
CYBER ATTACKS AND DEFENSE
SWISS CYBER STORM
WWW.SWISSCYBERSTORM.COM
Cyber Threat Intelligence:
What Vendors are NOT telling you!
Raoul "Nobody" Chiesa
&
Almerindo Graziano
SIR, IT'S TOO MUCH! WE NEED TO ORGANIZE ALL THIS INTELLIGENCE AND MAKE SENSE OUT OF IT!
INFOSEC DEPARTMENT
Security Vendor
CYBER THREAT INTELLIGENCE
silensec
SecurityBrokers
GLOBAL CYBER DEFENSE & SECURITY SERVICES

Disclaimer

Disclaimer

- The information contained within this presentation **do not infringe** on any intellectual property nor does it contain tools or recipe that could be in breach with known laws.
- The statistical data presented **belongs to** the Hackers Profiling Project by **UNICRI** and **ISECOM**.
- Quoted trademarks belongs to **registered owners**.
- The views expressed are those of the author(s) and speaker(s) and **do not necessary reflect** the views of **UNICRI, ITU** or others **United Nations** agencies and institutes, nor the views of **ENISA** and its **PSG** (Permanent Stakeholders Group), neither **Security Brokers** ones, and its Associates.
- Contents of this presentation **may not be quoted or reproduced but partially (10%)**, provided that the **source of information is acknowledged**.

The Speaker & co-Author – Raoul Chiesa

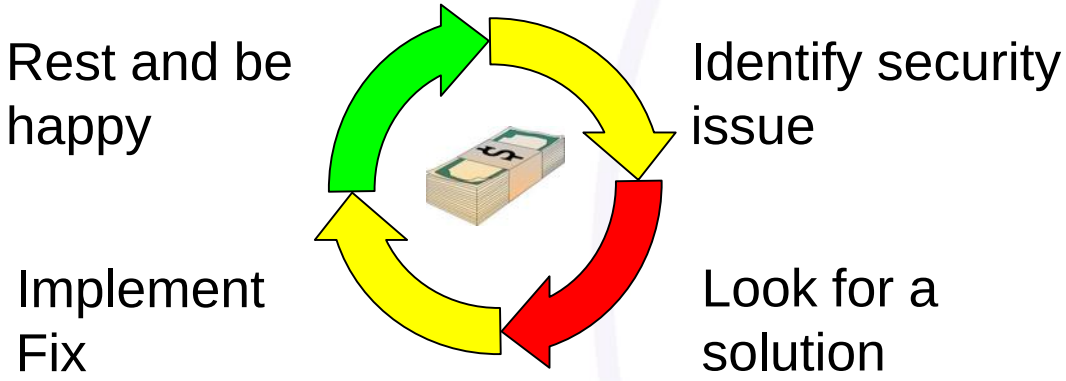
- President, Founder, **The Security Brokers**
- Principal, **CyberDefcon Ltd.**
- Indipendent Special Senior Advisor on Cybercrime @ **UNICRI** (United Nations Interregional Crime & Justice Research Institute)
- Roster of Experts, **ITU** (UN International Telecommunication Union)
- Former PSG Member, **ENISA** (Permanent Stakeholders Group @ European Union Network & Information Security Agency)
- Founder, @ **CLUSIT** (Italian Information Security Association)
- Steering Committee, **AIP/OPSI**, Privacy & Security Observatory
- Board of Directors, **ISECOM**
- Board of Directors, **OWASP** Italian Chapter
- Cultural Attachè. Scientific Committee, **APWG** European Chapter
- Board Member, **AIIC** (Italian Association of Critical Infrastructures)
- **Supporter at various security communities**

The Speaker & co-Author – Almerindo Graziano

- 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

The Wheel of Security Waste

- Most companies are trapped in the wheel of security waste
  - Fueled by security vendors
  - No feeling of measurable achievement



About Cybercrime: the main mistake

- Cybercrime is an ecosystem **which is too often underevaluated**: most of times, it is the **starting** or the **transit point** towards different ecosystems:
  - **Information Warfare**
  - **Black Ops**
  - **Industrial Espionage**
  - **Hacktivism**
  - (private) **Cyber Armies**
  - **Underground Economy and Black Markets**
    - Organized Crime
    - Carders
    - Botnet owners
    - 0days
    - Malware factories (APTs, code-writing outsourcing)
    - Lonely wolves
    - “cyber”-mercenaries, Deep Web, etc

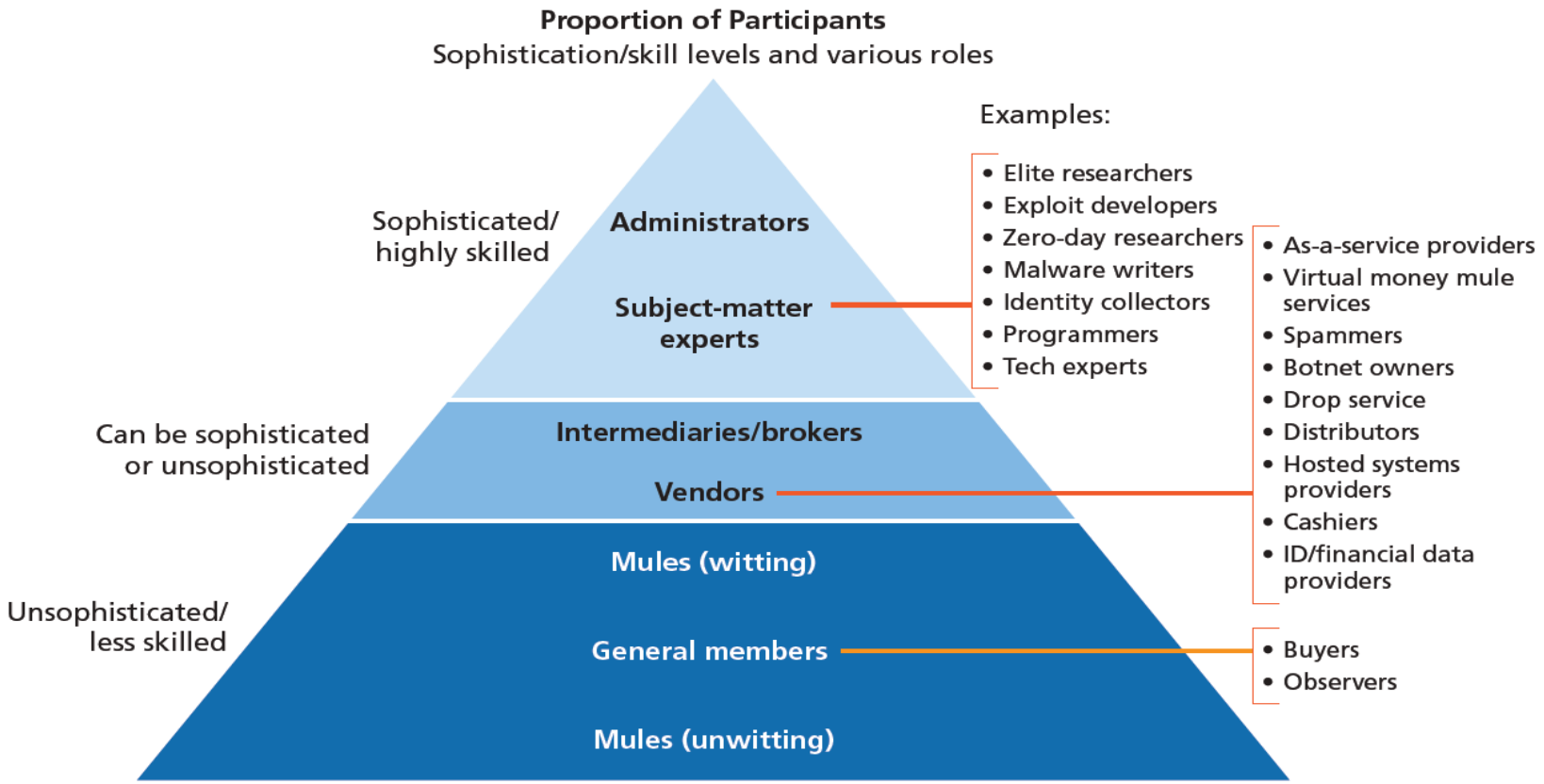
The Hackers' Profiling Project (HPP v1.0)

HPP: the 9 emerged profiles

	OFFENDER ID	LONE / GROUP HACKER	TARGET	MOTIVATIONS / PURPOSES
Wanna Be Lamer	9-16 years "I would like to be a hacker, but I can't"	GROUP	End-User	For fashion, It's "cool" => to boast and brag
Script Kiddie	10-18 years The script boy	GROUP: but they act alone	SME / Specific security flaws	To give vent of their anger / attract mass-media attention
Cracker	17-30 years The destructor, burned ground	LONE	Business company	To demonstrate their power / attract mass-media attention
Ethical Hacker	15-50 years The "ethical" hacker's world	LONE / GROUP (only for fun)	Vendor / Technology	For curiosity (to learn) and altruistic purposes
Quiet, Paranoid, Skilled Hacker	16-40 years The very specialized and paranoid attacker	LONE	On necessity	For curiosity (to learn) => egoistic purposes
Cyber-Warrior	18-50 years The soldier, hacking for money	LONE	"Symbol" business company / End-User	For profit
Industrial Spy	22-45 years Industrial espionage	LONE	Business company / Corporation	For profit
Government Agent	25-45 years CIA, Mossad, FBI, etc.	LONE / GROUP	Government / Suspected Terrorist/ Strategic company/ Individual	Espionage/ Counter-espionage Vulnerability test Activity-monitoring
Military Hacker	25-45 years	LONE / GROUP	Government / Strategic company	Monitoring / controlling / crashing systems

