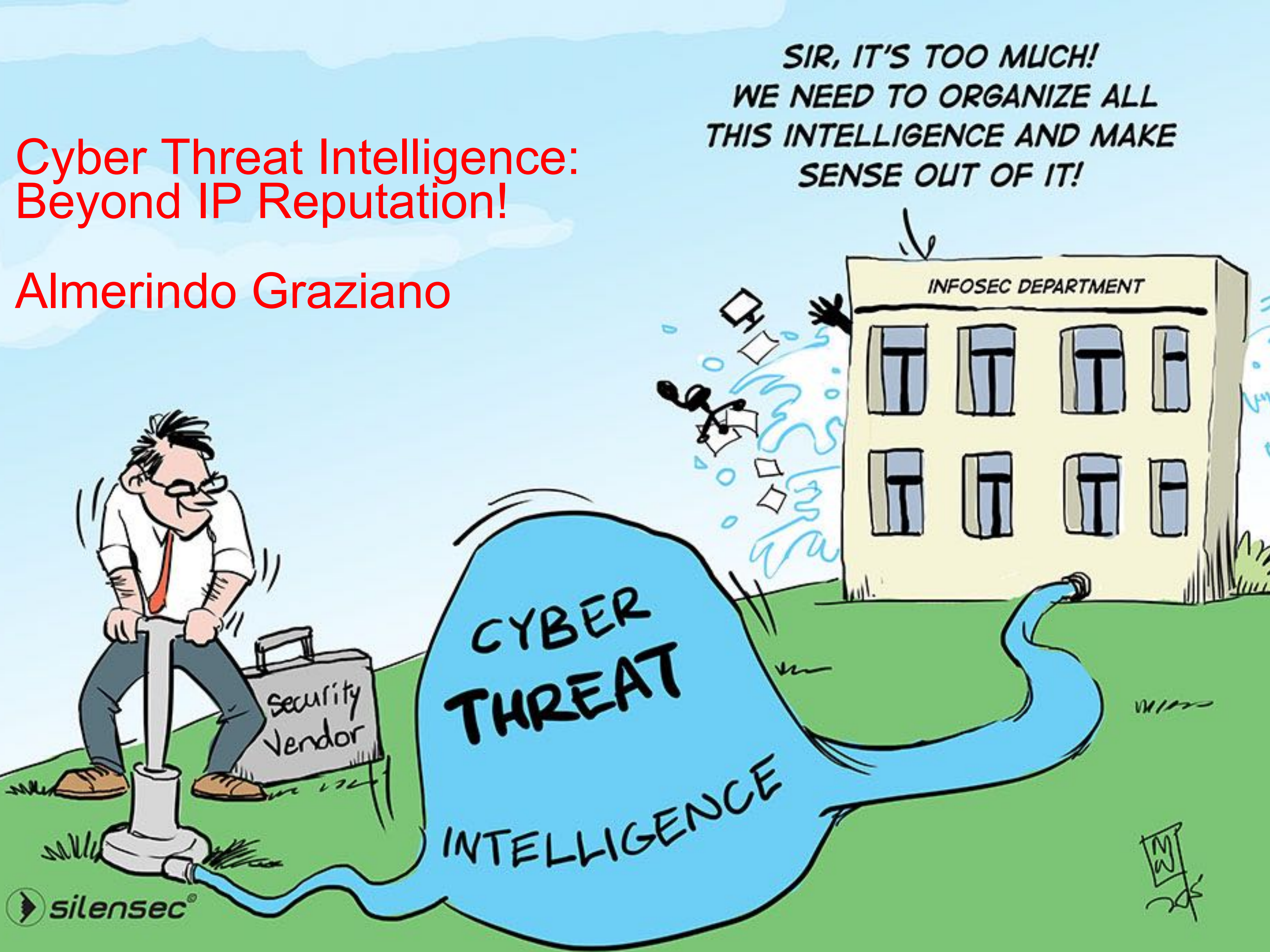
Cyber Threat Intelligence: Beyond IP Reputation!

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

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

Certified Ethical Ninja SAMA · Certified Forensic BEE · Certified Red Bundi · Certified Red CHUNGU · Certified Rev Code Panther · Certified Octopus Ninja · Certified Forensic iSpector

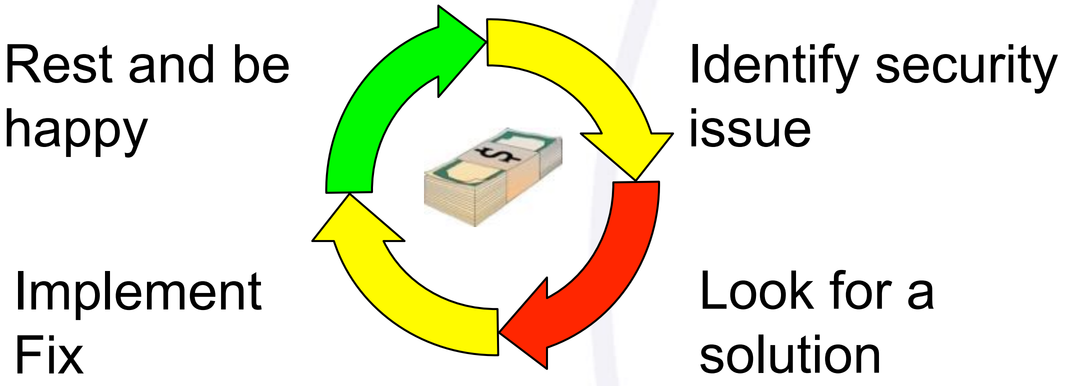
Follow us on Linkedin and Facebook

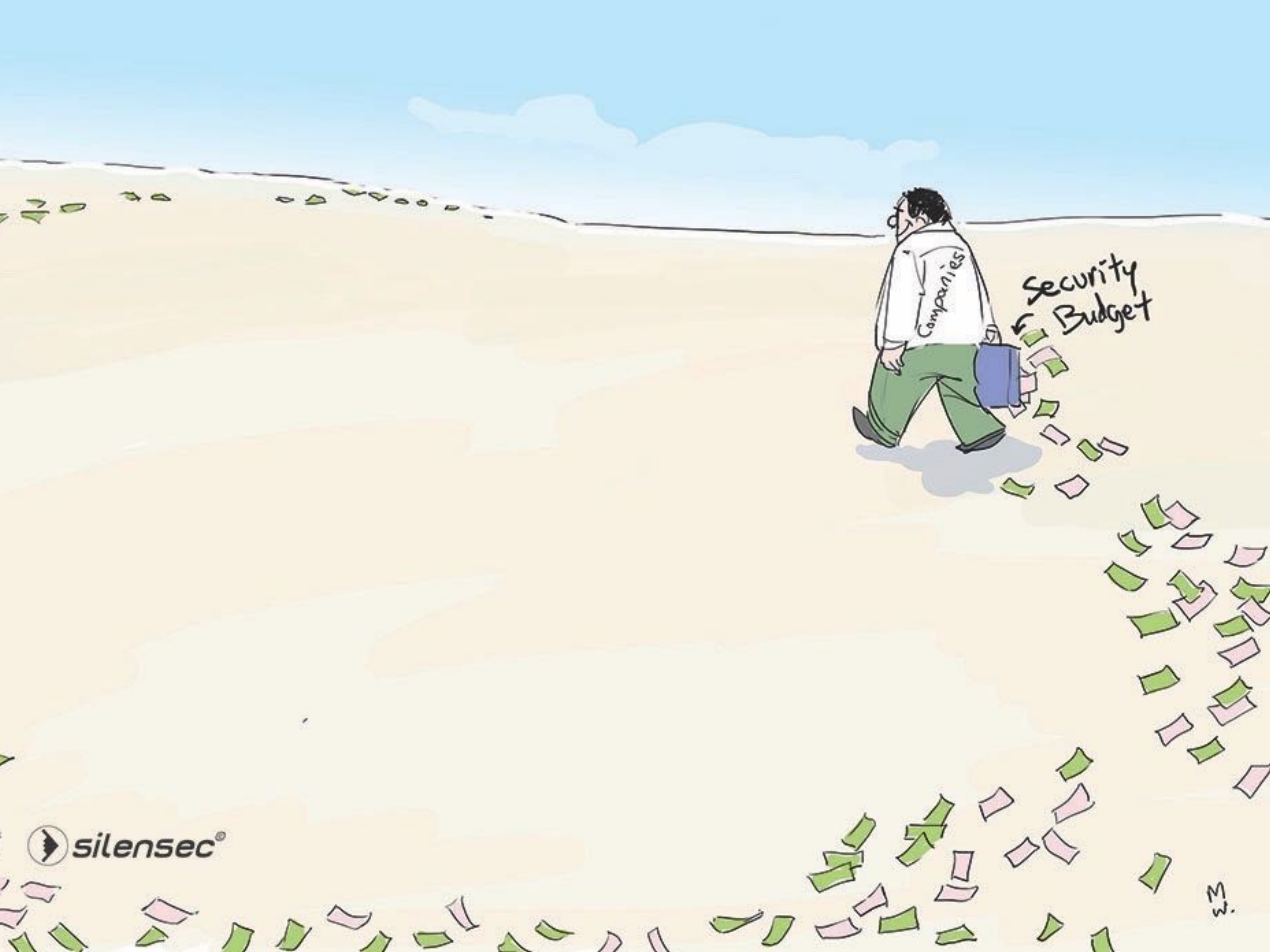
- Awareness Cartoons
  - Security Awareness
  - Security Editorials
  - Life of the Security Consultant

