

Mongolian Cyber Emergency Response Team / Coordination Center



#### HISTORY

ESTABLISHED IN 2014 AS SECURITY COMMUNITY MEETUP

Transformed as non-governmental, non-profit organization in 2015

#### MISSION

Improve the technical capabilities of constituents

Provide support during incident response and threat intelligence activities

Establish the professional trust community for cyber security related information sharing and collaboration.

Raise the security awareness of the general public





Cyber drill



Training



Information sharing







Mongolian Cyber Emergency Response Team / Coordination Center

#### INTERNATIONAL RELATION



# **Microsoft**<sup>®</sup>





### COLLABORATION



#### ХАРИЛЦАА ХОЛБООНЫ ЗОХИЦУУЛАХ ХОРОО





МОНГОЛ УЛСЫН ШИНЖЛЭХ УХААН ТЕХНОЛОГИЙН ИХ СУРГУУЛЬ

МЭДЭЭЛЭЛ, ХОЛБООНЫ ТЕХНОЛОГИЙН СУРГУУЛЬ





## MEMBERS

#### Service Providers:





Banking/Financial:

**GOLOMT BANK** 🕑 ТӨРИЙН БАНК

**KHAN BANK** 

B ХУДАЛДАА ХӨГЖЛИЙН БАНК



Others:



ҮНЭТ ЦААСНЫ ТӨВЛӨРСӨН ХАДГАЛАМЖИЙН ТӨВ



**RioTinto** 

NATIONWIDE BROADBAND NETWORK

## ORGANISED EVENTS



## "Haruul Zangi" CTF

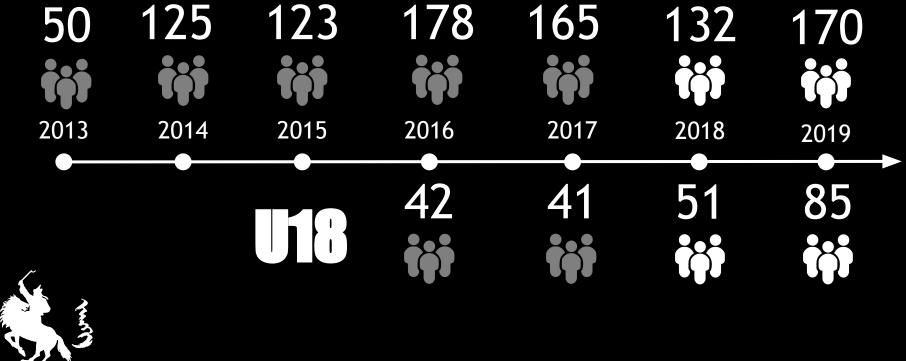
Since 2013







"Haruul Zangi" CTF Participants







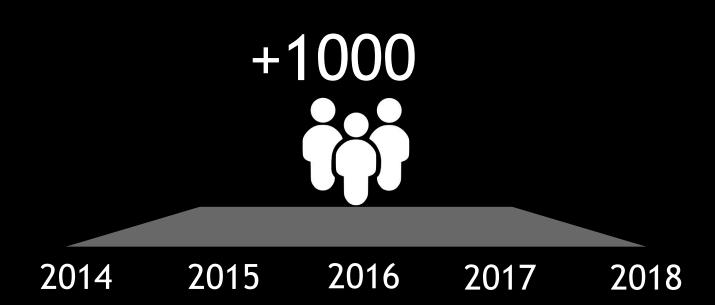
### INFO SECURITY CONFERENCE

Since 2014





MNSEC CONFERENCE





## CYBER DRILL

Since 2016



# Cyber Security Training

Since 2016



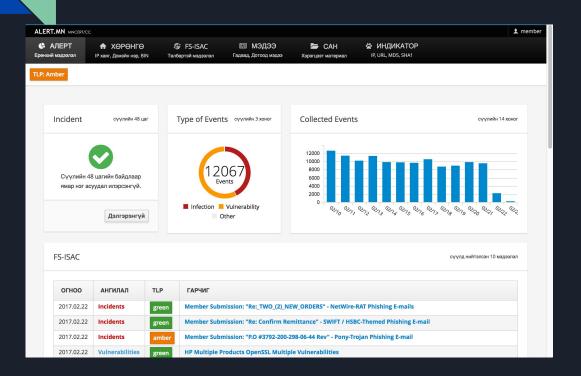
## FIRST CSIRT training

## CISSP training MISP training



## ACTIVE PROJECTS

#### ALERT.MH



ncident	normalia di	w Te	pe of Events	eventie 1 mm	Collected Duerts	provenile 16
	осо байдлаар нөөр нэ ан инзэрсэнгүй. Дэнгэрээгү		1407 Dets	72		
IS-ISAC						evyra nethanan 13 saa
o-low.						and a second sec
001100	ANTADAD	TLP	TAP-OF			
2017.01.13	Valnerabilities	green		tiple Products libors	(2 vulnerability	
2017.01.13	Valnerabilities	Sueer.	Blue Cost Multip			
2017.01.13	Valnerabilities	green			Discovery Manager Multiple Vulnerabilities	
2017.01.13	Valeerabilities	green	Red Hat update f	for java-1.6.0-openjil	R	
2017.01.13	Valeesbillties	green	Oracle Linux upd	dete for kernel-uek		
2017.01.13	Valuerabilities	green	Lesono Multiple	ThinkStation and Th	hinkCentre Products MVIDIA Graphics Drivers M	uddiple Vulserabilities
2017.01.13	Valverabilities	green	IBM Image Const.	truction and Compo	alkion Tool Multiple Vulnerabilikies	
2017.01.13	Incidents	arther	Nember Submiss	alon: Part Scen Activ	rity observed December 2016	
		_				
2017.01.13	Incidents	amber	Member Submiss	sion: "BBAT Online J	Access Limitation(SUSPECTED SPAN) * - BEAT (P	enred Phishing E-mail
2017.01.13	Incidents Incidents	anber			teres UnitativeSUPPCTED SPAN(* - BBATF)	erned Pricking I mad
2017.01.13	incidents	anther				
2017.01.13	incidents	anther				By:
2017.01.13 Гадвад, дото	Incidents KO, M3,000 FAM-68*	antiter antiter	Menther Schmitt	sice: Trojan-Checkin		Byon cycra withous 19 and
арадад дото алное	Incidents NJ, M3,000 FAP-86* An Unseally We		Menther Schmitt	alce: Trojan-Checkin	Jaching observed on january 12, 2017	Byc cyre without 11 cu 38 CYPEACK
арлад, дото адаад, дото агноо артго2.15	Incidents IO() MO()DO FAIP-ber An Unseently We BBIT Turns Webbe	n 1889 A Cyberse	Mender Submiss	alce: Trojan-Chackin ric Hew I Almoot Gel	Anthrity sharred or january 13, 2017 Linkensed With a Replagar M	Bits syna et resettes anyo syna et resettes to correcte nosceneration
2017.01.13 a,g,aa,a,g, g,oroo 07900 2017.02.15 2017.02.14 2017.02.14 2017.02.14	Incidents NUL MALOO FAMARY An Unscutty We Maparese Cell No. Maparese Cell No.	n Into A Cyberse dgets far better MAXX wenre root	Member Submiss Neare Science on Upwer existing Weapon Acelot security by vasite the a near topor spowers	silee: Trojan-Chackin rie Taw I Almost Go Ethile House Inter sol a scale of a sol anazzigan Gaiwa	Activity observed on january 12, 2017 Linkness (VDA: a Knylegger od ana to Tablast	Byre cycleswitzen i fact 25 COVENCE Rectamonscom Universitation Theographic Ask Bickson
8077.61.13 a,gaaa,g. goroo 879800 2077.62.15 2077.62.14 2077.62.13 2077.62.13	Incidents	n 1980 A Cyberse dgets far better blick worde edd 1 150,000 Printer	Member Solenies Insere Sciencen Upwere escrity Weapen Avaid insolating by nating the an other support agreement to Science Maker the In	alon: Trojan-Chaoldin riz Time I Almont Gol IIII-bio Sissee Intern reast on a scale of a pi neuropae of Things is 1	Agthly skarred as junary 12, 2017 Lisketed WK & Koylagar ek ek ek ek ek ek ek ek ek ek ek ek ek	By cycewhoor too Adorman.com Independ Integration Integration Integration Integration
2017.61.13 adjanad, A0100 019600 2017.60.15 2017.60.15 2017.60.15 2017.60.13 2017.60.13 2017.60.12	An Unserity Meson Therease Earliers Maparate Speep This Teen Hacket Ball Secrity pr	n 1859 A Cyberse dgets far better aanse aeere eaan 1 150,000 Printer scautiens far no	Member Solenies Innere Scenn on Upwer exertig Weapen Avid I society by rating the at near topic spowers to Show How the in	sloe: Trojan-Chackin ric: Trav I Almost Got I Mihot House Loten reats on a scale of a bit managam Galow receives of Things Is 1	Agthly skarred as junary 12, 2017 Lisketed WK & Koylagar ek ek ek ek ek ek ek ek ek ek ek ek ek	Environmentation Between the Materian com Materian Materi
