DRS
HACKER Threat Intelligence SECURITY

EXECUTIVE SUMMARY
XXXX

BSI Ranking:

Incident Response Hierarchy:

M

XXXX ➜

Pyramid levels (top to bottom): ACT, TRACK, HUNT, BEHAVIORS, THREATS, TRIAGE, DETECTION, TELEMETRY, INVENTORY
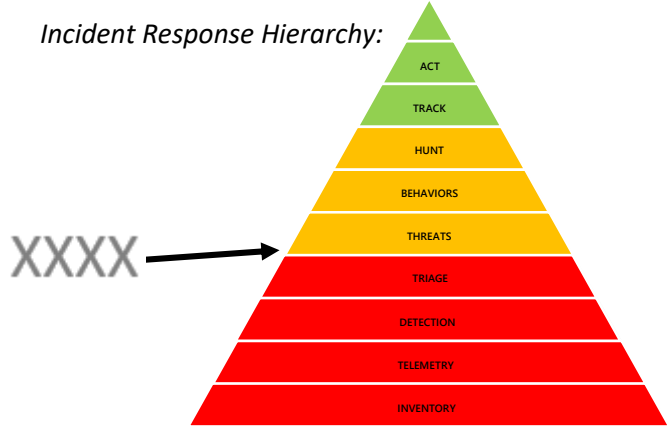
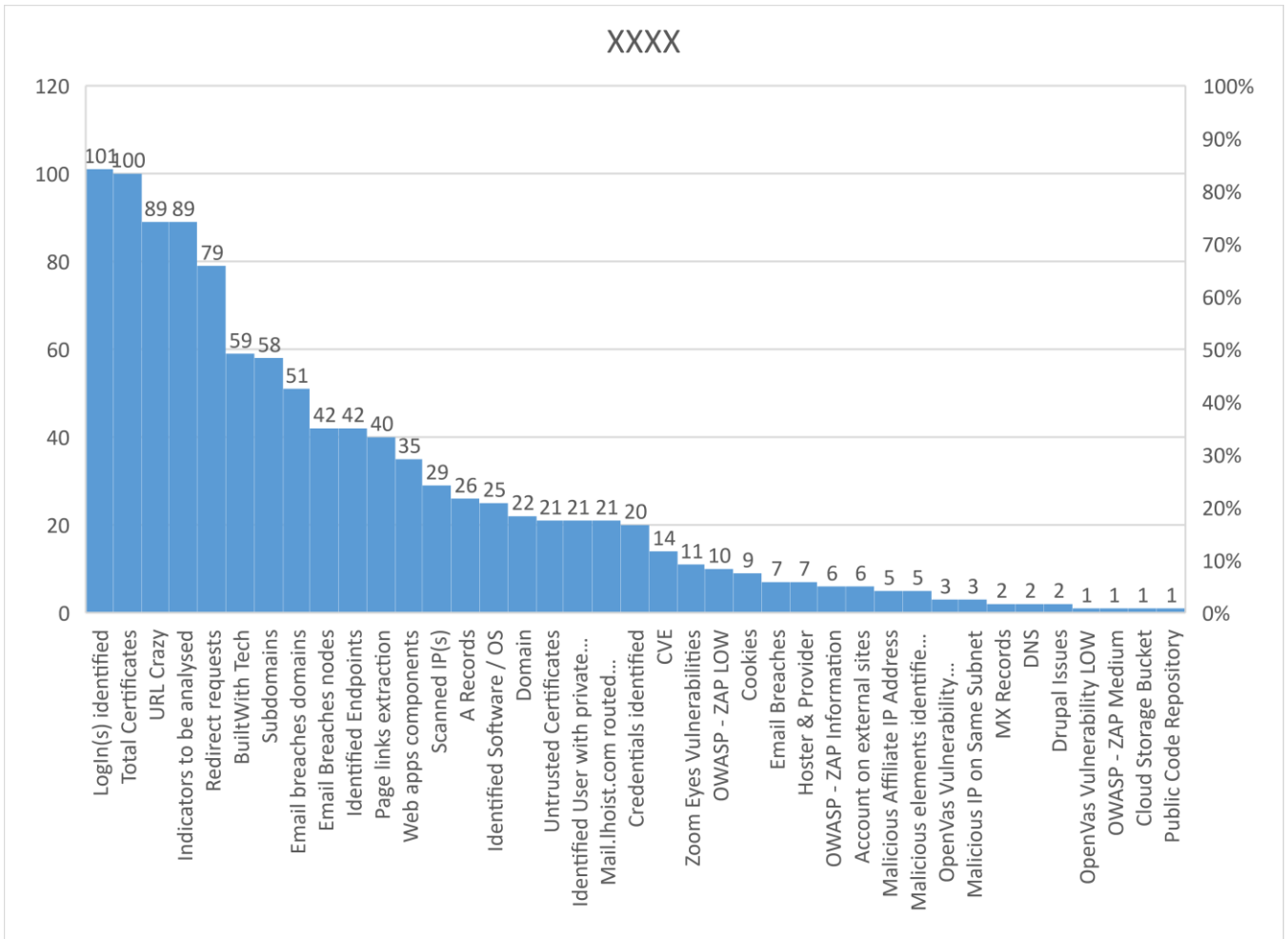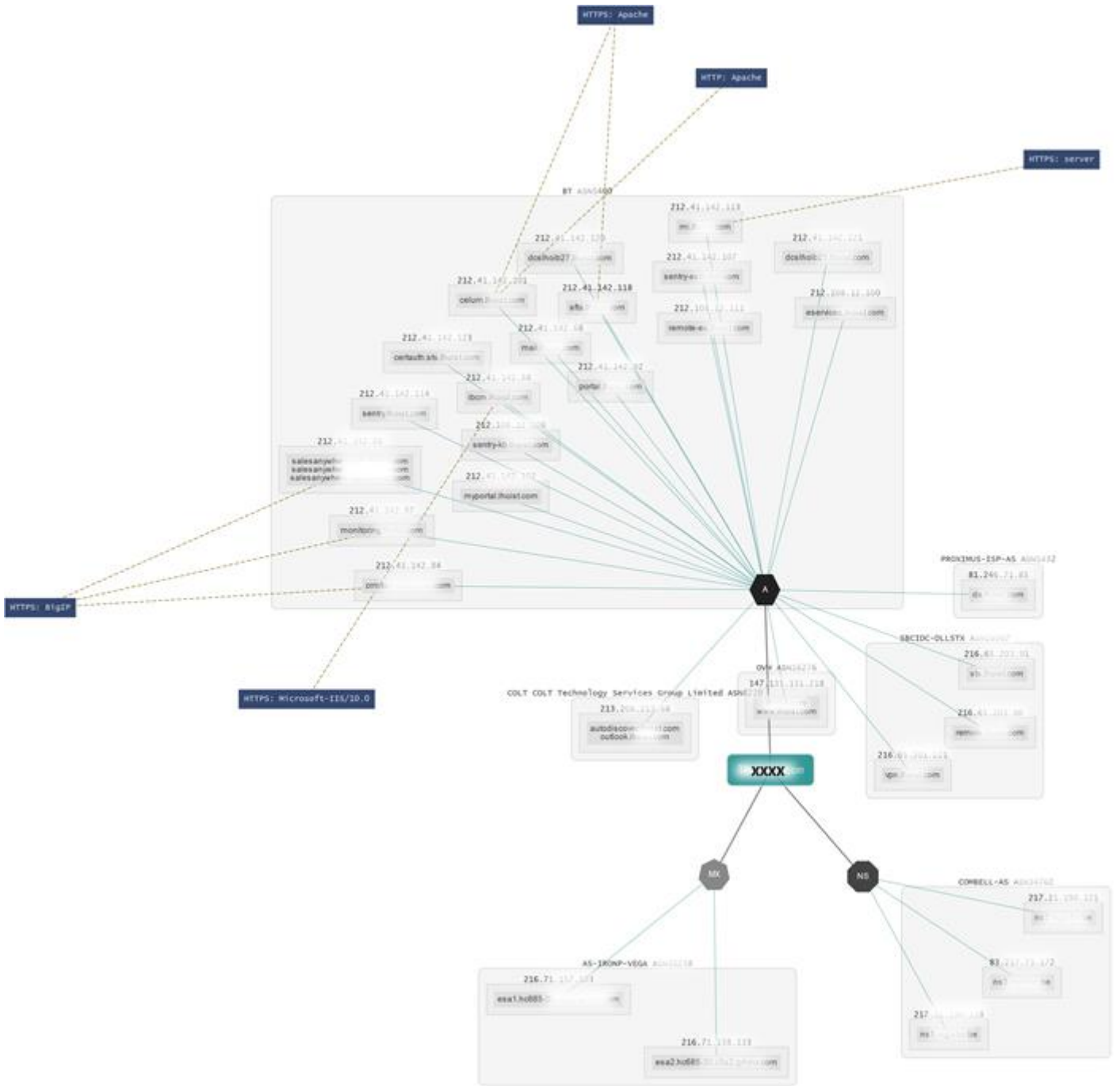|				
A - D	100% - 88,6%		Can you collaborate with trusted partners to disrupt adversary campaigns?	"During incident response, I operate at the same tempo as the adversary to protect my business assets."
		ACT	Can you deploy proven countermeasures to evict and recover?	
		TRACK	During an intrusion, can you observe adversary activity in real time?	
E - M	**84,8% - 54,4%**	HUNT	Can you detect an adversary that is already embedded?	***"When my red team emulates a real-world adversary, I detect their intrusion at multiple points along the kill chain."***
		BEHAVIORS	Can you detect adversary activity within your environment?	
		THREATS	*Who are your adversaries? What are their capabilities?*	
N - Z	50,6% - 5%	TRIAGE	Can you accurately classify detection results?	"I detect hygiene issues and operator activity that does not follow best practices."
		DETECTION	Can you detect unauthorized activity?	
		TELEMETRY	Do you have visibility across your assets?	
		INVENTORY	Can you name the assets you are defending?	