THERE'S DENIAL OF SERVICE INCIDENTS AND I THINK IT'S BECAUSE OF MAN IN THE MIDDLE ATTACKS...
MARRIAGE COUNSELLOR
silensec
INFOSEC Consultant

The Wheel of Security Waste

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





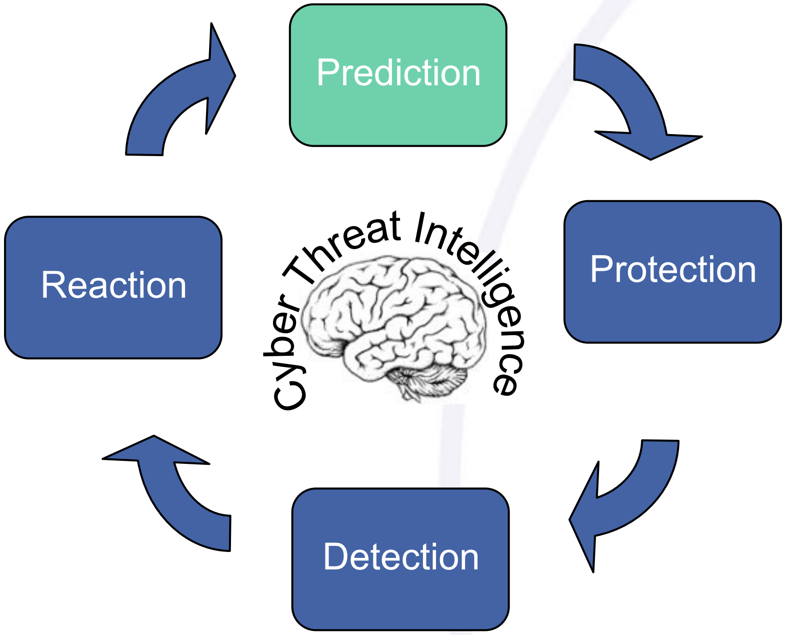
silensec®

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



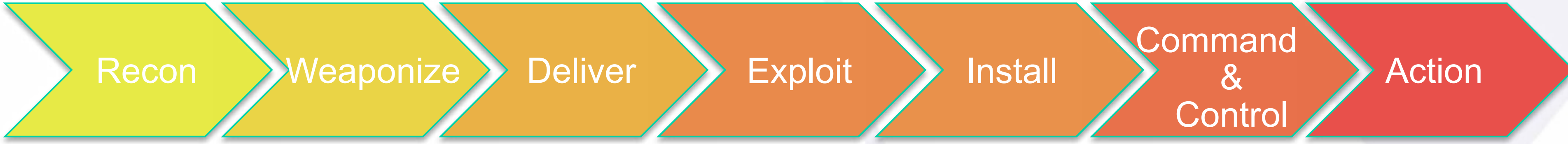
Processes and methods to investigate intrusions and respond to a compromise

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

Process of monitoring to identify intrusions and attacks

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.

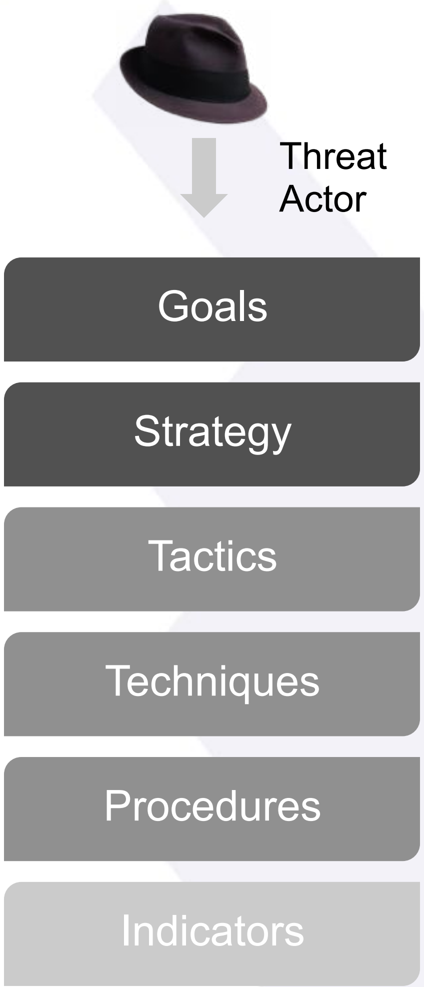


What is Threat Intelligence

- *"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

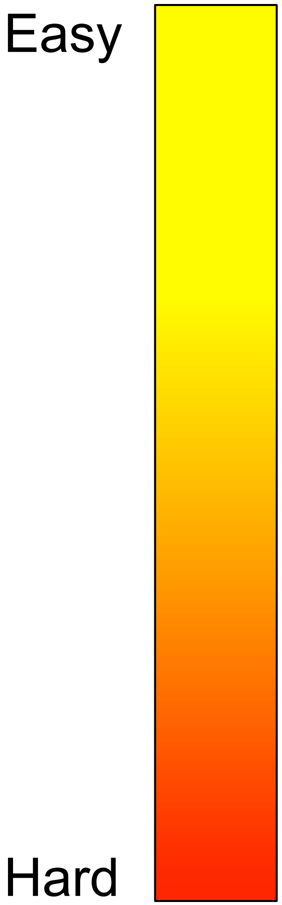
Indicators

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



Indicator of Compromise (IoC)

- Any piece of information that objectively describes an intrusion.

