CERT/CC

Mongolian Cyber Emergency Response Team / Coordination Center

ЦАХИМ АЮУЛГҮЙ БАЙДЛЫН МЭДЭЭЛЭЛ УДИРДЛАГЫН ТӨВ

А.МӨНХБОЛД

MN CERT/CC

Mongolian Cyber Emergency Response Team / Coordination Center

MN CERT/CC

ҮЙЛ АЖИЛЛАГАА

Cyber drill

Training

Information sharing

Public awareness

Collaborate

MN CERT/CC

Mongolian Cyber Emergency Response Team / Coordination Center

MN CERT/CC

ОЛОН УЛСЫН ХАРИЛЦАА

ОЛОН УЛСЫН ХАРИЛЦАА

ХАМТЫН АЖИЛЛАГАА

ХАМТЫН АЖИЛЛАГАА

ХАРИЛЦАА ХОЛБООНЫ ЗОХИЦУУЛАХ ХОРОО

DCERT
DATACENTER EMERGENCY RESPONSE TEAM

ШУТИС
МОНГОЛ УЛСЫН ШИНЖЛЭХ УХААН ТЕХНОЛОГИЙН ИХ СУРГУУЛЬ
МЭДЭЭЛЭЛ, ХОЛБООНЫ ТЕХНОЛОГИЙН СУРГУУЛЬ

НМТГ

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ГАЗАР

ГИШҮҮН БАЙГУУЛЛАГУУД

GOLOMT BANK

itools
ЗОГСОЛТГҮЙ ХӨГЖИЖ, АМЖИЛТААРАА ЯЛГАРЪЯ

XACBANK

MobiCom

ТӨРИЙН БАНК

ҮНЭТ ЦААСНЫ ТӨВЛӨРСӨН ХАДГАЛАМЖИЙН ТӨВ

UNITEL

KHAN BANK

MONGOLIA NETCOM
NATIONWIDE BROADBAND NETWORK

TDB
