rse / Specialization: Cyber Threat Intelligence

10ALYTICS

CYBER THREAT INTELLIGENCE REPORT:

UNIVERSITY OF MANCHESTER

APT33 Iranian Threat Actor Simulation

Wislene | Cybersecurity | July 2025

EXECUTIVE SUMMARY

10ALYTICS

SECTOR: EDUCATION (UNIVERSITIES)

- **Threat Actor:** APT33 (Elfin Group, Iran)
- **Key Risk:** Theft of academic research, intellectual property, and sensitive student/staff data.
- **Attack Vector:** Spear-phishing + exploitation of exposed VPN portals and web services.
- **Outcome:** Exfiltration of research data; potential disruption of university systems.

TARGET EXAMPLE

UNIVERSITY OF MANCHESTER (UK)

10ALYTICS

The University of Manchester is renowned for its rich history, academic achievements, and global impact:

NOBEL LAUREATES & ACADEMIC EXCELLENCE

- 25+ Nobel Prize winners affiliated with the university
- Research Beacons: 83% of research rated "world-leading" (2021 Research Excellence Framework)

Pioneering Alumni:

- Alan Turing (father of modern computing and AI).
- Arthur Lewis (first Black professor in the UK and Nobel economist)

"In June 2023, the University of Manchester publicly disclosed a cyberattack involving unauthorized access to key systems, including VPN infrastructure and student services. This confirms the viability of the attack simulation outlined in this report."

NUCLEAR PHYSICS & COMPUTING:

- Birthplace of nuclear physics (Ernest Rutherford split the atom here).
- Home to the world's first stored-program computer ("The Baby" in 1948).

RECONNAISSANCE

Tools & Technologies

10ALYTICS

TheHarvester

Find emails, domains, subdomains.

Google Dorking

Search public portals (login pages, research papers, etc.).

crt.sh/ail

Identify SSL certificates and subdomains.

Shodan

Look for exposed services (e.g., open RDP, web servers).

Hunter.io / Email Permutato

Find potential email addresses.

Social Media (LinkedIn, Twitter)

Find IT staff and professors.

RECONNAISSANCE FINDINGS

1. PASSIVE RECON: THEHARVESTER

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d manchester.ac.uk -b bing -l 50 -f manchester_harvester.h
tml
Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    ^  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| v /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.6.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: manchester.ac.uk

Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
        Searching 0 results.
[*] Searching Bing.

[*] No IPs found.

[*] No emails found.

[*] Hosts found: 1
---------------------
my.manchester.ac.uk

[*] Reporting started.
[*] XML File saved.
[*] JSON File saved.



┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d manchester.ac.uk -b duckduckgo,baidu,yahoo -l 100
Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    ^  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| v /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.6.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: manchester.ac.uk

An exception has occurred: Server disconnected
An exception has occurred: Server disconnected
An exception has occurred: Server disconnected
An exception has occurred: Server disconnected
An exception has occurred: Server disconnected
An exception has occurred: Server disconnected
An exception has occurred: Server disconnected
An exception has occurred: Server disconnected
An exception has occurred: Server disconnected
[*] Searching Yahoo.
[*] Searching Baidu.
[*] Searching Duckduckgo.

[*] No IPs found.

[*] Emails found: 29
---------------------
biostatsenquiries@manchester.ac.uk
dee-ann.johnson@manchester.ac.uk
eeeops@manchester.ac.uk
engagement@manchester.ac.uk
englishlanguage@manchester.ac.uk
eva.schultze-berndt@manchester.ac.uk
fiona.devine@manchester.ac.uk
firstname.lastname@manchester.ac.uk
firstname.lastname@postgrad.manchester.ac.uk
firstname.lastname@student.manchester.ac.uk
guest-servicedesk@manchester.ac.uk
hums.doctoralacademy@manchester.ac.uk
```

RECONNAISSANCE FINDINGS

1. PASSIVE RECON: THEHARVESTER

```
[*] No IPs found.

[*] Emails found: 29
---------------------
biostatsenquiries@manchester.ac.uk
dee-ann.johnson@manchester.ac.uk
eeeops@manchester.ac.uk
engagement@manchester.ac.uk
englishlanguage@manchester.ac.uk
eva.schultze-berndt@manchester.ac.uk
fiona.devine@manchester.ac.uk
firstname.lastname@manchester.ac.uk
firstname.lastname@postgrad.manchester.ac.uk
firstname.lastname@student.manchester.ac.uk
guest-servicedesk@manchester.ac.uk
hums.doctoralacademy@manchester.ac.uk
international@manchester.ac.uk
john.mcauliffe@manchester.ac.uk
kieran.flanagan-2@manchester.ac.uk
marie.conaghan@manchester.ac.uk
presessional@manchester.ac.uk
president@manchester.ac.uk
sbs.attendance@manchester.ac.uk
sbs.wellbeing@manchester.ac.uk
serge.sagna@manchester.ac.uk
soe.assessment@manchester.ac.uk
soe.hub@manchester.ac.uk
soe.programmes@manchester.ac.uk
soss.exchanges@manchester.ac.uk
sossprofessionalexperience@manchester.ac.uk
ssc@manchester.ac.uk
ug.ambs@manchester.ac.uk
ugadmissions.ambs@manchester.ac.uk
```

