



Mongolian Cyber Emergency Response Team / Coordination Center

ЦАХИМ АЮУЛГҮЙ БАЙДЛЫН МЭДЭЭЛЭЛ УДИРДЛАГЫН ТӨВ

А.МӨНХБОЛД



Mongolian Cyber Emergency Response Team / Coordination Center

ҮЙЛ АЖИЛЛАГАА



Cyber drill



Training



Information sharing



Public awareness



Collaborate



Mongolian Cyber Emergency Response Team / Coordination Center

ОЛОН УЛСЫН ХАРИЛЦАА

ОЛОН УЛСЫН ХАРИЛЦАА



ХАМТЫН АЖИЛЛАГАА

ХАМТЫН АЖИЛЛАГАА



ХАРИЛЦАА ХОЛБООНЫ
ЗОХИЦУУЛАХ
ХОРОО



DCERT

DATACENTER EMERGENCY RESPONSE TEAM



МОНГОЛ УЛСЫН ШИНЖЛЭХ УХААН
ТЕХНОЛОГИЙН ИХ СУРГУУЛЬ

МЭДЭЭЛЭЛ, ХОЛБООНЫ ТЕХНОЛОГИЙН
СУРГУУЛЬ



МЭДЭЭЛЛИЙН АЮУЛГҮЙ
БАЙДЛЫН ГАЗАР

ГИШҮҮН БАЙГУУЛЛАГУУД



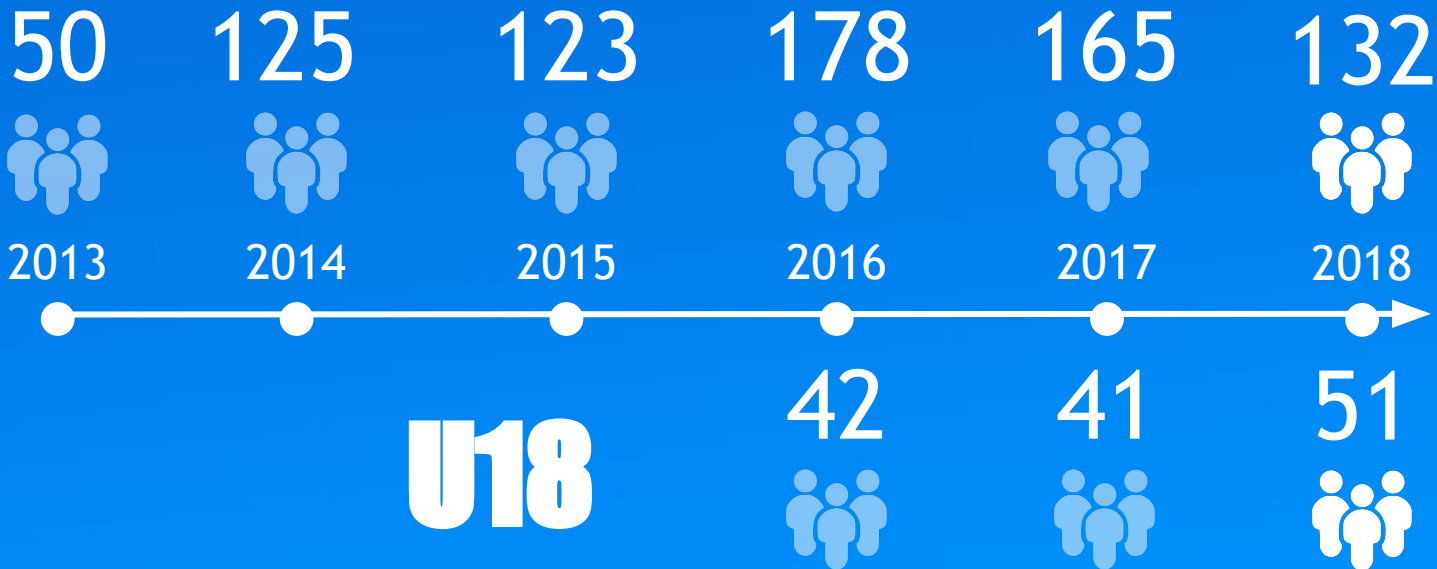
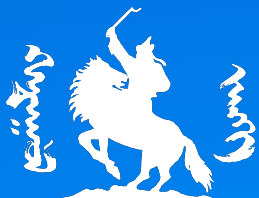
ЗОХИОН БАЙГУУЛСАН АЖИЛ