A	100		N	50,6
B	96,2		O	46,8
C	92,4		P	43,0
D	88,6		Q	39,2
E	84,8		R	35,4
F	81,0		S	31,6
G	77,2		T	27,8
H	73,4		U	24,0
I	69,6		V	20,2
J	65,8		W	16,4
K	62,0		X	12,6
L	58,2		Y	8,8
M	**54,4**		Z	5,0

XXXX

Chart values (left to right): 101, 100, 89, 89, 79, 59, 58, 51, 42, 42, 40, 35, 29, 26, 25, 22, 21, 21, 21, 20, 14, 11, 10, 9, 7, 7, 6, 6, 5, 5, 3, 3, 2, 2, 2, 1, 1, 1, 1

Categories: LogIn(s) identified, Total Certificates, URL Crazy, Indicators to be analysed, Redirect requests, BuiltWith Tech, Subdomains, Email breaches domains, Email Breaches nodes, Identified Endpoints, Page links extraction, Web apps components, Scanned IP(s), A Records, Identified Software / OS, Domain, Untrusted Certificates, Identified User with private..., Mail.lhoist.com routed..., Credentials identified, CVE, Zoom Eyes Vulnerabilities, OWASP - ZAP LOW, Cookies, Email Breaches, Hoster & Provider, OWASP - ZAP Information, Account on external sites, Malicious Affiliate IP Address, Malicious elements identifie..., OpenVas Vulnerability..., Malicious IP on Same Subnet, MX Records, DNS, Drupal Issues, OpenVas Vulnerability LOW, OWASP - ZAP Medium, Cloud Storage Bucket, Public Code Repository

All elements are suported by 4.677 proof pages

DRS
HACKER Threat Intelligence SECURITY

XXXX Domain Profiler

(Details in the Annexe)

Strip down XXXX Domain Profile

Hash	IPv4 Address	NS Record
Email Address	Document	Tracking Code
Domain	WHOIS Postal Code	BuiltWith Relationship
WHOIS State	WHOIS Street	BuiltWith Technology
Tag	Document Snapshot	WHOIS Registrar
Website	WHOIS City	DNS Name
Phrase	pt.whoisExpiresAt	WHOIS Country
Phone Number	Person	Location
Company	WHOIS Organization	Node
WHOIS Email	SSL Certificate	Netblock
MX Record	WHOIS Registered	Image
pt.whoisRegistryUpdatedAt	maltego ASNumber	Snapshot
WHOIS Nameserver	WHOIS Name	URL
SSL Certificate	Website Title	

4.326 Entities   719 Nodes   7.416 Links   2.926 Edges

(Details in the Annexe)

DRS
HACKER Threat Intelligence SECURITY

L1 Hashes XXXX Domain Profile (T.B.A. & Seen with great Care)

(Details in the Annexe)

L1 Hashes XXXX Domain Profile (T.B.A. & Seen with great Care)

