Монголын банкны сектор руу чиглэсэн имэйл халдлага

МБХ – МАБ мэргэжлийн зөвлөл
З.Ганбагана (Голомт банк)

Яагаад имэйлийн аюулгүй байдал чухал вэ?

1

10,000 ажилтантай байгууллага нь фишингд 1.6 сая доллар алддаг.

2

Нийт имэйлийн 60 хувь имэйл халдлага байдаг

3

Имэйл хүлээсэн авсан ажилчдын 31 хувь фишинг имэйлийг нээдэг.

4

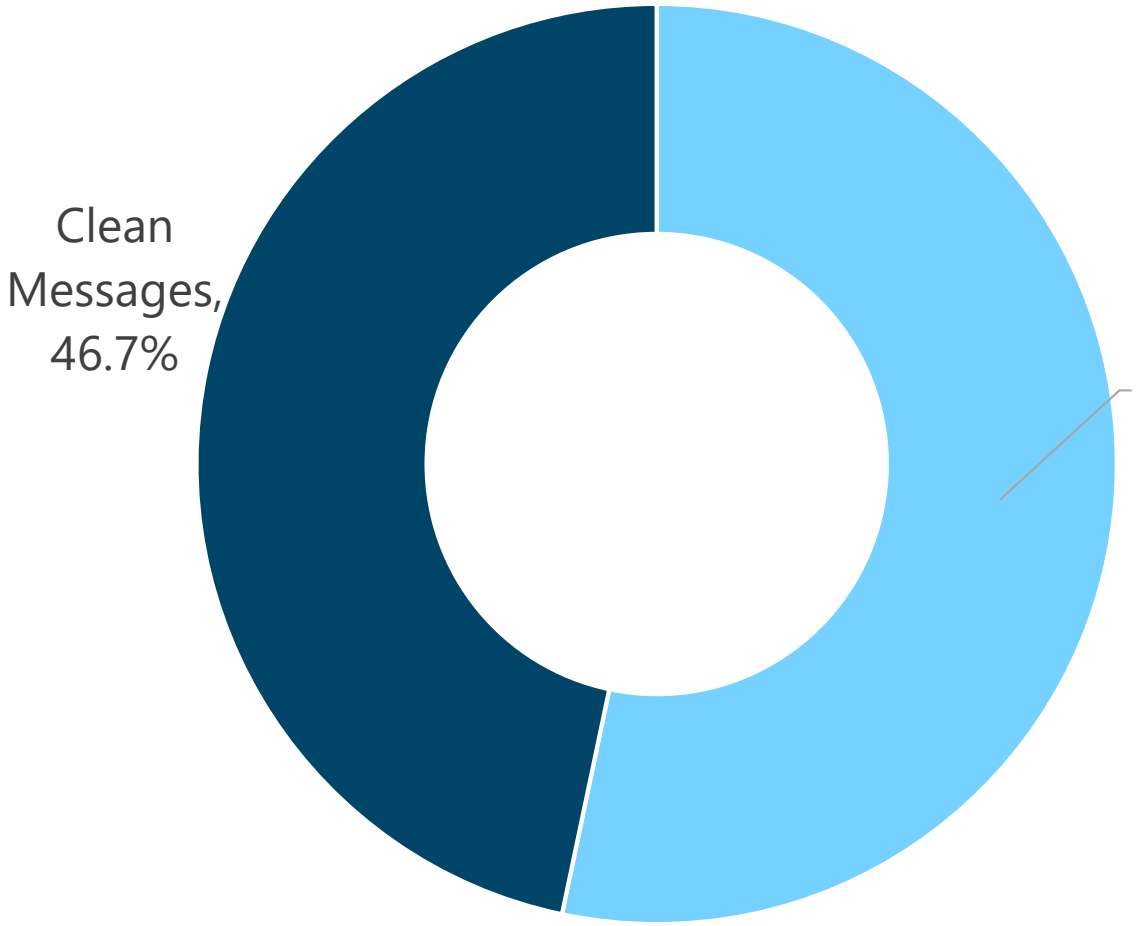
12 хувь нь фишинг өртдөг.

