



Mongolian Cyber Emergency Response Team / Coordination Center

ЦАХИМ АЮУЛГҮЙ БАЙДЛЫН МЭДЭЭЛЭЛ УДИРДЛАГЫН ТӨВ

Ж.Наранбат



Mongolian Cyber Emergency Response Team / Coordination Center

ҮЙЛ АЖИЛЛАГАА



Mongolian Cyber Emergency Response Team / Coordination Center

ҮЙЛ АЖИЛЛАГАА



Cyber Drill



Training



Information Sharing



Collaborate



Public Awareness

ОЛОН УЛСЫН ХАРИЛЦАА



ХАМТЫН АЖИЛЛАГАА



ХАРИЛЦАА ХОЛБООНЫ
ЗОХИЦУУЛАХ
ХОРОО



ЗАСГИЙН ГАЗРЫН ТОХИРУУЛАГЧ АГЕНТЛАГ
ХАРИЛЦАА ХОЛБОО, МЭДЭЭЛЛИЙН ТЕХНОЛОГИЙН ГАЗАР



МОНГОЛ УЛСЫН ШИНЖЛЭХ УХААН
ТЕХНОЛОГИЙН ИХ СУРГУУЛЬ

МЭДЭЭЛЭЛ, ХОЛБООНЫ ТЕХНОЛОГИЙН
СУРГУУЛЬ



MOSA

MONGOLIAN SOFTWARE INDUSTRY ASSOCIATION

ГИШҮҮН БАЙГУУЛЛАГУУД



ЗОХИОН БАЙГУУЛСАН АЖИЛ



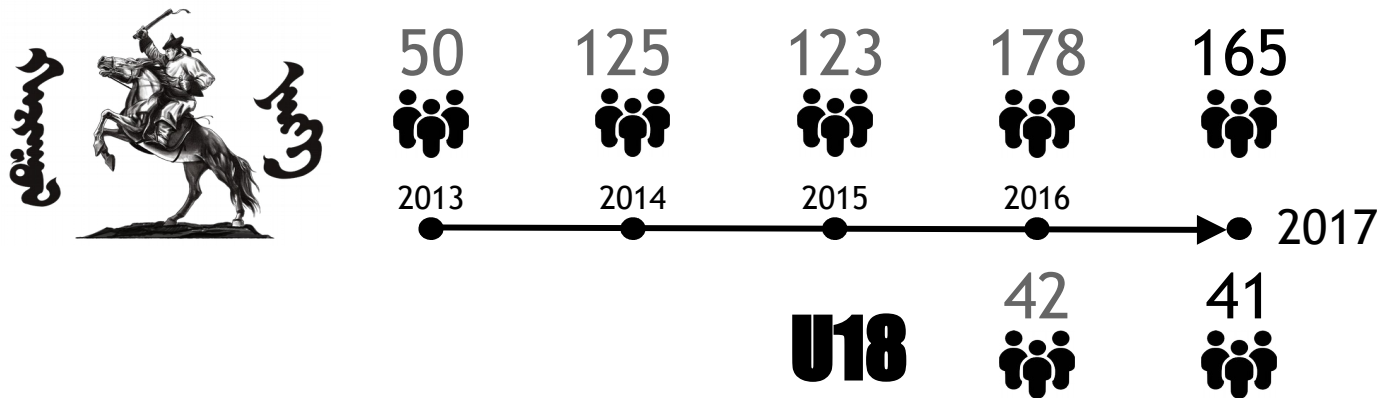
Mongolian Cyber Emergency Response Team / Coordination Center