DRS
HACKER Threat Intelligence SECURITY
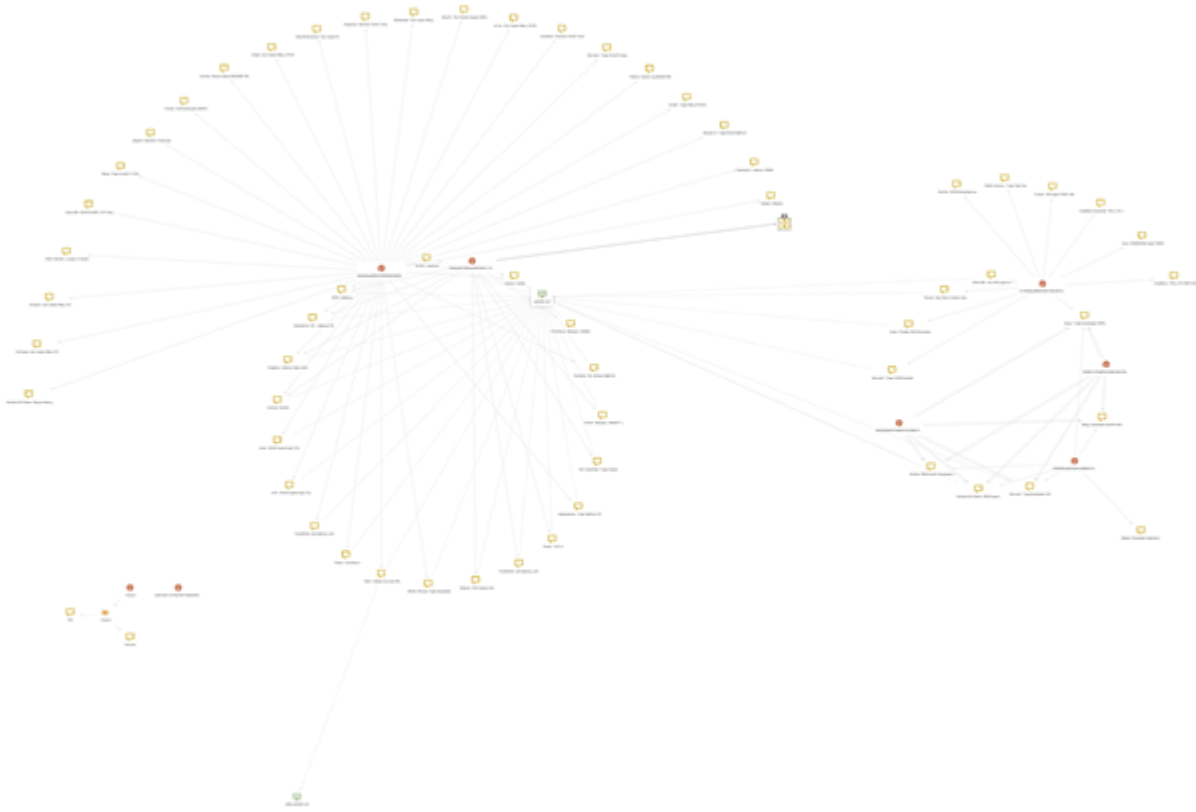
SF - STATUS XXXX Domain Profile