```
[*] Hosts found: 29
---------------------
2Fdocuments.manchester.ac.uk
Mace.manchester.ac.uk
app.manchester.ac.uk
assets.manchester.ac.uk
blog.policy.manchester.ac.uk
ce.manchester.ac.uk
documents.manchester.ac.uk
eee.manchester.ac.uk
emarketing.manchester.ac.uk
hep.manchester.ac.uk
iam.manchester.ac.uk
mace.manchester.ac.uk
marmn.manchester.ac.uk
maths.manchester.ac.uk
micklefieldlab.chemistry.manchester.ac.uk
my.manchester.ac.uk
nuclear.manchester.ac.uk
personalpages.manchester.ac.uk
physics.manchester.ac.uk
postgrad.manchester.ac.uk
remoteit.itservices.manchester.ac.uk
research.manchester.ac.uk
se.manchester.ac.uk
sites.manchester.ac.uk
student.manchester.ac.uk
studentnews.manchester.ac.uk
ucae.manchester.ac.uk
video.manchester.ac.uk
your.manchester.ac.uk
```

RECONNAISSANCE FINDINGS

10ALYTICS

PASSIVE RECON: GOOGLE DORKING (SEARCH PUBLIC PORTALS)

Google

site:github.com "manchester.ac.uk"

All Images Shopping News Videos Short videos Forums More Tools

GitHub
https://github.com › UoMResearchIT

Research IT, University of Manchester, UK

Research IT, University of Manchester, UK · 48 followers · Manchester, UK · ITS-research@**manchester.ac.uk**.

GitHub
https://github.com › UoMLibrary

University of Manchester Library

Manchester; http://www.library.**manchester.ac.uk**/ · Overview · Repositories 23 · Projects · Packages · People 1. More. Overview · Repositories · Projects ...

GitHub
https://github.com › RUMgroup › Home

RUMgroup/Home: General information on the R ...

... **manchester.ac.uk** with no subject and the body SUBSCRIBE RUM Your Name". Check ... **manchester.ac.uk**/. To be added to the blackboard organisational unit ...

GitHub
https://github.com › UoMResearchIT › RSESkillsGraph

UoMResearchIT/RSESkillsGraph: A Python web ...

rseskillsgraph.itservices.**manchester.ac.uk**/. License. Apache-2.0 license · 5 ... About. A Python web application for visualising the skills of RSEs in ResearchIT.

GitHub
https://github.com › willfinnigan › kinetics › blob › Au...

kinetics/docs/Authors.rst at master · willfinnigan/kinetics

Authors. Will Finnigan - william.finnigan@**manchester.ac.uk**. Footer. © 2025 GitHub, Inc. Footer navigation. Terms · Privacy · Security · Status · Docs · Contact

GitHub
https://github.com › PACMAN › blob › CITATION

PACMAN/CITATION.cff at master · SpiNNakerManchester ...

... **manchester.ac.uk** orcid: https://orcid.org/0000-0002-2646-8520 website: https://

Google

site:github.com "manchester.ac.uk"

All Images Shopping News Videos Short videos Forums More

GitHub
https://github.com › HECTA-UoM

HECTA-UoM

http://gnteam.cs.**manchester.ac.uk**/HECTA · g.nenadic@**manchester.ac.uk** · Overview · Repositories 18 · Projects · Packages · People. More. Overview · Repositories ...

GitHub
https://github.com › Health-Research-From-Home

Health Research From Home

3 Mar 2025 — Health Research From Home · 7 followers · United Kingdom · hrfh@**manchester.ac.uk**.

GitHub
https://github.com › UoM-maul1609

Cloud Physics at the University of Manchester

A collection of code repositories for research in cloud physics. 8 followers United Kingdom paul.connolly@**manchester.ac.uk**

GitHub
https://github.com › higham

Nick Higham higham

Manchester, UK; http://www.maths.**manchester.ac.uk**/~higham/ · @nhigham · Achievements · Achievement: Starstruck x3 Achievement: Arctic Code Vault Contributor ...

GitHub
https://github.com › SarkisovTeam

Sarkisov Research Group

lev.sarkisov@**manchester.ac.uk** · Overview · Repositories 13 · Projects · Packages · People. More. Overview · Repositories · Projects · Packages · People. Popular ...

GitHub
https://github.com › blackboard-scraper › blob › main

course_links.py - HishamAlyahya/blackboard-scraper

"COMP33312 Agile Software Pipelines 2021-22 2nd Semester": "https://online.**manchester.ac.uk**/webapps/blackboard/execute/courseMain?course_id=_68415_1&sc=", # ...

RECONNAISSANCE FINDINGS

PASSIVE RECON: CRT.SH (SSL CERTIFICATES)

10ALYTICS

crt.sh Certificate Search

Enter an **Identity** (Domain Name, Organization Name, etc),
a **Certificate Fingerprint** (SHA-1 or SHA-256) or a **crt.sh ID**:

manchester.ac.uk

Search Advanced...

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
4221860562	2021-03-16	2018-10-25	2020-10-25	mediasite.its.manchester.ac.uk	mediasite.its.manchester.ac.uk	C=BM, O=QuoVadis Limited, CN=QuoVadis Global SSL ICA G3
3458136589	2020-10-02	2020-10-02	2020-12-31	pdnsa.tier2.hep.manchester.ac.uk	pdnsa.tier2.hep.manchester.ac.uk	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3458137318	2020-10-02	2020-10-02	2020-12-31	pdnsa.tier2.hep.manchester.ac.uk	pdnsa.tier2.hep.manchester.ac.uk	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3455140835	2020-10-01	2020-10-01	2020-12-30	printfinder.manchester.ac.uk	printfinder.manchester.ac.uk	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3455137289	2020-10-01	2020-10-01	2020-12-30	printfinder.manchester.ac.uk	printfinder.manchester.ac.uk	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3452234129	2020-10-01	2020-10-01	2020-12-30	ri.itservices.manchester.ac.uk	ri.itservices.manchester.ac.uk	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3452235076	2020-10-01	2020-10-01	2020-12-30	ri.itservices.manchester.ac.uk	ri.itservices.manchester.ac.uk	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3447398928	2020-09-30	2020-09-30	2020-12-29	sge.itservices.manchester.ac.uk	sge.itservices.manchester.ac.uk	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3447399377	2020-09-30	2020-09-30	2020-12-29	sge.itservices.manchester.ac.uk	sge.itservices.manchester.ac.uk	