ХАРУУЛ ЗАНГИ

2013 оноос жил бүр



ХАРУУЛ ЗАНГИ



МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ӨДӨРЛӨГ

2014-оос хойш жил бүр



2017



324



40

ЭМЭГТЭЙ



284

ЭРЭГТЭЙ



47

ОЮУТАН



277

АЖИЛТАН



52

ТӨРИЙН
ТӨЛӨӨЛӨЛ



225

ХУВИЙН
ХЭВШИЛ

2016



210



10

ЭМЭГТЭЙ



200

ЭРЭГТЭЙ



28

ОЮУТАН



182

АЖИЛТАН



45

ТӨРИЙН
ТӨЛӨӨЛӨЛ



137

ХУВИЙН
ХЭВШИЛ

CYBER DRILL

2016 оноос жил бүр



CYBER DRILL



RANSOMWARE

CYBER SECURITY TRAINING

2016 оноос жил бүр



МАБ СУРГАЛТ



FORENSICS

ХЭРЭГЖҮҮЛЖ БАЙГАА ТӨСЛҮҮД

ALERT.MN

ALERT.MN MNCERT/CC member

АЛЕРТ Ерөнхий мэдээлэл | ХӨРӨНГӨ IP хянг., Домейн нэр, BIN | FS-ISAC Төлбөргүй мэдээлэл | МЭДЭЭ Гадаад, Дотоод мэдээ | САН Харцрагт материал | ИНДИКАТОР IP, URL, MDS, SHA1

TLP: Amber

Incident сүүлийн 48 цаг

✔

Сүүлийн 48 цагийн байдлаар ямар нэг асуудал илэрсэнгүй.

Далгэрэнгүй

Type of Events сүүлийн 3 хоног

12067 Events

■ Infection
 ■ Vulnerability
 ■ Other

Collected Events сүүлийн 14 хоног

FS-ISAC сүүлд нийтэлсэн 10 мэдээлэл

ОГНОО	АНГИЛАЛ	TLP	ГАРЧИГ
2017.02.22	Incidents	green	Member Submission: "Re: TWO (2)_NEW_ORDERS" - NetWire-RAT Phishing E-mails
2017.02.22	Incidents	green	Member Submission: "Re: Confirm Remittance" - SWIFT / HSBC-Themed Phishing E-mail
2017.02.22	Incidents	amber	Member Submission: "P.O #3792-200-298-06-44 Rev" - Pony-Trojan Phishing E-mail
2017.02.22	Vulnerabilities	green	HP Multiple Products OpenSSL Multiple Vulnerabilities

ALERT.MN MNCERT/CC member

АЛЕРТ Ерөнхий мэдээлэл | ХӨРӨНГӨ IP хянг., Домейн нэр, BIN | FS-ISAC Төлбөргүй мэдээлэл | МЭДЭЭ Гадаад, Дотоод мэдээ | САН Харцрагт материал | ИНДИКАТОР IP, URL, MDS, SHA1

TLP: Amber

Incident сүүлийн 48 цаг

✔

Сүүлийн 48 цагийн байдлаар ямар нэг асуудал илэрсэнгүй.

Далгэрэнгүй

Type of Events сүүлийн 3 хоног

14072 Events

■ Infection
 ■ Vulnerability
 ■ Other

Collected Events сүүлийн 14 хоног

FS-ISAC сүүлд нийтэлсэн 10 мэдээлэл

ОГНОО	АНГИЛАЛ	TLP	ГАРЧИГ
2017.02.13	Vulnerabilities	green	CVE-2017-10135: Multiple Products (Bash) vulnerability
2017.02.13	Vulnerabilities	green	Blue Coat Multiple Vulnerabilities
2017.02.13	Vulnerabilities	green	IBM Trust Application Security Manager Multiple Vulnerabilities
2017.02.13	Vulnerabilities	green	Red Hat updates for glibc 2.19 on glibc
2017.02.13	Vulnerabilities	green	Oracle Linux updates for kernel-uk
2017.02.13	Vulnerabilities	green	Lenovo Multiple ThinkPad and ThinkCentre Products NVIDIA Graphics Drivers Multiple Vulnerabilities
2017.02.13	Vulnerabilities	green	IBM Edge Gateway and CloudGateway Host Multiple Vulnerabilities
2017.02.13	Incidents	orange	Member Submission: Post-Coin Activity observed December 2016
2017.02.13	Incidents	orange	Member Submission: "BANK Online Access Limited/SUSPECTED SPAM" - BBK-Themed Phishing E-mail
2017.02.13	Incidents	orange	Member Submission: Trojan Checkin Activity observed on January 12, 2017