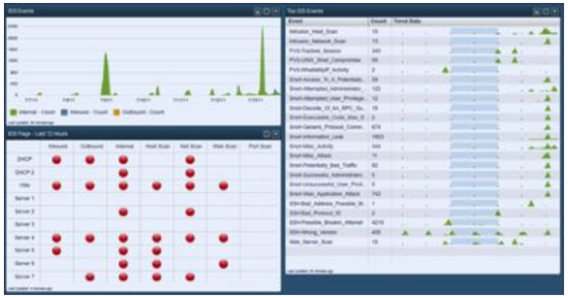
Indicator of Attack (IoA)

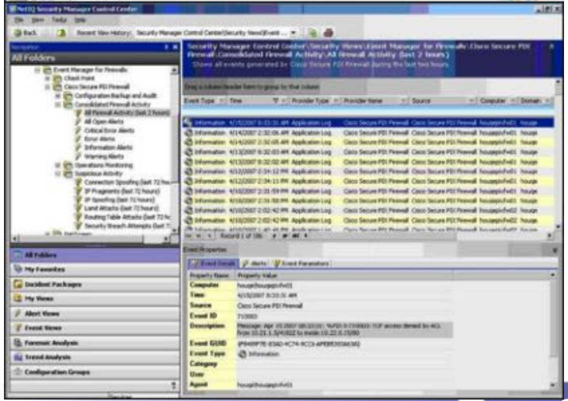
- Any piece of information that objectively describes an action taken towards achieving a compromise

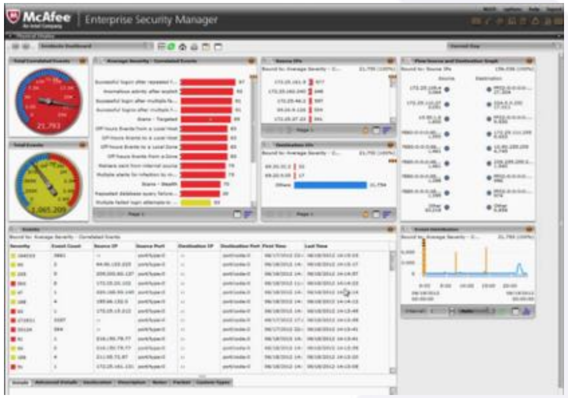
Indicator of Deception (IoD)

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

What Intelligence Do you Need?





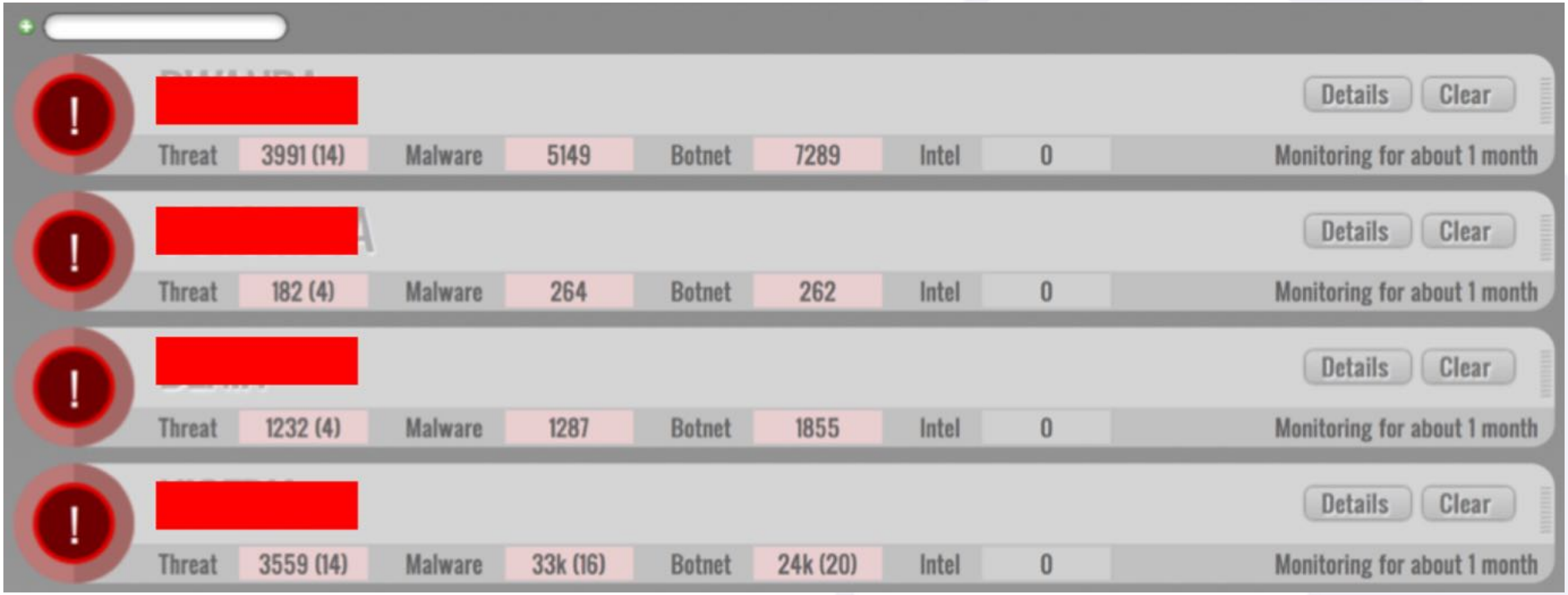


About Cyber Threat Intelligence

- 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



[redacted]

Threat 3991 (14) Malware 5149 Botnet 7289 Intel 0 Monitoring for about 1 month

[redacted]

Threat 182 (4) Malware 264 Botnet 262 Intel 0 Monitoring for about 1 month

[redacted]

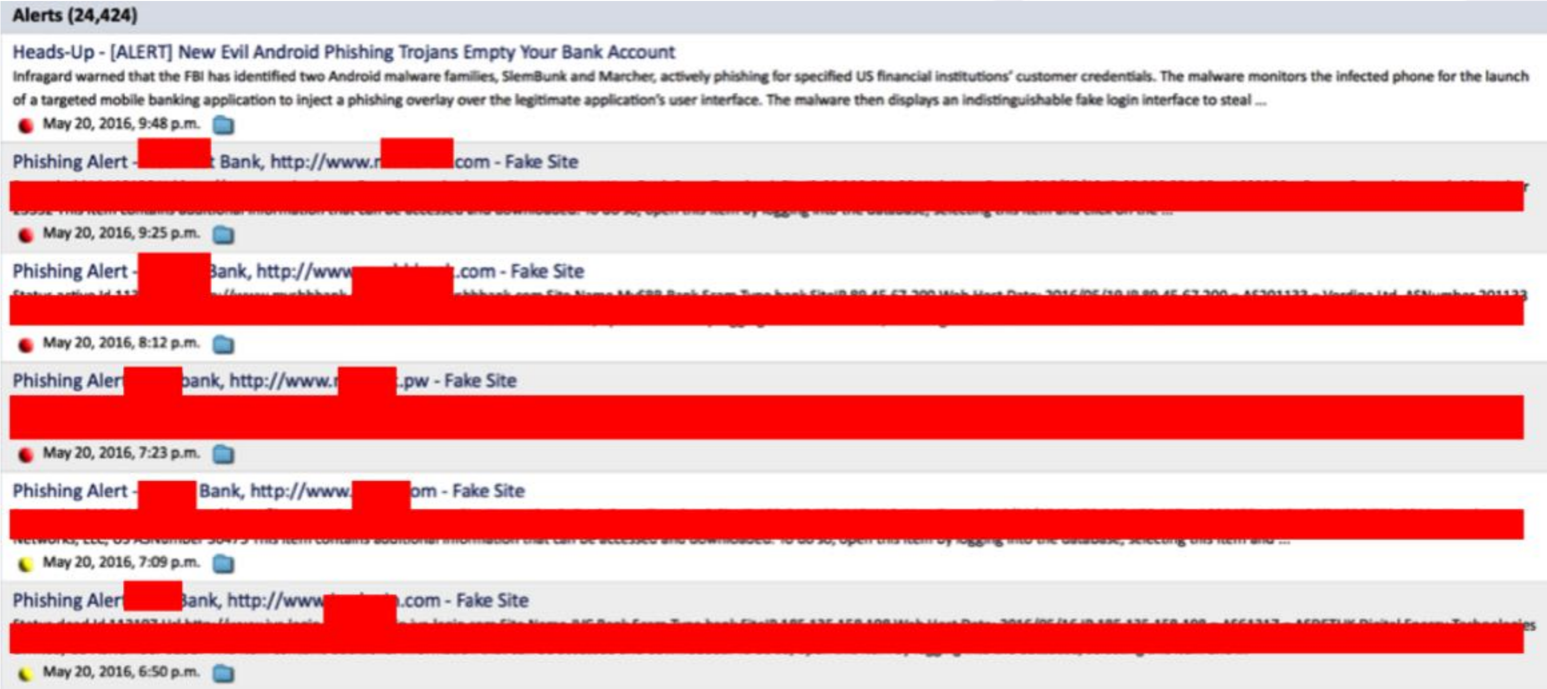
Threat 1232 (4) Malware 1287 Botnet 1855 Intel 0 Monitoring for about 1 month