Type	Unique Data Elements	Total Data Elements	Last Data Element
Account on External Site	1554	1554	2020-08-20 05:18:14
Affiliate - Company Name	33	150	2020-08-20 03:57:47
Affiliate - Domain Name	112	160	2020-08-20 03:57:47
Affiliate - Domain Whois	83	96	2020-08-20 03:57:47
Affiliate - Email Address	43	160	2020-08-20 03:57:48
Affiliate - IP Address	89	89	2020-08-20 03:04:50
Affiliate - Internet Name	223	257	2020-08-20 03:57:43
Affiliate - Internet Name - Unresolved	3	5	2020-08-20 03:57:51
Affiliate - Web Content	27	143	2020-08-20 03:07:02
Affiliate Description - Abstract	3	3	2020-08-20 02:24:48
Affiliate Description - Category	22	22	2020-08-20 02:27:37
BGP AS Membership	7	9	2020-08-20 02:58:36
BGP AS Peer	1859	3410	2020-08-20 02:58:39
Bitcoin Address	1	1	2020-08-20 04:22:19
Bitcoin Balance	1	1	2020-08-20 04:22:19
Blacklisted Affiliate IP Address	1	1	2020-08-20 02:43:35
Cloud Storage Bucket	1	1	2020-08-19 16:44:07
Co-Hosted Site	146	147	2020-08-20 03:07:02
Co-Hosted Site - Domain Name	20	25	2020-08-20 03:07:06
Co-Hosted Site - Domain Whois	12	13	2020-08-20 03:06:34
Company Name	22	45	2020-08-20 05:17:39
Cookies	9	10	2020-08-20 03:28:57
Country Name	30	194	2020-08-20 03:57:48
DNS SPF Record	2	4	2020-08-20 03:57:43
DNS SRV Record	4	7	2020-08-20 03:14:10
DNS TXT Record	6	8	2020-08-20 03:57:51
Domain Name	1	12	2020-08-20 02:58:56
Email Address	50	56	2020-08-20 04:36:09
Email Gateway (DNS 'MX' Records)	2	2	2020-08-20 03:57:10
Externally Hosted Javascript	1	139	2020-08-20 02:20:32
HTTP Headers	209	211	2020-08-20 05:28:45
HTTP Status Code	4	211	2020-08-20 05:28:45
Hacked Email Address	60	60	2020-08-20 04:36:34
Hash	215	386	2020-08-20 05:28:48
Historic Interesting File	20	20	2020-08-20 05:18:36
Hosting Provider	1	1	2020-08-20 02:45:45
Human Name	34	108	2020-08-20 05:28:48
IBAN Number	2	2	2020-08-20 01:56:33
IP Address	30	49	2020-08-20 03:55:02
IPv6 Address	1	1	2020-08-20 02:36:15
Interesting File	31	31	2020-08-20 05:18:34
Internet Name	45	670	2020-08-20 05:28:47
Internet Name - Unresolved	6	30	2020-08-20 03:33:43
Leak Site URL	11	11	2020-08-20 04:20:13

Linked URL - External	108	108	2020-08-20 05:18:38
Linked URL - Internal	3008	3013	2020-08-20 05:28:46
Malicious Affiliate	9	9	2020-08-20 03:57:51
Malicious Affiliate IP Address	5	5	2020-08-19 17:30:47
Malicious Co-Hosted Site	13	13	2020-08-20 02:29:57
Malicious IP Address	4	4	2020-08-20 02:30:01
Malicious IP on Same Subnet	19	19	2020-08-20 02:58:21
Name Server (DNS 'NS' Records)	3	3	2020-08-20 03:57:36
Netblock Membership	8	29	2020-08-20 03:56:29
Non-Standard HTTP Header	15	992	2020-08-20 05:28:45
Open TCP Port	24	38	2020-08-20 03:47:23
PGP Public Key	14	18	2020-08-20 04:58:59
Phone Number	17	20	2020-08-20 01:56:44
Physical Address	12	24	2020-08-20 04:58:39
Physical Coordinates	4	5	2020-08-20 04:58:38
Physical Location	6	7	2020-08-20 04:58:59
Public Code Repository	12	12	2020-08-20 04:28:20
Raw DNS Records	8	8	2020-08-20 03:57:51
Raw Data from RIRs/APIs	213	252	2020-08-20 04:58:59
Raw File Meta Data	696	721	2020-08-20 05:28:42
SSL Certificate - Issued by	5	40	2020-08-20 03:47:23
SSL Certificate - Issued to	9	40	2020-08-20 03:47:23
SSL Certificate - Raw Data	58	132	2020-08-20 03:47:23
SSL Certificate Host Mismatch	2	7	2020-08-20 03:09:01
Search Engine's Web Content	16	16	2020-08-20 04:29:19
Similar Domain	21	21	2020-08-19 17:00:22
Similar Domain - Whois	1	1	2020-08-19 16:53:21
Social Media Presence	10	10	2020-08-20 04:58:59
Software Used	43	97	2020-08-20 05:27:02
Telecommunications Provider	2	2	2020-08-19 21:43:01
URL (Accepts Passwords)	2	2	2020-08-20 03:17:10
URL (Form)	146	146	2020-08-20 05:28:45
URL (Purely Static)	39	39	2020-08-20 03:23:07
URL (Uses Javascript)	164	164	2020-08-20 05:28:45
URL (Uses a Web Framework)	2	166	2020-08-20 05:28:45
Username	112	113	2020-08-20 05:28:48
Web Analytics	3	428	2020-08-20 05:28:45
Web Content	178	207	2020-08-20 05:28:47
Web Content Type	8	203	2020-08-20 05:28:45
Web Server	6	201	2020-08-20 05:28:45
Web Technology	1	1	2020-08-20 03:28:57
Wikipedia Page Edit	157	157	2020-08-20 04:24:21