2017.61.13 adjanad, dorto atribos 2017.62.15 2017.62.15 2017.62.15 2017.62.15 2017.62.15 2017.62.15 2017.62.15	Incidents	n 1899 A Cyberne dgets far better skilot seere road 150,000 Primter scautions far no ttacks on unpat	Member Solverlas Neare Scen on Upware excity Weapon And a near sope spectra resolution by reach as near sope spectra as portion How How In a spectra and journal expertises and journal	sloe: Trojan-Chackin ric: Trav I Almost Got I Mihot House Loten reats on a scale of a bit managam Galow receives of Things Is 1	Agthly skarred as junary 12, 2017 Lisketed WK & Koylagar ek ek ek ek ek ek ek ek ek ek ek ek ek	See cyce without if an <b>3 contact</b> <b>1 cont</b>
2017.01.13 A,BBAB, AOTO 071600 2017.02.14 2017.02.14 2017.02.13 2017.02.12 2017.02.13 2017.02.13 2017.02.13	And Annual States State	n 1899 A Cyberse dgets far ketter auxic seere room 150,000 Prinser scautions far no ttacks on unpath stricks on unpath	Interdier Solanies Inter Scient on Upware exerty Weapen Avail recerty Weapen Avail recerty by rating th a rear topic apware to School Networks in opprefits and journal school WedPress sites defenses	nice: Inegine Checkin ric Time I Almost Got TRNNe Houses Unite matter as a scalar of a matter as a scalar of things in t misma of Timings (in the United Scalar Sca	Agthly skarred as junary 12, 2017 Lisketed WK & Koylagar ek ek ek ek ek ek ek ek ek ek ek ek ek	The systematics of the sector
2017.61.13 adjanad, dorto atribos 2017.62.15 2017.62.15 2017.62.15 2017.62.15 2017.62.15 2017.62.15 2017.62.15	And Annual States State	n Into A Cyberse dgets for better maxic users soot I 150,000 Prinser ecoutions for no tacks on unput mix attacks and nixs hacked, info	Mender Scen on Upware excity Wanger Andre assard y by saving the an encity and y saving the an encity and y and y and y and and y and	nice: Inegine Checkin ric Time I Almost Got TRNNe Houses Unite matter as a scalar of a matter as a scalar of things in t misma of Timings (in the United Scalar Sca	Agthly skarred as junary 12, 2017 Lisketed WK & Koylagar ek ek ek ek ek ek ek ek ek ek ek ek ek	See cyce without if we become Sectors Research R
2017.01.13 ALBRAD, ADTON 071900 2017.02.15 2017.02.15 2017.02.13 2017.02.13 2017.02.13 2017.02.13 2017.02.13 2017.02.13	AUG M3,000 FAP48F An Unseatly We BB Tares Wess Th Tares Wess The Tares Wess The Tares Wess The Tares Wess The Tares Wess The Tares Wess This Tares Wess Magazana dana Magazana dana Magazana Mag	n Into A Cyberse dgets for better maxic users soot I 150,000 Prinser ecoutions for no tacks on unput mix attacks and nixs hacked, info	Mender Scen on Upware excity Wanger Andre assard y by saving the an encity and y saving the an encity and y and y and y and and y and	nice: Inegine Checkin ric Time I Almost Got TRNNe Houses Unite matter as a scalar of a matter as a scalar of things in t misma of Timings (in the United Scalar Sca	Agthly skarred as junary 12, 2017 Lisketed WK & Koylagar ek ek ek ek ek ek ek ek ek ek ek ek ek	EXP Expension Accessor
2017.01.13 adjanaja, dorton 019400 2017.00.15 2017	AUG M3,000 FAP48F An Unseatly We BB Tares Wess Th Tares Wess The Tares Wess The Tares Wess The Tares Wess The Tares Wess The Tares Wess This Tares Wess Magazana dana Magazana dana Magazana Mag	n Telo A Cyllerse dgets fur lastar lasts were soo 150,000 Primar nostions for no tacks on unput mo attacks on shis hashed, Infe Ransamuare, Pu	Mender Scen on Upware excity Wanger Andre assard y by saving the an encity and y saving the an encity and y and y and y and and y and	nice: Trogin-Checkin rice: How I Advesses Goo Historia Hanness Lorden Santa Santa Santa Ali Santa Santa Santa Hanna Santa Santa Hanna Santa Santa Hanna Santa Hann	Agthly skarred as junary 12, 2017 Lisketed WK & Koylagar ek ek ek ek ek ek ek ek ek ek ek ek ek	ana
2017.01.13 adjanaja, dorton 019400 2017.00.15 2017	Addents Addent	In Table A Cyberned dgetes five herter manor water 1150,000 Printear mount of the Company tackto on unper- ment attackto and risks hardwell, lefe facesammaner. Pri-	Mandar fulnis here San of Upware early Wayne And searchy Wayne And searchy Wayne And searchy Wayne And searchy Wayne And searchy Wayne And searchy Wayne And San	nice: Trojan Checkin nice Haves I Almost Go (1994) Children I Almost Go Children I Almost Go and Children I Almost Go	Agthly skarred as junary 12, 2017 Lisketed WK & Koylagar ek ek ek ek ek ek ek ek ek ek ek ek ek	Line where the sequences of ear Sectors and Management Management Management Management Management

