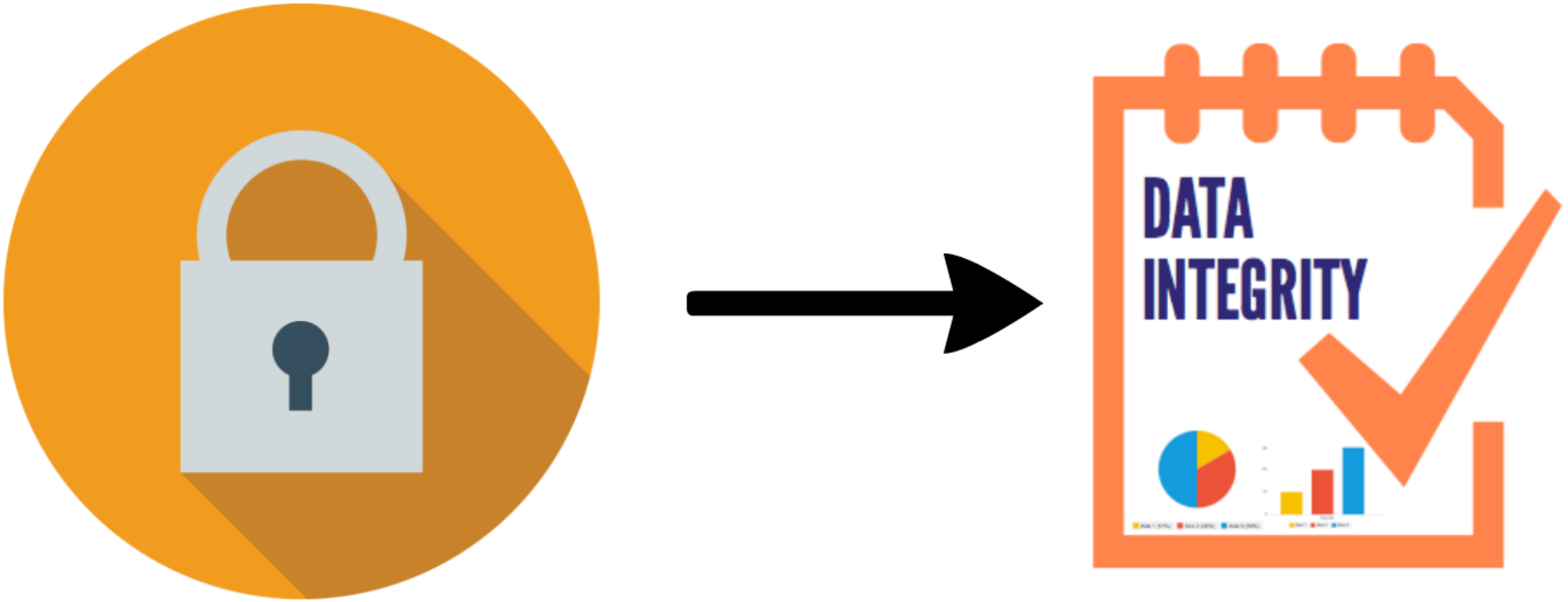
MEMBER SEARCH

MY CHAPTER

MALWARE INVESTIGATOR

GUARDIAN

VIDEOS


DATA
INTEGRITY

CyberDIVISION

FEDERAL BUREAU OF INVESTIGATION

SSA John Caruthers | FBI San Diego | jcaruthers@fbi.gov