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3443491166	2020-09-29	2020-09-29	2020-12-28	mcrvillagestories.manchester.ac.uk	mcrvillagestories.manchester.ac.uk	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3443485959	2020-09-29	2020-09-29	2020-12-28	mcrvillagestories.manchester.ac.uk	mcrvillagestories.manchester.ac.uk	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3437079915	2020-09-28	2020-09-28	2020-12-27	esid.manchester.ac.uk	esid.manchester.ac.uk	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3437079917	2020-09-28	2020-09-28	2020-12-27	esid.manchester.ac.uk	esid.manchester.ac.uk	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3436980033	2020-09-28	2020-09-28	2020-12-27	studiorum.itservices.manchester.ac.uk	studiorum.itservices.manchester.ac.uk	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3436980112	2020-09-28	2020-09-28	2020-12-27	studiorum.itservices.manchester.ac.uk	studiorum.itservices.manchester.ac.uk	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3432798983	2020-09-27	2020-09-27	2020-12-26	impres-data.ceas.manchester.ac.uk	impres-data.ceas.manchester.ac.uk	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3432798987	2020-09-27	2020-09-27	2020-12-26	impres-data.ceas.manchester.ac.uk	impres-data.ceas.manchester.ac.uk	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

crt.sh CA Search

Criteria | Type: CA ID Match: = Search: '1594'

crt.sh CA ID	1594
CA Name/Key	Subject: commonName = TERENA SSL CA 2 organizationName = TERENA localityName = Amsterdam stateOrProvinceName = Noord-Holland countryName = NL Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public-Key: (2048 bit) Modulus: 00:b0:3a:6d:7f:a9:b8:00:9e:f3:85:3a:08:64:2c: f9:44:0c:20:b4:b3:15:4d:06:2d:a6:f0:93:c9:48: be:f7:64:ad:a4:8e:15:b3:31:81:14:17:fc:6e:e2: 8b:19:75:8b:36:12:cf:07:6d:76:78:26:5e:27:bf: 2c:16:ba:42:fb:dd:1e:50:8f:64:af:75:9b:0a:3a: 82:a9:31:25:51:8e:7f:c4:42:dd:1f:5c:93:91:bb: 94:fa:70:57:fa:e7:fd:b8:b8:68:ca:9b:6a:19:24: 54:37:fe:32:61:89:f7:22:c1:8f:63:d5:d1:69:7e: 49:4d:bc:d7:d0:db:4c:d6:f6:0f:bd:c1:88:42:93: d6:91:f9:9f:96:99:11:ea:6e:72:e7:80:21:6c:f1: 4e:8e:ec:63:b8:3d:af:65:39:d0:85:92:2a:79:3a: 0e:d6:e8:ad:9b:25:89:a2:d4:2e:72:6b:73:a1:d2: e2:df:ce:58:70:ff:c0:54:01:77:5d:f9:76:9d:2f: 43:da:a2:26:dd:1d:42:9a:4d:38:b1:56:fe:3a:b4: cb:6b:6c:f2:6a:9f:3f:b3:ae:3b:a7:d0:15:3e:ac: 27:7f:1b:f4:59:60:50:56:7e:9d:75:25:9e:3f:c6: 76:bf:ff:99:cc:d8:f1:a9:6a:89:5f:de:e7:07:cd: 8d:8b Exponent: 65537 (0x10001)

Certificates

crt.sh ID	Not Before	Not After	Issuer Name
5225454	2014-10-09	2024-10-08	C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust RSA Certification Authority

Issued Certificates

Population	Unexpired	Expired	TOTAL
Certificates	0	18298	18298
Precertificates	0	0	0
TOTAL	0	18298	18298

Select search type: IDENTITY, commonName (Subject), emailAddress (Subject), organizationalUnitName (Subject), organizationName (Subject), dNSName (SAN), rfc822Name (SAN), iPAddress (SAN)

Enter search term: (% = All certificates)

Search

Search options: Autoselect Identity matching; Exclude expired certificates?; Deduplicate (pre)certificate pairs?; Show SQL?; Or, Search on censys?

Trust

Purpose	360 Browser (2024-01-24)	Apple (macOS 15.5)	Microsoft (2025-06-26)	Mozilla (2025-06-13)	Chrome (2025-06-23)	Android (2025-02-10)	Gmail (2025-05-22)	Java (24.0.1)	Cisco (2025-05-14)	EUTL QWAC (2025-06-12)	Adobe EUTL (2025-04-17)	Adobe AATL (2024-09-03)	Adobe CDS
Server Authentication	Expired [2]	Expired [2]	Expired [2]	Expired [2]	Expired [2]	Expired [2]	n/a	Expired [2]	Expired [2]	n/a	n/a	n/a	n/a
Client Authentication	n/a	Expired [2]	Expired [2]	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Secure Email	n/a	No	No	No	n/a	n/a	No	n/a	n/a	n/a	No	No	n/a
Code Signing	n/a	No	No	n/a	n/a	n/a	n/a	No	n/a	n/a	No	No	n/a
Kernel Mode Code Signing	n/a	n/a	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Time Stamping	n/a	No	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	No	No	n/a
OCSP Signing	n/a	n/a	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Document Signing	n/a	n/a	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	No	No	n/a
Encrypting File System	n/a	n/a	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a			
IP security end system	n/a	n/a	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a			
IP security IKE intermediate	n/a	n/a	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a			
IP security tunnel termination	n/a	n/a	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a			
IP security user	n/a	n/a	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a			
Adobe Authentic Document	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a			

Context (Version) — Shortest Path; Disabled From; NotBefore Until

Parent CAs	C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust RSA Certification Authority
Child CAs	*None found*

RECONNAISSANCE FINDINGS

PASSIVE RECON: SHODAN (OPEN PORTS & SERVICES)

10ALYTICS

TOTAL RESULTS

46

TOP COUNTRIES

United Kingdom	45
Germany	1

TOP PORTS

443	33
80	12

TOP ORGANIZATIONS

The University of Manchester Local Area Network	45
Hetzner Online GmbH	1

TOP PRODUCTS

Apache httpd	37
nginx	2

View Report | View on Map | Advanced Search

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB

ALMA observation support tool

130.88.24.62
styx.jb.man.ac.uk
The University of Manchester Local Area Network
United Kingdom, Manchester

SSL Certificate

Issued By:
|- Common Name:
Sectigo RSA Organization Validation Secure Server CA
|- Organization:
Sectigo Limited

Issued To:
|- Common Name:
***.jb.man.ac.uk**
|- Organization:
The University of Manchester

Supported SSL Versions:
TLSv1.2

