IHRP INCIDENT CONTACT LIST

CISO / CIO

Name: Salma Abdelmonem

Title: Chief Information Security Officer

Phone: [redacted]

Mobile: [redacted]

Fax:

Email: Salma@ainshams.com

Address: Corporate Headquarters, Main Building,
Suite 205

SPOC OF: INCIDENT HANDLING OR CSIRT TEAM

Name: Abdelrahman Khaled

Title: Incident Response Specialist

Phone: [redacted]

Mobile: [redacted]

Fax:

Email: A.Khaled@ainshams.com

Address: Incident Response Office, Data Center Wing

ISP SPOC

Name: Abdelrahman Sohsah

Title: Network Security Manager

Phone: [redacted]

Mobile: [redacted]

Fax:

Email: A.Sohsah@ainshams.com

Address: ISP HQ, Security Operations Center

LOCAL CYBER CRIME UNIT

Name: Zeiad Mahmoud

Title: Cybercrime Investigator

Phone: [redacted]

Mobile: [redacted]

Fax:

Email: Zeiad@ainshams.com

Address: Regional Cyber Crime Unit Office, Floor 3,
Government Building

LEGAL DEPARTMENT CONTACT

Name: Nour Bahgat

Title: Corporate Counsel

Phone: [redacted]

Mobile: [redacted]

Fax:

Email: Nour@ainshams.com

Address: Legal Department, Corporate HQ, Suite 301

PUBLIC RELATIONS CONTACT

Name: Moamen Mahmoud

Title: Director of Public Relations

Phone: [redacted]

Mobile: [redacted]

Fax:

Email: Moamen@ainshams.com

Address: PR Office, Corporate HQ, Main Lobby

IHRP INCIDENT DETECTION

GENERAL INFORMATION

Incident Detected By:

Name: Ahmed Khaled

Title: SOC tier 1 analyst

Phone: 01

Mobile: 01

Signature:

Fax:

Email: AhmedKhaled@ainshams.com

Address: Incident response office , Data center wing

INCIDENT SUMMARY

Type of Incident Detected

□ External Exploitation
□ Internal Exploitation
□ Information Leakage
☑ Malware
☑ Malicious Email
□ Other:
□ Denial of Service

Incident Location

Site: Student Affairs Office , second building

Unit (IT) Manager: Mina Gamal

Phone: 01

Mobile: 01

Fax:

Email: mina@ainshams.com

Address:

How and When was the Incident Detected? The incident was detected when the EDR solution triggered an alert identifying a suspicious powershell.exe script running on the affected system.

Are There Any Physical Security Measures in Place? What are They? Surveillance cameras and motion sensors in every room of the university , Security guards in all entrances.

Additional Information: The EDR triggered an alert detecting a suspicious modification to a registry key on the affected system, indicative of potential fileless malware activity.

IHRP INCIDENT CONTAINMENT

One Form per Affected System is Advised

ISOLATION ACTIVITIES PERFORMED

Did the Incident Handling Team Decide to Isolate the Affected Machine? ☑ YES □ NO

Did the Incident Handling Team Need the Business Unit (IT) Manager to Proceed? ☑ YES □ NO

Date of System's Isolation? (if applicable): 12/14/2024

In What Way was the System Isolated? (if applicable):

Affected systems (DESKTOP-12345 and SERVER-67890) were disconnected from the corporate network at [11:34:00] on [12/14/2024]. User accounts associated with the endpoints were locked to prevent further unauthorized access.

BACK-UP ACTIVITIES PERFORMED

Was the System Restored Successfully? ☑ YES □ NO

Incident Handler in Charge of System's Restoration:

Mohamed Khaled , contact info [email : mohamedkhaled@ainshams.com , phone: 0109016602]

Backup Image Used:

The backup image used for restoration was a verified, malware-free snapshot stored on the university's secure backup server.

When was the System Restoration Started: 15:30:00 12/15/2024

When was the System Restoration Completed: 22:10:00 12/15/2024

Did the Business Unit Confirm the System is in Working Condition? ☑ YES □ NO

Signature:

Date: 12/17/2024

IHRP INCIDENT ERADICATION

Incident Handler(s) in Charge of the Investigation

1- Ahmed Khaled, SOC Tier 1, was the first to discover the incident and initiated the initial response.

2-Abdelrahman Khaled, SOC Tier 2, conducted digital forensics and took the necessary actions for system containment.

3- Mohamed Khaled, SOC Tier 2, was responsible for system restoration and ensuring recovery procedures were executed effectively.

Was the Incident's Root Cause Discovered? ☑ YES □ NO

(Root Cause Analysis)

An attacker launched a phishing campaign using a spoofed domain, [@aiinshams.com], resembling the university's official domain, [@ainshams.com]. The email tricked the Student Affairs Officer [mohamedayaad@ainshams.com] into downloading an attachment, triggering a fileless malware attack.

Describe the Actions Taken to Ensure the Incident's Root Cause was Remediated and the Possibility of a New Incident Eliminated:

1- Purchasing and implementing an advanced email security appliance. This appliance is designed to detect and block malicious emails, including phishing attempts, malware, and other email-based threats.

2- Removed malicious registry entries: HKCU:Software\Microsoft\Windows\CurrentVersion\Run.

3- Applied patches to close vulnerabilities related to PowerShell execution.

4- Restricted PowerShell to Constrained Language Mode for non-administrators.

IHRP INCIDENT CASUALTIES

One Form per Affected System is Advised

Incident Handling Team's Deployment Date

16:00:00 12/14/2024

Affected Systems:

Hardware Vendor: DELL technologies

Serial Number: CN-0V64X2-74290-42C-1033.

Network Connectivity Details:

(If applicable)

Host Name: DESKTOP-12345

IP Address: 192.168.1.62

MAC Address: 00-14-22-01-23-45

Additional Notes/Information:

IHRP INCIDENT CASUALTIES

One Form per Affected System is Advised

Incident Handling Team's Deployment Date

15:00:00 12/14/2024

Affected Systems:

Hardware Vendor: DELL technologies

Serial Number: CN-0VFFF2-74290-555-1083.

Network Connectivity Details:

(If applicable)

Host Name: SERVER-67890

IP Address: 192.168.1.2

MAC Address: 00-14-22-44-68-88

Additional Notes/Information: