Hardening Office 365 to reduce attack surface for small business companies

Nasanbuyan Otgonbaatar

Information security specialist
at Mobicom Corporation

Агуулга

- Office 365 үйлчилгээнд гарч буй халдлагууд, түүнээс урьдчилан сэргийлэх
- Office 365 үйлчилгээний аюулгүй байдлыг хангах стандарт, зөвлөмж
- Тохиргоонд үнэлгээ өгөх, дүн шинжилгээ хийх зөвлөмж

Office 365 үйлчилгээнд гарч буй халдлагын зорилго ?

1. **Business email compromises (BECs)**
2. **APT or state-sponsored intrusions**

2019 Crime Types *Continued*

By Victim Loss

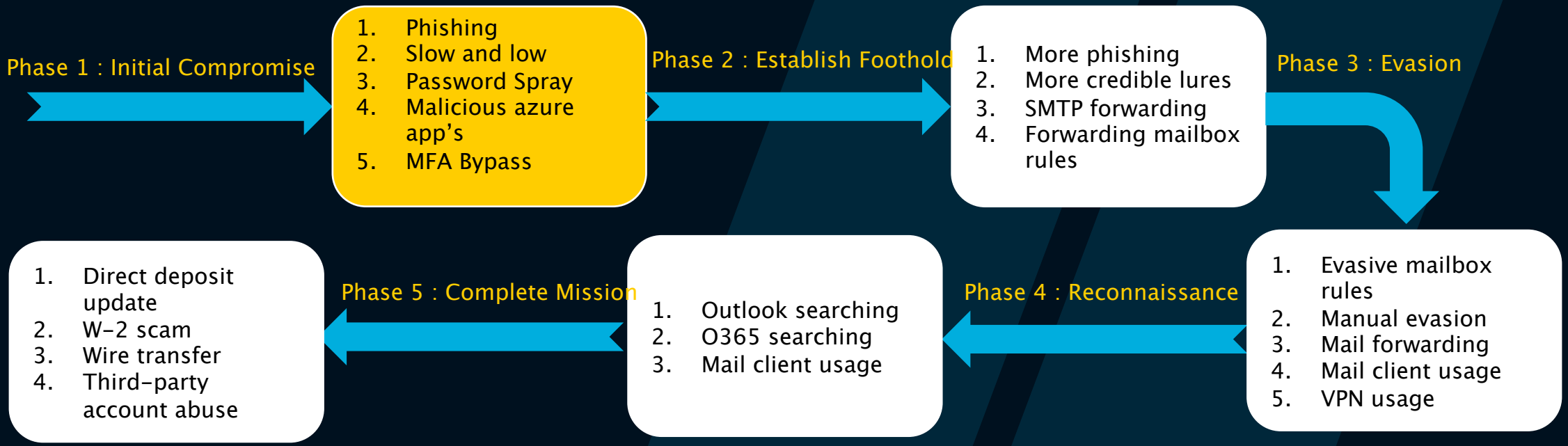
Crime Type	Loss
BEC/EAC	$1,776,549,688
Confidence Fraud/Romance	$475,014,032
Spoofing	$300,478,433
Investment	$222,186,195
Real Estate/Rental	$221,365,911
Non-Payment/Non-Delivery	$196,563,497
Identity Theft	$160,305,789
Government Impersonation	$124,292,606
Personal Data Breach	$120,102,501
Credit Card Fraud	$111,491,163
Extortion	$107,498,956
Advanced Fee	$100,602,297
Other	$66,223,160
Phishing/Vishing/Smishing/Pharming	$57,836,379
Overpayment	$55,820,212
Tech Support	$54,041,053
Corporate Data Breach	$53,398,278
Lottery/Sweepstakes/Inheritance	$48,642,332

Эх сурвалж:

https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120

https://www.fireeye.com/blog/threat-research/2020/07/insights-into-office-365-attacks-and-how-managed-defense-investigates.html

O365 BECs – н бүтэц



Эх сурвалж : https://www.fireeye.com/blog/threat-research/2020/07/insights-into-office-365-attacks-and-how-managed-defense-investigates.html

1. Initial Compromise : Phishing

#	Brand	Unique Phishing URLs	QoQ Growth
1	- PayPal Category: Financial Services	11,392	-31.2%
2	↑2 Facebook Category: Social Media	9,795	-18.7%
3	↓1 Microsoft Category: Cloud	8,565	-38.2%
4	↓1 Netflix Category: Cloud	6,758	-50.2%
5	↑63 WhatsApp Category: Social Media	5,020	13,467.6%
6	↓1 Bank of America Category: Financial Services	4,375	-21.5%

