Cyber Security on 2017, National Solutions and Turkey «WHATs and HOWs"



Mustafa AFYONLUOGLU

Cyber Security, e-Governance & e-Government Chief Expert



Cyber World on 2017



2014	2015	2016
1,523	1,211	1,209
805	466	927
1,200,000,000	564,0 <mark>00,000</mark>	1,100,000,000
11	13	15
	1,523 805 1,200,000,000	1,523 1,211 805 466 1,200,000,000 564,000,000

In the last 8 years more than 7.1 BILLION identities have been exposed in data breaches



RANSOMWARE	2014	2015	2016
NUMBER OF DETECTIONS	0	340,665	463,841
RANSOMWARE FAMILIES	30	30	101
AVERAGE RANSOM AMOUNT (US Dollar)	373	294	1,077



PHISHING RATE by INDUSTRY	2016
Agriculture, Forestry & Fishing	1 for each 1815 e-mails
Finance, Insurance & Real Estate	1 for each 1918 e-mails
Mining	1 for each 2254 e-mails
Public Administration	1 for each 2329 e-mails
Minimum: Transportation & Public Utilities	1 for each 6176 e-mails

April 27th, 2017 Symantec Corp. Internet Security Thread Report, Vol: 22

ISRC





BOĞAZİÇİ ÜNİVERSİTESİ Yönetim bilişim sistemleri siber güvenlik merkezi



CERT's in TURKEY and NATIONAL PRODUCTS in CYBER SECURITY

Attack Groups	Aliases	Country	Start Year	Motivation	Target Categories & Regions
Sandworm	Quedagh, BE2 APT	Russia	2014	Espionage, Sabotage	Governments, International Organizations, Europe, US, Energy
Fritillary	Cozy Bear, APT29, Office Monkeys	Russia	2010	Espionage, subversion	Governments, Think Tanks, Media, Europe, US
Swallowtail	Fancy Bear, APT28, Sednit	Russia	2007	Espionage, subversion	Governments, Europe, US
Cadelle	/None/	Iran	2012	Espionage	Airlines, telecommunications, Iranian Citizens, Governments, NGO's
Appleworm	Lazarus	North Korea	2012	Espionage, Sabotage, subversion	Financial, Military, Governments, Entertainment, Electronics
Housefly	Equation	US	2001	Espionage	Targets of interest to nation-state attackers
Strider	Remsec	Western	2011	Espionage	Embassies, <mark>airlines,</mark> Russia, China, Sweden, Belgium
Suckfly	/None/	China	2014	Espionage	e-Commerce, Governments, Technology, healthcare, Financial, shipping
Buckeye	APT3, UPS, Gothic Panda	China	2009	Espionage	Military, defense industry , Media, Education, US, UK, Hong Kong
Tick	/None/	China	2006	Espionage	Technology, broadcasting, Japan, aquatic engineering

Aubor World on 0047

Notable Targeted Attack Groups that have been publicly connected to nation states April 27 th, 2017 Symantec Corp. Internet Security Thread Report, Vol: 22









CERT's in TURKEY and NATIONAL PRODUCTS in CYBER SECURITY

CYBER SECURITY & NATIONAL SECURITY

National Security: Identification of threats and opportunities by monitoring the regional and global environment in order to take measures against the threats to the national state and security, and the processes to determine the politics appropriate to these issues and to implement the most appropriate policies (National Security Committee)*