Cybercrime ≠ “hackers”

Figure 2.1
Different Levels of Participants in the Underground Market



SOURCES: Drawn from interviews; Schipka, 2007; Panda Security, 2011; Fortinet, 2012; BullGuard, undated.
NOTE: Almost any participant can be a ripper; see text for discussion.
RAND *RR610-2.1*

Different shades of gray…

Low level hackers “script-kiddies”

- Phishing, Remote low-level social engineering attacks
- Insiders
- Disgruntled Employees

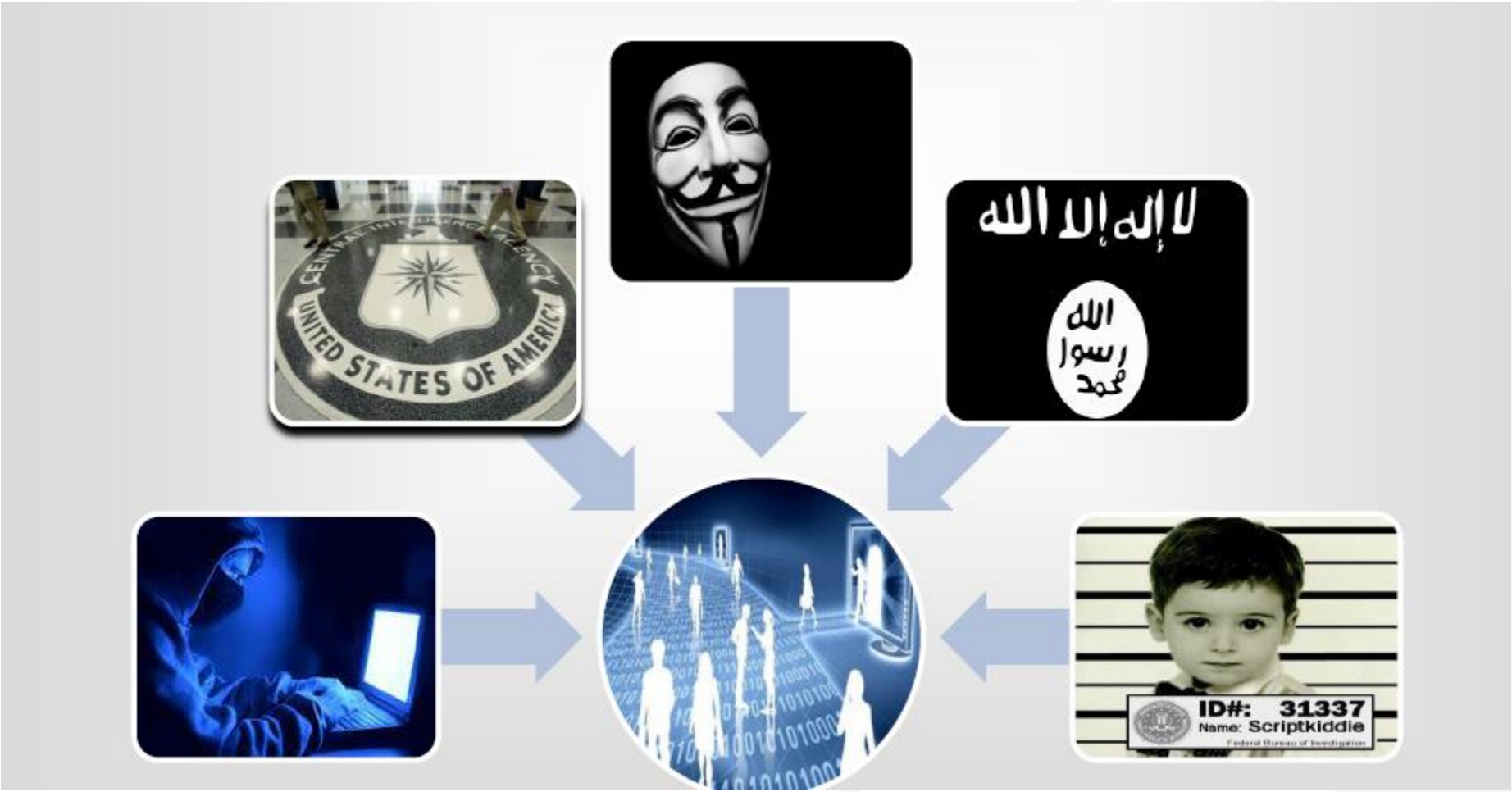
High-level, sophisticated hackers, organized crime-mediu

- Hobbyist Hackers
- Unethical “security guys” VS Intelligence Agencies (the Telecom Italia and the Vodafone Greece affairs; the Belgacom hack, etc…)
- Structured/Unstructured Attacks

Industrial Espionage-Terrorism

- Foreign Espionage
- Hacktivists
- Terrorist Groups
- State Sponsored Attacks

The new Hackers Profiling Project (HPP v2.0)



PROFILE	MAY BE LINKED TO	WILL CHANGE ITS BEHAVIOR?	TARGET	(NEW) MOTIVATIONS & PURPOSES
Wanna Be Lamer		No		
Script Kiddie	Urban hacks	No	Wireless Networks, Internet Café, neighborhood, etc..	
Cracker	Phishing Spam Black ops	Yes	Companies, associations, whatever	Money, Fame, Politics, Religion, etc…
Ethical Hacker	Massive Vulnerabilities	Probably	Competitors (Telecom Italia Affair), end-users	Big money
Quiet, Paranoid, Skilled Hacker	Black ops	Yes	High-level targets	Hesoteric request (i.e., hack "Thuraya" for us)
Cyber-Warrior	CNIs attacks Gov. attacks	Yes	"Symbols": from Dali Lama to UN, passing through CNIs and business companies	Intelligence ?
Industrial Spy		Yes	Business company / Corporation	For profit
Government Agent		Probably	Government / Suspected Terrorist/ Strategic company/ Individual	Espionage/ Counter-espionage Vulnerability test Activity-monitoring
Military Hacker		Probably	Government / Strategic company	Monitoring / controlling / crashing systems


Companies
Security Budget
silensec®

Let's Talk about the Problem

- Reactive Approach
  - Traditional tools focus is on the vulnerability element of the risk rather than the threat
- Limping Incident response
  - Focused on reaction and getting the business back on track
  - Focusing on the small fires
  - Little learning

Defense in Depth

Proactive measures to identify potential attackers, intentions and methods

Prediction

Protection

Security measures and controls to protect from, deter and stop attacks as well minimize the impact of a compromise

Detection

Process of monitoring to identify intrusions and attacks

Reaction

Processes and methods to investigate intrusions and respond to a compromise

Cyber Threat Intelligence

The Kill Chain

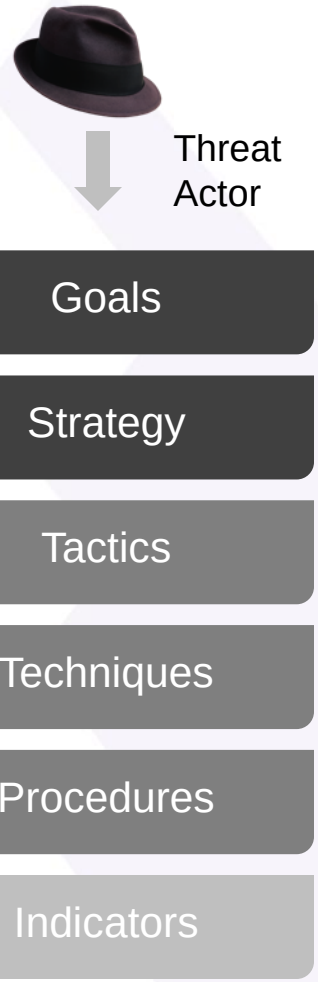
- Systematic process of finding and engaging an adversary to create the desired effects (US Army, 2007)
  - Adapted by Hutchins et al. in 2011
- Key observations
  - Going from the Recon phase to the final Action phase is NOT immediate
  - The time taken for the kill chain process to execute can be used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

Indicators

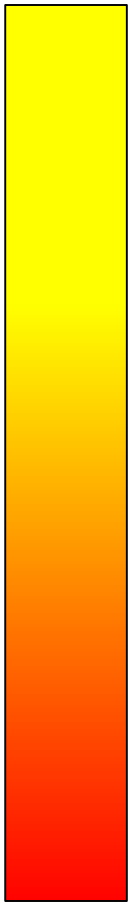
Samples

- Tipical 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

Indicators

A Classification of Indicators

Easy



Hard

Indicator of Compromise (IoC)

- Any piece of information that objectively describes an intrusion.