ХУДАЛДАА ХӨГЖЛИЙН БАНК

SKYtel

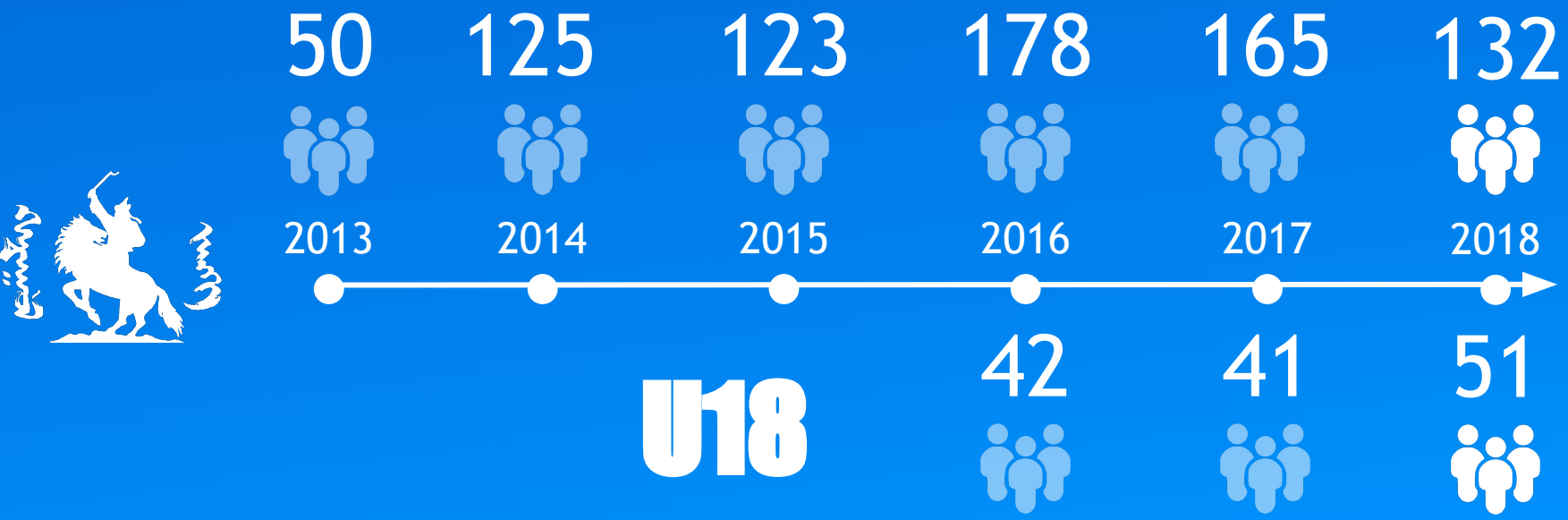
ЗОХИОН БАЙГУУЛСАН АЖИЛ

ХАРУУЛ ЗАНГИ

2013 оноос жил бүр

MN CERT/CC
Mongolian Cyber Emergency Response Team - Coordination Center

ХАРУУЛ ЗАНГИ



МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ӨДӨРЛӨГ

2014-оос хойш жил бүр

MN CERT/CC

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ӨДӨРЛӨГ

2014 2015 2016 2017 2018

MN CERT/CC
Mongolian Cyber Emergency Response Team Coordination Center

MNSEC 2017

210

10
ЭМЭГТЭЙ

200
ЭРЭГТЭЙ

28
ОЮУТАН

182
АЖИЛТАН

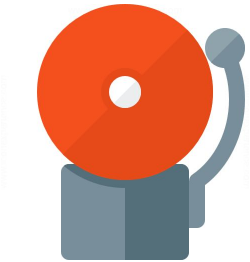
45
ТӨРИЙН
ТӨЛӨӨЛӨЛ

137
ХУВИЙН
ХЭВШИЛ

MN CERT/CC
Mongolian Cyber Emergency Response Team - Coordination Center

CYBER DRILL

2016 оноос жил бүр



MN CERT/CC

Cyber Security Training

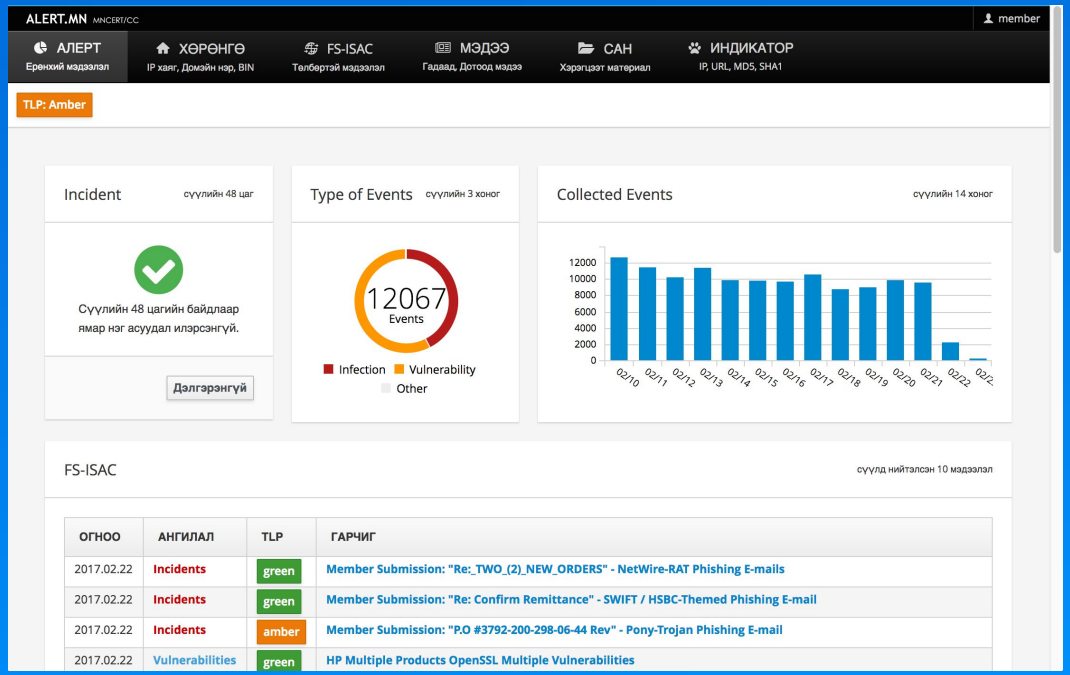
2016 оноос жил бүр

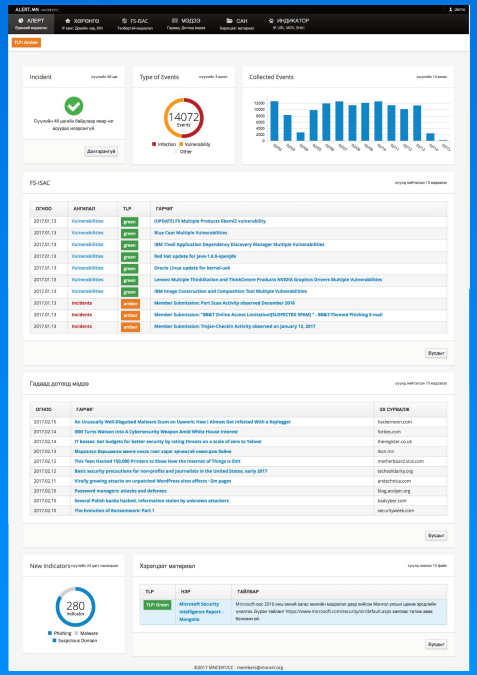
MN CERT/CC
Mongolian Cyber Emergency Response Team Coordination Center