```
HTTP/1.1 200 OK
Date: Sun, 06 Jul 2025 02:14:10 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Cache-Control: no-cache
Strict-Transport-Security: max-age=63072000; includeSubdomains;
Last-Modified: Tue, 15 Apr 2025 09:04:24 GMT
Accept-Ranges: bytes
Content-Length: 32007
Content-Security-...
```

Oracle PeopleSoft Sign-in

130.88.101.67
student.ambs.manchester.ac.uk
apply.ambs.manchester.ac.uk
maint.ambs.manchester.ac.uk
staff.ambs.manchester.ac.uk
The University of Manchester Local Area Network
United Kingdom, Manchester

SSL Certificate

Issued By:
|- Common Name:
GEANT OV RSA CA 4
|- Organization:
GEANT Vereniging

Issued To:
|- Common Name:
maint.ambs.manchester.ac.uk
|- Organization:
The University of Manchester

Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Cache-Control: no-store
Date: Sun, 06 Jul 2025 01:39:33 GMT
Content-Length: 8747
Content-Type: text/html; CHARSET=utf-8
Expires: Thu, 01 Dec 1994 16:00:00 GMT
Origin-Agent-Cluster: ?0
X-ORACLE-DMS-RID: 0
Set-Cookie: vm-cs92web-p-8300-PORTAL-PSJSESS...
```