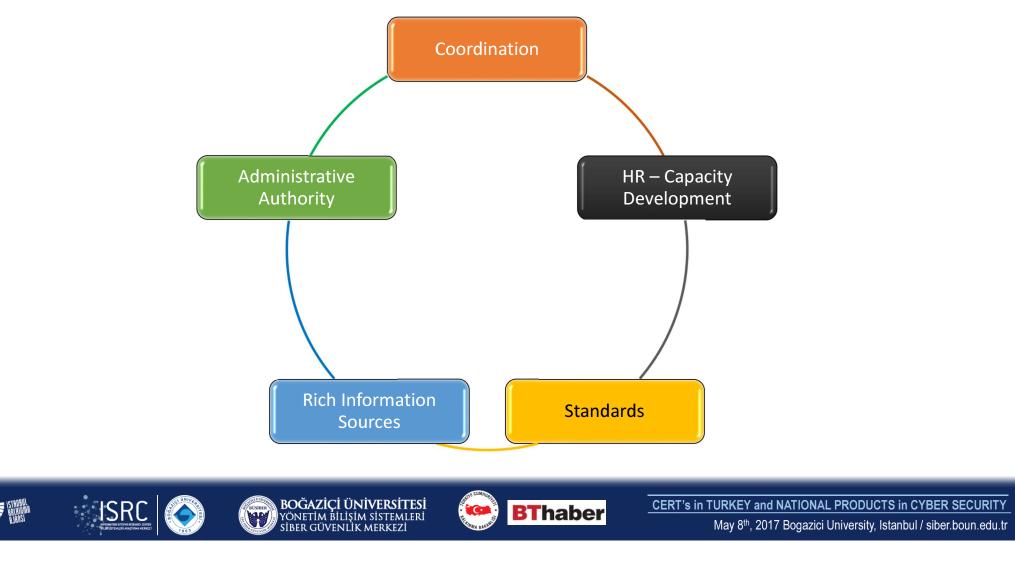


* http://www.mgk.gov.tr/index.php/milli-guvenlik-kurulu/genel-bilgi

** http://www.nato.int/docu/review/2017/Also-in-2017/nato-priority-spending-success-cyber-defence/EN/index.htm



CERT's and Critical Components: «What» is required ?



«HOW» ?

NOTIFICATION ON CERT'S FOUNDATION, DUTIES AND WORKING PROCEDURES AND PRINCIPLES

November 11th, 2013

Duties and Responsibilities of Institutional CERT's

Article 5: (2) Institutional CERTs provide advice on technical and administrative measures in the study of the establishment, operation or development of information systems of institutions in order to prevent or mitigate cyber incidents.









CERT's in TURKEY and NATIONAL PRODUCTS in CYBER SECURITY

Where CERT should be located: Institutional Governance

CURRENT SITUATION in TURKEY











CERT's in TURKEY and NATIONAL PRODUCTS in CYBER SECURITY May 8th, 2017 Bogazici University, Istanbul / siber.boun.edu.tr

Where CERT should be located: Institutional Governance

SUGGESTED ADMINISTRATIVE GOVERNANCE MODEL











CERT's in TURKEY and NATIONAL PRODUCTS in CYBER SECURITY May 8th, 2017 Bogazici University, Istanbul / siber.boun.edu.tr

«HOW» ?

NOTIFICATION ON CERT'S FOUNDATION, DUTIES AND WORKING PROCEDURES AND PRINCIPLES

November 11th, 2013

Duties and Responsibilities of Institutional CERT's

Article 5: (2) Institutional CERTs provide advice on technical and administrative measures in the study of the establishment, operation or development of information systems of institutions in order to prevent or mitigate cyber incidents.

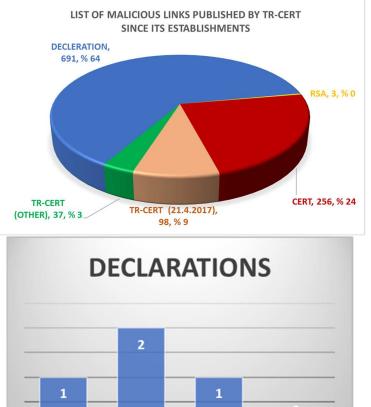
(4) While corporate CERTs meet with a cyber event, they first try to eliminate the event with their own capabilities by giving information to TR-CERT and the sectoral CERT they work with.

