

# The Importance of Cyber Threat Intelligence for CERTs

Almerindo Graziano

*SIR, IT'S TOO MUCH!  
WE NEED TO ORGANIZE ALL  
THIS INTELLIGENCE AND MAKE  
SENSE OUT OF IT!*

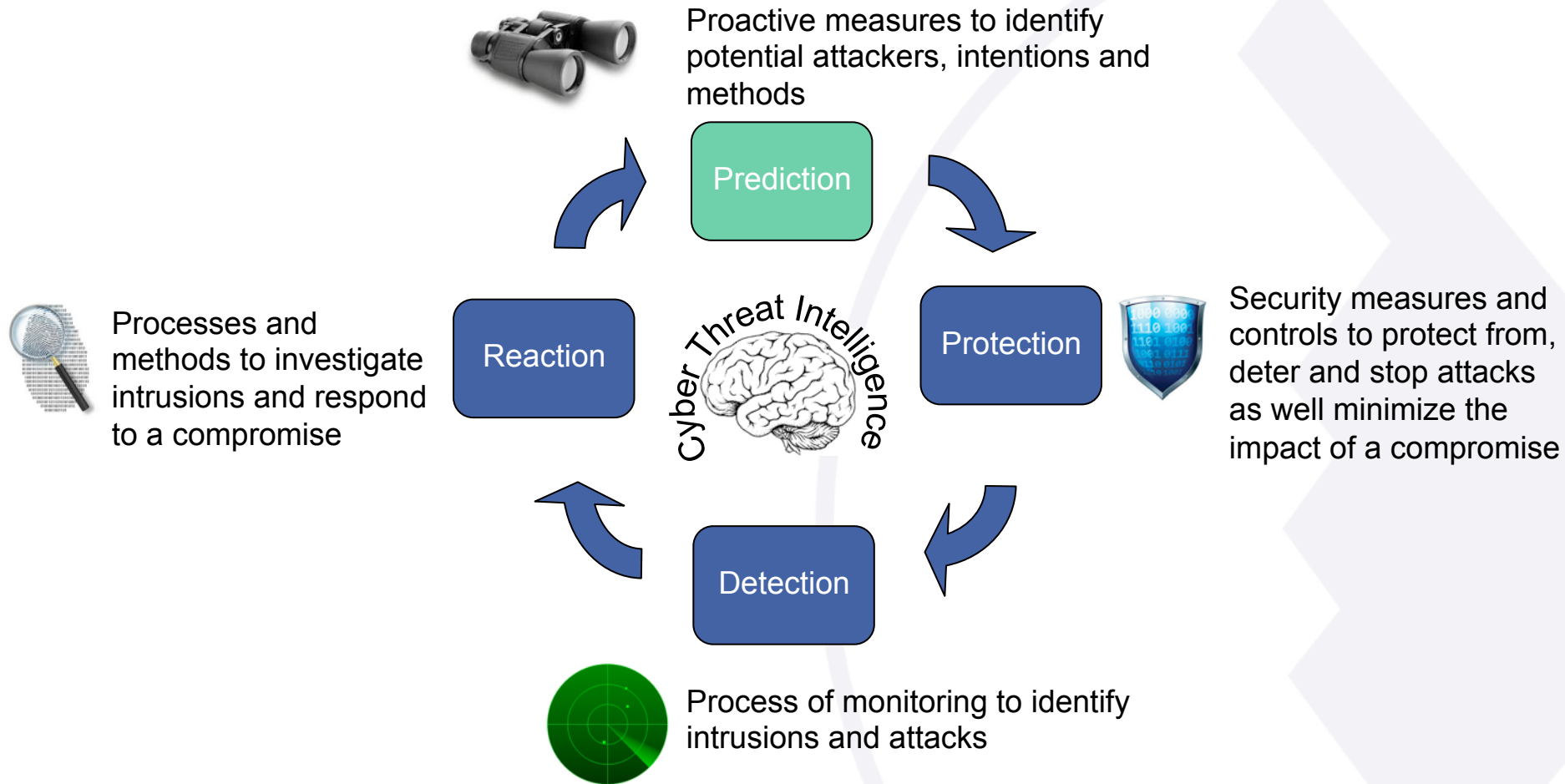


# About Silensec

- Information Security Management Consultancy Company (ISO27001 Certified)
  - IT Governance, Security Audits
  - Security System Integration (SIEM, LM, WAFs)
  - Managed Security Services
- Offices: England, Cyprus, Kenya,  
- Cyber Threat Intelligence
  - Monitoring, Threat Assessment, Investigations
- Independent Security Training Provider
  - ISO27001, Business Continuity, PCI DSS, CISSP, Ethical hacking, Computer Forensics, Mobile Forensics, Reverse Engineering, Intrusion Detection, Log Management