ХАРУУЛ ЗАНГИ

2013 оноос жил бүр



ХАРУУЛ ЗАНГИ



МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ӨДӨРЛӨГ

2014-оос хойш жил бүр



МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ӨДӨРЛӨГ

+1000



2014

2015

2016

2017

2018

MNSEC 2017



210



10

ЭМЭГТЭЙ



200

ЭРЭГТЭЙ



28

ОЮУТАН



182

АЖИЛТАН



45

ТӨРИЙН
ТӨЛӨӨЛӨЛ

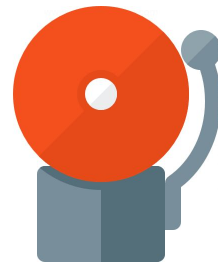


137

ХУВИЙН
ХЭВШИЛ

CYBER DRILL

2016 оноос жил бүр



Cyber Security Training

2016 оноос жил бүр



CISSP training



ХЭРЭГЖҮҮЛЖ БАЙГАА ТӨСЛҮҮД

ALERT - MNCERT/CC

ALERT.MN MNCERT/CC
member

АЛЕРТ
Ерөнхий мэдээлэл

ХӨРӨНГӨ
IP хянг., Домайн нэр, BIN

FS-ISAC
Төлбөргүй мэдээлэл

МЭДЭЭ
Гадаад, Дотоод мэдээ

САН
Харууцат материал

ИНДИКАТОР
IP, URL, MDS, SHA1

TLP: Amber

Incident сүүлийн 48 цаг

Сүүлийн 48 цагийн байдлаар ямар нэг асуудал илэрсэнгүй.

Далгарангүй

Type of Events сүүлийн 3 хоног

12067
Events

Infection

Vulnerability

Other

Collected Events сүүлийн 14 хоног

FS-ISAC 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., Домайн нэр, BIN

FS-ISAC
Төлбөргүй мэдээлэл

МЭДЭЭ
Гадаад, Дотоод мэдээ

САН
Харууцат материал

ИНДИКАТОР
IP, URL, MDS, SHA1

TLP: Amber

Incident сүүлийн 48 цаг

Сүүлийн 48 цагийн байдлаар ямар нэг асуудал илэрсэнгүй.

Далгарангүй

Type of Events сүүлийн 3 хоног

14072
Events

Infection

Vulnerability

Other

Collected Events сүүлийн 14 хоног

FS-ISAC нийтэлсэн 12 мэдээлэл

ОГНОО	АНГИЛАЛ	TLP	ГАРЧИГ	ИХ СУРГАЛ
2017.02.13	Vulnerabilities	green	(CVE/2017-0523) HP Multiple Products Emscrt Vulnerability	hp.com
2017.02.13	Vulnerabilities	green	Mac OSx Multiple Vulnerabilities	apple.com
2017.02.13	Vulnerabilities	green	Mac OSx Multiple Vulnerabilities	apple.com
2017.02.13	Vulnerabilities	green	MS Threat Operations Threatening Recovery Manager: Multiple Vulnerabilities	ms.com
2017.02.13	Vulnerabilities	green	Red Hat updates for glibc 2.6 branches	redhat.com
2017.02.13	Vulnerabilities	green	Oracle Linux updates for kernel-ck	oracle.com
2017.02.13	Vulnerabilities	green	Lenovo Multiple ThinkPad and ThinkCentre Products X250X Graphics Drivers Multiple Vulnerabilities	lenovo.com
2017.02.13	Vulnerabilities	green	Net Range Corporation and Cisco IOS: Net Multiple Vulnerabilities	netrange.com
2017.02.13	Incidents	amber	Member Submission: Post-Scan Activity observed December 2016	secops.com
2017.02.13	Incidents	amber	Member Submission: "WEB Online Access Limitation/SUSPECTED SPAM" - BBA Themed Phishing E-mail	bbat.com
2017.02.13	Incidents	amber	Member Submission: Trojan Check Activity observed on January 12, 2017	secops.com