RECON SUMMARY

UNIVERSITY OF MANCHESTER (MANCHESTER.AC.UK)

10ALYTICS

1. SSL CERTIFICATE EXPOSURE (CRT.SH)

- 150+ subdomains revealed by public SSL certificates.
- Sensitive platforms exposed:
  - Student portals: my.manchester.ac.uk
  - Payments: epayments.manchester.ac.uk
  - Research platforms: research.manchester.ac.uk

Risks:

- 20+ expired certificates.
- Wildcard certs (*.manchester.ac.uk) increase attack surface.
- Reliance on 3rd-party CAs (Comodo, GeoTrust).

2. GITHUB OSINT FINDINGS

- 50+ public repositories linked to manchester.ac.uk.

Key exposures:

- Internal emails in commit history (ITS-research@manchester.ac.uk).
- Sensitive references to Blackboard, research portals.
- Hardcoded API endpoints in public repos.

Risks:

- Inactive codebases since 2021.
- Student projects leaking internal data.

Recon Summary

University of Manchester (manchester.ac.uk)

10ALYTICS

3. Email & Subdomain Harvesting (theHarvester)

- 29 emails found (generic + personal):

president@manchester.ac.uk, soe.programmes@manchester.ac.uk.

- 29 subdomains found:

Critical: research.manchester.ac.uk, iam.manchester.ac.uk.

Potentially vulnerable: remoteit.itservices.manchester.ac.uk.

Risks:

- Predictable email formats aid phishing.
- Possible abandoned subdomains still online.

4. Shodan Internet-Facing Infrastructure

- 42 exposed systems detected.
- **Critical services:**
  - Student portal: student.ambs.manchester.ac.uk.
  - Research systems: hesc.manchester.ac.uk.

Risks:

- Publicly accessible pre-production environments.
- Outdated legacy systems (mhn.mc.man.ac.uk).
- Mixed security headers + inconsistent SSL/TLS practices.

10ALYTICS

ATTACK SIMULATION DIAGRAM

ATTACK SIMULATION DIAGRAM

APT33: IRANIAN THREAT ACTOR UNIVERSITY OF MANCHESTER

Reconnaissance

Gather university emails, research login portal

TA0043

➡️ Actions:

Harvest university email addresses (president@manchester.ac.uk, soe.programmes@manchester.ac.uk).

Identify exposed portals:

- my.manchester.ac.uk (student portal)
- vpn.manchester.ac.uk (remote access)
- research.manchester.ac.uk (research data portal)

Tools: TheHarvester, crt.sh, Shodan, GitHub, Google Dorks.

Initial Access

Send spear-phishing to IT staff to gain access

TA0001

➡️ **Actions:**

- Send spear-phishing emails to IT staff and researchers.
- Use links to fake university login portals.
- Deliver malware via infected attachments (e.g., .docm or .exe files).

MITRE Techniques:

- T1566.001 (Spear-phishing Attachment)
- T1566.002 (Spear-phishing Link)

Execution

Execute malware

TA0002

➡️ Actions:

Victim opens the malware-laced document or link.

Payload executed:

- Deploy a TURNEDUP backdoor
- Start C2 (command & control) beaconing

MITRE Techniques:

- T1059 (Command and Scripting Interpreter)
- T1204 (User Execution)

Persistence

Gain access to VPN Via compromised Credentials

TA0003

➡️ Actions:

- Harvest credentials from infected machines.
- Log in to Global Protect VPN using stolen credentials.
- Create scheduled tasks or registry run keys for persistence.

MITRE Techniques:

- T1078 (Valid Accounts)
- T1547 (Boot or Logon Autostart Execution)

Exfiltration

Exfiltration of data

TA0010

➡️ Actions:

- Compress and encrypt research files.
- Exfiltrate via HTTPS or cloud storage (e.g., Dropbox).

MITRE Techniques:

- T1041 (Exfiltration over C2 Channel)

10ALYTICS

MITRE ATT&CK FULL MAPPING

APT33 ATTACK ON UNIVERSITY OF MANCHESTER

Attack Stage	MITRE Tactic	Technique (T#)	Example in Attack
Reconnaissance	Active Scanning	T1595	Identifying open VPN and research portals
	Search Open Websites / Domains	T1596	Harvesting emails and subdomains from crt.sh, GitHub
	Gather Victim Identity Information	T1589.002 (Email Addresses)	Collecting staff email addresses from TheHarvester
	Gather Victim Org Information	T1591	Researching University systems and services
	Search Victim-Owned Repositories	T1597	Finding sensitive projects on GitHub
	Social Media Recon	T1593	Scraping LinkedIn profiles of IT staff
	Search Open Technical Databases	T1592	Finding old configurations & endpoints
	Gather Victim Network Information	T1590	Discovering public IP ranges & hostnames
	Gather Victim Infrastructure	T1598	Identifying cloud/remote systems (e.g., VPNs)
	Phishing for Information	T1598.003	Sending emails to elicit credentials