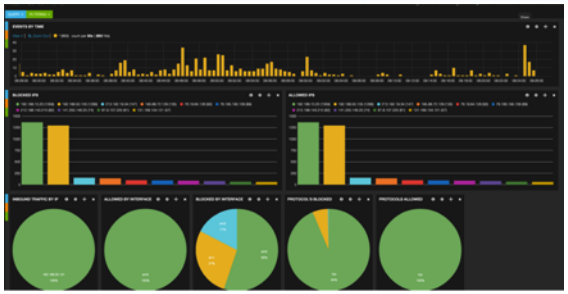
Indicator of Attack (IoA)

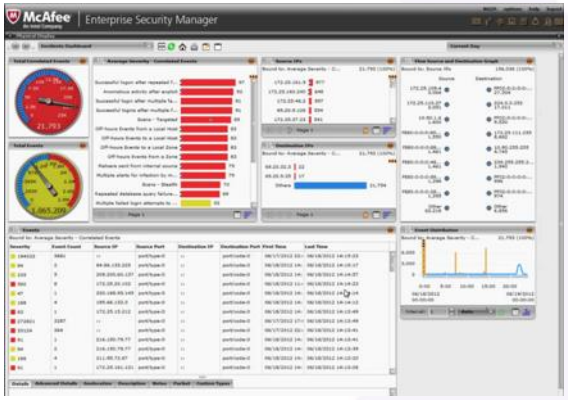
- Any piece of information that objectively describes an action taken towards achieving a compromise

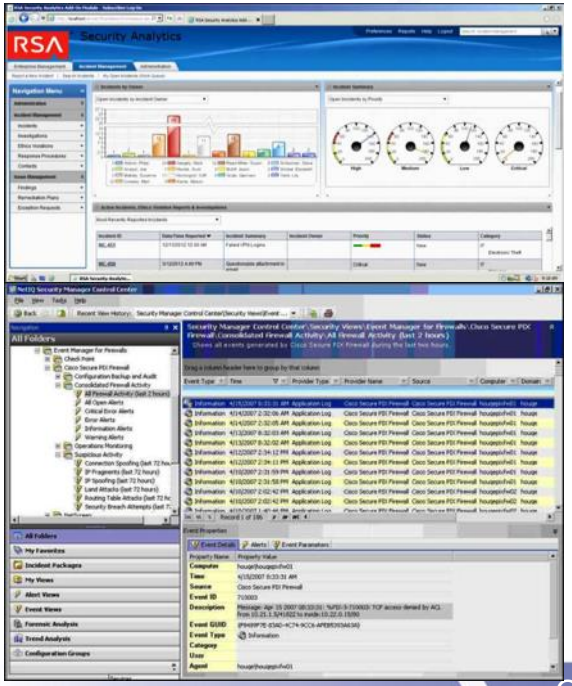
Indicator of Deception (IoD)

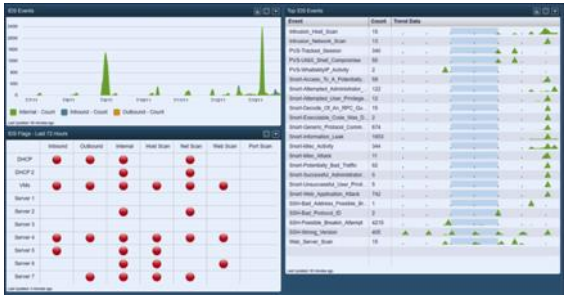
- Any piece of information that objectively identifies an attempted deception about the intended target or threat actor

What Intelligence Do you Need?







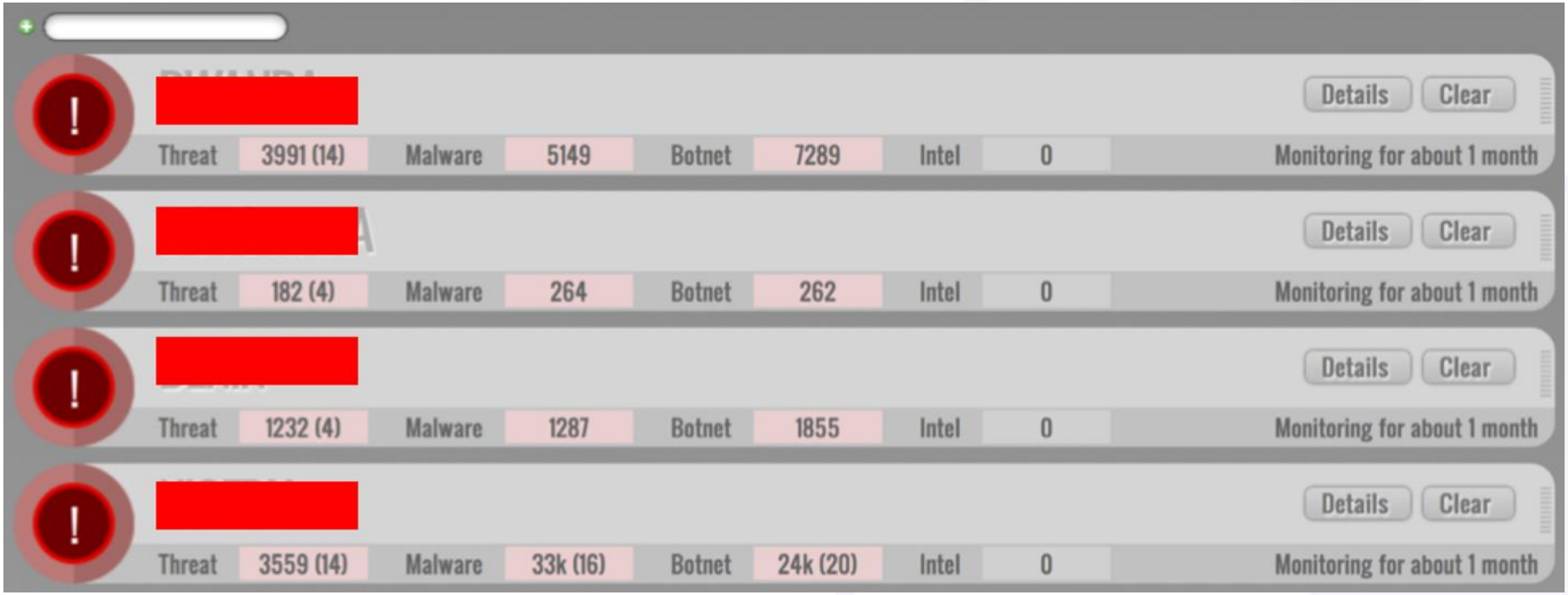


About Cyber Threat Intelligence

- 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



CTI Monitoring

Phishing

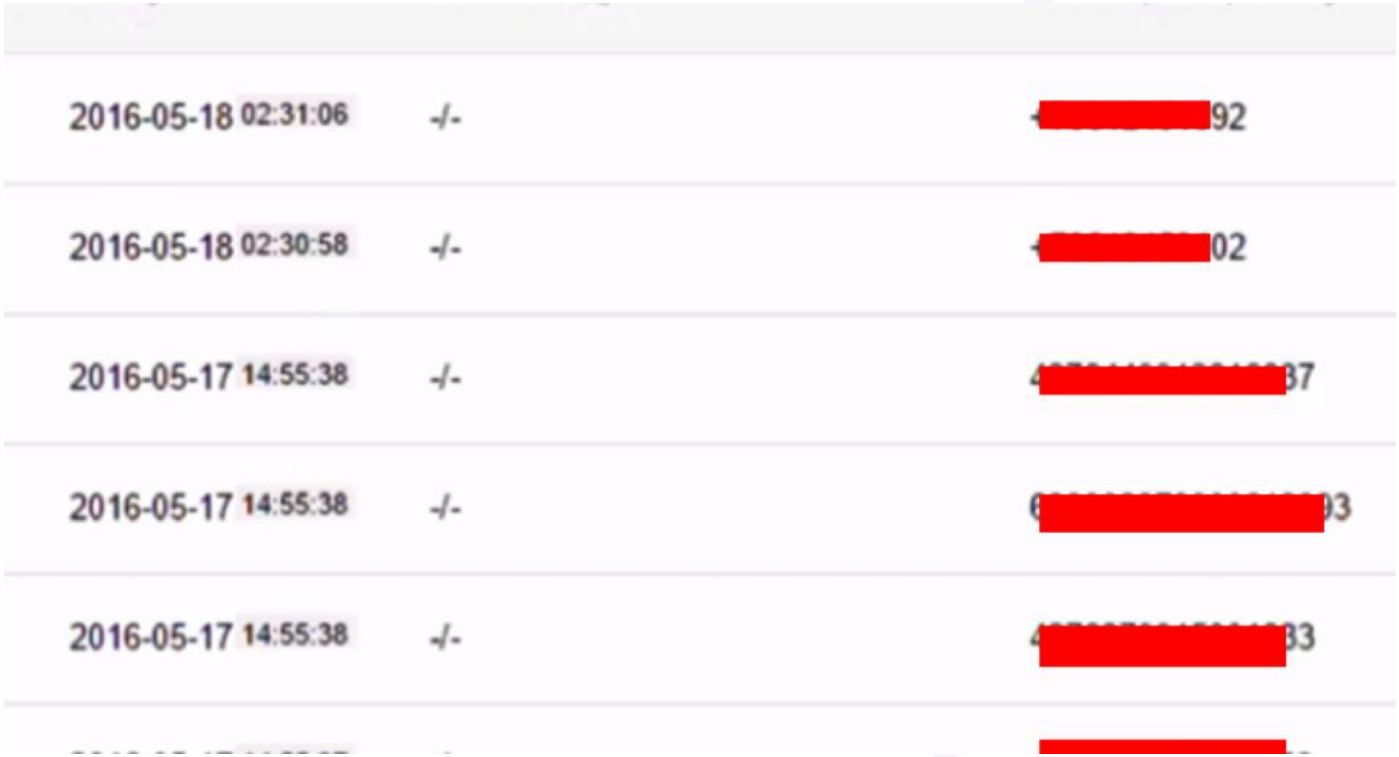
CTI Monitornig

Loss Data – Compromised Credit Crads

-/-	2016-05-18 10:56:13	MASTERCARD	[redacted]66
Romanian IRC	2016-05-18 10:02:32	MASTERCARD	[redacted]35
Romanian IRC	2016-05-18 10:02:32	MASTERCARD	[redacted]81
Romanian IRC	2016-05-18 10:02:32	MASTERCARD	[redacted]58
Romanian IRC	2016-05-18 10:02:32	VISA	[redacted]03

