Security Intelligence

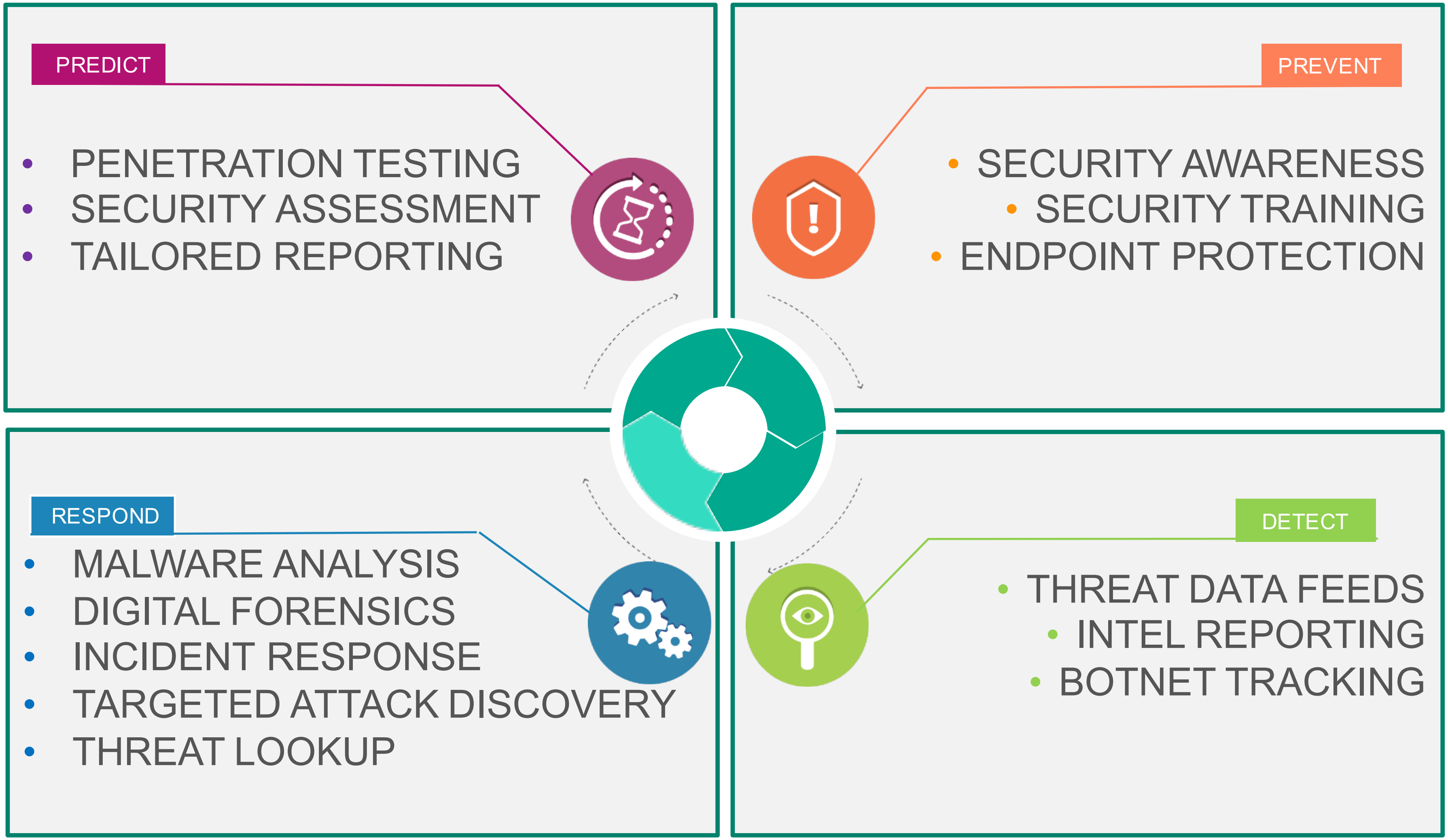
HOW GOVERNMENTAL AGENCIES FIGHT AGAINST CYBERCRIME. BEST PRACTICES AND REAL CASES