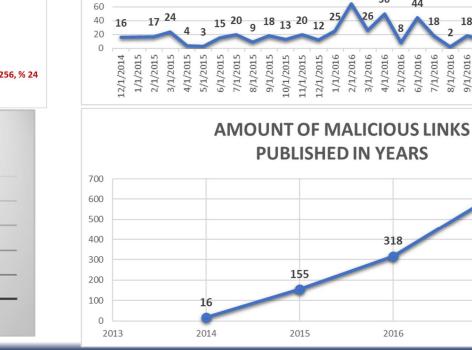












AMOUNT OF MALICIOUS LINKS PUBLISHED IN MONTHS

64

50

https://www.usom.gov.u/uri-iist.xiiii



2015

2014

BOĞAZİÇİ ÜNİVERSİTESİ YÖNETİM BİLİŞİM SİSTEMLERİ SİBER GÜVENLİK MERKEZİ

2017

2016

BThaber

200

180

160

140 120

100

80

CERT's in TURKEY and NATIONAL PRODUCTS in CYBER SECURITY

May 8th, 2017 Bogazici University, Istanbul / siber.boun.edu.tr

2017

183₁₇₈

2/1/2017 3/1/2017 4/1/2017

2018

140

95

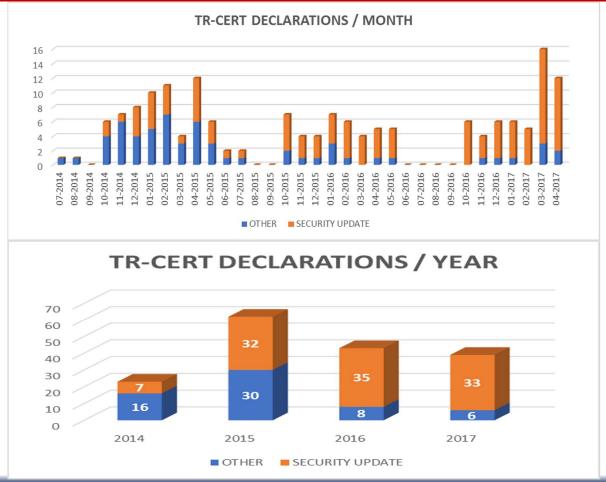
1/1/2017

¹⁸ 12

9/1/2016 10/1/2016

11/1/2016 12/1/2016

596



https://www.usom.gov.tr/tehdit.html

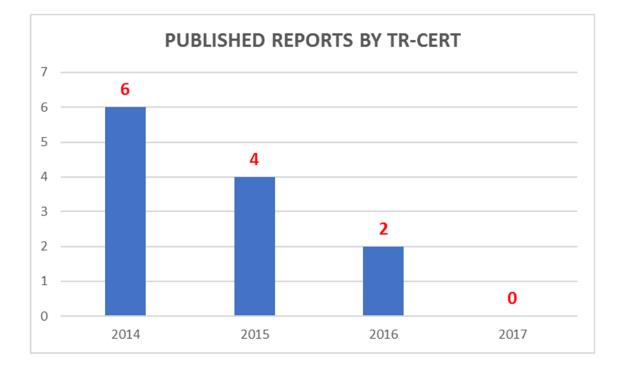




BOĞAZİÇİ ÜNİVERSİTESİ yönetim bilişim sistemleri siber güvenlik merkezi

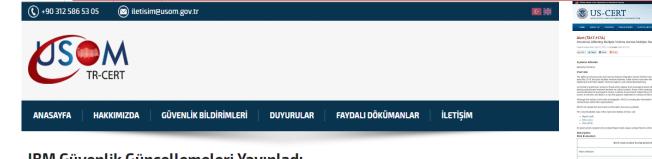


CERT's in TURKEY and NATIONAL PRODUCTS in CYBER SECURITY



https://www.usom.gov.tr/dokuman.html





IBM Güvenlik Güncellemeleri Yayınladı

Genel Bilgi

IBM; IBM Domino server IMAP EXAMINE ürününde bulunan zafiyetleri gidermek için güvenlik güncellemeleri yayınladı.

Etki

Mevcut güvenlik acıklıkları nedeniyle siber saldırganlar tarafından etkilenen sistemlerin kontrol altına alınması ihtimal dâhilindedir.

Çözüm

Ulusal Siber Olaylara Müdahale Merkezi (USOM), kullanıcı ve sistem yöneticilerine IBM'in güvenlik bülteni ve CERT/CC VU#676632 kodlu zafiyet raporunu incelemelerini ve gerekli güncellemeleri yapmalarını tavsiye etmektedir.

İlgili Güncellemeler:

https://www.us-

Domino 9.0.1 Feature Pack 8 Interim Fix 2 .