CISSP training

ХЭРЭГЖҮҮЛЖ БАЙГАА ТӨСЛҮҮД

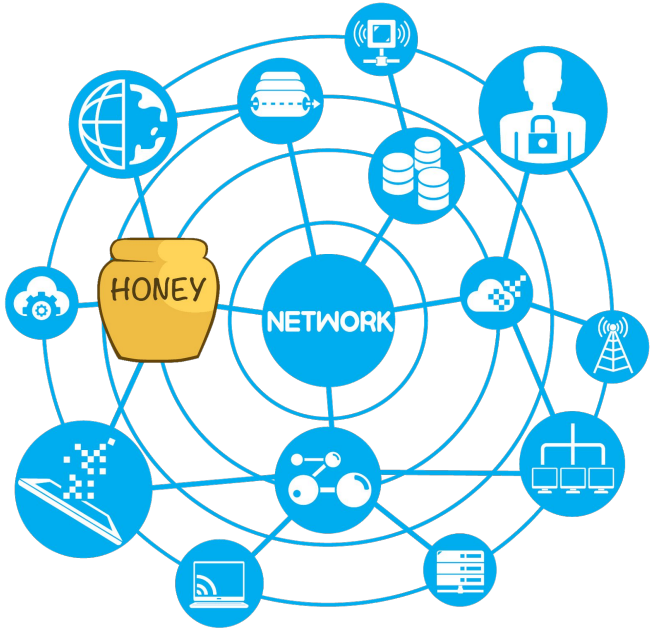
ALERT - MNCERT/CC





MN CERT/CC
Mongolian Cyber Emergency Response Team - Coordination Center

HONEYPOT



Цаашид хийгдэх ажил

MN CERT/CC

Mongolian Cyber Emergency Response Team / Coordination Center

MN CERT/CC

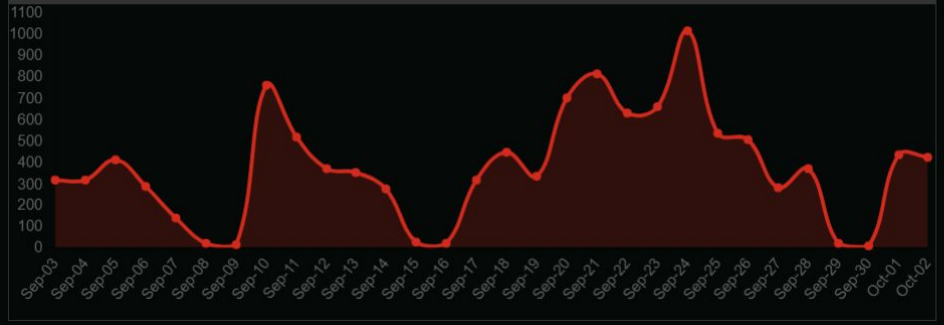
Malware information sharing platform

MN CERT/CC
Mongolian Cyber Emergency Response Team Coordination Center

MAIL

Mongolia ▾ Infected Mail ▾ TIME PERIOD: ○ Last week ◉ Last month