### MISP.ALERT.MN

Home	Event Actions	Galaxies Ir	nput Filters	Global Actions	s Sync	Actions	Administra	ation	Audit											MISP	Tuvshint	oayar 🐱	Log out	
List Events																								
Add Event		Events	5																					
Import from																								
REST client		« previous	1 2	3 4 5	6 7	8 9	10 11	12	13	14	15	16	17	18	19	20	21	next	* »					
List Attributes	S	Q M	ly Events C	Org Events																Enter valu	e to searc	h	Filter	
Search Attrib	outes	Published	d Org	Owner	org Id	Cluster	s Tags														#Attr.	Email		
View Proposa	als	• •	NCFTA_357	7 MNCEF	T 6243	7	S trickb	ot													14356	tuvshinba	yar@mncert.o	ra
Events with p	proposals		NCFTA_357				C Emot	_															•	-
View delegati	ion requests						_	-													15967		yar@mncert.o	
			NCFTA_357			4	S trickb	_													1722	tuvshinba	yar@mncert.o	g
Export			camichel.co	om MNCEF	IT 6846		Stlp:gr	een 🤇	misp	threat-le	evel="lo	ow-risk"	0	circl:in	cident	-classi	ficatior	n="phis	shing"		3821	otgonpure	ew@mncert.or	g
Automation			NCFTA_357	7 MNCEF	T 6243	6	S trickb	oot													1279	tuvshinba	yar@mncert.o	rg
		□ ◄	NCFTA_357	7 MNCEF	T 6243	5	S trickb	oot													2614	tuvshinba	yar@mncert.o	rg
		□ ✔	NCFTA_357	7 MNCEF	T 6243	3	S trickb	ot													2436	tuvshinba	yar@mncert.o	rg
		□ ✓	NCFTA	MNCEF	T 6192	D	S trickb	ot													1223	tuvshinba	yar@mncert.o	rg
		□ ✓	NCFTA	MNCEF	T 61934	4	S Ram	nitRIG													7	tuvshinba	yar@mncert.o	rg
		•	SwissPost	MNCEF	T 6234	7	O DESK	(TOP-g	roup	🕉 tlp:gr	reen										442	tuvshinba	yar@mncert.o	rg
			NCFTA	MNCEF	T 6193	6	S Emot		_		_										9616	tuvshinba	yar@mncert.o	ra
			CIRCL 377					-	circle	incident	classif	ication-	"ecam	. 0	aceirt	other-	-"unkn	own"	Circl:topic	-"individual"	639		ew@mncert.or	
						_	_	_											_			• •		•
			camichel.co	om MNCEF	T 1073	2	osint: misp- misp-	galaxy	:banker	="Retef	e" 🔇	misp-ga	alaxy:to	ool="S	moke	Loade	r"		tlp:amber oader"		62	tuvshinba	yar@mncert.o	g
		□ ✓	MIL.be_269	3 MNCEF	T 8910																35	tuvshinba	yar@mncert.o	rg