[redacted]

Threat 3559 (14) Malware 33k (16) Botnet 24k (20) Intel 0 Monitoring for about 1 month

CTI Monitoring

Phishing



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 Aler[redacted] bank, http://www.[redacted].pw - Fake Site

[redacted]

● May 20, 2016, 7:23 p.m.

Phishing Alert - [redacted] Bank, http://www.[redacted]om - Fake Site

[redacted]

● May 20, 2016, 7:09 p.m.

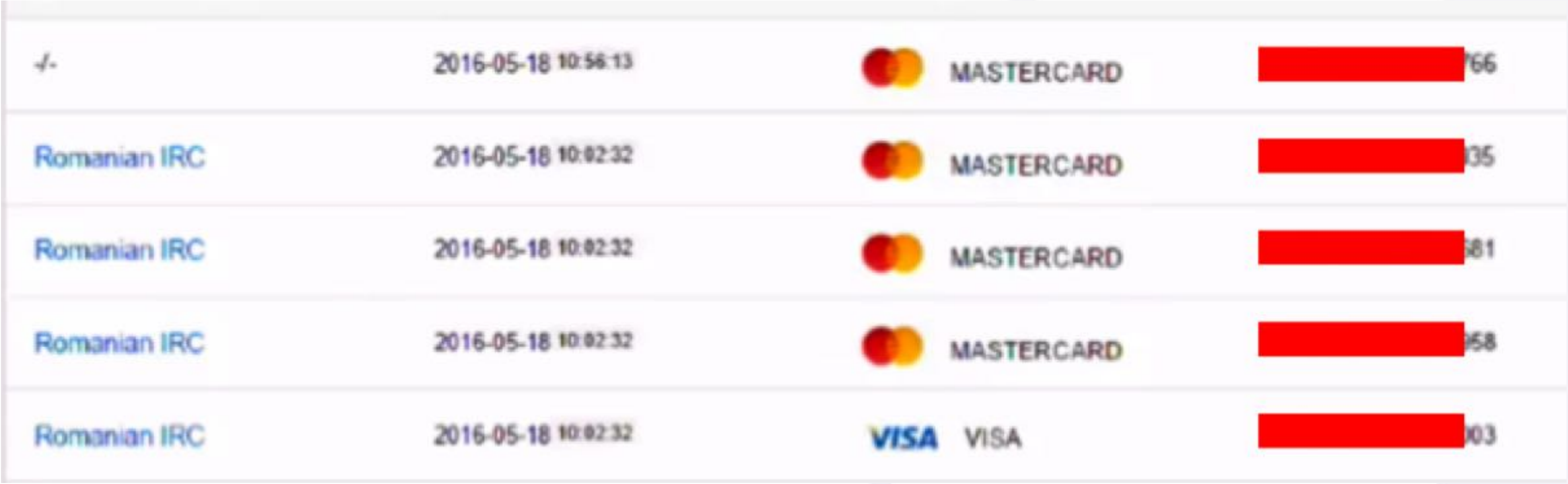
Phishing Aler[redacted] Bank, http://www[redacted].com - Fake Site

[redacted]

● May 20, 2016, 6:50 p.m.

CTI Monitornig

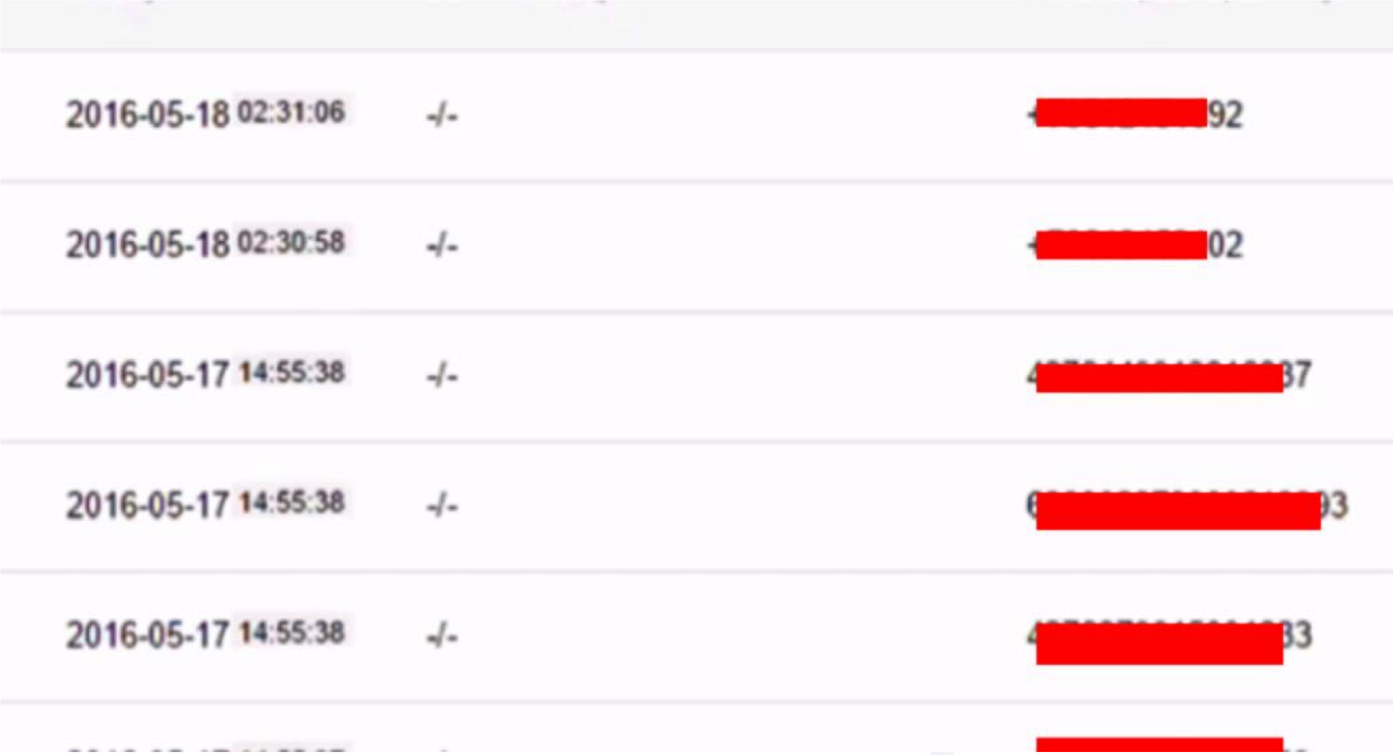
Loss Data – Compromised Credit Crads



-/-	2016-05-18 10:56:13	MASTERCARD	[redacted]
Romanian IRC	2016-05-18 10:02:32	MASTERCARD	[redacted]
Romanian IRC	2016-05-18 10:02:32	MASTERCARD	[redacted]
Romanian IRC	2016-05-18 10:02:32	MASTERCARD	[redacted]
Romanian IRC	2016-05-18 10:02:32	VISA VISA	[redacted]