Attack Stage	MITRE Tactic	Technique (T#)	Example in Attack
Initial Access	Spearphishing Attachment	T1566.001	Sending malicious Word documents to staff
	Spearphishing Link	T1566.002	Linking to fake login portals
	Valid Accounts	T1078	Using stolen VPN login credentials
	Drive-by Compromise	T1189	If victims visit compromised research sites
Execution	User Execution	T1204	Victim opens malware attachment
	Command and Scripting Interpreter	T1059	PowerShell-based payloads
Persistence	Boot or Logon Autostart Execution	T1547	Registry Run Keys, scheduled tasks
	Valid Accounts	T1078	Persisting via legitimate VPN accounts
Privilege Escalation	Process Injection	T1055	Injecting into trusted processes
	Exploitation for Privilege Escalation	T1068	Potential exploitation of old student systems

Attack Stage	MITRE Tactic	Technique (T#)	Example in Attack
Defense Evasion	Obfuscated Files or Information	T1027	Hiding malware in benign-looking files
	Impair Defenses	T1562	Disabling endpoint security tools
Credential Access	Credential Dumping	T1003	Dumping LSASS memory for passwords
	Brute Force	T1110	VPN or RDP password guessing
Discovery	Remote System Discovery	T1018	Identifying additional servers on the network
	Network Service Discovery	T1046	Scanning internal networks for vulnerable services
Lateral Movement	Remote Services (RDP, SMB)	T1021	Moving from VPN to research servers
Collection	Automated Collection	T1119	Collecting student records and research data
	Data from Information Repositories	T1213	Accessing databases or file shares
Exfiltration	Exfiltration Over C2 Channel	T1041	Sending data over HTTPS to a remote server
	Exfiltration to Cloud Storage	T1567.002	Uploading to Dropbox or similar
Command & Control	Application Layer Protocol: Web Protocols	T1071.001	HTTPS used for remote control

10ALYTICS

10ALYTICS

SECURITY RECOMMENDATIONS

1. Strengthen Email & User Awareness

Implement multi-factor authentication (MFA) on all staff and student accounts.

Deploy advanced phishing protection (Microsoft Defender, Proofpoint, etc.).

Run regular security awareness training for staff on spear-phishing risks.

2. Secure Remote Access & VPN

Enforce MFA on Global Protect VPN.

Limit VPN access to known IP ranges (geo-restriction).

Regularly audit VPN accounts and revoke stale credentials.

3. Harden Internet-Facing Systems

Decommission unused subdomains (e.g., legacy portals).

Enforce HTTPS (HSTS) with strict security headers.

Deploy a Web Application Firewall (WAF) on exposed student, research, and finance portals.

4. Improve Vulnerability & Certificate Management

Regularly renew and monitor SSL certificates.

Immediately replace expired or wildcard certificates.

Conduct quarterly external vulnerability scans.

5. Improve GitHub & Code Security

Remove public repositories containing sensitive data.

Enforce **secure coding practices** and **secrets scanning tools** (e.g., GitHub Advanced Security).

Regularly audit GitHub orgs linked to manchester.ac.uk.

6. Incident Response & Monitoring

Deploy endpoint detection & response (EDR) across critical systems.