Top - Infected Mail IN THE LAST MONTH

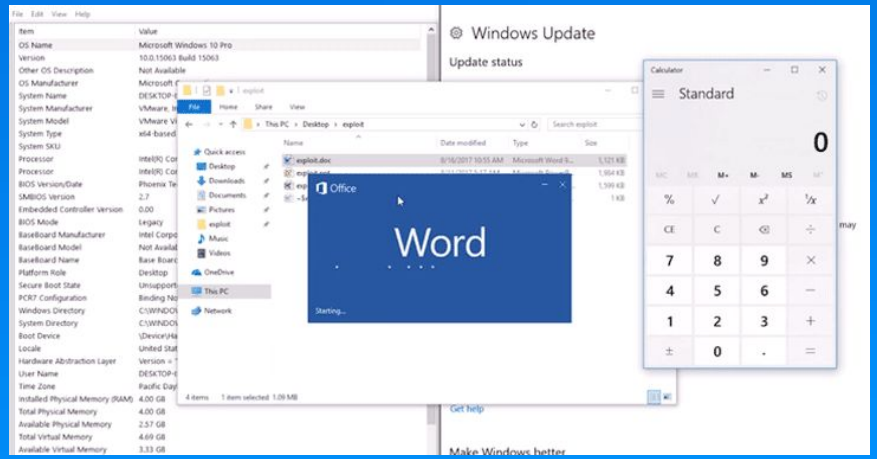


Top - Infected Mail IN THE LAST MONTH

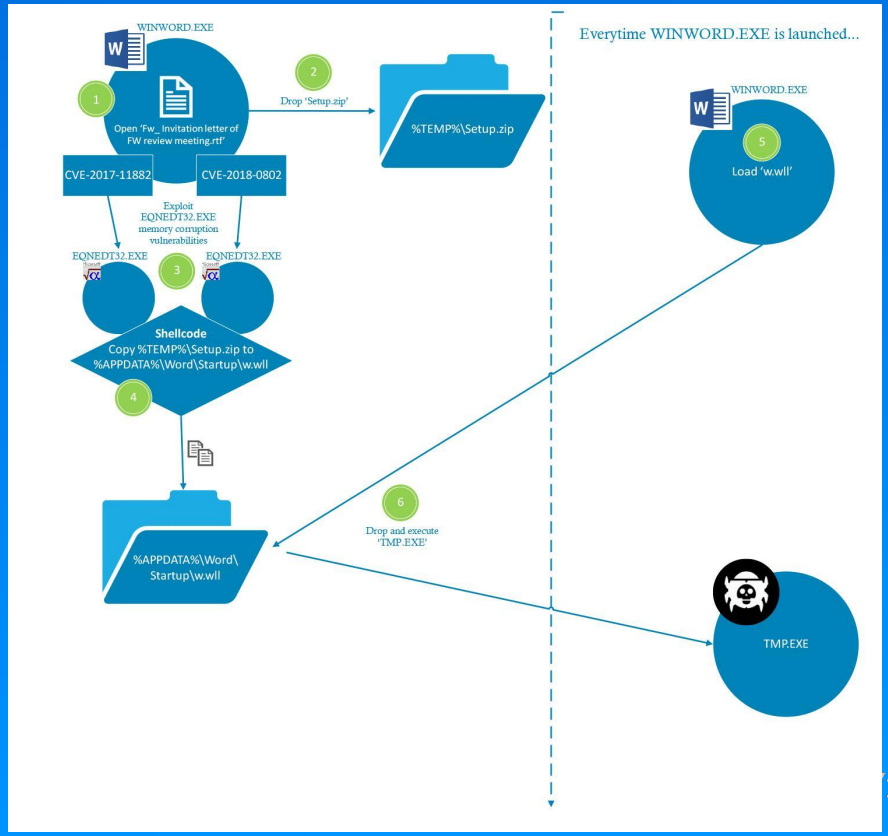
1	Exploit.Win32.CVE-2017-11882.gen	14.25%
2	Trojan.PDF.Badur.gen	11.6%
3	Backdoor.Win32.Androm.gen	6.27%
4	Exploit.RTF.Agent.a	5.66%
5	Trojan-Dropper.PDF.Bedih.a	4.81%
6	Worm.Win32.WBVB.vam	3.77%
7	DangerousObject.Multi.Generic	3.69%
8	Trojan-Dropper.Win32.Injector.gen	3.29%
9	Trojan.OLE2.Badur.gen	3.29%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