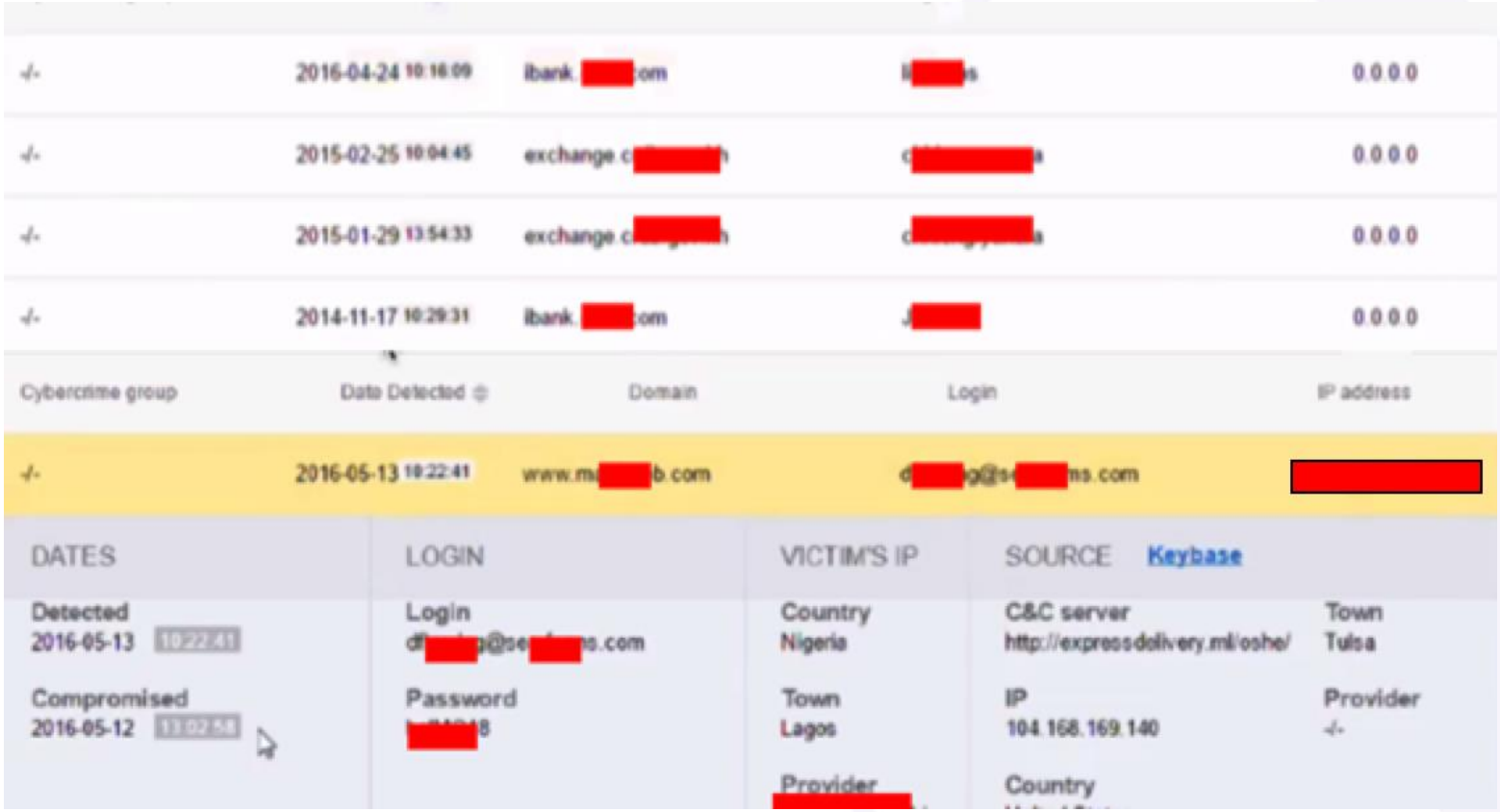
CTI Monitoring

Loss Data – Compromised Accounts (Money Mules)



CTI Monitoring

Loss Data – Credentials



CTI Monitoring

Social Media

CTI Monitoring

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

Rogue Mobile Applications

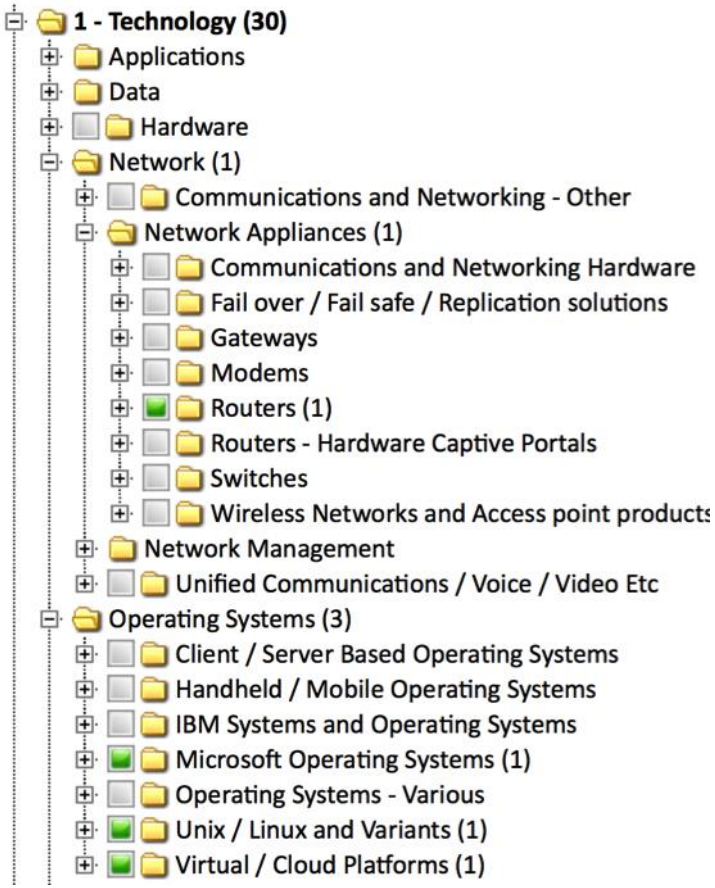
Sample Alternative Marketplaces

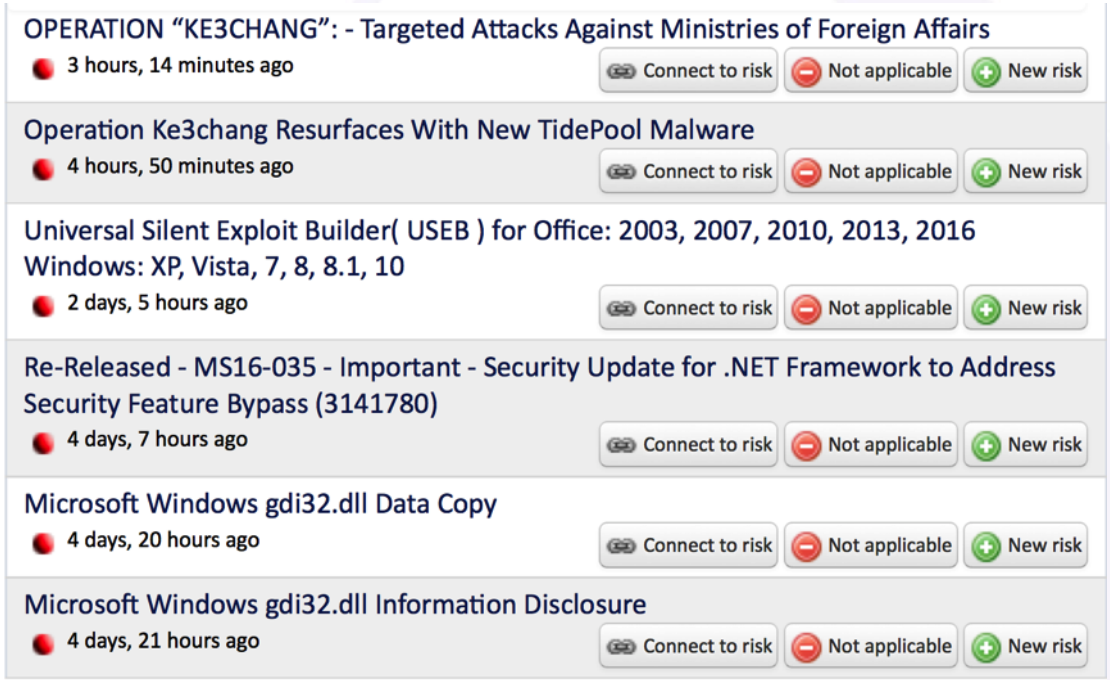
Marketplace	Number of Users/Apps
AppChina	**30 million users**
Tencent App Gem	**80 million users**
Anzhi	**25 million users**
Amazon Appstore	**25 million apps** downloaded every month
Opera Mobile Store	**30 million apps** downloaded every month
AppChina	**600 million apps** downloaded every month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

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

CTI Monitoring

Technology Watch





CTI Monitoring

TTPs and Indicators

CTI Monitoring

TTPs and Indicators

Analysis of KRIPTOVOR: Infostealer+Ransomware-JH

Published To: **demo01**

Tags: data theft

Analysis of KRIPTOVOR: Infostealer+Ransomware

April 08, 2015 | By Erye Hernandez | Threat Research, Advanced Malware

KRIPTOVOR, from the Russian word *'kripto'* which means crypto and *'vor'* which means thief, is what we named this malware family due to its Russian stomping grounds and the malware's behavior. FireEye Labs has collected several samples of this malware (see the Appendix), which primarily targets Russian businesses, or any international companies that do business in Russia.