BECs фишинг имэйлын нийтлэг төрлүүд

1. Voice message
2. Action required
3. Shared files
4. …

Missed Audio Calls 181 181 **** at 11/14/2019 12:51:35 PM

AR

[redacted]
emily
Thursday, November 14, 2019 at 8:08 AM
Show Details

Office | Notifications

Hello [redacted]

This voice note was sent by +1 1813[redacted]
You can play the voice call here now

Sent on 11/14/2019 12:51:35 PM

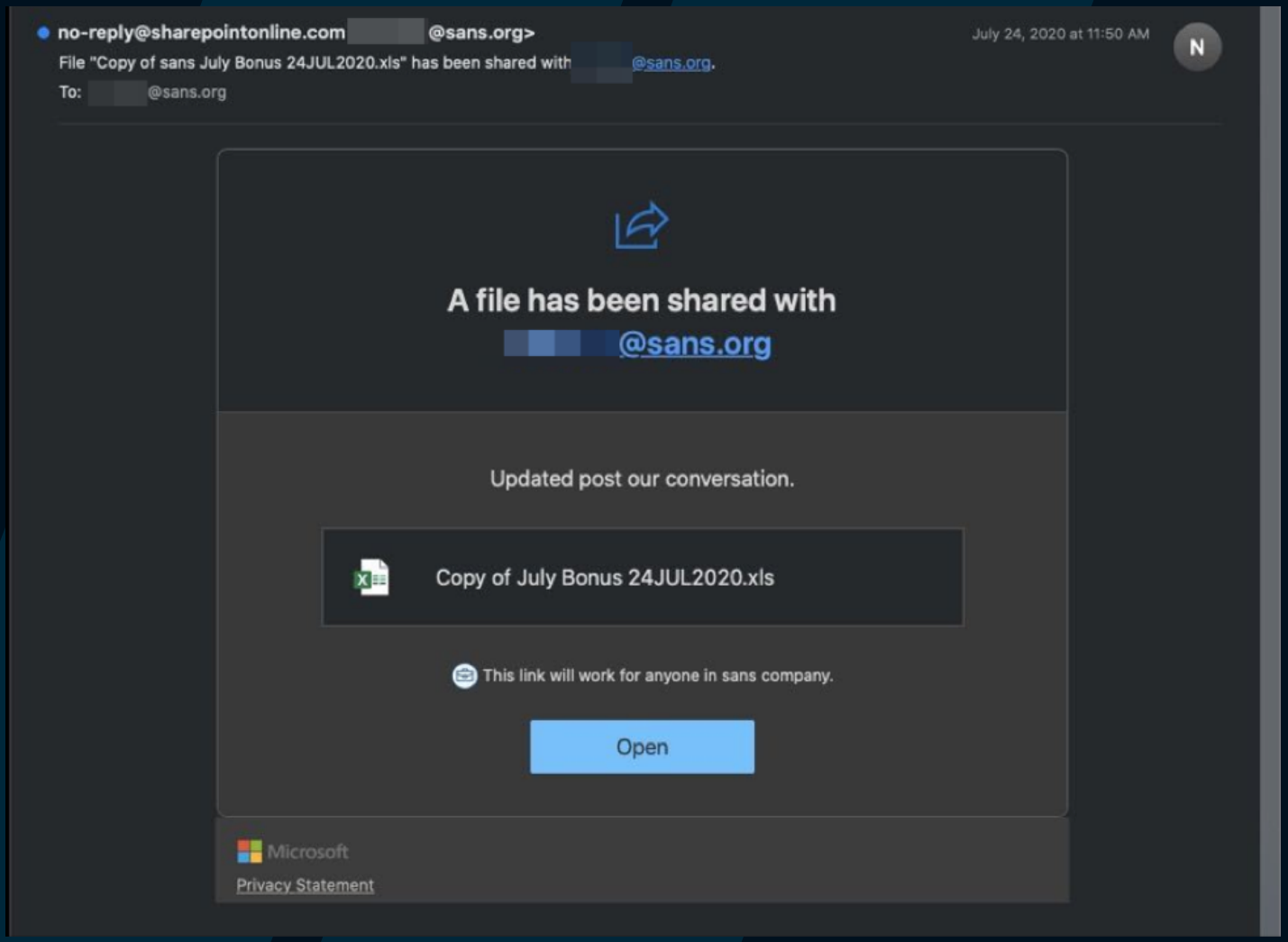
PLAY NOW

сурвалж : https://www.helpnetsecurity.com/2020/02/11/brands-phishing-attacks/

1. Initial Compromise : Phishing

SANS Case : Shared file

- Malicious O365 add-in : Enable4Excel
- Forwarding rule name : Anti Spam Rule
- Keywords for forwarding rule : Bank, cash, fund, Payment, transfer, purchase etc



урвалж : https://www.sans.org/blog/sans-data-incident-2020-indicators-of-compromise/

1. Initial Compromise : Phishing

Халдлагаас сэргийлэх боломжууд ?