Cyberdrill, Quito, Ecuador

MIKHAIL NAGORNY

HEAD OF SECURITY SERVICES, ENTERPRISE BUSINESS

GARTNER'S ADAPTIVE SECURITY CYCLE



PREDICT

- PENETRATION TESTING
- SECURITY ASSESSMENT
- TAILORED REPORTING

PREVENT

- SECURITY AWARENESS
- SECURITY TRAINING
- ENDPOINT PROTECTION

RESPOND

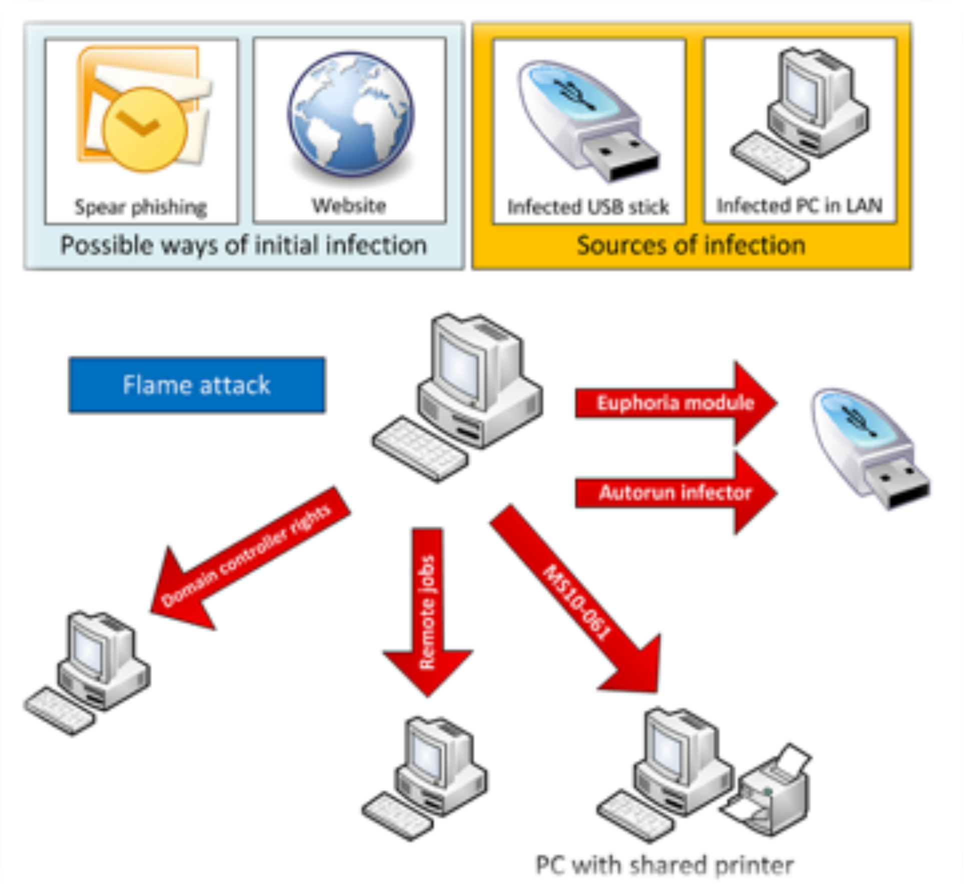
- MALWARE ANALYSIS
- DIGITAL FORENSICS
- INCIDENT RESPONSE
- TARGETED ATTACK DISCOVERY
- THREAT LOOKUP