#### Galaxies

Input Filters **Global Actions**  Administration

**Related Events** 

#### View Event

View Correlation Graph

#### View Event History

Edit Event **Delete Event** Add Attribute Add Object Add Attachment Populate from... Enrich Event Merge attributes from... **Propose Attribute Propose Attachment** 

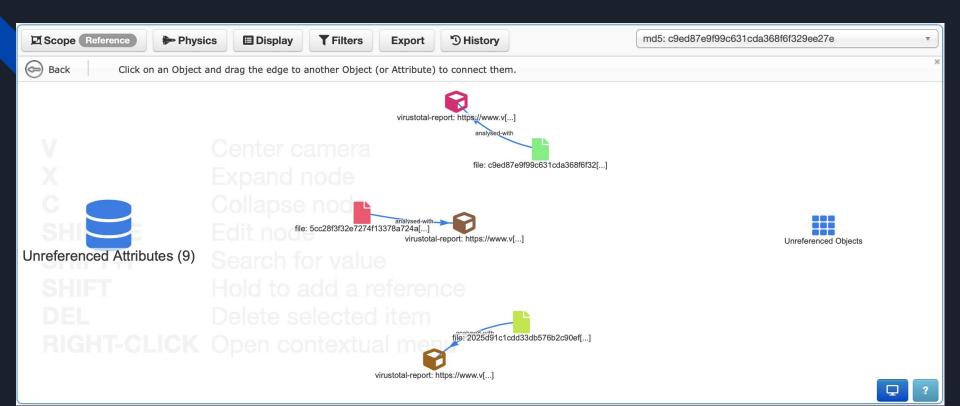
#### Download as...

List Events Add Event

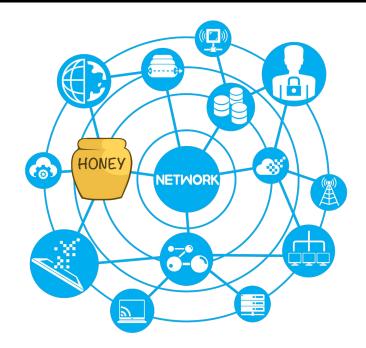
#### 2019-01-25: Lazarus Pakistan Toolkits

Event ID	10092	Air Lazarus PowerRatankba.B toolkit
UUID	5c4cb9a7-0454-42eb-8f63-383368f8e8cf +	су 2019-01-28 9
Creator org	VK-Intel	Air Lazarus DPRK Malware Sample
Owner org	MNCERT	cy 2019-01-25 3
Email	tuvshinbayar@mncert.org	
Tags	<ul> <li>Actor: Lazarus X OPRK X Malware: PowerRatankba, b X PowerShell Installer X</li> <li>Keylogger X Country: Pakistan X O type:OSINT X O osint:lifetime="perpetual" X</li> <li>osint:certainty="50" X O tip:white X O misp-galaxy:threat-actor="Lazarus Group" X</li> <li>misp-galaxy:malpedia="PowerRatankba" X</li> <li>misp-galaxy:mitre-enterprise-attack-intrusion-set="Lazarus Group - G0032" X</li> <li>misp-galaxy:mitre-intrusion-set="Lazarus Group" X O misp-galaxy:tool="PowerRatankba" X</li> <li>misp-galaxy:mitre-enterprise-attack-intrusion-set="Lazarus Group - G0032" X</li> <li>misp-galaxy:mitre-intrusion-set="Lazarus Group" X O misp-galaxy:tool="PowerRatankba" X O +</li> </ul>	
Date	2019-01-26	
Threat Level	Medium	
Analysis	Initial	
Distribution	All communities	
Info	2019-01-25: Lazarus Pakistan Toolkits	
Published	<b>Yes</b> (2019-09-26 02:02:05)	
#Attributes	27 (6 Objects)	
First recorded change	2019-01-27 10:50:55	
Last change	2019-09-25 10:03:20	

Audit



## HONEYPOT



## MEMBERSHIP



Mongolian Cyber Emergency Response Team / Coordination Center

## Information sharing

- Local and international threat sharing, warning, vulnerability disclosures within member organizations.
- Fast, responsible and professional.

## Trainings and Meet-ups

- Information security trainings
- Security experts monthly meet-ups and experience sharing

## **Professional Services**

- Cyber drill workshops (onsite & webex)
- Incident Response (MNCERT members and worldwide)
- International conferences and event participation



Mongolian Cyber Emergency Response Team / Coordination Center