- Common attachment types filter
- Exchange online spam policies
- Block client forwarding rules
- ATP safe links
- ATP safe attachments
- DKIM for all domains
- Notifications for internal user sending malware
- Anti-phishing policy

2. Initial Compromise : Slow and low (cloud-to-cloud)

User	Source IP	Org Name	Unix Timestamp	Date
william_warner			1484282725000	20170113
wiwarner@			1484282727000	20170113
warner.william@			1484282727000	20170113
williamwarner@			1484282727000	20170113
williamc@			1484282727000	20170113
warnerwilliam@			1484282727000	20170113
william.warner@			1484282727000	20170113
warner_william			1484282727000	20170113
william-warner@			1484282727000	20170113
warner-william@			1484282727000	20170113
william_c@			1484282728000	20170113
warner.w@			1484282728000	20170113
william-c@			1484282728000	20170113
warnerwi@			1484282728000	20170113
bill.warner@			1484282729000	20170113
wich@			1484282729000	20170113
warner_w@			1484282729000	20170113
will_warner@			1484282729000	20170113
warner.bill@			1484282730000	20170113
warnerwill@			1484282730000	20170113
billwarner@			1484282730000	20170113
billc@			1484282730000	20170113
willwarner@			1484282730000	20170113
warnerbill@			1484282730000	20170113
will-warner@			1484282730000	20170113
bill-warner@			1484282731000	20170113

Эх сурвалж :

https://www.skyhighnetworks.com/cloud-security-blog/skyhigh-discovers-a-targeted-brute-force-attack-on-enterprise-customers/

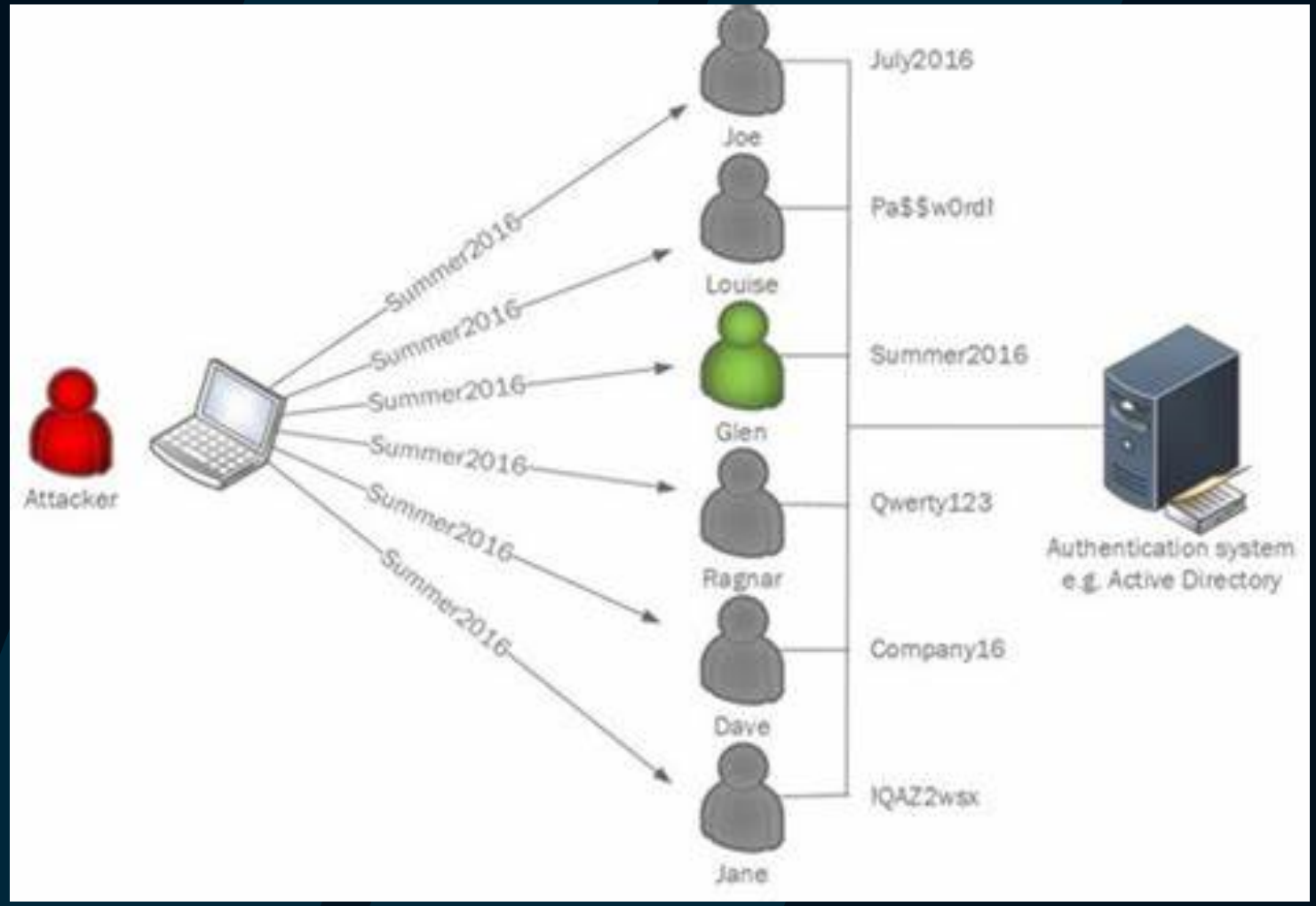
https://threatpost.com/apt28-theft-office365-logins/159195/