DETECT

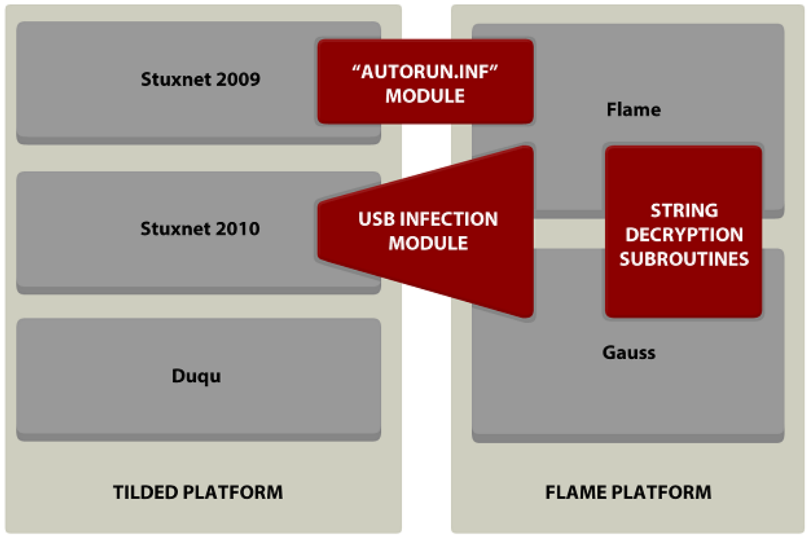
- THREAT DATA FEEDS
- INTEL REPORTING
- BOTNET TRACKING

EUGENE KASPERSKY CALLS FOR CLOSER COLLABORATION BETWEEN GOVERNMENT AND BUSINESS TO COMBAT CYBER THREATS

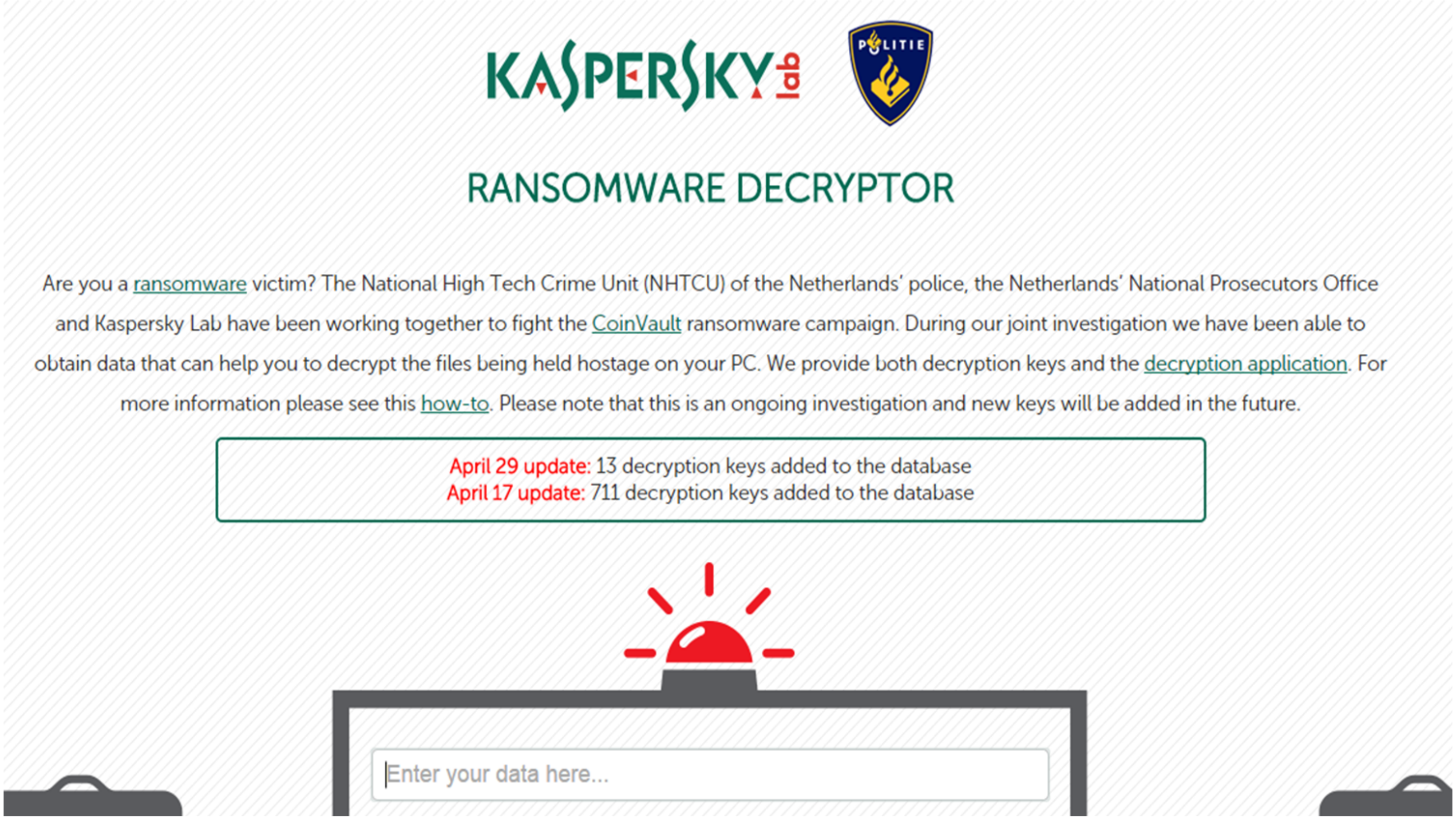
KASPERSKY LAB AND ITU RESEARCH REVEALS NEW ADVANCED CYBER THREAT



The relationship of Stuxnet, Duqu, Flame and Gauss



CRIMINALS BEHIND THE COINVAULT RANSOMWARE ARE BUSTED BY KASPERSKY LAB AND DUTCH POLICE



RANSOMWARE DECRYPTOR

Are you a ransomware victim? The National High Tech Crime Unit (NHTCU) of the Netherlands' police, the Netherlands' National Prosecutors Office and Kaspersky Lab have been working together to fight the CoinVault ransomware campaign. During our joint investigation we have been able to obtain data that can help you to decrypt the files being held hostage on your PC. We provide both decryption keys and the decryption application. For more information please see this how-to. Please note that this is an ongoing investigation and new keys will be added in the future.

April 29 update: 13 decryption keys added to the database
April 17 update: 711 decryption keys added to the database

FIGHTING CYBERCRIME, COLLABORATING WITH AROUND 90 CERTS/CIRTS

ICT Qatar

CERT.GOV.AZ

CERT.br

INTECO

CERT EU

CERT.LV

GovCERT - Austria

Hong Kong CERT

UNAM-CERT

CERT-PY

NCSC

Ecuador CERT

Nippon CSIRT Association

CERT Australia

CERT-BY

Thai CERT

CERT-MX

UK Cert

RIPE NCC

CSIRT Panama

CERT Societe Generale

CIRCL LU

CERT-PL

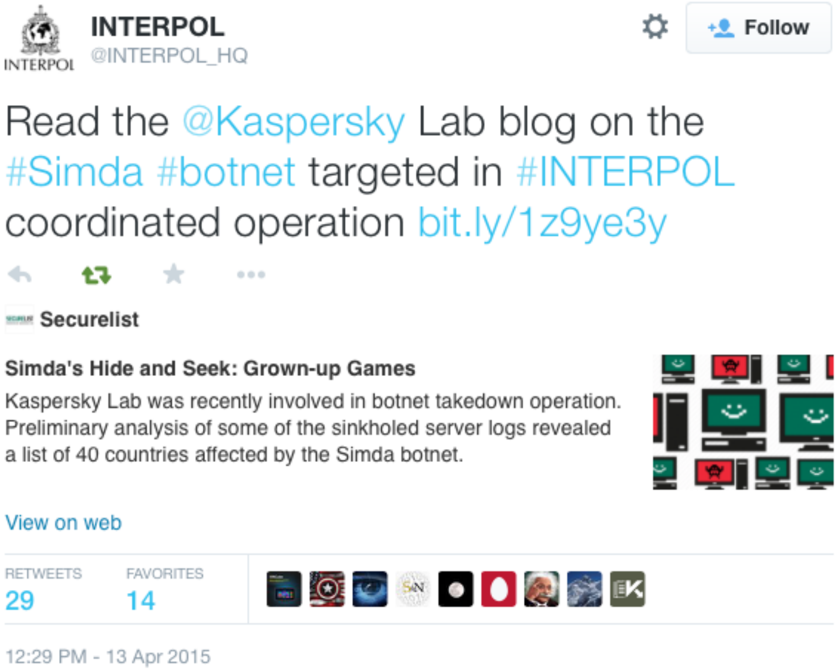
Siemens CERT

NorCERT

Canadian Cyber Incident Response Centre

BEST PRACTICES ABOUT COLLABORATION BETWEEN KASPERSKY GREAT TEAM AND CERTS/CIRTS

- Signing collaboration agreements
- Sharing Intelligence
- Working as a Team
- Law enforcement coordination



INTERPOL @INTERPOL_HQ

Read the @Kaspersky Lab blog on the #Simda #botnet targeted in #INTERPOL coordinated operation bit.ly/1z9ye3y