The malware is modular, which makes it easy for the author to add more functionality. Analysis of an early variant shows that it was first used to steal cryptocurrency wallets from its victims. Over time it evolved to include a ransomware component.

The earliest known infection of the variant with the ransomware component is in early 2014. Several victims reported to have lost their files. Their documents were encrypted and the file extensions were changed to .JUST. The malware also leaves a ransom note taking the victim hostage.

The author put a lot of effort into making it difficult to detect this malware. It employs several evasion techniques and it even cleans up after itself whether or not it was successful in stealing or encrypting its targets. The malware also checks if the victim belongs to specific network segments, which suggests that the author intended on keeping the infections to specific regions.

In this blog, we discuss KRIPTOVOR in detail from the infection vector to the ransom note. Figure 1 depicts the entire cycle of this malware. It starts with the attacker sending an email to the victim. The victim opens the email and the attached Word document. The Word document contains an embedded binary file, which the attacker crafted to look like a PDF file. Opening the binary launches a PDF file containing a resume. Unbeknownst to the victim, the malware begins its routine in the background.

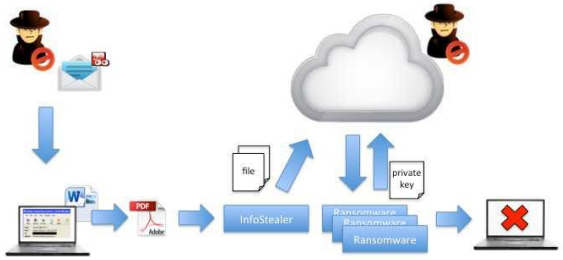


Figure 1. Overview of KRIPTOVOR

81 indicators

were derived from your document. download all

FQDN (7)

- kirova.ls
- nic.ru
- plantsroyal.org
- ripola.net
- valanoice.org
- adorephoto.org
- jackropely.org

IP (1)

- 66.96.147.86

HASH (64)

- 488ba9382c9ee260bbca1ef03e843981
- e426309faa42e406e5c0691bf5005781
- 00e3b69b18bfad7980c1621256ee10fa
- 3d8e0471b822e7cb8efb490ea2801262
- 6fc98a27bda791282ba101ac696bffa1
- 19266c9182e8232ff286ff2f276000c5
- 2191510667defe7f386fc1c889e5b731

SIGNATURES

have been auto generated from the indicators to the left.

FORMAT	INDICATORS USED	OPTIONS
OPENIOC V1.0	81	
OPENIOC V1.1	81	
SNORT V2.9	17	
IPTABLES V1.4	1	
BRO V2.3	81	
STIX V1.2	72	

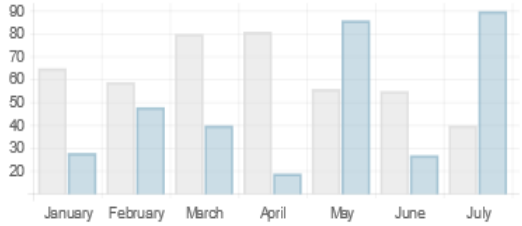
CUSTOM SIGNATURES add a custom signature

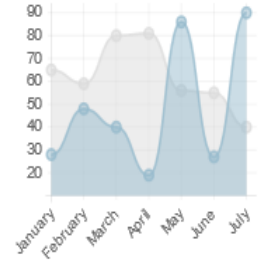
You have not added any custom signatures yet.

ADD CUSTOM SIGNATURE

CTI: Ransomwares (extract)

RansomWare





Outbreak Update Centre - Ransomware	
Ransomware - New Repor...	142 red 6 yellow 1 green
Locky Ransomware	41 red 66 yellow 1 green
Cerber / Cerber 2 Rans...	27 red 50 yellow
CryptXXX Ransomware	18 red 14 yellow
CrypMIC Ransomware	14 red 17 yellow
Zepto Ransomware	14 red 11 yellow 1 green
Mamba / HDDCryptor Ran...	7 red 15 yellow
Nymaim Ransomware	7 red 4 yellow
MarsJoke Ransomware	6 red 26 yellow
CTB-Locker / Critroni ...	6 red 25 yellow
WildFire Ransomware	6 red 22 yellow
Crypt0L0cker / Torrent...	

Outbreak Update Centre - Ransomware	
CryptFile2 Ransomware	5 red 6 yellow
Hades Locker Ransomware	5 red 3 yellow
Odin Ransomware	5 red 3 yellow
Cryptolocker / PowerLo...	4 red 17 yellow
Fantom Ransomware	4 red 14 yellow
CryLocker / Cry Ransom...	4 red 10 yellow
Crysis Ransomware	4 red 7 yellow
Rex Linux Trojan	4 red 7 yellow
Stampado Ransomware	4 red 7 yellow
Hidden Tear Ransomware	4 red 6 yellow
Cryptowall Ransomware	3 red 11 yellow 1 green
DetoxCrypto Ransomware	

Outbreak Update Centre - Ransomware	
CryPy Ransomware	3 red 9 yellow
EDA2 / EDAD2 Ransomware	3 red 8 yellow
FairWare Ransomware	2 red 16 yellow
TeslaCrypt ransomware	2 red 13 yellow 1 green
Polyglot Ransomware	2 red 12 yellow 1 green
DXXD Ransomware	2 red 11 yellow 1 green
PETYA Ransomware	2 red 9 yellow 1 green
Encryptor RaaS	2 red 6 yellow
PokemonGo Ransomware	2 red 6 yellow
RAA Ransomware	2 red 5 yellow
Troldesh / XTBL / Shad...	2 red 4 yellow
VirLock Ransomware	

Outbreak Update Centre - Ransomware	
Alma Locker Ransomware	2 red 3 yellow
Exotic Ransomware	2 red 3 yellow
FSociety Ransomware	2 red 2 yellow
Xorist Ransomware	2 red
CoinVault	1 red 5 yellow
Samas/Samsam/MSIL.B/C ...	1 red 5 yellow
Shark Ransomware	1 red 5 yellow
Apocalypse Ransomware	1 red 4 yellow
Jigsaw Ransomware	1 red 4 yellow
Enigma Ransomware	1 red 2 yellow
ZCryptor Ransomware	1 red 2 yellow
Globe Ransomware	

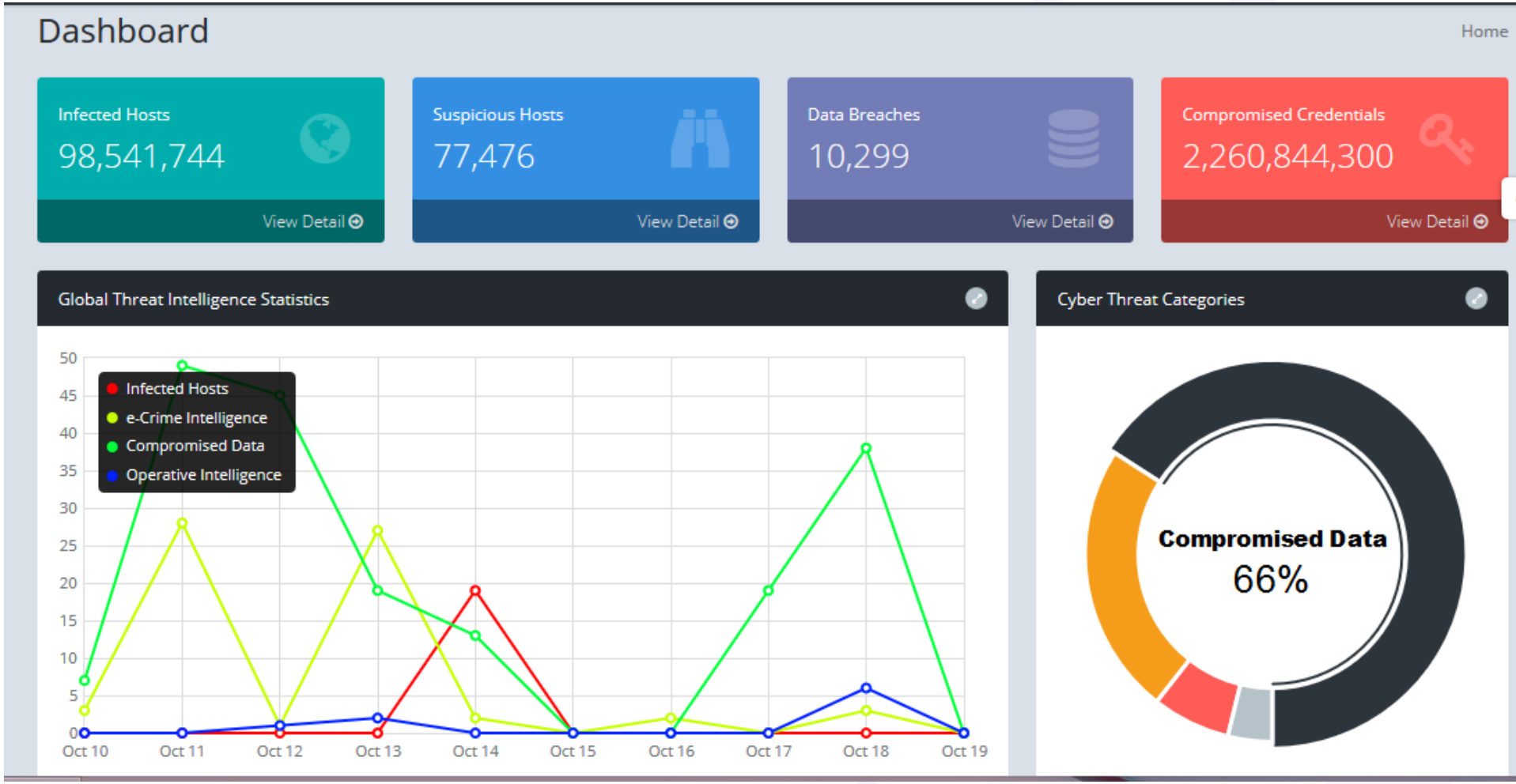
CTI monitoring (open source feeds)

Latest Generic Subjects And Updates

1,056,588 alerts available.