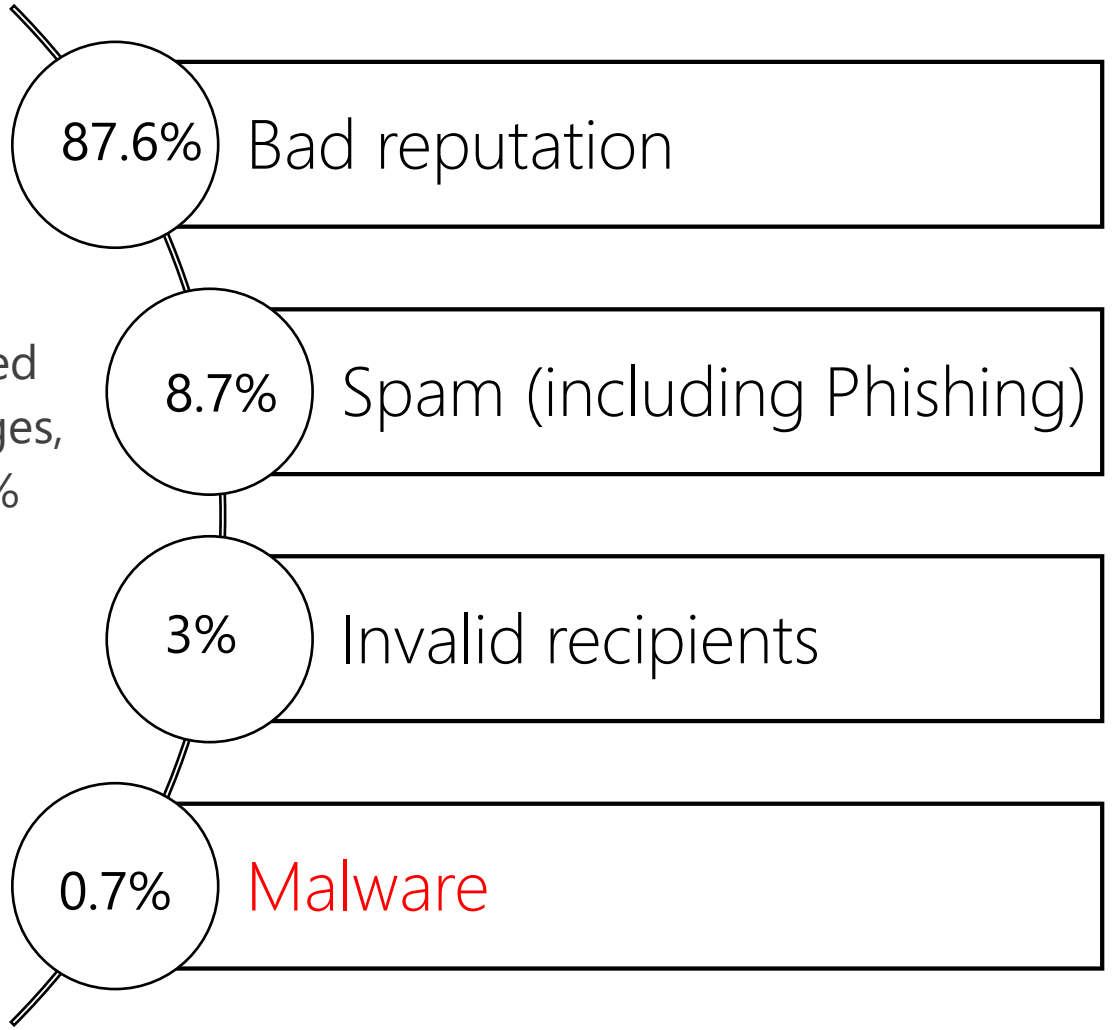
5

131 имэйл тутамд нэг хортой хавсралт файл байдаг.

Эх сурвалж: https://heimdalsecurity.com/blog/cyber-security-threats-types/

Монголын банкны сектор - Имэйл урсгалын шинжилгээ





Date Range: 2019/01/01 to 2019/08/31

Total email: 2,426,153

№	Sender Domain	Stopped by Reputation Filtering
1	No Domain Information	46.17%
2	google.com	3.55%
3	hostwindsdns.com	2.83%
4	arubacloud.fr	2.46%
5	163data.com.cn	1.45%
6	sendgrid.net	1.01%
7	vnpt.vn	1.00%
8	zare.com	0.85%
9	quadranet.com	0.75%
10	arubacloud.com	0.68