Securelist

Simda's Hide and Seek: Grown-up Games

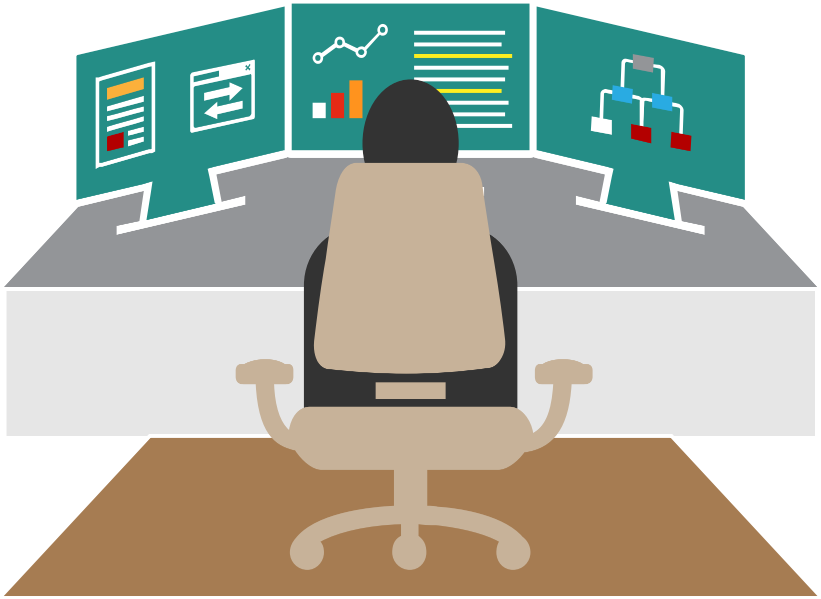
Kaspersky Lab was recently involved in botnet takedown operation. Preliminary analysis of some of the sinkholed server logs revealed a list of 40 countries affected by the Simda botnet.

View on web

RETWEETS 29 FAVORITES 14

12:29 PM - 13 Apr 2015

HOW TO BE READY TO FIGHT AGAINST CYBERCRIME

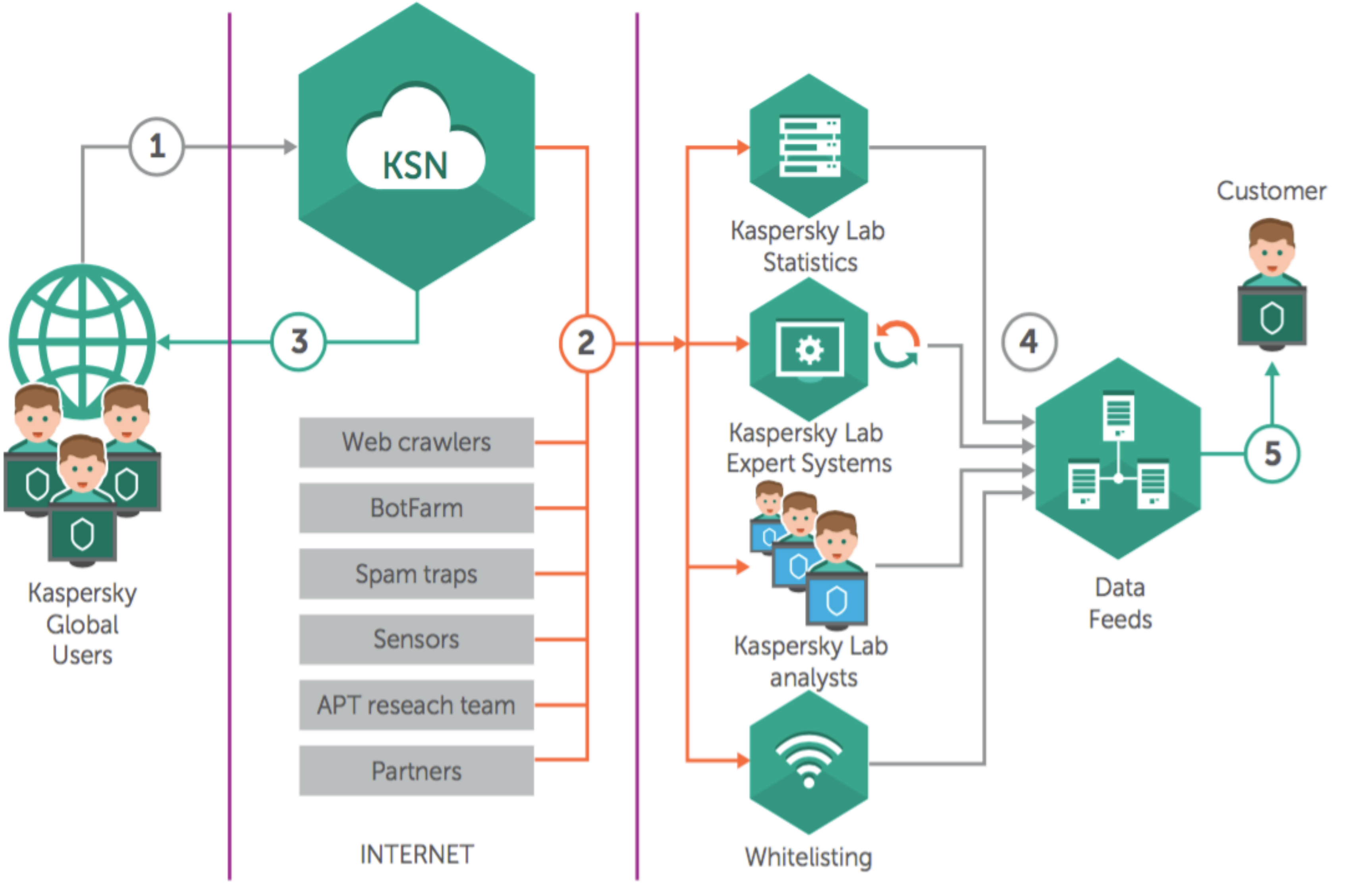


ACTIONABLE THREAT INTELLIGENCE

SOC & INCIDENT RESPONSE TEAMS ARE EXPERIENCED IN DIGITAL FORENSICS AND MALWARE ANALYSIS

ANTI-MALWARE VENDOR SUPPORT IN MALWARE ANALYSIS AND DIGITAL FORENSICS

THREAT INTELLIGENCE FROM DIFFERENT SOURCES BECOMES MORE AND MORE IMPORTANT



THREAT DATA FEEDS

IP REPUTATION

IP Reputation — a set of IP addresses with context covering suspicious and malicious hosts. (JSON)