# Defense in Depth



# The Kill Chain

- Systematic process of finding and engaging an adversary to create the desired effects (US Army, 2007)
  - Adapted by Hutchins et al. in 2011
- Key observations
  - Going from the Recon phase to the final Action phase is NOT immediate
  - The time taken for the kill chain process to execute can be used to gather intelligence and capabilities to interfere with each step of the kill chain.



# What is Threat Intelligence

- *“Details of the motivations, intent, and capabilities of internal and external threat actors. Threat intelligence includes specifics on the tactics, techniques, and procedures of these adversaries. Threat intelligence's primary purpose is to inform business decisions regarding the risks and implications associated with threats” (Forrester)*

# The Big Picture

- Threat Actors
  - Different types, motivations, targets
- Goals and Strategy
  - Define what the attackers want and how the plan to achieve it
- Tactics Techniques and Procedures
  - Define what the attackers will do to implement their strategy and achieve their goals
- Indicators
  - Define the evidence left behind by the attackers



Threat Actor

Goals

Strategy

Tactics

Techniques

Procedures

Indicators

# Threat Actors

- The first step towards developing threat intelligence capability is the understanding of different threat actors
  - Different Threat Actors (e.g. government, organized crime, activists etc.)
  - Associate risk level depends on the context
- Important to distinguish between:
  - Threat Actors carrying out the attack
  - Threat Actors “commissioning” the attack

# Sample Threat Actors

Threat Actor	Description and Motivation	Potential Targets	Goal
Cyber Criminal	Varying degree of competence. Usually motivated by the achievement of financial gain or the affirmation of private justice	Potentially any target for personal reasons or as “for-hire guns” by a third party threat actor	Financial gain, private justice
Organized Crime	Structured, funded, consisting of different roles with associated competences and responsibilities. Usually motivated by the achievement of financial gain. Can be hired by other threat actors (e.g. industrial espionage, internal threats etc.)	Commercial organization but potentially any target as “for-hire guns” by a third party threat actor	Financial gain
Hactivists	Typically decentralized groups or individuals with varying degree of technical skills. Highly motivated by their ethics and principles and the advancement of a cause	Targets are specific to the sectors of interest to the activist group (environmentalist, animal lovers etc.)	To cause reputational damage or advance specific causes through information gathering
State-sponsored criminals	Technically skilled with virtually unlimited resources at their disposal, motivated by the country political agenda	Foreign government institutions and officials, large foreign commercial organizations	Acquire information, monitor and control
Competitors/ Industrial Espionage	Good level of resources and varying degree of competences, usually motivated by the achievement of business objectives	Targets varies according to the relevance to the threat actor	Acquire information, disrupt business (image, reputation and operations)
Employees/Internal Threat	Quite varied in age, technical competence and intent but all in possession of sensitive information that has a critical impact to the organization. Can be used by other threat actors. Motivated by malcontent, spirit of revenge or financial gain	Typically commercial organizations but potentially applicable to any type of organization	Personal gain or revenge
Opportunists	Unaffiliated hackers (usually young) looking for recognition by the hackers community and for new learning opportunities. Rarely financially motivated	Various targets both from the private and public sectors. Target sensitivity varies with the capability of the threat actor.	Achieve recognition, improve competence



# Observables and Indicators

- Observable
  - Any piece of information related to the operations of computers and networks
- Indicator
  - Any piece of information (observable) that, enriched with contextual information, allows to represent artifacts and/or behaviors of interest within a cyber security context such as attacks, intrusions etc.
- Context turns an observable into an indicator
  - An IP address used in attack
  - The hash of an executable found on a system

## Samples

- Typical indicators address by cyber threat intelligence include
  - Domain name, IP address, hash (MD5, SHA1, SHA256), email address, SSL hash (SHA1), malware name (e.g. Trojan.Enfal), filename (e.g. .scr, resume.doc), URI string (e.g. main.php), User-Agent string (e.g. Python-urllib), a registry key string
- Support fo indicators varies across CTI solutions