Date Range: 2019/01/01 to 2019/08/31

1

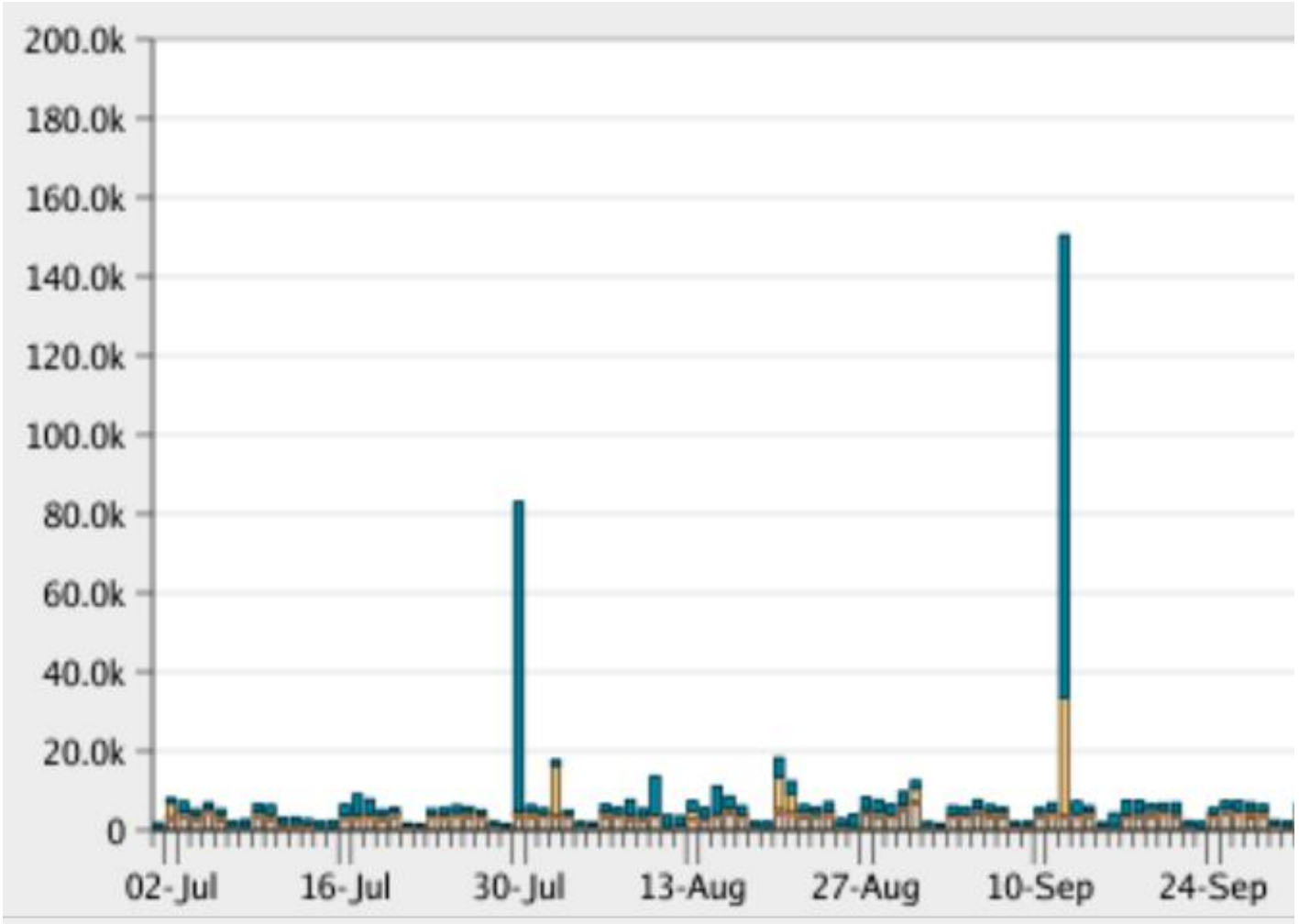
Bad reputation

- **Sender Base Reputation Score (SBRS)**
- **Spam complaints, spam traps, unknown users**

Case

Email Bomb

ID	1	2
Date	30-Jul	12-Sep
Hostname	exmoda.jp	No domain
Quantity	82.1k	154.1k
Blocked Reason	Black Listed	Unknown Domain
IP address	133.242.24[.]196	176.107.198[.]174



№	Sender Domain	Total
1	yahoo.com	3.79%
2	latest-businesstrends.com	3.51%
3	corporate-courses.com	2.97%
4	Beastmasterclass.com	2.60%
5	outlook.com	2.43%
6	unistrategic.com	2.38%
7	Google.com	1.82%
8	i-globalearning.com	1.72%
9	masterclass-learninggroup.com	1.53%
10	eventtrainingexpert.com	1.50%

Date Range: 2019/01/01 to 2019/08/31

2

Spam (including Phishing)

- **Free Email service**
- **Training (Kuala Lumpur, Malaysia)**

№	Spam/Phishing
1	Mailbox size limit exceeded
2	Electrical Maintenance (High Voltage)
3	[Copied display name]
4	Power & Distribution Transformers
5	Хүлээгдэж буй Мэйлүүдээ хүлээн авахын тулд шинэчилнэ үү

Wed 3/6/2019 8:09 PM

HV

High Voltage Maintenance <will@bestmasterclass.com>

[SUSPECTED SPAM] Electrical Maintenance (High Voltage)

To [redacted]

High Voltage Electrical Maintenance

Enhance your understanding in Maintenance Requirements of an Electrical Network System and learn the Interaction between Supply Authorities and HV Customers

25th – 26th April 2019 in Kuala Lumpur, Malaysia
&
28th – 29th April 2019 in Dubai, UAE

Dear Colleagues,

The primary reason that power is transmitted at high voltages is to increase efficiency.

As electricity is transmitted over long distances, there are inherent energy losses along the way.

High voltage transmission minimizes the amount of power lost as electricity flows from one location to the next.

The higher the voltage, the lower the current. The lower the current, the lower the resistance in the conductors.
And when resistance is low, energy losses are low also. Electrical engineers consider factors such as the power being transmitted and the distance required for transmission whendetermining the optimal transmission voltage.

In this workshop, participants will have the opportunity to understand the additional requirement of an Electrical Industry Workforce and learn the case studies of High Voltage Electrical Incidents.