URL FEEDS

Malicious URLs — a set of URLs covering malicious links and websites. Masked and non-masked records are available. (JSON)

Phishing URLs — a set of URLs covering phishing links and websites. Masked and non-masked records are available. (JSON)

Botnet C&C URLs — a set of URLs covering botnet C&C servers and related malicious objects. (JSON)

HASH FEEDS

Malware Hashes — a set of file hashes and corresponding verdicts covering the most dangerous and prevalent malware delivered through the intelligence of KSN. (JSON)

Mobile Malware Hashes — a set of file hashes for detecting malicious objects that infect mobile Android and iPhone platforms (JSON)

MOBILE THREAT FEEDS

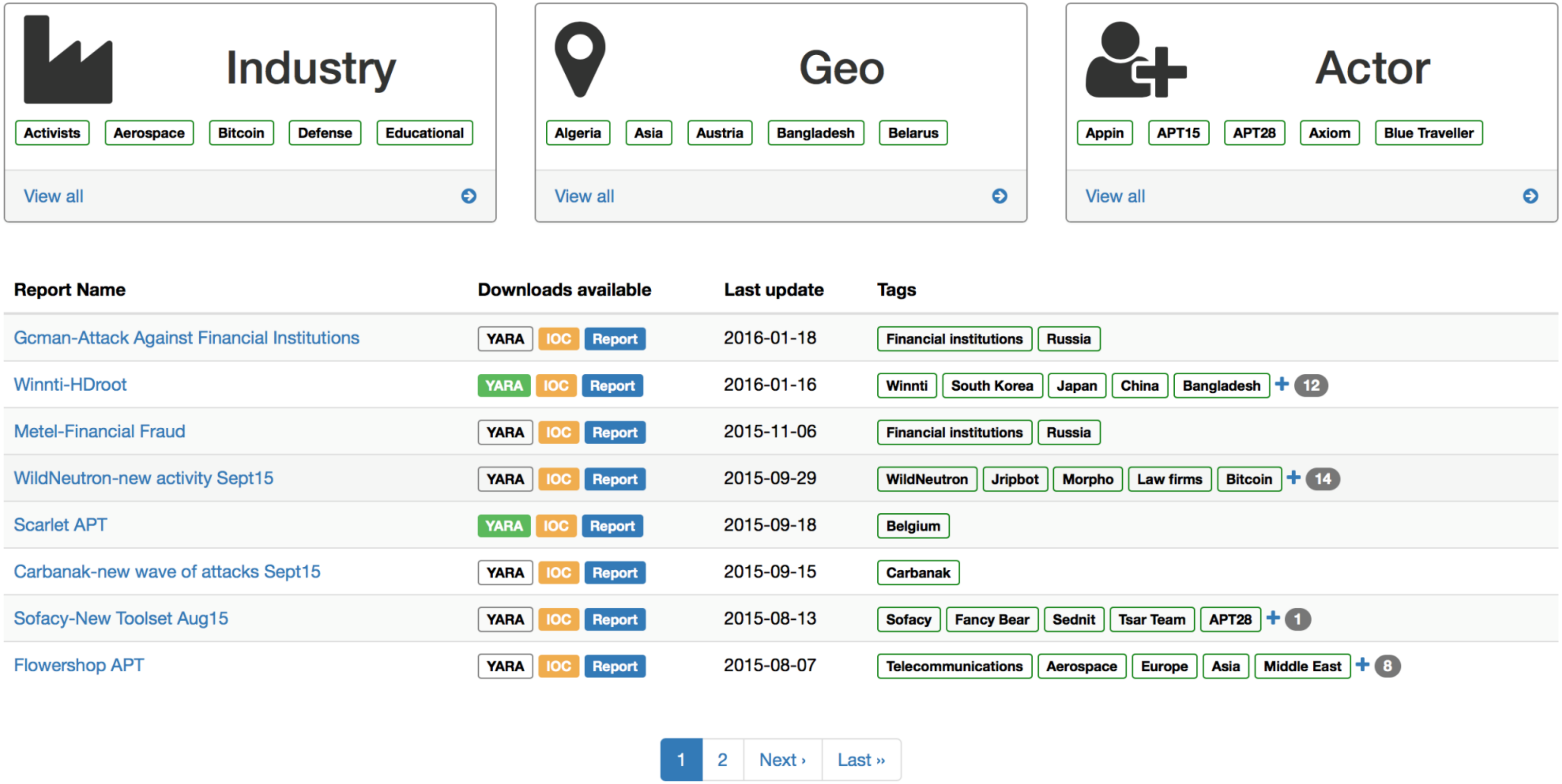
P-SMS Trojan Feed — a set of Trojan hashes with corresponding context for detecting SMS Trojans ringing up premium charges for mobile users as well as enabling an attacker to steal, delete and respond to SMS messages. (JSON)

Mobile Botnet C&C URLs — a set of URLs with context covering mobile botnet C&C servers. (JSON)