CTI Monitoring

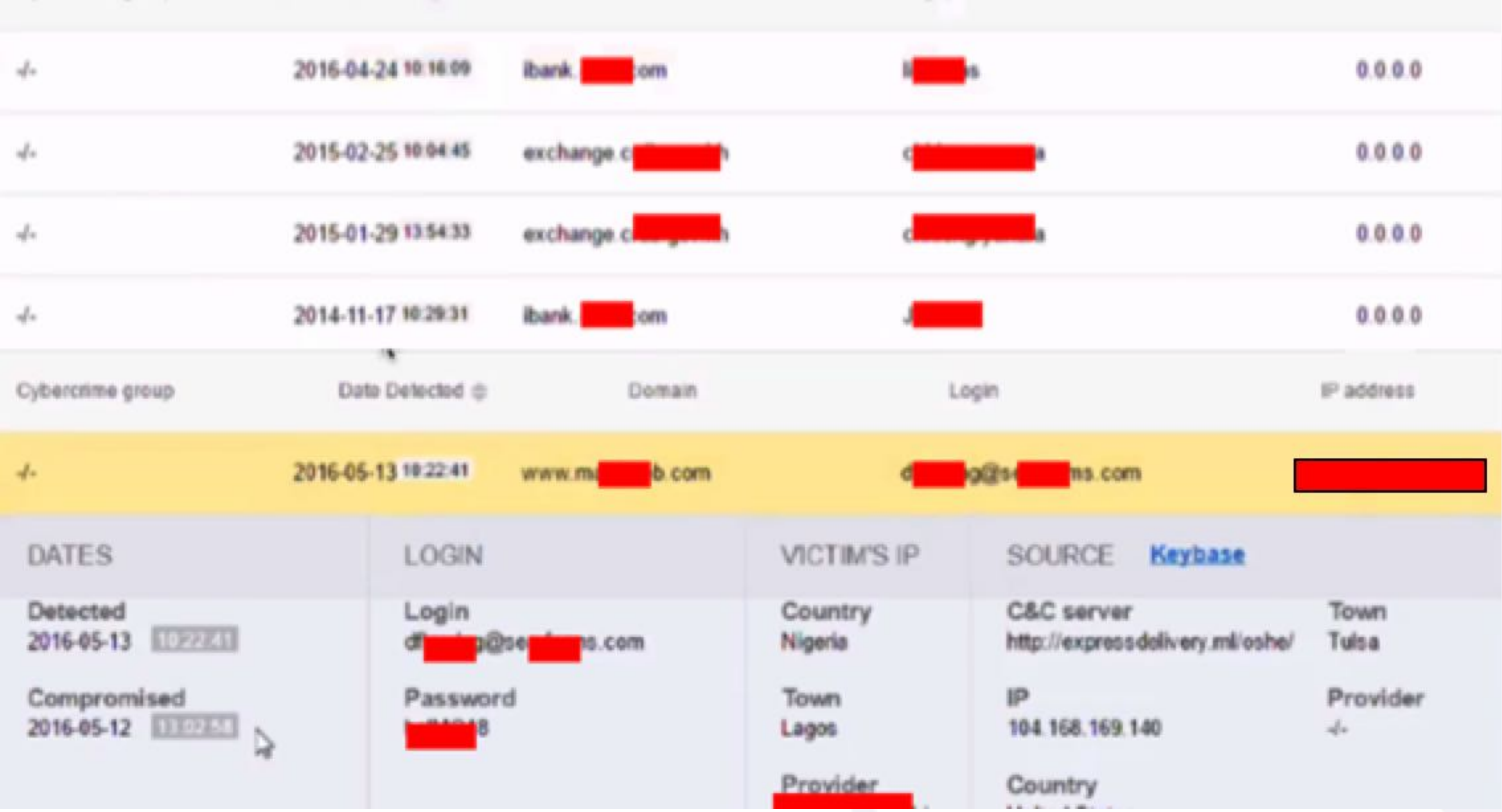
Loss Data – Compromised Accounts (Money Mules)



2016-05-18 02:31:06	-/-	[redacted]
2016-05-18 02:30:58	-/-	[redacted]
2016-05-17 14:55:38	-/-	[redacted]
2016-05-17 14:55:38	-/-	[redacted]
2016-05-17 14:55:38	-/-	[redacted]

CTI Monitoring

Loss Data – Credentials



-/-	2016-04-24 10:16:09	ibank.[redacted]om	l[redacted]s	0.0.0.0
-/-	2015-02-25 10:04:45	exchange.c[redacted]h	c[redacted]a	0.0.0.0
-/-	2015-01-29 13:54:33	exchange.c[redacted]h	c[redacted]a	0.0.0.0
-/-	2014-11-17 10:29:31	ibank.[redacted]om	J[redacted]	0.0.0.0
Cybercrime group	Date Detected ⇕	Domain	Login	IP address
-/-	2016-05-13 10:22:41	www.m[redacted]b.com	d[redacted]g@s[redacted]ns.com	[redacted]

DATES

Detected
2016-05-13 10:22:41

Compromised
2016-05-12 11:02:58

LOGIN

Login
d[redacted]g@se[redacted]s.com

Password
[redacted]8

VICTIM'S IP

Country
Nigeria

Town
Lagos

Provider
[redacted]