- EXAMINE the Training Requirements of an Electrical Industry Workforce and what should be considered
- IDENTIFY the Maintenance Requirements of an Electrical Network System
- LEARN the advantages and disadvantages of Live Line Maintenance compared with Shutting off the Power Supply
- EXPLORE the case studies related to High Voltage (HV) Electrical Incidents
- DESCRIBE the Live Line Capabilities in terms of Glove & Barrier, Hot Stick, Bare Hand and Helicopter Maintenance

Wed 8/7/2019 2:57 AM

A

Administrator <htk@huitoukefood.com>

[External]You will soon exceed your limit {[redacted]}

To [redacted]

You will soon exceed your limit.

Hello {[redacted]}

4560MB 5096MB

Your [redacted] will soon exceeds its limit, you are advised to clean up by deleting unwanted files to increase your [redacted] space without losing any files Follow here.

Thanks,
Administrator.

[SPAM] account was hacked

To . [redacted]

You forwarded this message on 9/26/2018 9:13 AM.

Hello!
I'm a member of an international hacker group.

As you could probably have guessed, your account [redacted] was hacked, I sent message you from it.

Now I have access to you accounts! You still do not believe it?
So, this is your password: com_da , right?

Within a period from July 5, 2018 to September 21, 2018, you were infected by the virus we've created, through an adult website you've visited.
So far, we have access to your messages, social media accounts, and messengers.
Moreover, we've gotten full damps of these data.

We are aware of your little and big secrets...yeah, you do have them. We saw and recorded your doings on porn websites. Your tastes are so weird, you know..

But the key thing is that sometimes we recorded you with your webcam, syncing the recordings with what you watched!
I think you are not interested show this video to your friends, relatives, and your intimate one...

Transfer $700 to our Bitcoin wallet: 1DzM9y4fRgWqpZZCsvf5Rx4HupbE5Q5r4y
I guarantee that after that, we'll erase all your "data" :D

A timer will start once you read this message. You have 48 hours to pay the above-mentioned amount.

Indicators of Compromise (IOC) фишинг сан бүрдүүлэх.

```
attachment-contains("000webhostapp.com", 1)
attachment-contains("<pdf:Producer>Zamzar</pdf:Producer>", 1)
attachment-contains("submit.jotform.us", 1)
attachment-dictionary-match("Free_Hosting_List", 1)
subject == "包装单: Гэрээний гарын үсэг зурсан"
subject == "Гэрээний гарын үсэг зурсан"
attachment-filename == ".uue"
body-contains("Draft Contract Invoice", 1)
body-contains("CONFIRM PROFORMER INVOICE", 1)
body-contains("БАЙГУУЛЛАГЫН ТАТАЖ БАЙНА", 1)
attachment-contains("document.write", 1)
attachment-contains("MABH-SEC-2018", 1)
attachment-contains("<img png;base64", 1)
attachment-contains("dsewxcxdxerdtyjhm.com.ng", 1)
body-contains("000webhostapp.com", 1)
only-body-contains("Consinee Group康赛妮集团", 1)
```

Indicators of Compromise (IOC)
фишинг сан бүрдүүлэх.

```
attachment-contains("MABH-SEC-2018", 1)
attachment-contains("<img png;base64", 1)
attachment-contains("dsewxcxdxerdtyjhm.com.ng", 1)
body-contains("000webhostapp.com", 1)
only-body-contains("Consinee Group康赛妮集团", 1)
attachment-filename == "Fwd 答复 New order.exe"
subject == "20171214Tourtelcom Co., Ltd, Mongolia invoice"
attachment-contains("www.proxiplace.fr", 1)
attachment-contains("dmsseguridad.cl/", 1)
attachment-filename == "Quotation Invoice_9453902538"
attachment-filename == "scan000019"
subject == "account was hacked"
attachment-contains("CARGO CLAIMS MASTER CLASS", 1)
attachment-contains("https://stone-ir.us/honest/honest/r/?email", 1)
attachment-contains("http://my-spa.rs/", 1)
attachment-contains("http://space.makstrimlab.com", 1)
attachment-contains("https://stone-ir.us/", 1)
attachment-contains("https://www.royalfx.co.id/", 1)
attachment-contains("http://pikappasu.com/", 1)
attachment-contains("dapojian.cc", 1)
```

Top Virus Type	Total Infected Messages
CXmail/MalPE-AC	48.32%
CXmail/IsoDl-A	13.24%
Mal/Fareit-U	4.09%
CXmail/RtfObf-D	3.26%
Troj/PDFUri-GXL	3.16%
CXmail/MalPE-P	2.33%
Troj/RtfExp-FB	2.07%
CXmail/PEAut-D	1.81%
CXmail/MalPE-H	1.55%
CXmail/RtfObf-B	1.45%