APT INTEL REPORTING – DELIVERY

Via APT Intel Portal

> Convenient Search



Industry

Activists | Aerospace | Bitcoin | Defense | Educational

View all

Geo

Algeria | Asia | Austria | Bangladesh | Belarus

View all

Actor

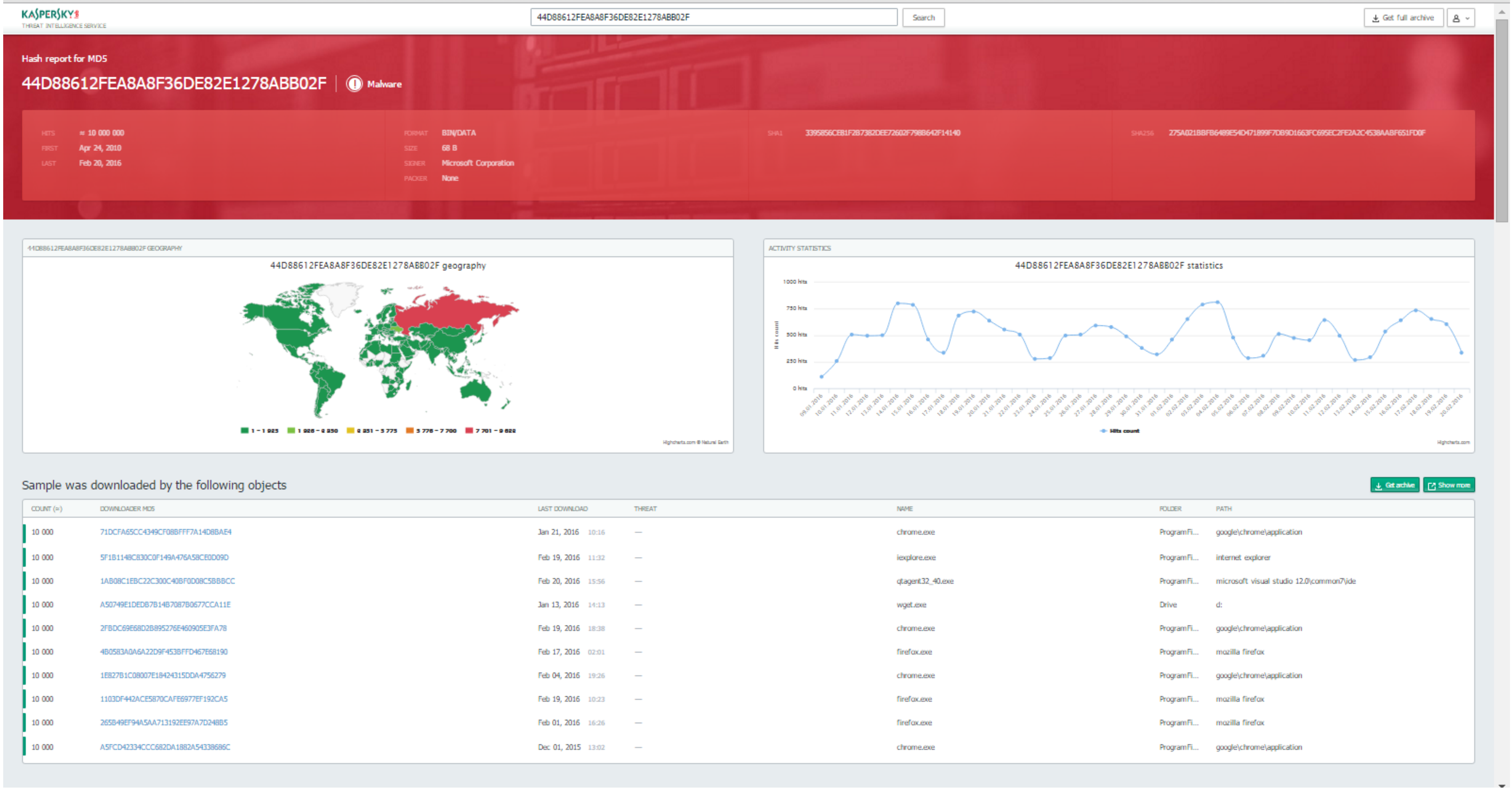
Appin | APT15 | APT28 | Axiom | Blue Traveller

View all

Report Name	Downloads available	Last update	Tags
Gcman-Attack Against Financial Institutions	YARA IOC Report	2016-01-18	Financial institutions, Russia
Winnti-HDroot	YARA IOC Report	2016-01-16	Winnti, South Korea, Japan, China, Bangladesh + 12
Metel-Financial Fraud	YARA IOC Report	2015-11-06	Financial institutions, Russia
WildNeutron-new activity Sept15	YARA IOC Report	2015-09-29	WildNeutron, Jripbot, Morpho, Law firms, Bitcoin + 14
Scarlet APT	YARA IOC Report	2015-09-18	Belgium
Carbanak-new wave of attacks Sept15	YARA IOC Report	2015-09-15	Carbanak
Sofacy-New Toolset Aug15	YARA IOC Report	2015-08-13	Sofacy, Fancy Bear, Sednit, Tsar Team, APT28 + 1
Flowershop APT	YARA IOC Report	2015-08-07	Telecommunications, Aerospace, Europe, Asia, Middle East + 8

1 | 2 | Next › | Last »

THREAT LOOKUP & HUNTING SERVICES



Hash report for MD5

44D88612FEA8A8F36DE82E1278ABB02F | Malware

HITS	≈ 10 000 000	FORMAT	BIN/DATA	SHA1	3395856CE81F2B7382DEE72602F798B642F14140	SHA256	275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F
FIRST	Apr 24, 2010	SIZE	68 B				
LAST	Feb 20, 2016	SIGNER	Microsoft Corporation				
		PACKER	None				