.

Domi SHOULD HAVE WIDER SCOPE, NOT ONLY CAUTIONARY BUT ALSO INSTRUCTIVE Kaynaklar

https://www-01.ibm.com/support/docview.wss?uid=swg22002280

http://www.kb.cert.org/vuls/id/676632

2017-04-27

	MON. The implant can also execute command via a remote their that is generated and passed through a named pipe. A Data's the C2 event to reduce at a mende shell or attematively to another process or these that can communicate with that multi-PRE advectation address.
tle Nyslein Enumeratio Girs	The implant has the ability to enumerate data within a specified directory where it pathets therames, such the times, and the
iebwork Traffic Compre- teta for this implant camp ppendect;	alon and Exclygible. The implant care a form of L2D component on to compose data that is sent to its C2. Alor componentian, the a more RCs-ophened with the key ColARFWEIGT122333000 (this composed to the string "store 1234" with the null byte
etroli Communications deniet/pent/itit The & he form that is generated	RECEIVES connects to the C2 even YDP pot 443, but deels not use the secure flag intenceting the API function is in our encycled and there is no 303, thandbhare as would normally would initially part 433 haffs, but latter the data is basened in is the WC4 open.
ANNER SECONDES IN	pies that have been examined have a hard-coded C2. Inside the implant's cantiguration block in memory were the strings in Table
	par that have been scattlined have a hard-coded C2. Inside the instant's configuration block in memory were the attrippe in Table spec Stronge Found in C2
L Bale I. PEDLEAVEE SA	
L Bale I. PEDLEAVEE SA	upe Zhonge Power H CZ med to determine if the impliest in elevery results (Peties from respire to respire)
1000 / PEDLEAVER 10 20141030 - mintek 1 2014-9-1-1200 -tua	upe Zhonge Power H CZ med to determine if the impliest in elevery results (Peties from respire to respire)

	Varione	
	This product a provided valgests that hadfaction and this Privacy & Kine prior.	Contact Us
: HENN bytes (HELF 28) > Ment 30 year (HELF 20) constant, the first still remain two maximum salid featureses/Difinitioning and (Diffed, 21 should be constant, the first still asympty contains, fir with the particle salid states and states of a system to include spectrum verticals, matter if provents, the AL of 20 softwareses.	State Holden Control on and address Report Indexes	Download P
which deal family beams the ADC reporting into agree study. 2012. All study have an even warry which at the ADC is an element of the dealership controls are experimented as a study of the ADC is an element of the ADC is an element to be experimented as a study of the ADC is a study of the ADC is a study of the ADC is a study of the ADC is a beam of the ADD is a study of the ADC is a study of t	Here: 1 Fri2 1 Canastro 1 Hanc Lamberto 1 Fri2 1 Hold Hanc Here 1 Hanc 1	

https://www.usom.gov.tr/dokuman.html







CERT's in TURKEY and NATIONAL PRODUCTS in CYBER SECURITY

TR-CERT

CAPACITY BUILDING SUGGESTIONS

- TR-CERT should become a stronger and more qualified source of information for CERTs and coordinate relevant institutions within this aim.
- More informative reports and guides should be prepared:
- Related ENISA Reports, NIST Documents and CERT Guidelines (such as First Responders Guide to Computer Forensics) may be translated to Turkish.
- These studies made by TR-CERT and universities should be published in easy accessible format in «Documents section of TR-CERT Website».
- In the TR-CERT website, public / private sector, universities, NGOs, CERTs and TR-CERT can
 publish the activities carried out / realized in the field of cyber security and the result
 reports obtained therefrom.
- Webinars should be organized and a Cyber Security Webinar Library should be created on the site. Distance learning and 24/7 training approach should be targeted.
- Systematic CERT training should be provided in cooperation with the universities, and labs should be included which will create practical experience in these trainings. «The Lessons-learnt and good-practices» should be given. «Experience Exchange Trainings» from institutional experts who are actively involved in cyber-incident interventions.









«HOW» ?