2. Initial Compromise : Slow and low (cloud-to-cloud)

Халдлагаас сэргийлэх боломжууд ?

- Multi-factor authentication идэвхжүүлэх
- Амжилтгүй болсон нэвтрэх оролдлогуудыг хянах – Cloud access security broker (CASB)
- Attack simulator in Office 365 ATP
- Ажилчдын мэдлэг чадварыг сайжруулах

3. Initial Compromise : Password Spray



Халдлагаас сэргийлэх боломжууд ?

- Multi-factor authentication
- Azure AD password protection

Эх сурвалж :

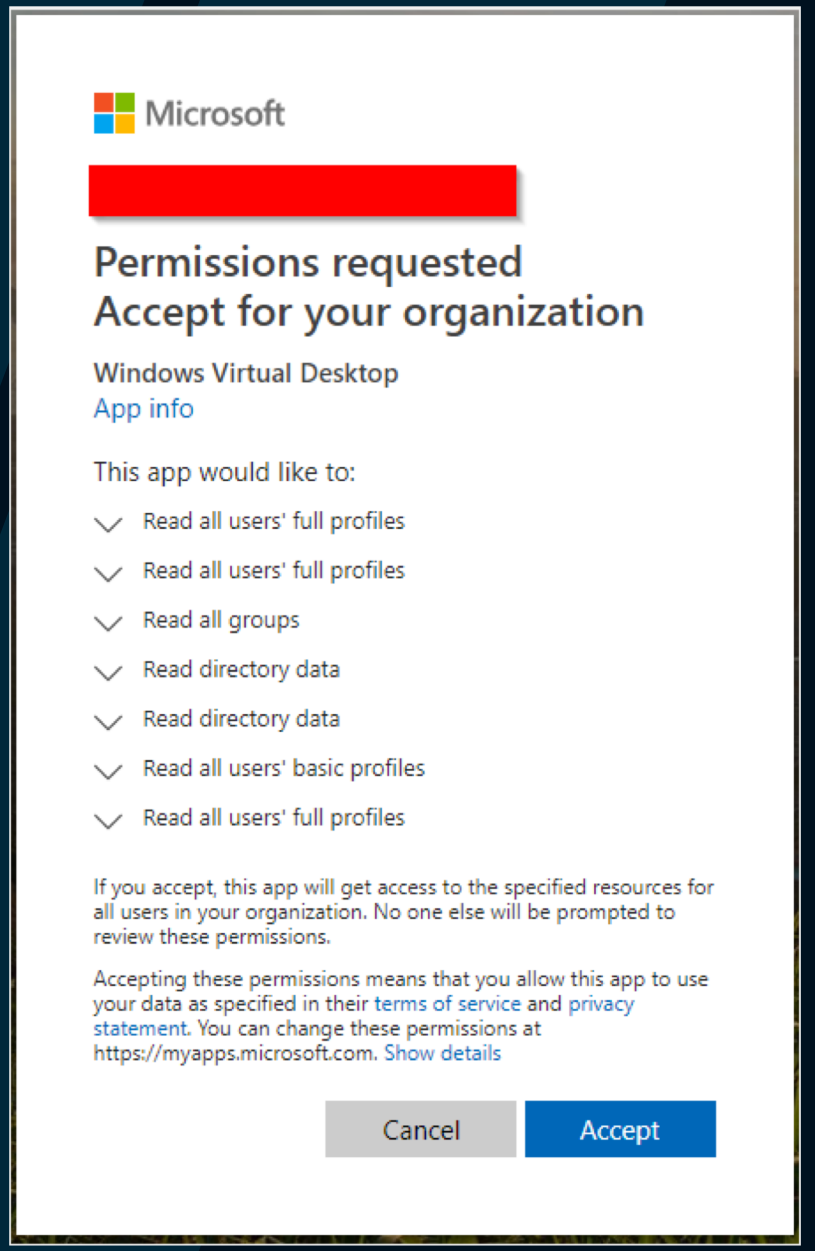
https://www.microsoft.com/security/blog/2020/04/23/protecting-organization-password-spray-attacks/