ГЭМЭЭНИЙ МЭДЭЭЛЭЛ

ОГНОО	ГАРЧИГ	БХ ОРГАНИЗМ
2017.02.15	An Unusually High Phished Message Seen on Twitter from Kinross Gas Refinery With a Manager	kinross.com
2017.02.14	Web Site Reported with a Vulnerability Reported and Other Issues Reported	hugoboss.com
2017.02.14	IT Issues: Get Budgets for better security by using threat on a wide of sites to reduce	hugoboss.com
2017.02.13	Response Requested from Korea (KSP) report network intrusion from	netsec
2017.02.12	Web Site Reported with a Vulnerability Reported and Other Issues Reported	member@red-it.com
2017.02.12	Bank security procedures for non-profile and journalists in the United States, early 2017	techradar.com
2017.02.11	Strong growing interest on corporate websites and other sites affected - on Japan	cyberint.com
2017.02.10	Forward engineering attacks and defenses	longsight.org
2017.02.10	Several Public banks hacked, information stolen by unknown attackers	bankdata.com
2017.02.10	The Evolution of Hackerspace Part 1	netsecjournal.com

Нэгдүгээр сарын 10-ны өдөр

Нэгдүгээр сарын 10-ны өдөр

TLP: Amber | MDP: Member Security Intelligence Report - Emerging | TLP: Amber | MDP: Member Security Intelligence Report - Emerging

COLLECTED EVENTS

НИЙТ БҮРТГЭГДСЭН ДОХИО



384'411

НИЙТ IP ХАЯГ



15'251

ХАМГИЙН ИХ БҮРТГЭГДСЭН 10 IP ХАЯГ



1.	3607	183.81.171.X
2.	3316	202.70.43.X
3.	3173	122.201.19.X
4.	3132	202.72.245.X
5.	3118	202.131.250.X
6.	3116	202.131.228.X
7.	3014	122.201.25.X
8.	2945	202.131.245.X
9.	2822	202.70.36.X
10.	2822	124.158.95.X

БИДНИЙ СҮЛЖЭЭНД ЮУ БАЙНА



BankPatch

429

Mirai

5'824

Sality

2'834

Virut

72'319

Conficker

295'001

БИДНИЙ СҮЛЖЭЭНД ЮУ БАЙНА



<http://geo-mongol.mn/>

<http://opendoor.mn/>

<http://selengepress.mn/>

<http://www.mccl.mn/>

<http://umch.ub.gov.mn/>

<http://emergency-update-service.wiwa.mn/>

<https://emergency-update-service.wiwa.mn/>

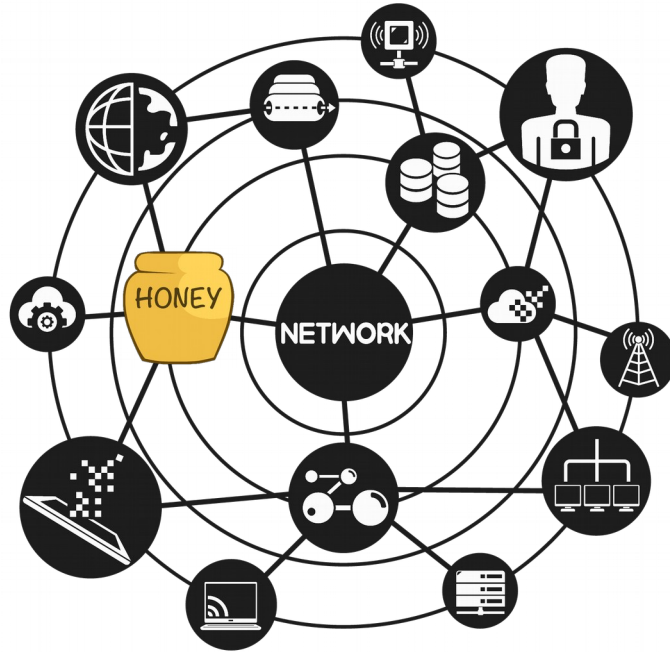
<https://emergency-update-login.wiwa.mn/>

<http://wiwa.mn/>

<http://ekhenbosgo.mn/>

<http://deedbolovsrol.num.edu.mn/>

DEPLOY HONEYNET





АСУУЛТ



Mongolian Cyber Emergency Response Team / Coordination Center