44D88612FEA8A8F36DE82E1278ABB02F GEOGRAPHY

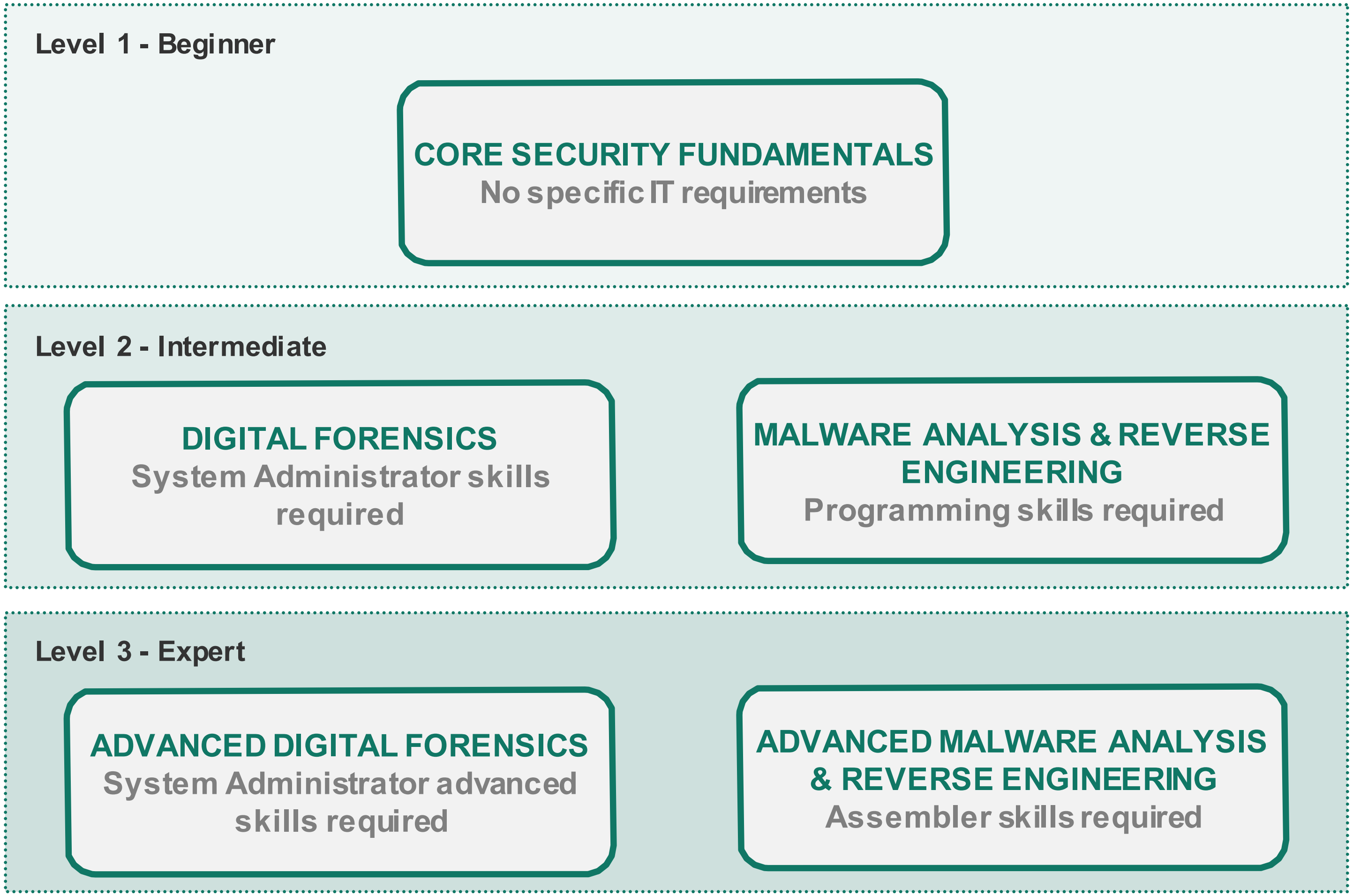
44D88612FEA8A8F36DE82E1278ABB02F geography
🟩 1 – 1 925
🟩 1 926 – 3 850
🟨 3 851 – 5 775
🟧 5 776 – 7 700
🟥 7 701 – 9 625
Highcharts.com © Natural Earth

ACTIVITY STATISTICS

Sample was downloaded by the following objects

COUNT (≈)	DOWNLOADER MD5	LAST DOWNLOAD	THREAT	NAME	FOLDER	PATH
10 000	71DCFA65CC4349CF08BFFF7A14D8BAE4	Jan 21, 2016 10:16	—	chrome.exe	ProgramFi...	google\chrome\application
10 000	5F1B1148C830C0F149A476A58CE0D09D	Feb 19, 2016 11:32	—	iexplore.exe	ProgramFi...	internet explorer
10 000	1AB08C1EBC22C300C40BF0D08C5BBBCC	Feb 20, 2016 15:56	—	qtagent32_40.exe	ProgramFi...	microsoft visual studio 12.0\common7\ide
10 000	A50749E1DEDB7B14B7087B0677CCA11E	Jan 13, 2016 14:13	—	wget.exe	Drive	d:
10 000	2FBDC69E68D2B895276E460905E3FA78	Feb 19, 2016 18:38	—	chrome.exe	ProgramFi...	google\chrome\application
10 000	4B0583A0A6A22D9F453BFFD467E68190	Feb 17, 2016 02:01	—	firefox.exe	ProgramFi...	mozilla firefox
10 000	1E827B1C08007E18424315DDA4756279	Feb 04, 2016 19:26	—	chrome.exe	ProgramFi...	google\chrome\application
10 000	1103DF442ACE5870CAFE6977EF192CA5	Feb 19, 2016 10:23	—	firefox.exe	ProgramFi...	mozilla firefox
10 000	265B49EF94A5AA713192EE97A7D248B5	Feb 01, 2016 16:26	—	firefox.exe	ProgramFi...	mozilla firefox
10 000	A5FCD42334CCC682DA1882A54338686C	Dec 01, 2015 13:02	—	chrome.exe	ProgramFi...	google\chrome\application