3

Malware

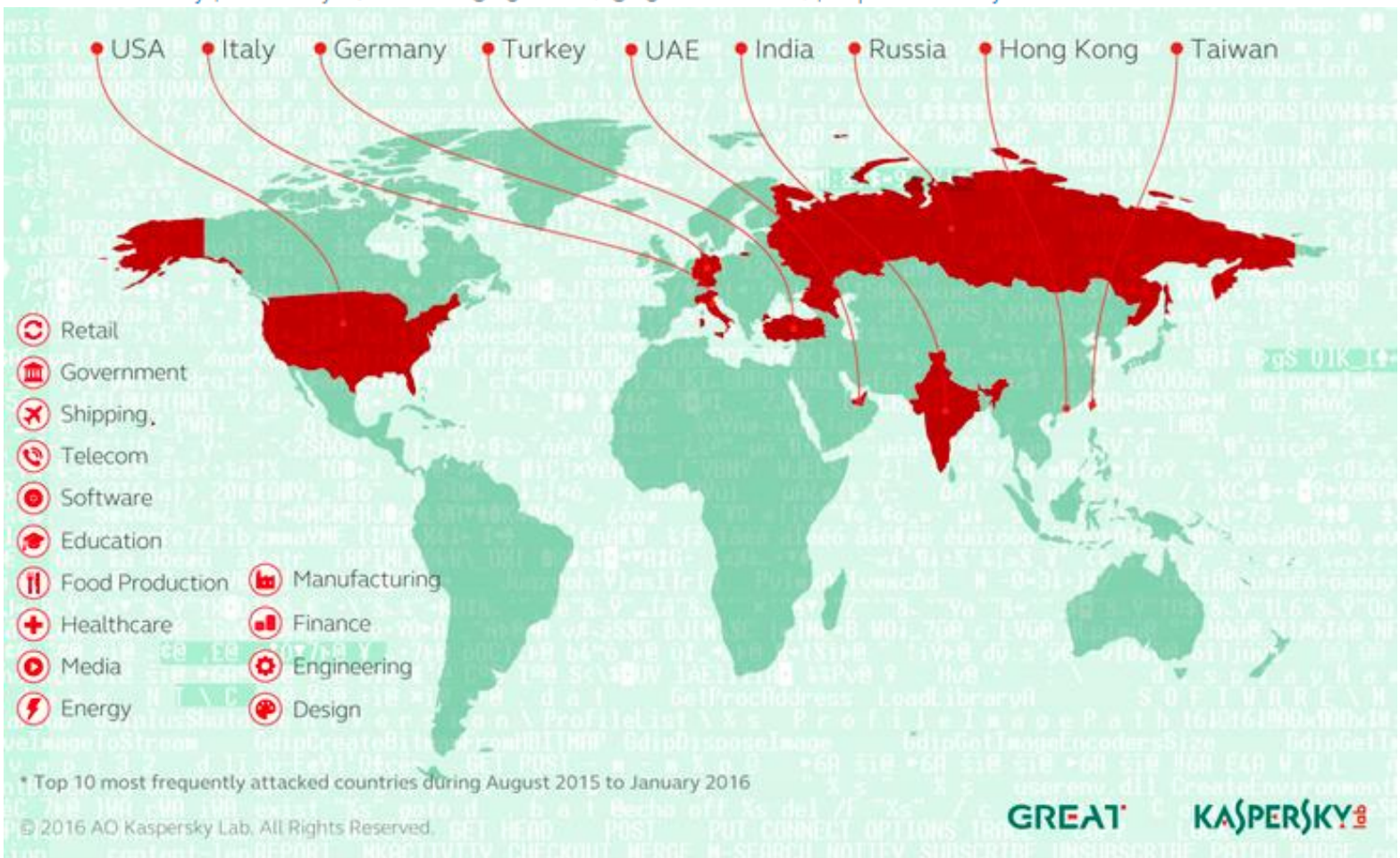
Detected by Anti-Virus: 1933

Detected by Advanced Malware Protection: 138 (can't detect AV)

AlienSpy RAT strikes over 400,000 victims worldwide

Otherwise known as Adwind, the malware-as-a-service platform is still actively attacking both individuals and businesses.

By Charlie Osborne for Zero Day | February 8, 2016 -- 15:29 GMT (23:29 GMT+08:00) | Topic: Security



Campaign 1

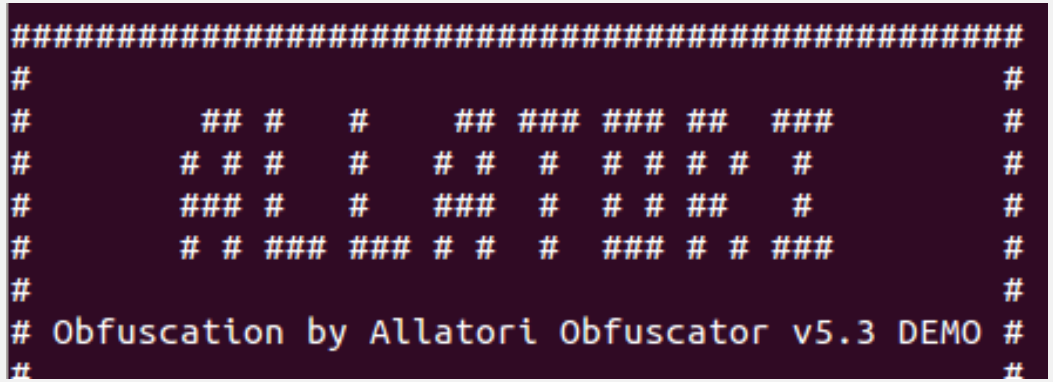
Alien Spy RAT

Date	Phase – 1: 2019-06-11 Phase – 2: 2019-06-13
Sender email	bmw@investpalata.net
Target	Mongolia
Source IP	193.5.85[.]67
Subject	RE: Swarovski Purchase Order 47234614
Attachment	Invoice_revsered_.jar
Malware Name	AlienSpy RAT
Primary CnC host	95.140.125.91
Backup CnC Host	mattwems38.ddns.net
MD5	c320c306fc40e98fb367299ae41237a1

- AlienSpy RAT нь Java суурьтай.
- Windows, Linux, OSX үйлдлийн систем дээр ажиллах чадамжтай.