4. Initial Compromise : Malicious Azure app’s

URL : https://login.microsoftonline.com/common/oauth2/authorize?response_type=token&client_id={CLIENT_ID}&resource={RESOURCE}&redirect_uri={REDIRECT_URI}

Халдлагаас сэргийлэх боломжууд ?

- Шаардлагагүй Azure дээрх application – уудыг идэвхгүй болгох
- Шаардлагагүй redirect_uri – г Azure дээрээс устгах
- Ажилчдын сэжигтэй имэйлыг таних мэдлэг чадварыг сайжруулах
- https://black.direct/ – account takeover vulnerability байгаа эсэхийг шалгах



5. Initial Compromise : MFA Bypass

MFA bypass хийх нийтлэг 3 техник

- Real time phishing
- Channel jacking
- Legacy protocols
- Social engineering

Халдлагаас сэргийлэх боломжууд ?

- Legacy authentication protocols – г идэвхгүй болгох
- Application ашиглах

Office 365 үйлчилгээний аюулгүй байдлыг хангах стандарт, зөвлөмж

- Azure active directory
- Application permissions
- Data management
- Email security / Exchange Online
- Auditing
- Storage
- Mobile Device management
- Versioning

Эх сурвалж :
https://www.cisecurity.org/benchmark/microsoft_office/

Тохиргоонд үнэлгээ өгөх, дүн шинжилгээ хийх зөвлөмж

- CIS Benchmark – н тохиргоо хийгдсэн эсэхийг шалгах скрипт
- Business email compromised болсоны дараа дүн шинжилгээ хийх зөвлөмж
- …

Дэлгэрэнгүй : https://github.com/nasamoskva/Office365-forensic-guide

Business email compromised forensic example

- Check new mail rule activity in powershell

```
Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-90) -EndDate (Get-Date) -ResultSize 5000 -
Operations "New-InboxRule","Set-InboxRule","Enable-InboxRule" | Export-CSV \path\to\file.csv -
NoTypeInformation -Encoding utf8
```

- Check SMTP forwarding rule activity

```
Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-90) -EndDate (Get-Date) -ResultSize 5000 -
FreeText "ForwardingSmtpAddress" | Export-CSV \path\to\file.csv -NoTypeInformation -Encoding utf8
```

- Suspicious IP address

```
Search-UnifiedAuditLog -StartDate mm/dd/yyyy -EndDate (Get-Date) -ResultSize 5000 -IPAddresses
1.2.3.4, 2.3.4.5 | Export-CSV \path\to\file.csv -NoTypeInformation -Encoding utf8
```

- Message trace （last 10 days of email sent by victim）

```
Get-MessageTrace -StartDate (Get-Date).AddDays(-10) -EndDate (Get-Date) -
SenderAddress victim@client.com | Select-Object Received, SenderAddress, RecipientAddress,
Subject, Status, FromIP, Size, MessageID | Export-CSV \path\to\file.csv -NoTypeInformation -
Encoding utf8
```


Дэлгэрэнгүй : https://github.com/nasamoskva/Office365-forensic-guide

Анхаарал хандуулсанд баярлалаа!

Your P@$$w0rd doesn’t matter but MFA does!