SOURCE Keybase

C&C server
http://expressdelivery.ml/oshe/

IP
104.168.169.140

Country

Town
Tulsa

Provider
-/-

ITU Cyberdrill
Tunisia
23rd - 27th May 2016

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

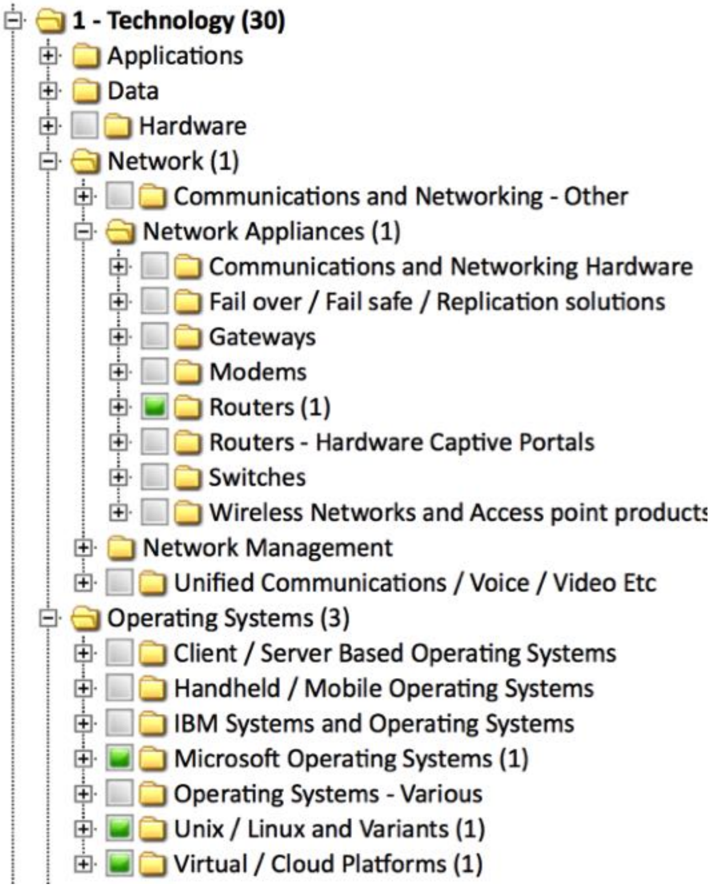
Sample Alternative Marketplaces

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**

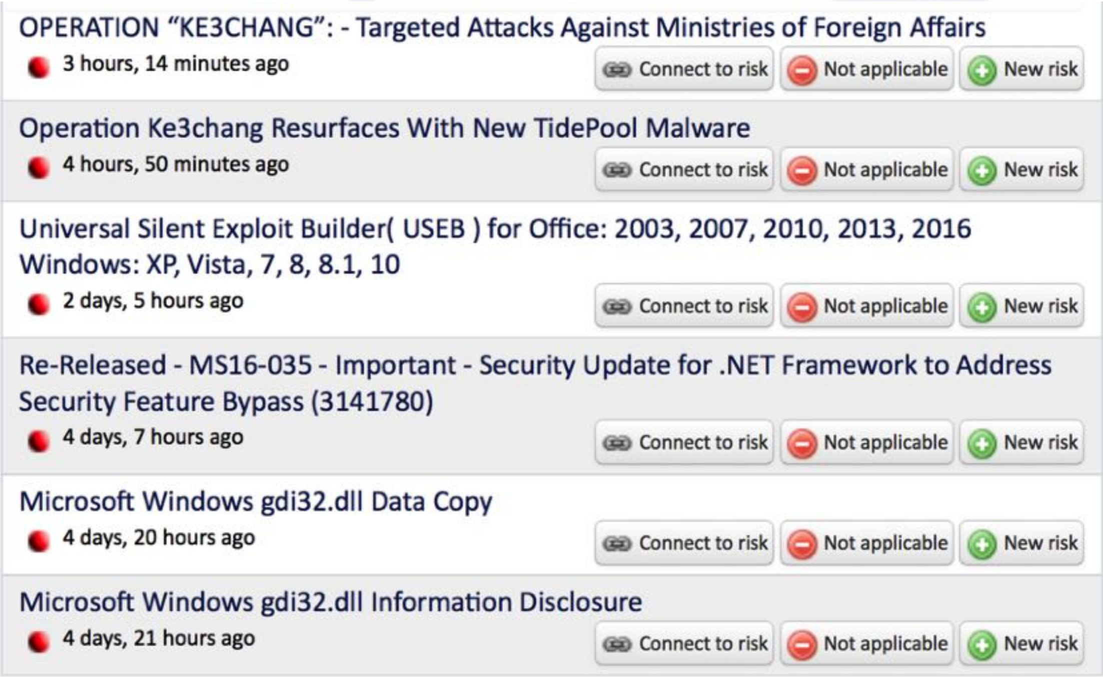
http://www.businessofapps.com/the-ultimate-app-store-list/

CTI Monitoring

Technology Watch



- 1 - Technology (30)
  - Applications
  - Data
  - ☐ Hardware
  - Network (1)
    - ☐ Communications and Networking - Other
    - Network Appliances (1)
      - ☐ Communications and Networking Hardware
      - ☐ Fail over / Fail safe / Replication solutions
      - ☐ Gateways
      - ☐ Modems
      - 🟩 Routers (1)
      - ☐ Routers - Hardware Captive Portals
      - ☐ Switches
      - ☐ Wireless Networks and Access point products
    - Network Management
    - ☐ Unified Communications / Voice / Video Etc
  - Operating Systems (3)
    - ☐ Client / Server Based Operating Systems
    - ☐ Handheld / Mobile Operating Systems
    - ☐ IBM Systems and Operating Systems
    - 🟩 Microsoft Operating Systems (1)
    - ☐ Operating Systems - Various
    - 🟩 Unix / Linux and Variants (1)
    - 🟩 Virtual / Cloud Platforms (1)



OPERATION “KE3CHANG”: - Targeted Attacks Against Ministries of Foreign Affairs

● 3 hours, 14 minutes ago — Connect to risk | Not applicable | New risk

Operation Ke3chang Resurfaces With New TidePool Malware

● 4 hours, 50 minutes ago — Connect to risk | Not applicable | New risk

Universal Silent Exploit Builder(USEB) for Office: 2003, 2007, 2010, 2013, 2016 Windows: XP, Vista, 7, 8, 8.1, 10

● 2 days, 5 hours ago — Connect to risk | Not applicable | New risk

Re-Released - MS16-035 - Important - Security Update for .NET Framework to Address Security Feature Bypass (3141780)

● 4 days, 7 hours ago — Connect to risk | Not applicable | New risk

Microsoft Windows gdi32.dll Data Copy

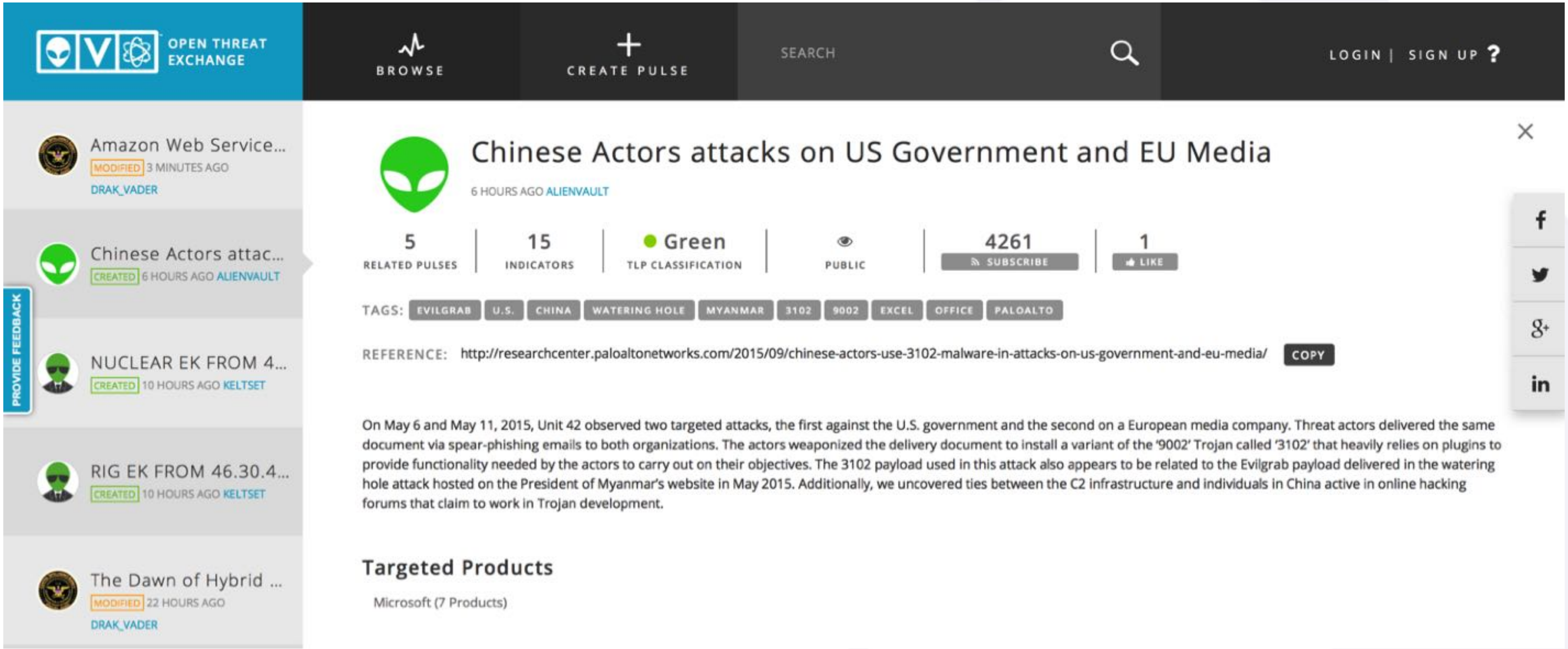
● 4 days, 20 hours ago — Connect to risk | Not applicable | New risk