Боломжууд:

- Дэлгэц хянах
- Зайнаас удирдах
- Keystroke
- Нэмэлт хортой код татаж суулгах.



1. Obfuscator

AlienSpy payloads seen in the wild are typically obfuscated using.

```
Reader)new java.io.InputStreamReader(a));


(new StringBuilder().insert(0, s).append("ALSKEOPQLFKJDUSIKSJAUIE").toString())
```

2.Encryption

The payload is encrypted using an RC4 encryption scheme.

```
Runtime a9 = Runtime.getRuntime();
String[] a10 = new String[10];
a10[0] = "reg";
a10[1] = "add";
a10[2] = "HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run";
a10[3] = "/v";
a10[4] = System.getProperty("JAR_REGISTRY");
a10[5] = "/t";
a10[6] = "REG_SZ";
a10[7] = "/d";
a10[8] = new StringBuilder().append("\\\"").append(System.getProperty("JRE_PATH")).append("\\\"").append(" -jar ")
solutePath()).append("\\\"").toString();
a10[9] = "/f";
a9.exec(a10);
```

3.Persistence

Copied to new directory with %appdata%, create a registry file

```
public static boolean isVMWARE()
{
    if (util.Utils.isLinux())
    {
        return new java.io.File("/etc/vmware-tools").exists();
    }
    if (util.Utils.isMac())
    {
        return new java.io.File("/Library/Application Support/VMware Tools").exists();
    }
    if (!util.Utils.isWindows())
    {
        return false;
    }
    String s = (System.getProperty("os.arch").equalsIgnoreCase("x86")) ? System.getenv("ProgramFiles")
    return new java.io.File(new StringBuilder().append(s).append("\\VMware\\VMware Tools").toString())
}
```

4. Sandbox Detection

When executed AlienSpy checks if it is running within either a VirtualBox or VMWare environment.

```
Alias name: test
Creation date: 17-Jan-2015
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=assylias, O=assylias.Inc, C=FR
Issuer: CN=assylias, O=assylias.Inc, C=FR
Serial number: 1f239dbd
Valid from: Sat Jan 17 00:26:19 EST 2015 until: Mon Dec 24 00:26:19 EST 2114
Certificate fingerprints:
         MD5:  AB:2E:7C:A8:E2:B9:CE:CD:E9:DB:F0:F3:89:23:B8:A2
         SHA1: D6:2E:06:53:11:DF:FC:EC:AD:9F:8E:92:C3:16:AA:FB:60:19:39:4B
         SHA256: 68:99:B6:1C:46:C8:26:08:83:2C:94:45:BD:BA:04:6E:EC:B7:D1:E9
         Signature algorithm name: SHA256withRSA
         Version: 3
```