FAKAS БИРСЭН ӨМӨГ нийтэлсэн 11 мэдээлэл

ОГНОО	ГАРЧИГ	ИХ СУРГАЛ
2017.02.15	An University Web Page's Malware Scan on Open-Door: Mirror Site Infected With a Trojan	university.com
2017.02.14	Web Sites Reported to a Cybersecurity Researcher About Malware Infection	research.com
2017.02.14	IT Issues: Set Budgets for better security by using threats on a wide of sites to follow	firewatch.com
2017.02.14	Microsoft Response Center Issues: User Agent: unwanted-receive-ads	ms.com
2017.02.12	Web Sites Reported to a Cybersecurity Researcher About Malware Infection	research.com
2017.02.12	Bank security processes for non-profiles and journals in the United States, early 2017	bank.com
2017.02.11	Using group events on external webPages sites affects - On page	group.com
2017.02.10	Forward messages: attacks and defense	bing.com
2017.02.10	Several Polish banks hacked, information stolen by unknown attackers	bank.com
2017.02.10	The function of measurement tool 1	me.com

New Indicators нийтэлсэн 10 мэдээлэл

TLP: Amber

280
Indicators

Phishing

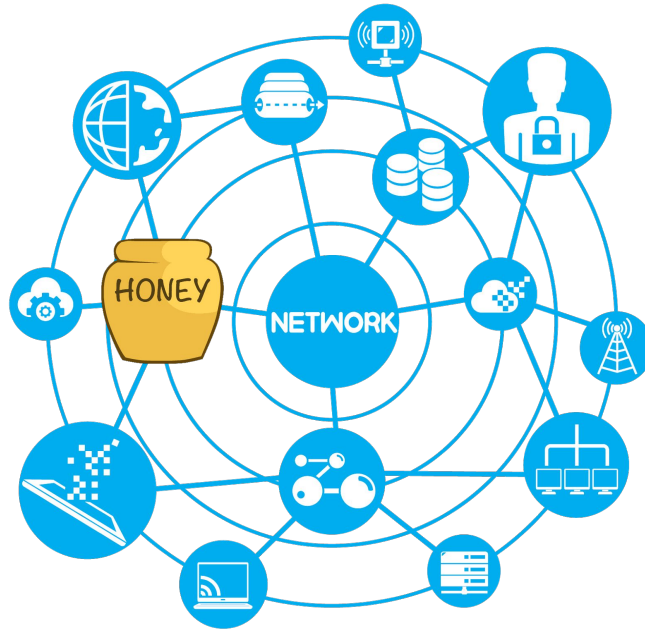
Malware

Харууцат мэдээлэл

TLP	ИП	Тайлбар
Green	Microsoft Security Intelligence Report - January	Microsoft: 2016 New Year's Eve security report: important steps to protect your company's website, apps, and data: https://www.microsoft.com/en-us/security/default.aspx?sa=msi-rpt-2017-01-01