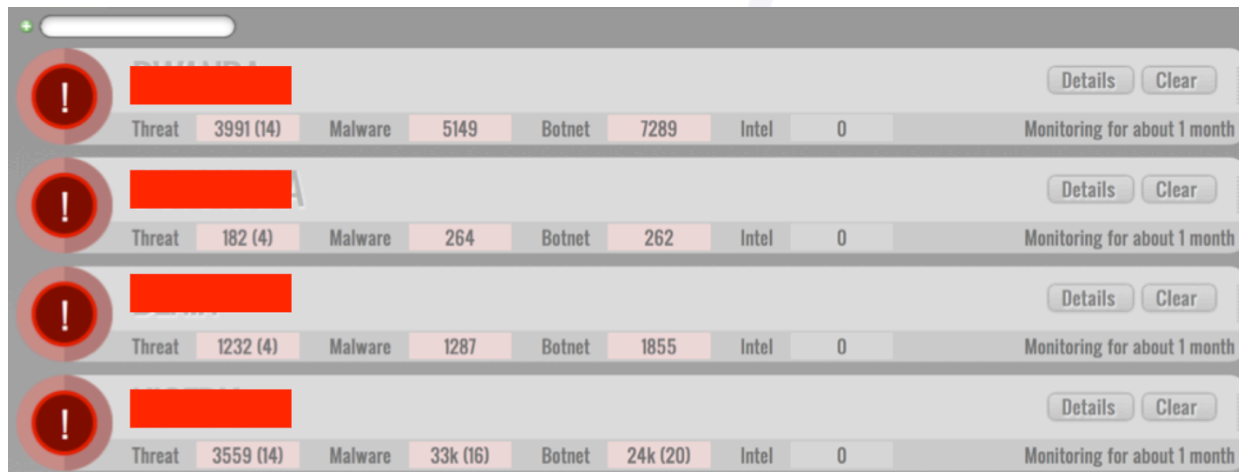
# About Cyber Threat Intelligence

- CTI is about managing risk exposure
  - Likelihood of a threat manifesting itself
  - Impact of attacks
- Three main use cases
  - Monitoring
    - Monitoring the risks from the threats we know about
  - Threat Assessments
    - Assessing risks from new threats
  - Investigations
    - Learning about current and future threats

# CTI Monitoring

## Network Threats

- Ability to monitor the risks exposure of an entire country and/or specific organizations
  - Examples: infected systems, malware and botnets



## Monitoring and Take Down of Phishing Sites

**Alerts (24,424)**

**Heads-Up - [ALERT] New Evil Android Phishing Trojans Empty Your Bank Account**  
Infragard warned that the FBI has identified two Android malware families, SlemBunk and Marcher, actively phishing for specified US financial institutions' customer credentials. The malware monitors the infected phone for the launch of a targeted mobile banking application to inject a phishing overlay over the legitimate application's user interface. The malware then displays an indistinguishable fake login interface to steal ...  
May 20, 2016, 9:48 p.m.

**Phishing Alert - [Redacted] Bank, http://www.[Redacted].com - Fake Site**  
[Redacted]  
May 20, 2016, 9:25 p.m.

**Phishing Alert - [Redacted] Bank, http://www.[Redacted].com - Fake Site**  
[Redacted]  
May 20, 2016, 8:12 p.m.

**Phishing Alert - [Redacted] bank, http://www.[Redacted].pw - Fake Site**  
[Redacted]  
May 20, 2016, 7:23 p.m.

**Phishing Alert - [Redacted] Bank, http://www.[Redacted].com - Fake Site**  
[Redacted]  
May 20, 2016, 7:09 p.m.

**Phishing Alert - [Redacted] Bank, http://www.[Redacted].com - Fake Site**  
[Redacted]  
May 20, 2016, 6:50 p.m.

# Deep and Dark Web

- Three levels
  - Surface Web
  - Deep Web
  - Dark Web
- The value of information cannot be realized unless it is possible to find it
  - Most common methods are paste sites and forums.
  - Cached content is very important