Microsoft Windows gdi32.dll Information Disclosure

● 4 days, 21 hours ago — Connect to risk | Not applicable | New risk

CTI Monitoring

TTPs and Indicators



Amazon Web Service...
MODIFIED 3 MINUTES AGO
DRAK_VADER

Chinese Actors attac...
CREATED 6 HOURS AGO ALIENVAULT

NUCLEAR EK FROM 4...
CREATED 10 HOURS AGO KELTSET

RIG EK FROM 46.30.4...
CREATED 10 HOURS AGO KELTSET

The Dawn of Hybrid ...
MODIFIED 22 HOURS AGO
DRAK_VADER

Chinese Actors attacks on US Government and EU Media

6 HOURS AGO ALIENVAULT

5	15	● Green		4261	1
RELATED PULSES	INDICATORS	TLP CLASSIFICATION	PUBLIC	SUBSCRIBE	LIKE

TAGS: EVILGRAB U.S. CHINA WATERING HOLE MYANMAR 3102 9002 EXCEL OFFICE PALOALTO

REFERENCE: http://researchcenter.paloaltonetworks.com/2015/09/chinese-actors-use-3102-malware-in-attacks-on-us-government-and-eu-media/

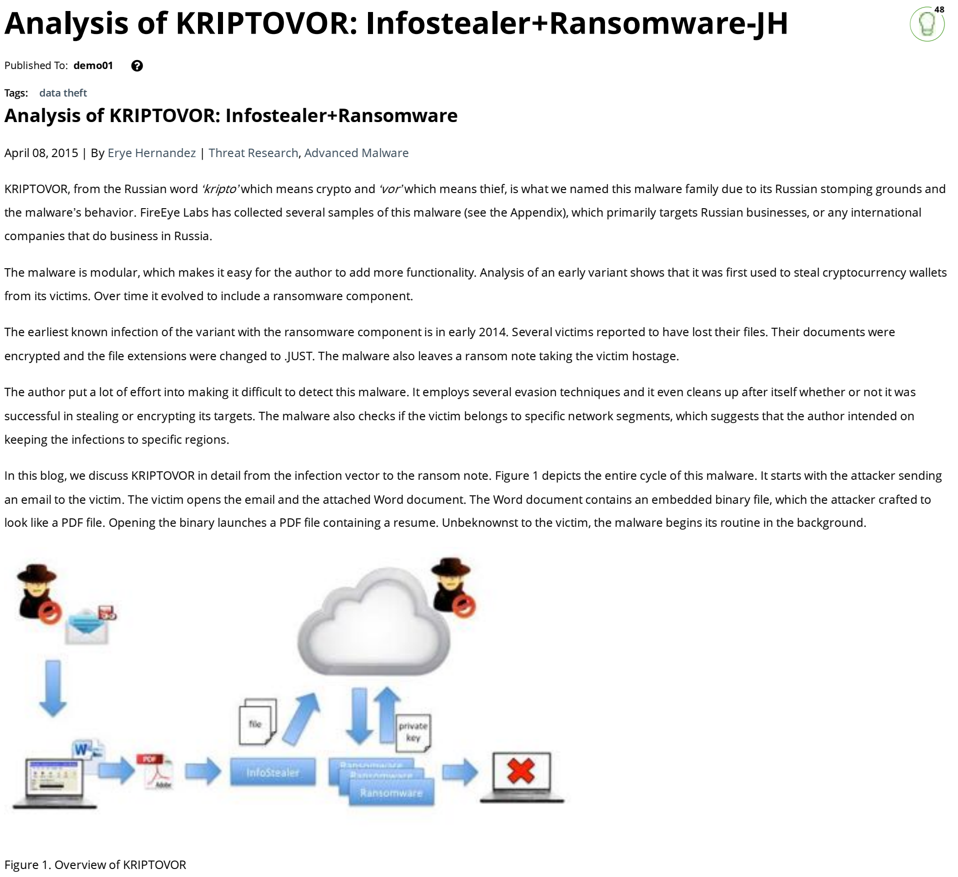
On May 6 and May 11, 2015, Unit 42 observed two targeted attacks, the first against the U.S. government and the second on a European media company. Threat actors delivered the same document via spear-phishing emails to both organizations. The actors weaponized the delivery document to install a variant of the '9002' Trojan called '3102' that heavily relies on plugins to provide functionality needed by the actors to carry out on their objectives. The 3102 payload used in this attack also appears to be related to the Evilgrab payload delivered in the watering hole attack hosted on the President of Myanmar's website in May 2015. Additionally, we uncovered ties between the C2 infrastructure and individuals in China active in online hacking forums that claim to work in Trojan development.

Targeted Products

Microsoft (7 Products)

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.

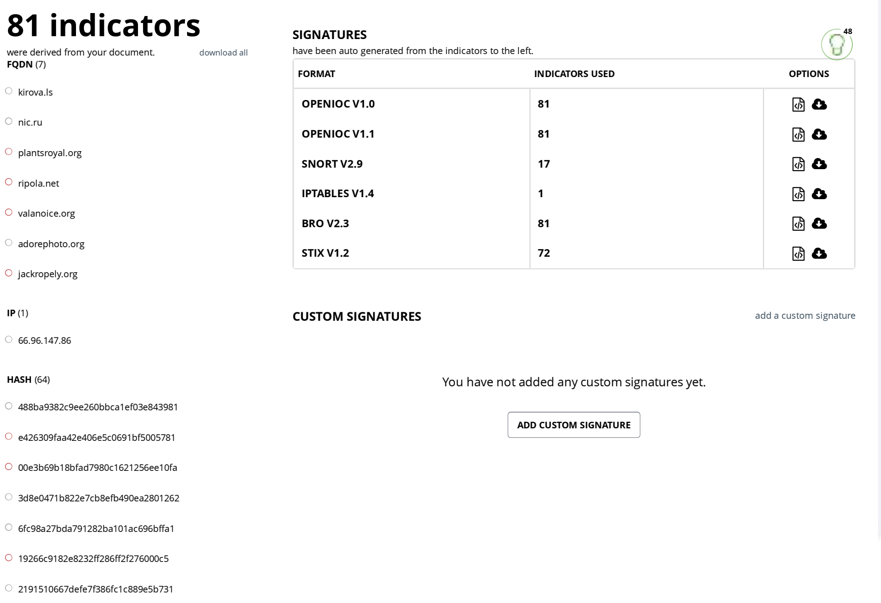
The malware is modular, which makes it easy for the author to add more functionality. Analysis of an early variant shows that it was first used to steal cryptocurrency wallets from its victims. Over time it evolved to include a ransomware component.

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.