Technology	Industry	Global
Critical: java-1.8.0-openjdk security update (RHSA-2016:2079-1) 8 minutes ago	SBI blocks 6 lakh debit cards after 'suspicious' security breach 2 hours, 53 minutes ago	Adult FriendFinder 'has a serious security flaw' 1 hour, 55 minutes ago
Advanced Upload (PHP) Script Version 1.0.2 MySQL Injection Vulnerabilities 3 hours, 29 minutes ago	Crims cram credit card details into product shots on e-shops 3 hours, 41 minutes ago	Crims cram credit card details into product shots on e-shops 3 hours, 41 minutes ago
NETGATE Data Backup 3.0.605 Privilege Escalation 3 hours, 31 minutes ago	HEADS UP - Nation-State Hackers Hit Japanese Nuclear Facility 4 hours, 27 minutes ago	Typosquatting: Combat Spear Phishing With Recorded Future 4 hours, 2 minutes ago
NETGATE AMITI Antivirus 23.0.305 Privilege Escalation 3 hours, 36 minutes ago	Ransomware attacks: Why healthcare data is at risk 4 hours, 50 minutes ago	pseudoDarkleech Rig EK 4 hours, 19 minutes ago
Crims cram credit card details into product shots on e-shops 3 hours, 41 minutes ago	Hacked Republican website skimmed donor credit cards for 6 months 5 hours, 16 minutes ago	HEADS UP - Nation-State Hackers Hit Japanese Nuclear Facility 4 hours, 27 minutes ago
NETGATE Registry Cleaner 16.0.205 Privilege Escalation 3 hours, 43 minutes ago	GOP Website Among Thousands Hit by Malware 5 hours, 55 minutes ago	HEADS UP - Eitest rig ek from 195.133.201.121 sends cryptfile2 ransomware 4 hours, 37 minutes ago
Researcher pressured to limit big reveal of Big Blue flaw 3 hours, 56 minutes ago	After Ransomware Attack, Clinic Faces More Woes 6 hours, 5 minutes ago	HEADS UP - Pseudo-darkleech rig ek from 5.200.35.126 sends cerber ransomware 4 hours, 48 minutes ago
Researchers Bypass ASLR via Hardware Vulnerability 5 hours, 21 minutes ago	HEADS UP - Security breach: SBI blocks over 6L debit cards 8 hours, 4 minutes ago	HEADS UP - Sundown ek from 37.139.47.53 sends locky ransomware 4 hours, 50 minutes ago
Important: mariadb-galera security and bug fix update (RHSA-2016:2077-1) 5 hours, 48 minutes ago	IL: Mercy Hospital & Medical Center notifies patients after billing service loses 547 patients' documents 8 hours, 6 minutes ago	HEADS UP - Eitest rig ek from 195.133.201.133 sends cryptfile2 ransomware 4 hours, 55 minutes ago
Security Bulletin: Security Vulnerabilities in Spring Framework affect IBM WebSphere Portal 5 hours, 54 minutes ago	Hackers stole credit card data from Republican website for 6 months: Report 8 hours, 15 minutes ago	HEADS UP - Pseudo-darkleech rig ek from 195.133.201.132 sends cerber ransomware 4 hours, 58 minutes ago
GOP Website Among Thousands Hit by Malware 5 hours, 55 minutes ago	Chinese Cyberspies Target European Drone Maker, Energy Firm 9 hours, 15 minutes ago	Hacked Republican website skimmed donor credit cards for 6 months 5 hours, 16 minutes ago
Security Bulletin:Multiple vulnerabilities in IBM Java SDK 7 affect IBM Systems Director 5 hours, 58 minutes ago	Schneider Electric PowerLogic PM8ECC Hard-coded Password Vulnerability (ICSA-16-292-01) 9 hours, 25 minutes ago	

CTI monitoring (closed source feeds)



CTI monitoring (closed source feeds)

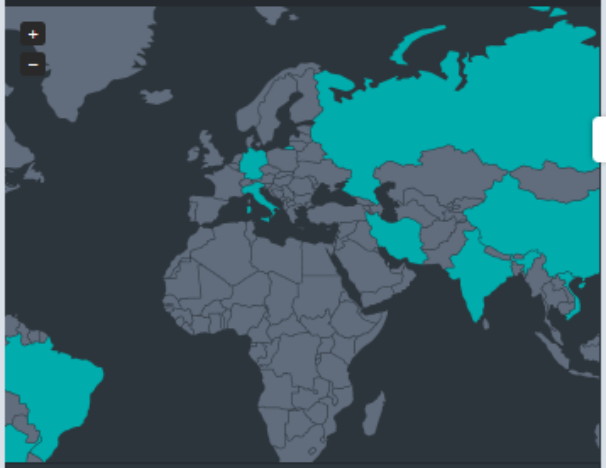
Security Intelligence - Your Network Matches

IP	Host	Country	Malware	C&C	Port	Last Seen
197.228.150.28	D?	ZA	s_conficker	104.244.14.252	80	2016-10-13
197.228.150.252	D?	ZA	auto	None	80	2016-10-06
82.114.76.81	kujtesa.com	CS	s_conficker	104.244.14.252	80	2016-10-06
82.114.76.78	kujtesa.com	CS	s_conficker	104.244.14.252	80	2016-10-06
82.114.76.75	kujtesa.com	CS	s_conficker	104.244.14.252	80	2016-10-06
82.114.76.84	kujtesa.com	CS	s_conficker	104.244.14.252	80	2016-10-06
197.228.150.12	D?	ZA	spamsalot	None	80	2016-10-05

Compromised Credentials - Your Report History

Date	Affected Identifiers	Number of Matches
2016-09-29	aceaspa.it, inail.it	56
2016-09-07	aceaspa.it, inail.it	12
2016-09-02	aceaspa.it, inail.it	42

Cyber Threats Map



1. INDIA	9,824,147
2. CHINA	8,570,864
3. VIET NAM	6,748,359
4. BRAZIL	6,252,373
5. RUSSIAN FEDERATION	4,953,834
6. IRAN, ISLAMIC REPUBLIC OF	4,482,103

CTI Threat Assessment

Executive Threat Assessment

Physical Security Threats

Cyveillance identified a threat to Mr. Burns posted by the hacking collective 'Anonymous' as part of its campaign against Ajax Corporation. The group posted personal details on Mr. Burns and his family, threatening to disclose more information in the future. Cyveillance recommends that a cyber-safety training is conducted to minimize the risk of exploitation. Additionally, Cyveillance suggests that Pastebin is continuously monitored for similar threats, or their propagation through social media.

Social Media Presence

While Mr. and Mrs. Burns' social media accounts remain partially open to the public, they do not contain any sensitive personal disclosures. Clifford Burns' social media accounts, on the other hand, are public and disclose a wealth of personal information. Clifford's Instagram and Twitter accounts provide updates on the Burns family's dynamic, lifestyle, and travel. Cyveillance recommends adjusting security settings for family's social media profiles, as such disclosures can be used to target Mr. Burns and his family with a strong social engineering attempt.

Disclosure of Personal and Residential Information

In addition to Mr. Burns' personal information disclosure through a doxxing attempt, Cyveillance identified family's primary residence, and a summer home through data aggregation sites and tax assessments. Mapping software, coupled with home's real estate listings, can provide a holistic view of the Burns' property, including the layout

Disclosure of Business Information

Aside from Mr. Burns' corporate biographies disclosed through an official website, Cyveillance identified Mr. and Mrs. Burns' affiliation with local charities and non-profit organizations. While seemingly benign, such information can be leveraged in social engineering attacks targeting the executive.

Reputational Risks

It appears Mr. Burns does not own http://www.charlesburns.com. The domain is currently available for purchase. An important precautionary action often taken by executives is to create an official online presence to deter impersonation accounts created for fraudulent purposes or to tarnish the executive's reputation. Cyveillance encounters many instances in which impersonation accounts used to generate business contacts and influence the business environment without the knowledge of the executive.

CTI Threat Assessment

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

CTI Threat Assessment

Third Party Threat Assessment

Sensitive Data in the Open Source

The public disclosure of ANVILS's sensitive data is a low risk to ACME. ANVILS does not disclose any proprietary intellectual property on its own websites. However, third parties have posted limited, but not critical, confidential documents.