NOTIFICATION ON CERT'S FOUNDATION, DUTIES AND WORKING PROCEDURES AND PRINCIPLES

November 11th, 2013

Duties and Responsibilities of Institutional CERT's

Article 5: (2) Institutional CERTs provide advice on technical and administrative measures in the study of the establishment, operation or development of information systems of institutions in order to prevent or mitigate cyber incidents.

(4) While corporate CERTs meet with a cyber event, they first try to eliminate the event with their own capabilities by giving information to TR-CERT and the sectoral CERT they work with.

(8) [and Article 7-(6)] Corporate (Sectoral) CERTs assign contact information of CERT members that is accessible 7/24 and notify / inform TR-CERT and the sectoral CERTs that they work with.









CERT's in TURKEY and NATIONAL PRODUCTS in CYBER SECURITY May 8th, 2017 Bogazici University, Istanbul / siber.boun.edu.tr

QUALIFIED HUMAN RESOURCES for CERT's

- Cyber Security, Data Security, Personal Data Expertizations should be defined
- Certificates of specialization must be given by universities' cyber security centers and accredited private sector training centers
- Cyber security centers in universities should set **international goals** with accreditation: «Global Capacity Development Power»
- Certification programs should also build on practical field experience
- Specific specialties for some national products: "Pardus Migration and Support Expert»
- Expert certification and practical experience on site is a prerequisite for precondition of duty in TR-CERT and CERTs
- Special financial incentive for CERT and TR-CERT Team because of 7 x 24 Work and Critical Mission Area









«EXACT NATIONAL» CYBER SECURITY

- Softwares should have full-source:
 - Open-Source is NOT a must (source-available / shared-source) but it should NOT include and component that does not have source code
- Should be developed by National private sector:
 - <u>Government should supply infrastructures and R&D only</u>
 - The state should not unfairly compete with the private sector for software development:
 - The state should implement frameworks, libraries, national R&D studies and set standards that will support private sector instead of software development
 - The national private sector should develop sectoral (health, education etc.) and horizontal (Electronic Document Management System etc.) software by using them
 - Exceptions to Public Procurement Law No. 8227 Article 3 should be re-addressed to support competition in the private sector
 - The sector should be divided into categories by leveling
 - The market in the public sector ensures the development of these categories
 - There should be **Sustainable** model:
 - There should not be non-product-only solutions left alone with AR-GE incentives
- State-supported from technical, administrative, financial and legal aspects





ISRC



STANDARDS - 27K FAMILY

SECURITY STANDARDS TO BE AWARDED BY TSI (TURKISH STANDARDS INSTITUTION) TO TURKEY

STANDARD	EXPLANATION / STANDARD NAME	PRIORITY
ISO/IEC 27019	Information security for process control in the energy industry	*
ISO/IEC 27021	Information technology — Security techniques — Competence requirements for information security management systems professionals	*
ISO/IEC 27032	Guideline for cybersecurity	*
ISO/IEC 27034-1	Application security Part 1: Guideline for application security	\star
ISO/IEC 27010	Information security management for inter-sector and inter-organizational communications	**
ISO/IEC 27033-6	Network security - Part 6: Securing wireless IP network access	**
ISO/IEC 27035-1	Information security incident management – Part 1: Principles of incident management	$\star\star\star$
ISO/IEC 27035-2	Information security incident management – Part 2: Guidelines to plan and prepare for incident response	***
ISO/IEC 27036-4	Information security for supplier relationships - Part 4: Guidelines for security of cloud services	$\bigstar\bigstar\bigstar$









CERT's in TURKEY and NATIONAL PRODUCTS in CYBER SECURITY

Cyber Security on 2017, National Solutions and Turkey «WHAT's and HOW's"



Mustafa AFYONLUOĞLU Cyber Security, e-Governance and e-Government Chief Expert afyonluoglu [at] gmail.com Linkedin: http://linkedin.com/in/afyonluoglu Twitter: http://twitter.com/#!/afyonluoglu Web: afyonluoglu.com







TÜRKİYE'DE SOME'LER ve SİBER GÜVENLİKTE YERLİ MİLLİ ÇÖZÜMLER

8 Mayıs 2017 Boğaziçi Üniversitesi, İstanbul / siber.boun.edu.tr