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

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

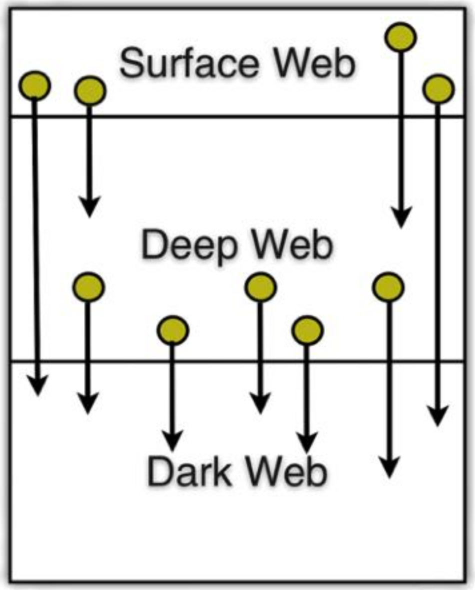
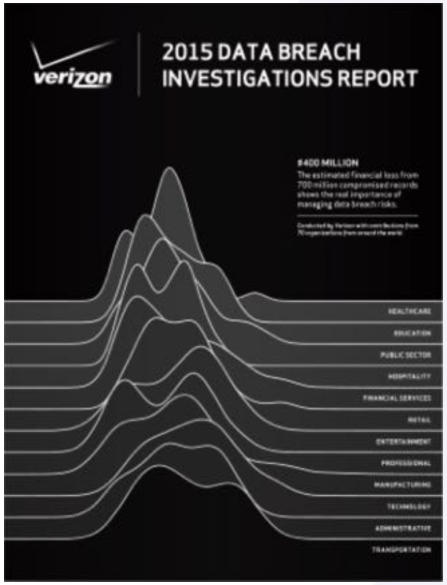


Image Source: RecordedFuture

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



verizon

2015 DATA BREACH INVESTIGATIONS REPORT

$400 MILLION

The estimated financial loss from 700 million compromised records shows the real importance of managing data breach risks.

Conducted by Verizon with contributions from 70 organizations from around the world.

Characteristics of Good Intelligence

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

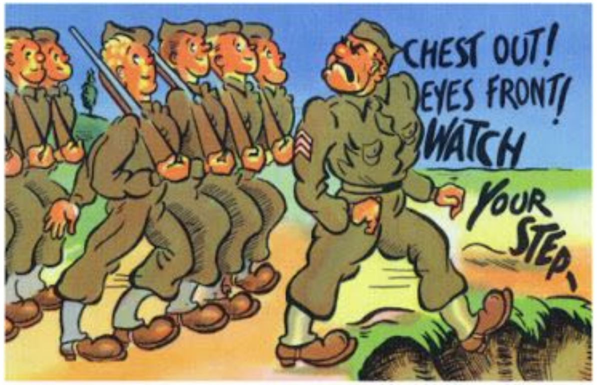
- **Accurate**
  - Accuracy is based on the number of false positive alerts or actions obtained from the threat intelligence. The lower the number of false positive, the more accurate the intelligence is.

- **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.

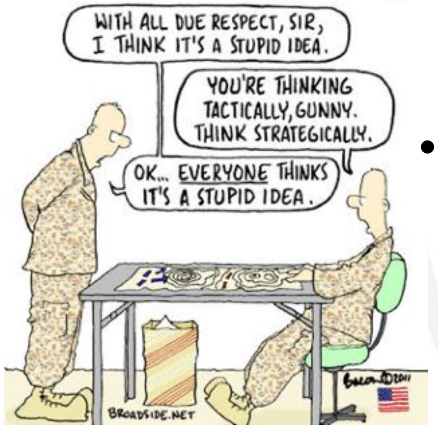
- **Tailored**
  - Different intelligence must be provided to different people to enable them to make the decisions relevant to their role

Types of Intelligence

- Senior Management (Strategy)
  - Policies
  - Coherent strategy to carry out the policy

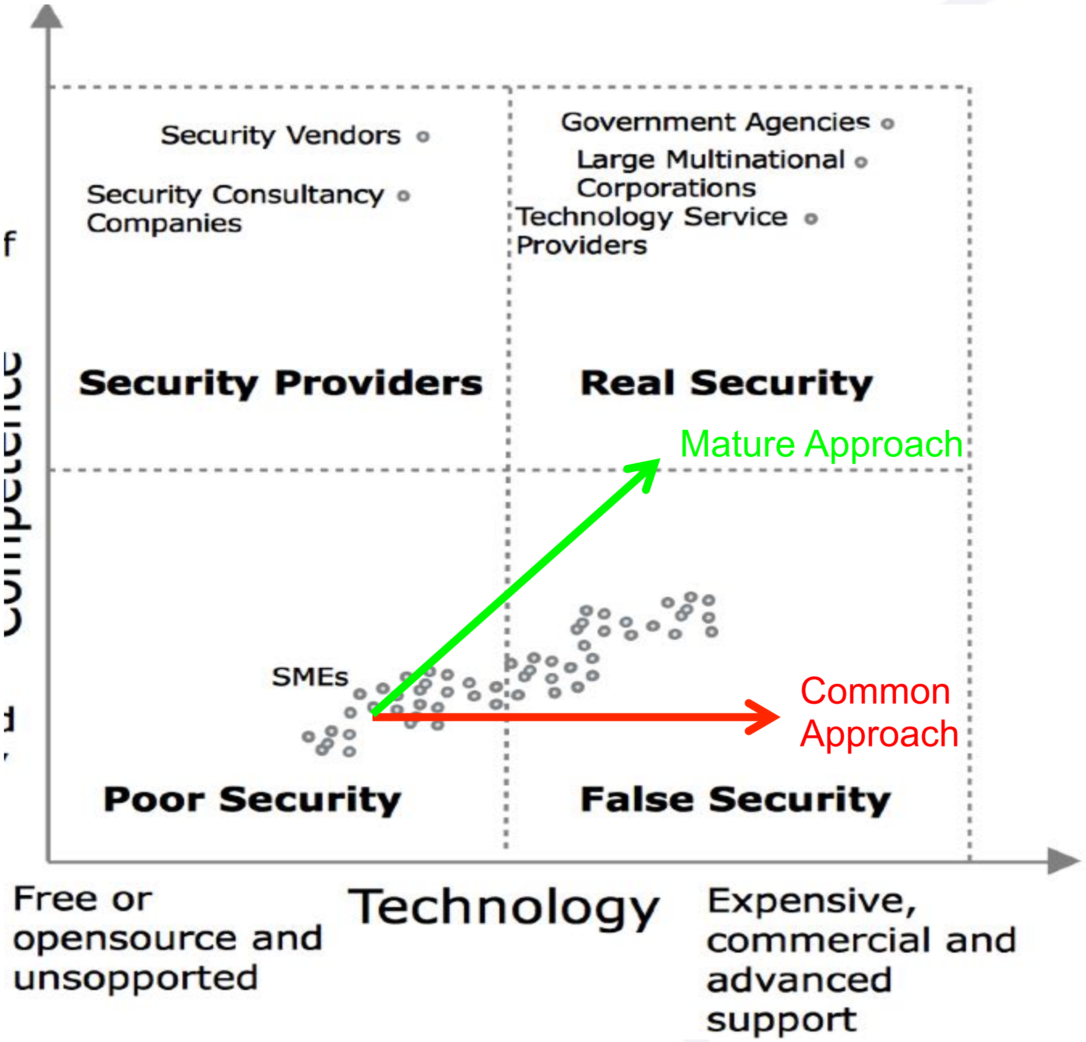


- Security Managers (Operations)
  - Organize resources and determine tactics to meet objectives
  - Take care of competences
  - Prioritize response


WITH ALL DUE RESPECT, SIR, I THINK IT'S A STUPID IDEA.
YOU'RE THINKING TACTICALLY, GUNNY. THINK STRATEGICALLY.
OK... EVERYONE THINKS IT'S A STUPID IDEA.
BROADSIDE.NET
Bacon ©2011

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

Are You Ready for Cyber Threat Intelligence?


Security Vendors
Security Consultancy Companies
Government Agencies
Large Multinational Corporations
Technology Service Providers
Security Providers
Real Security
Mature Approach
SMEs
Common Approach
Poor Security
False Security
Free or opensource and unsopported
Technology
Expensive, commercial and advanced support

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?