CVE 2017-11882

17 YEARS OLD



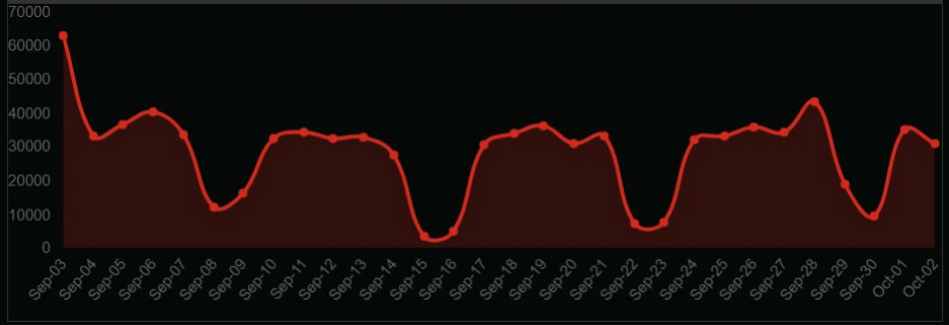
CVE-2018-0802



NETWROK

Mongolia ▾ Network attacks ▾ TIME PERIOD: Last week Last month

Top - Network attacks IN THE LAST MONTH



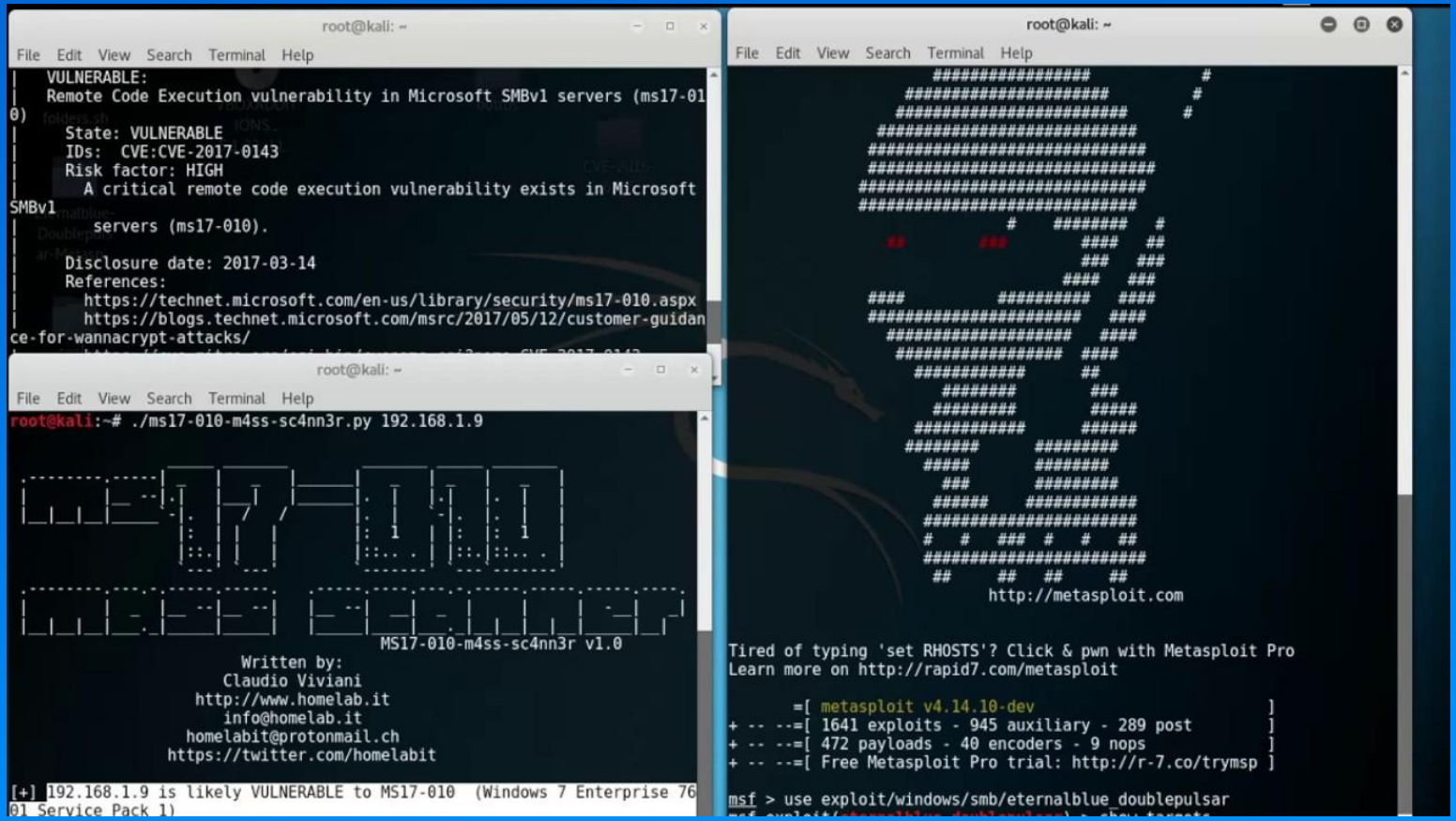
Top - Network attacks IN THE LAST MONTH

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%

MN CERT/CC

KASPERSKY lab

MS 17-010



WIN VISTA
WIN 7 (all)
WIN 2008
WIN 2008r2
WIN 10 (all)
WIN 2012
WIN 2012r2
WIN 2016 dc
WIN 2016


MISP
Threat Sharing
UI USERS
IP
EVENT A
EVENT B
Database
API USERS
API
MISP XML and JSON
OpenIOC
STIX XML and JSON (export)
Suricata export
Snort export
CSV export
GFI import

CERT/CC

Mongolian Cyber Emergency Response Team / Coordination Center