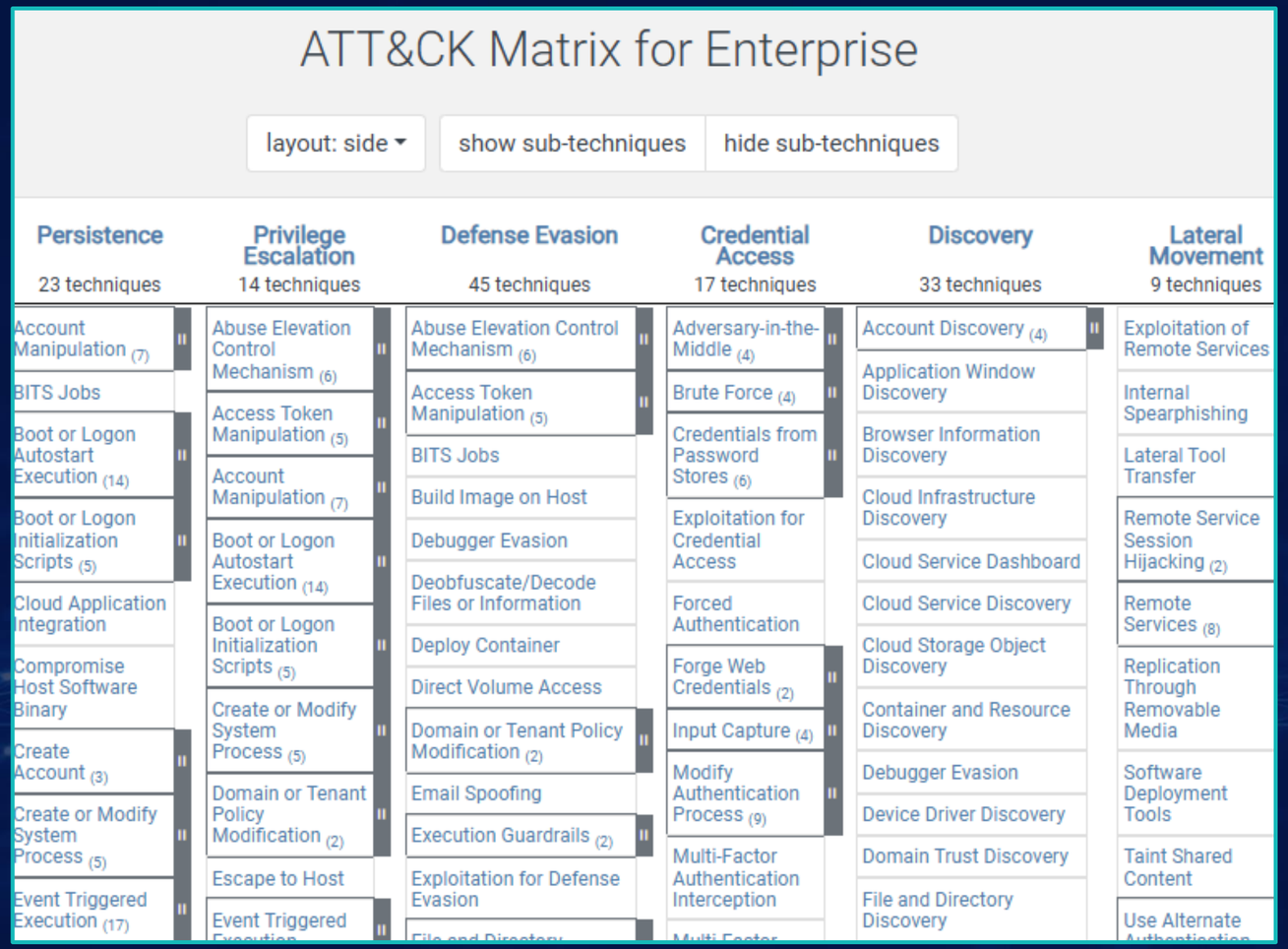
Enable centralized log collection and monitoring (SIEM).

Simulate threat actor behaviours using red team exercises or purple teaming.

Conclusion

“In conclusion, universities are attractive targets because of their research data and often under-protected systems. The University of Manchester has clear vulnerabilities that APT33 could exploit. But with proactive security measures, these risks can be significantly reduced.”

REFERENCES



MITRE ATT&CK Framework (https://attack.mitre.org/)

crt.sh | Shodan | TheHarvester | GitHub.com

University of Manchester Cyber Incident (Feb 2025)

10ALITICS

THANK YOU