Brand Infringement

ANVILS, LLC is a low risk for brand infringement. ANVILS has not misused authorized ACME logos, trademarks, or brand names; however, it has failed to register domain names with potentially objectionable Internet-address suffixes that could lead to future brand infringements.

Physical Security

There is a low risk of protests or disruptions at ANVILS facilities. There have been no protests or civil disruptions. However, the company has a presence in international locations that are less stable than the U.S.

HR/Regulatory Compliance

There is a low risk to ACME stemming from ANVILS's regulatory activity. In comparison to other companies, ANVILS has a higher amount of Financial Industry Regulatory Authority (FINRA) regulatory actions, including several significant violations resulting in high value fines.

Hacker Activity and Cyber Threats

ANVILS's websites are a moderate risk to ACME due to security vulnerabilities. While we did not identify any open-source discussions of ANVILS-focused cyber-attacks, Cyveillance has identified several potential vulnerabilities in the company's sites, including a moderate risk resulting from the presence of an enabled SSLv3 server, making the server vulnerable to potential compromise of sensitive information.

- In contrast to comparable financial institutions, there were no disclosures of critical ANVILS data on the public paste or code sharing sites commonly misused by hackers.
- ANVILS has not reported any significant security or data breaches since 2006.

Reputation Risk

The reputation of ANVILS was damaged in 2006 after a group of investors accused the company of playing an instrumental role in a multi-billion dollar scheme orchestrated by Daff E. Duck. While the investor claims were found invalid, users continue to comment on ANVILS being a dishonest company. Epithets like "crooks" and "liars" in reference to ANVILS were common in 2014-2015. Calls for FINRA to be

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
  - **ATTENTION**: “massive” Deep and Dark web cybercrime forums are different from the Organized Crime “cyberforums”

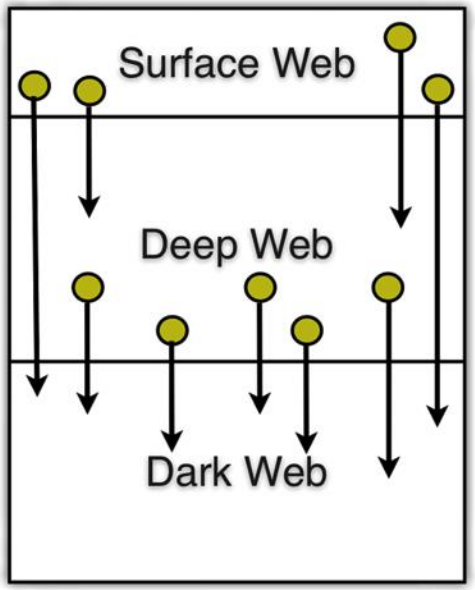
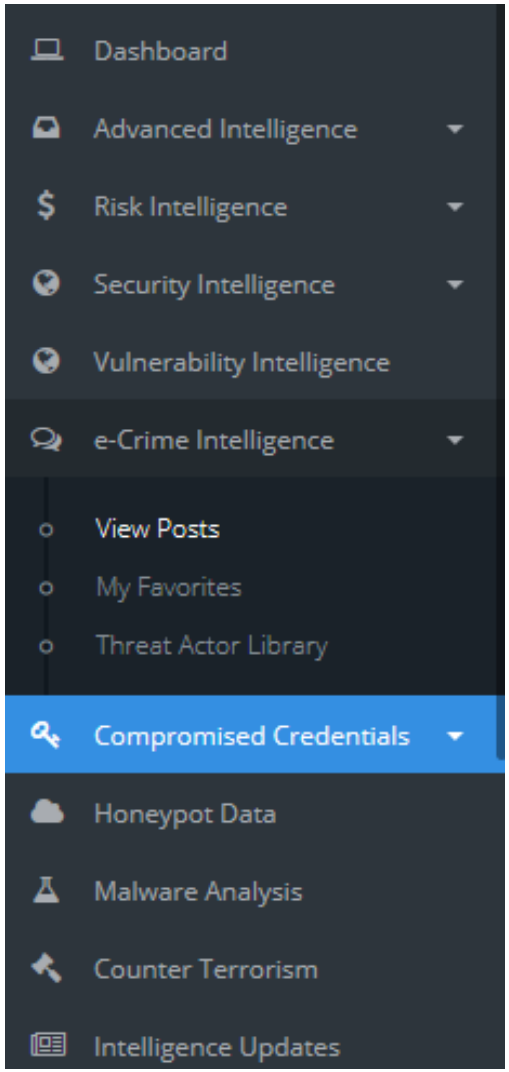
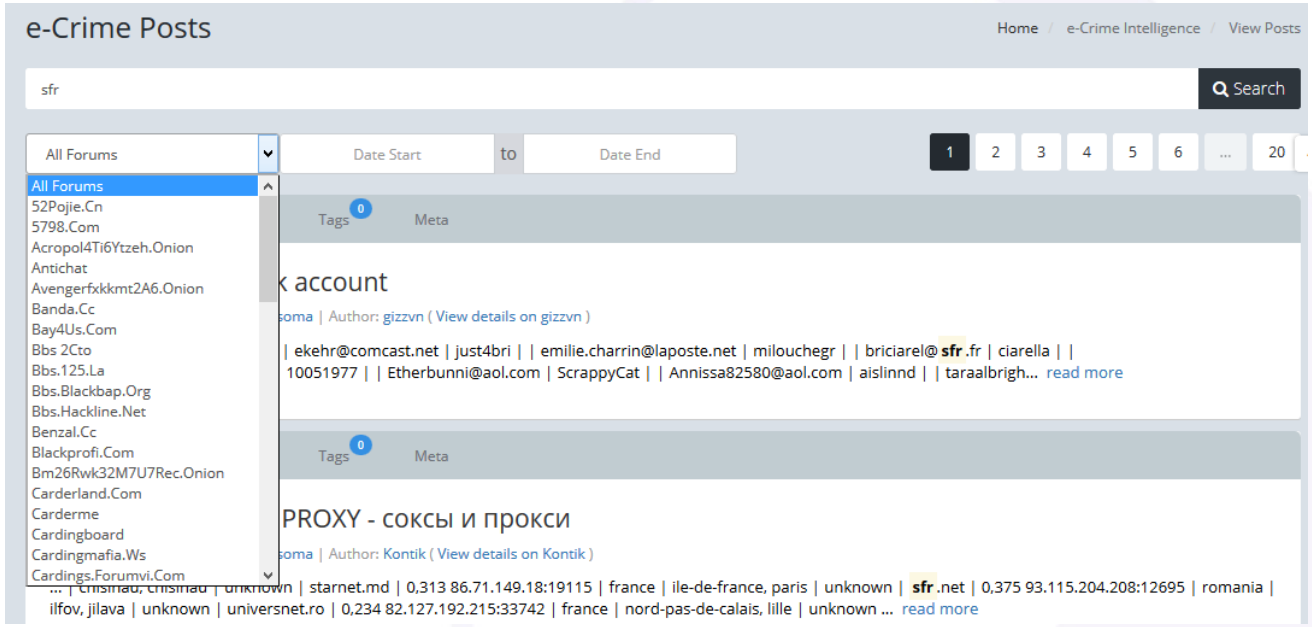


Image Source: RecordedFuture

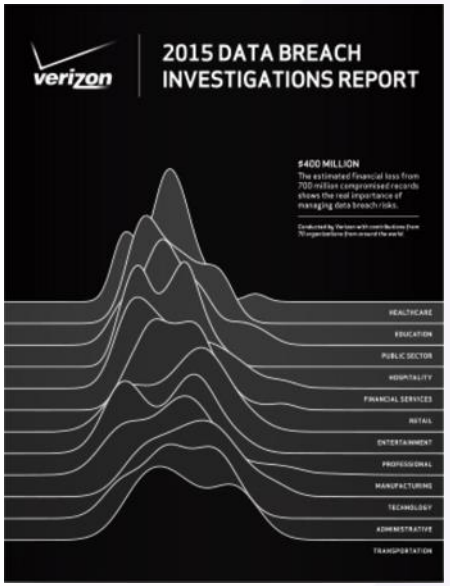
«Dirty forums» and Threat Actors





Bad Intelligence

- Only a small 5% of the intelligence is common across different organizations
  - Many Intelligence products and services are not targeted nor tailored
- Organizations must develop their own intelligence processes



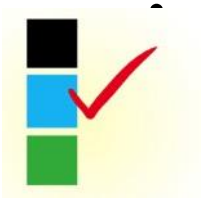
Characteristics of Good Intelligence

Timely

- It needs to be available in time for it to transformed into actions.

Accurate

- Accuracy is based on the number of false positive alerts or actions obtained from the threat intelligence. The lower the number of false positive, the more accurate the intelligence is.



Relevant

- Measured in terms of how the intelligence is organized and delivered to ensure it addresses the industry the organizations belongs to and the relevant threats.