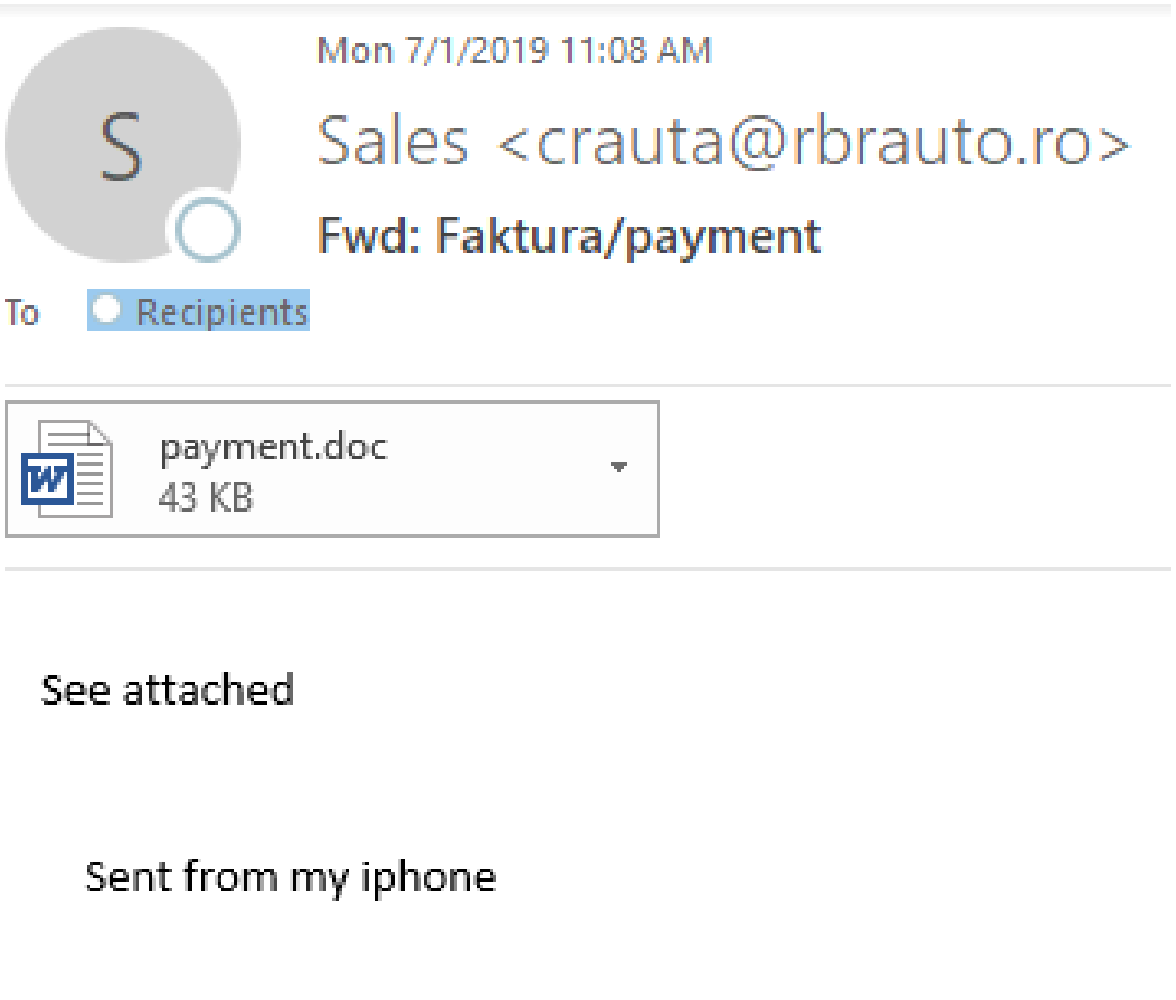
5. Communication

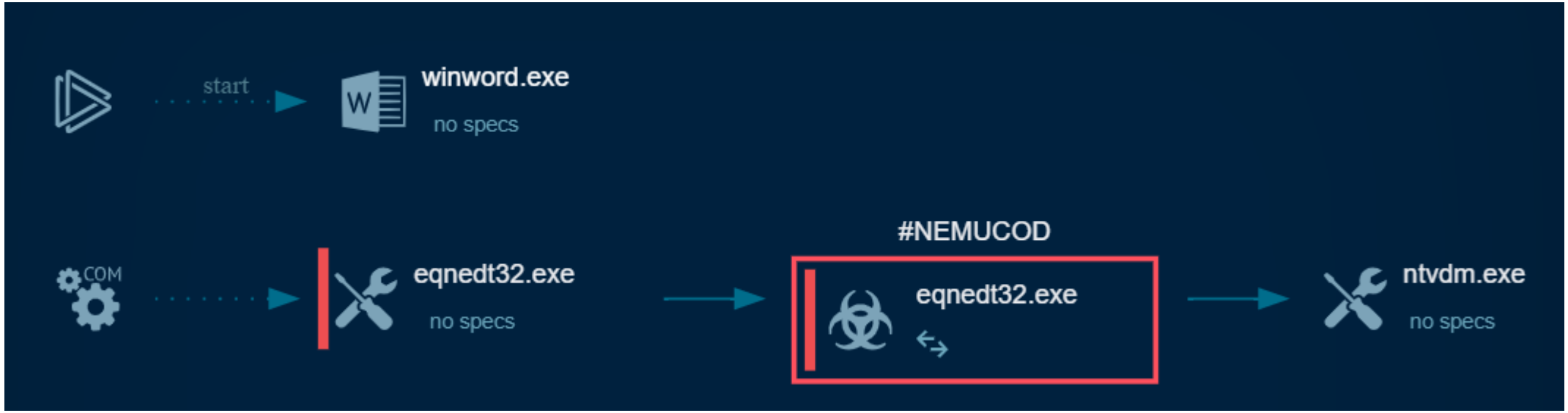
AlienSpy uses SSL Sockets to communicate with the C2 server.

Campaign 2

Trojan.Fareit

Date	2019-04-09 -> 2019-07-01
Sender email	*@fills.ro , *@rbrauto.ro
Target	Mongolia
Subject	Fwd: Faktura/payment
Attachment	payment.doc
Malware Name	Trojan.Fareit CVE-2017-11882 (17-Year Old)
Sender IP	89.40.239[.]246
Primary CnC host	my-spa[.]rs





1

Word файлыг нээнэ.

2

RTF файл ажиллаж эхлэнэ.

3

RTF нь Equation Editor ашиглана.

(CVE-2017-11882)

4

Команд ажиллуулах боломж бүхий CMD.EXE дуудагдана.