Монгол Улсын Ерөнхий Мэдээлэл, Судалгаа, Өргөтгөл, Өвчлөлтийн Төв

HONEYPOT



Цаашид хийгдэх ажил



Mongolian Cyber Emergency Response Team / Coordination Center

Malware information sharing platform

Mongolia

Infected Mail

TIME PERIOD: Last week Last month

Top - Infected Mail IN THE LAST MONTH

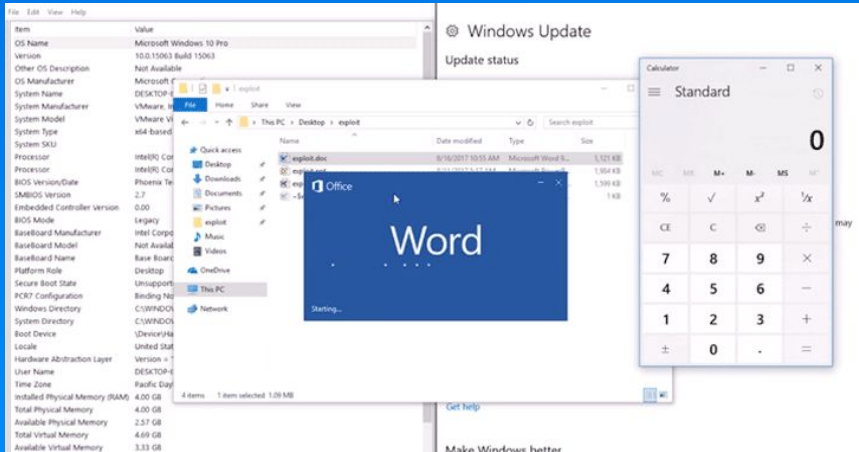


Top - Infected Mail IN THE LAST MONTH

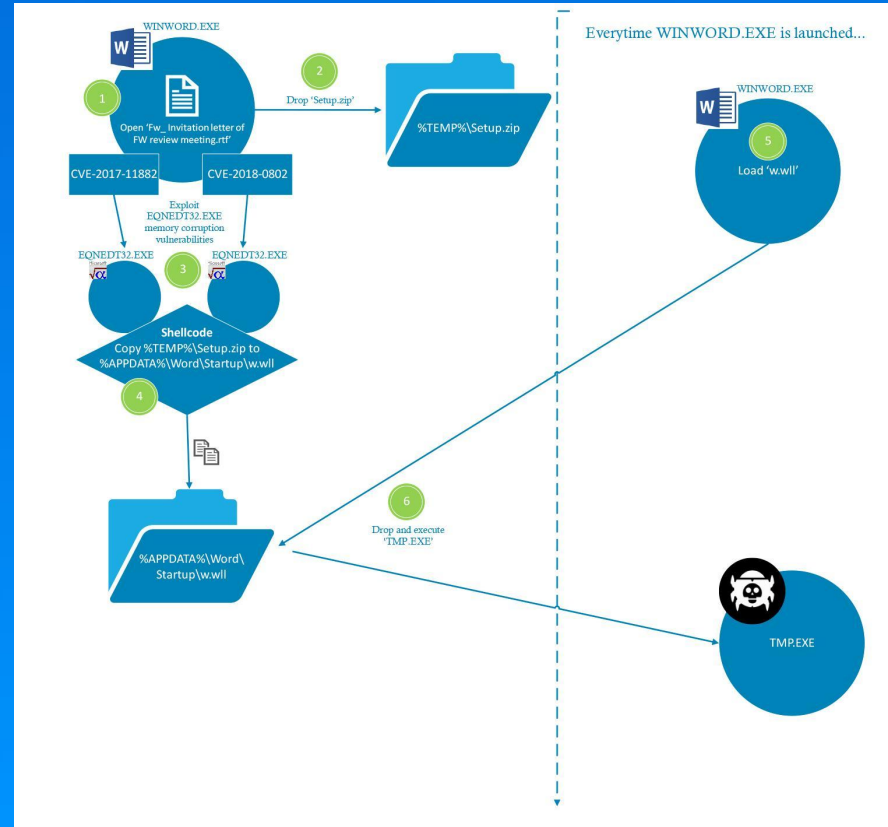
1	Exploit.Win32.CVE-2017-11882.gen	14.25%
2	Trojan.PDF.Badur.gen	11.6%
3	Backdoor.Win32.Androm.gen	6.27%
4	Exploit.RTF.Agent.a	5.66%
5	Trojan-Dropper.PDF.Bedih.a	4.81%
6	Worm.Win32.WBVB.vam	3.77%
7	DangerousObject.Multi.Generic	3.69%
8	Trojan-Dropper.Win32.Injector.gen	3.29%
9	Trojan.OLE2.Badur.gen	3.29%
10	Trojan.HTML.Fraud.gen	3.23%

CVE 2017-11882

17 YEARS OLD



CVE-2018-0802



NETWROK

Mongolia

Network attacks

TIME PERIOD: Last week Last month

Top - Network attacks IN THE LAST MONTH



Top - Network attacks IN THE LAST MONTH

1	Intrusion.Win.MS17-010.o	62.83%
2	Intrusion.Win.MS17-010.p	20.9%
3	Bruteforce.Generic.Rdp.d	1.25%
4	Bruteforce.Generic.Rdp.a	1.14%
5	Intrusion.Win.MS17-010.e	0.44%
6	Intrusion.Win.NETAPI.buffer-overFlow.exploit	0.41%
7	Intrusion.Win.CVE-2017-7269.cas.exploit	0.33%
8	Intrusion.Generic.CVE-2017-10271.exploit	0.07%
9	Intrusion.Win.CVE-2017-0147.sa.leak	0.04%
10	Bruteforce.Generic.Rdp.c	0.01%



- MISP XML and JSON
- OpenIOC
- STIX XML and JSON (export)
- Suricata export
- Snort export
- CSV export
- GFI Import



Mongolian Cyber Emergency Response Team / Coordination Center