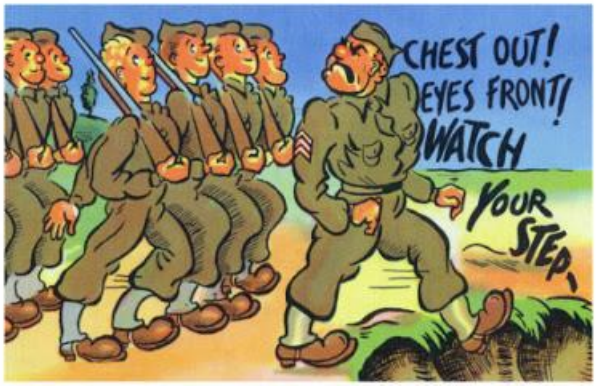
Tailored

- Different intelligence must be provided to different people to enable them to make the decisions relevant to their role

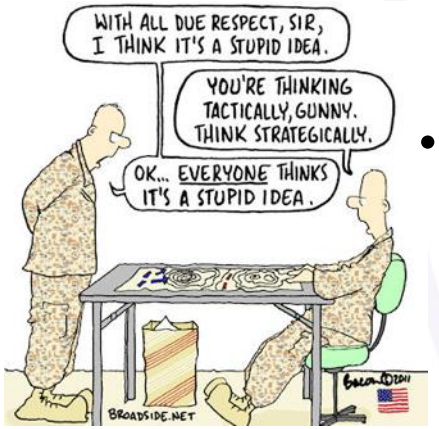
Types of Intelligence

Senior Management (Strategy)

- Policies
- Coherent strategy to carry out the policy

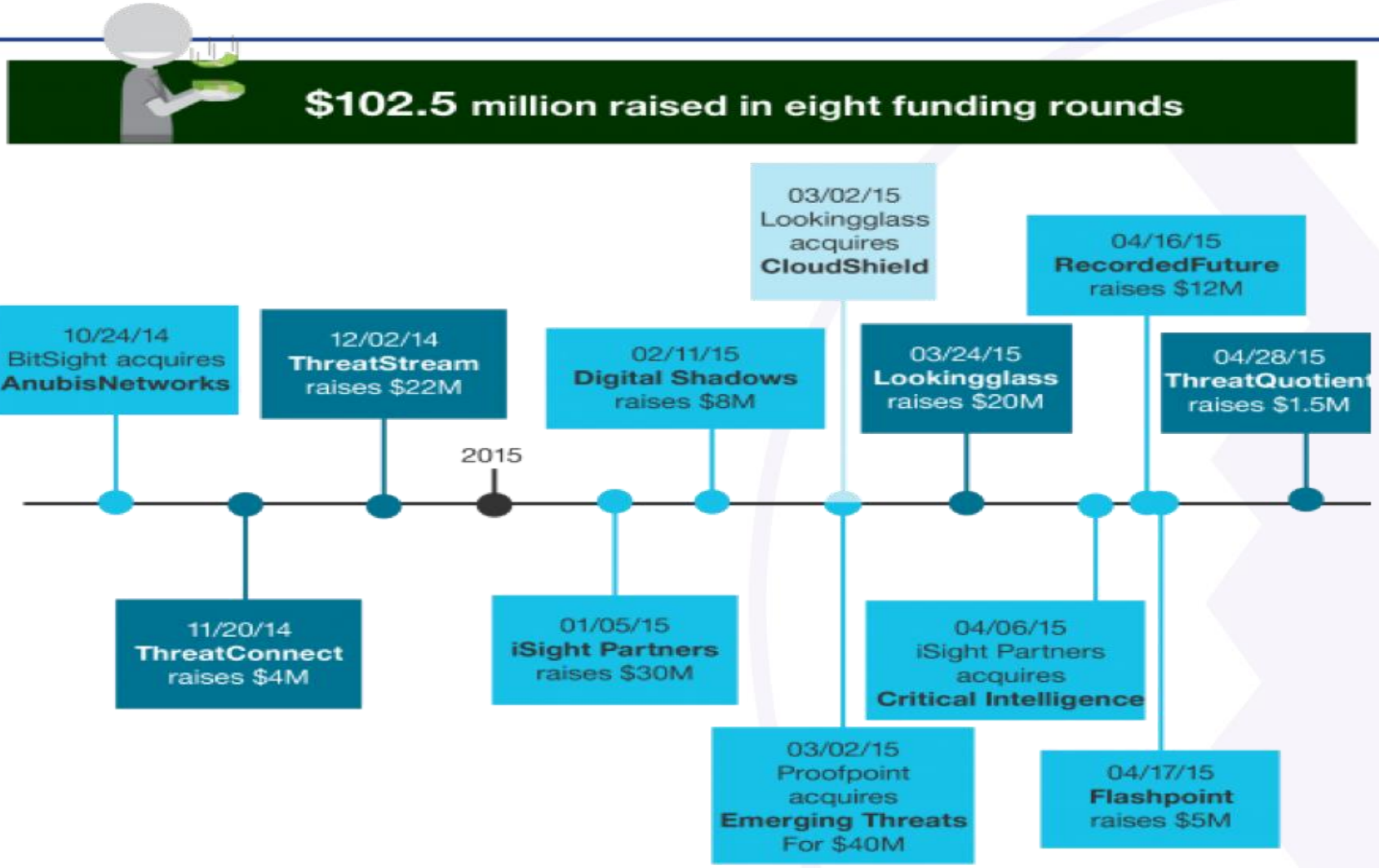


- **Security Managers (Operations)**
  - Organize resources and determine tactics to meet objectives
  - Take care of competences
  - Prioritize response

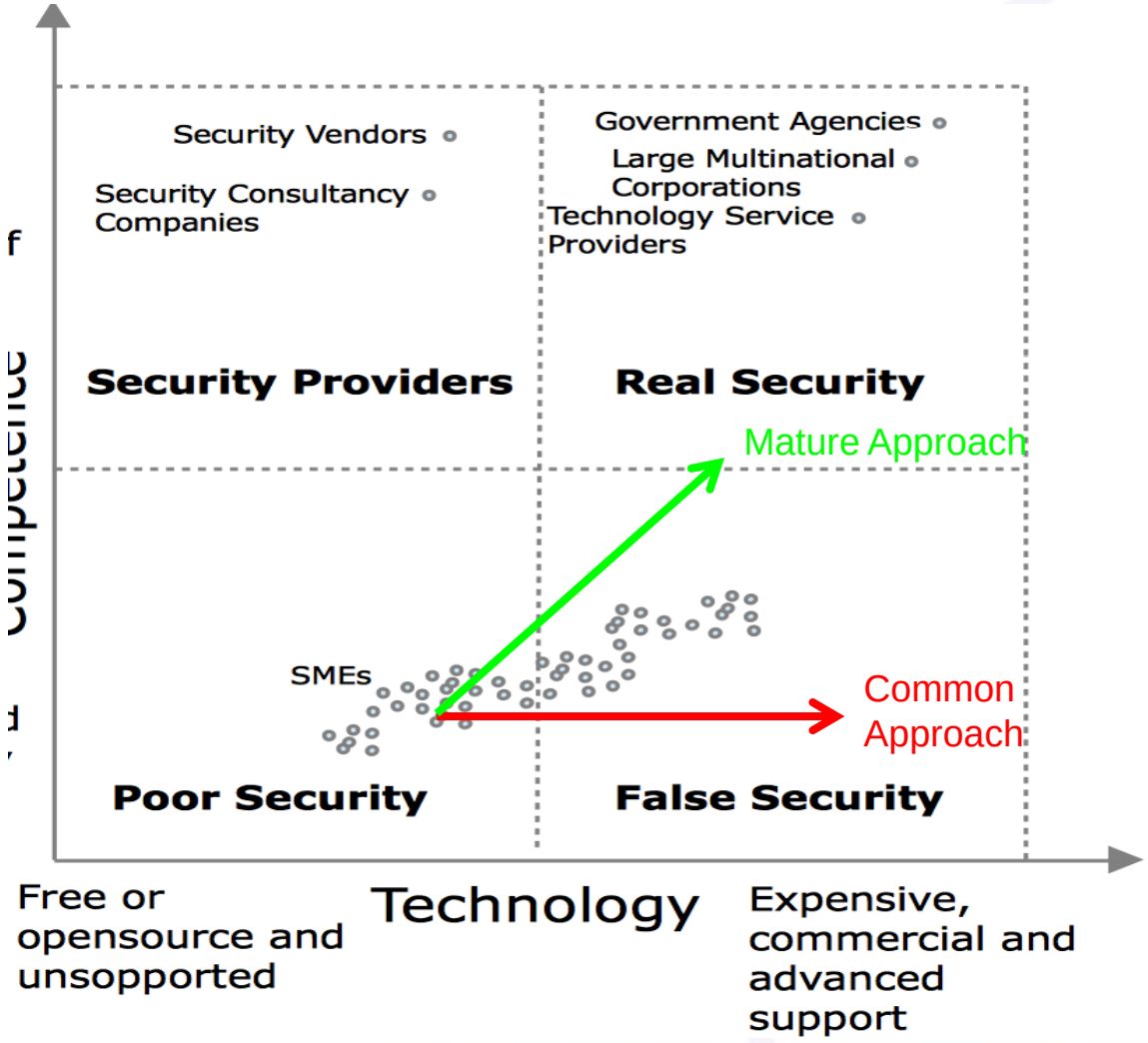


- **Security Staff (tactics)**
  - Engineering, analysts etc
  - Daily battles

A still immature market



Are You Ready for Cyber Threat Intelligence?



Final Remarks

- Is Cyber Threat Intelligence need?
- 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

CTI Challenges

- IPR used to sell black magic
- Miopic view (not always intentional)
- More development and technology integration needed by some vendors
- Immature business model
  - Many “how much would the client spend”
  - FEW “This is our price, take it or leave it”
- Not enough competences to evaluate vendors
- Companies too low in the maturity curve

Thank you
Questions?

[at] security-brokers [dot] com
SecurityBrokers
aoulchiesa