(Details in the Annexe)

XXXX PWND e-mails
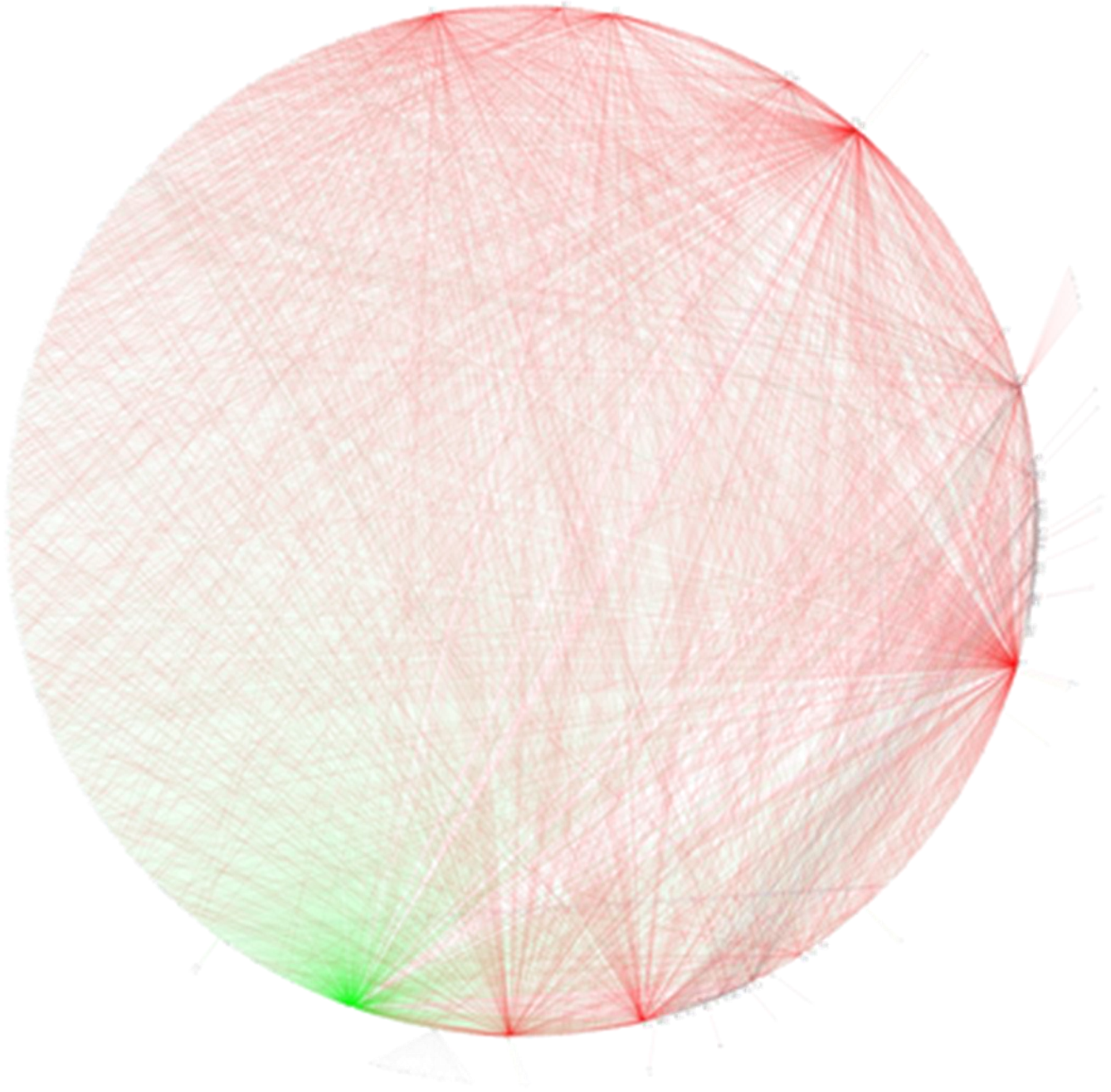
1.493 XXXX e-mail adresses   +/- 700 breached mail adresses
7 breaches   51 Domains

(Details in the Annexe)