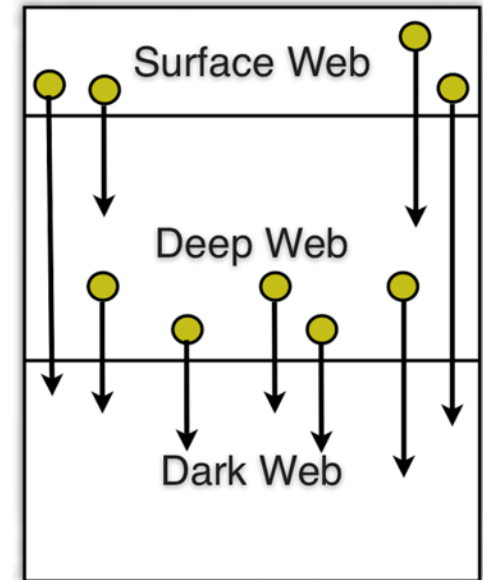












Image Source: RecordedFuture

## Loss Data – Compromised Credit Credentials

- Identification of compromised bank accounts internationally
  - Blocking fraudulent transactions to money mules

-	2016-05-18 10:56:13	 MASTERCARD	 766
Romanian IRC	2016-05-18 10:02:32	 MASTERCARD	 05
Romanian IRC	2016-05-18 10:02:32	 MASTERCARD	 81
Romanian IRC	2016-05-18 10:02:32	 MASTERCARD	 58
Romanian IRC	2016-05-18 10:02:32	 VISA VISA	 03

# CTI Monitoring

## Loss Data – Compromised Accounts (Money Mules)

- Monitoring underground cybercrime forums and the Deep/Dark Web to discover compromised bank accounts

2016-05-18 02:31:06	-/-	[REDACTED] 92
2016-05-18 02:30:58	-/-	[REDACTED] 02
2016-05-17 14:55:38	-/-	[REDACTED] 87
2016-05-17 14:55:38	-/-	[REDACTED] 93
2016-05-17 14:55:38	-/-	[REDACTED] 83



# CTI Monitoring

## Loss Data – Credentials

- Monitoring the Internet to discover compromised credentials (emails, username, passwords)
  - Acting before credentials are misused
  - Minimizing the impact of adverse media coverage

Cybercrime group	Date Detected	Domain	Login	IP address
-	2016-04-24 10:18:09	Bank [redacted].com	[redacted]	0.0.0.0
-	2015-02-25 10:04:45	exchange c[redacted].h	c[redacted].h	0.0.0.0
-	2015-01-29 13:54:33	exchange c[redacted].h	c[redacted].h	0.0.0.0
-	2014-11-17 10:29:31	Bank [redacted].com	[redacted]	0.0.0.0
-	2016-05-13 10:22:41	www.m[redacted].b.com	d[redacted]g@s[redacted].sa.com	[redacted]

DATES	LOGIN	VICTIM'S IP	SOURCE	Keybase
Detected 2016-05-13 10:22:41	Login d[redacted]g@s[redacted].sa.com	Country Nigeria	C&C server http://expresdelivery.ml/oshe/	Town Tulsa
Compromised 2016-05-12 11:07:01	Password [redacted]	Town Lagos	IP 104.168.169.140	Provider -
		Provider [redacted]	Country [redacted]	

## Rogue Mobile Applications

- Rogue Mobile Application
  - Unauthorized mobile application developed to look like and behave like a legitimate one
  - Objective: steal credentials, infect mobile phone
- Two main mobile app stores
  - Apple Store, Google Play, Windows Store
- Over 100 mobile apps store



## Sample Alternative Marketplaces



Marketplace	Number of Users/Apps
AppChina	<b>30 million users</b>
Tencent App Gem	<b>80 million users</b>
Anzhi	<b>25 million users</b>
Amazon Appstore	<b>25 million apps</b> downloaded every month
Opera Mobile Store	<b>30 million apps</b> downloaded every month
AppChina	<b>600 million apps</b> downloaded every month
Wandoujia	<b>200 million users</b> with over <b>30 million apps</b> downloaded <b>every day</b> – <b>500,000 new users</b> are acquired every day
Samsung Apps	Preinstalled on more than <b>100 million Galaxy smartphones</b>

<http://www.businessofapps.com/the-ultimate-app-store-list/>

## Monitoring Threats from Third Parties

- Large organizations deal with many third parties
  - Suppliers, business partners, external consultants etc.
  - Varying degree of access to the corporate network, systems, applications and data
- Managing risks from third parties
  - Continuous auditing
  - Security controls
  - Monitoring controls

# Final Remarks

- CERTs cannot do without CTI
- CTI means different things to different vendors
  - IP reputation, social media, deep/dark web etc
- Identify CTI needs
- Ensure capability to benefit from CTI
  - CTI Services
  - CTI feeds
  - CTI Investigations
  - CTI Platforms

Thank you  
Questions?