5

Хэрэглэгчийн мэдээллийг хулгайлах боломжтой.

Имэйл халдлагын нийтлэг шинж тэмдэг

1

Data Breach болон Public Email

2

Free Web Hosting and Compromised сервер ашигласан.

000webhostapp.com

3

HTTPS:// ашигласан буюу Free SSL/TLS (Let's Encrypt)

4

Document төрлийн файл ихэвчлэн илгээдэг.

(pdf, doc)

5

Банк, санхүүгийн холбогдолтой имэйлүүд

Имэйл халдлагаас урьдчилан сэргийлэх арга хэмжээнүүд

1

Имэйл хамгаалалтын гарц. (Secure Email Gateway)

2

Ажилчдыг имэйлээр ирж болох аюулуудыг ойлгуулах.

3

Сэжигтэй имэйл ирсэн тохиолдолд мэдээлэл хүлээж авах суваг.

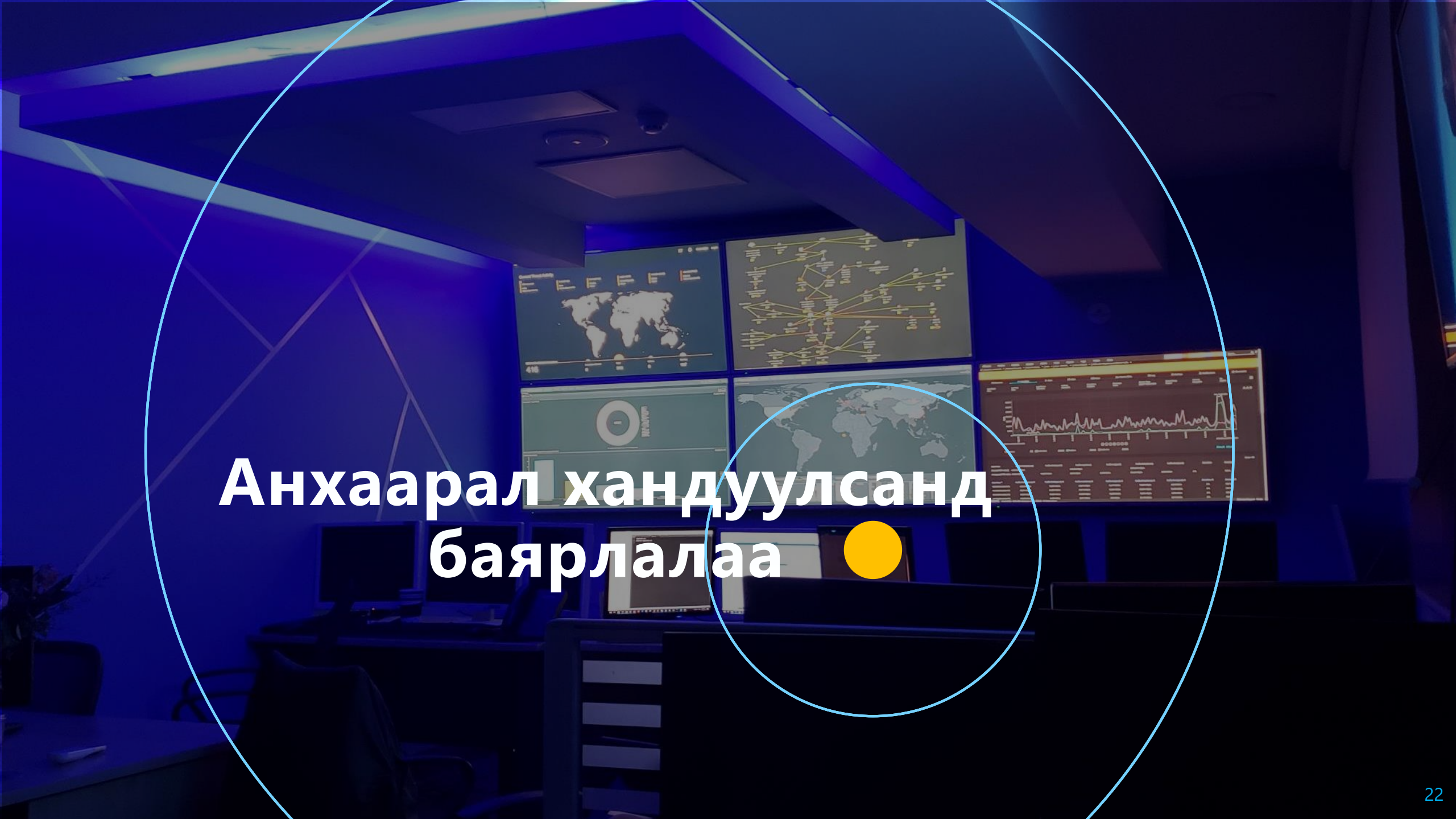
4

Имэйл халдлагын симуляци.

5

Блоклогдсон болон сэжиг бүхий имэйлүүд дээрх анализ

“Information Security Is Everyone’s Responsbility”



Анхаарал хандуулсанд баярлалаа