WHY SECURITY TRAINING AND SECURITY AWARENESS IS IMPORTANT. BEST PRACTICES FROM KASPERSKY LAB



Level 1 - Beginner

CORE SECURITY FUNDAMENTALS
No specific IT requirements

Level 2 - Intermediate

DIGITAL FORENSICS
System Administrator skills required

MALWARE ANALYSIS & REVERSE ENGINEERING
Programming skills required

Level 3 - Expert

ADVANCED DIGITAL FORENSICS
System Administrator advanced skills required

ADVANCED MALWARE ANALYSIS & REVERSE ENGINEERING
Assembler skills required

LEVEL 1 CORE SECURITY FUNDAMENTALS

COURSE DESCRIPTION	DURATION	COURSE AUDIENCE	SKILLS GAINED
Level 1 – core security fundamentals **TOPICS:** • Cyberthreats & Underground market overview • Spam & Phishing, Email security • Cyber threat types & protection technologies • Advanced persistent threats • Investigation basics using public web tools • Securing your workplace	2 days	Broad range of enterprise employees	• understand the threat landscape • be able to use your PC more safely • recognize different types of attacks • classify cyber weapons and malware and understand their goals and working principles • analyze phishing mails • recognize infected or faked websites

LEVEL 2 DIGITAL FORENSICS

COURSE DESCRIPTION	DURATION	COURSE AUDIENCE	SKILLS GAINED
Level 2 – digital forensics **TOPICS:** • Introduction to Digital Forensics • Live Response and Evidence Acquisition • Windows Registry Internals • Windows artifacts analysis • Browsers Forensics • Email analysis	5 days	Employees in the areas of incident response and digital forensics	• build the Digital Forensics lab • collect digital evidence and deal with it properly • reconstruct an incident and use time stamps • find traces of intrusion on investigation artifacts in Windows OS • find and analyze browser and email history • be able be apply with the tools and instruments of digital forensics

LEVEL 3 ADVANCED DIGITAL FORENSICS

COURSE DESCRIPTION	DURATION	COURSE AUDIENCE	SKILLS GAINED
Level 3 – advanced digital forensics **TOPICS:** • Deep Windows Forensics • Data recovery • Network and Cloud forensics • Memory forensics • Timeline analysis • Real world targeted attack forensics practice	5 days	Employees in the areas of incident response and digital forensics	• Be able to perform deep file system analysis • Be able to recover deleted files • Be able to analyze network traffic • Reveal malicious activities from Memory dumps • Reconstruct the incident timeline

LEVEL 2 MALWARE ANALYSIS & RE

COURSE DESCRIPTION	DURATION	COURSE AUDIENCE	SKILLS GAINED
Level 2 – malware analysis &re **TOPICS:** • Malware Analysis & Reverse Engineering goals and techniques • Windows internals, executable files, x86 assembler • Basic Static analysis techniques (strings extracting, import analysis, PE entry points at a glance, automatic unpacking, etc.) • Basic Dynamic analysis techniques (debugging, monitoring tools, traffic interception, etc.) • .NET, Visual basic, Win64 files analysis • Script and non-PE analysis techniques (Batch files; Autoit; Python; Jscript; JavaScript; VBS)	5 days	Employees in the areas of malware analysis and reverse engineering	• Build a secure environment for malware analysis: deploy sandbox and all needed tools • Understand principles of Windows program execution • Unpack, debug and analyze malicious object, identify its functions • Detect malicious sites through script malware analysis • Conduct express malware analysis

LEVEL 3 ADVANCED MALWARE ANALYSIS & RE

COURSE DESCRIPTION	DURATION	COURSE AUDIENCE	SKILLS GAINED
Level 3 – advanced ma&re **TOPICS:** • Malware Analysis & Reverse Engineering goals and technics • Advanced Static & dynamic analysis techniques (manual unpacking) • Deobfuscation techniques • Rootkit & Bootkit analysis • Exploits analysis (.pdf, .doc, .swf, etc.) • Non-Windows Malware Analysis (Android, Linux, Mac OS)	5 days	Employees in the areas of malware analysis and reverse engineering	• use the world best practices in reverse engineering • recognize anti-reverse engineering technics (obfuscation, anti-debugging) • apply advanced malware analysis for Rootkits/Bootkits • analyze exploit shellcode, embedded in different file types • analyze non-Windows malware

CYBER SECURITY TRAINING – CASE STUDIES

CUSTOMER CASE STUDY

KASPERSKY lab

DEVELOPING A NATIONAL RESPONSE TO CYBER CRIME

CITY of LONDON POLICE

CITY OF LONDON POLICE

- Kaspersky Lab has delivered several courses in the areas of Digital Forensics and Malware Analysis
- Public reference is available and you can request an official pdf approved by COLP management
- You can find more in public press releases:
  - http://www.kaspersky.com/about/news/virus/2014/City-of-London-Police-and-Kaspersky-Lab-lead-the-way-in-combatting-fraud
  - http://www.computerworlduk.com/news/security/3539039/city-of-london-police-brings-in-kaspersky-to-train-officers-to-tackle-cybercrime/

HOW TO RESPOND THE CYBERCRIME AND CYBER THREATS – MALWARE ANALYSIS.

Malware Analysis offers a complete understanding of the behavior and objectives of specific malware files that are targeting your organization.

Kaspersky Lab’s experts carry out a thorough analysis of the malware sample provided by your organization, creating a detailed report that includes:

- ✓ **Sample properties**: A short description of the sample and a verdict on its malware classification.
- ✓ **Detailed malware description**: An in-depth analysis of your malware sample’s functions, threat behavior and objectives - including IOCs - arming you with the information required to neutralize its activities.
- ✓ **Remediation scenario**: The report will suggest steps to fully secure your organization against this type of threat.

KASPERSKY lab

LET'S TALK?

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com