MI6: Secret Intelligence Services	
Cyber Security Division	
Mission Code:	**Alpha 02**
Priority:	**Critical**

CONFIDENTIAL
CONFIDENTIAL
CONFIDENTIAL

Mission Brief

Following a recent hacking attack on the MI6 central server and on all our secret agents' smartphones, a Network Forensics Team from the MI6 Cyber Security Division has been tasked to:

1. Conduct a **Network Forensics Analysis** of the recent **hacking attack**.
2. Perform a full review of the current **network security measures** in place at the MI6 to protect the network against a wide range of potential **threats**.

Network Forensics Report

To start with, the Network Forensics Team decided to identify the nature of the attack. At first, they believed the attack was a **passive attack** and that, though a hacker had managed to access the network, no data had been tampered with (edited or deleted) by the hacker. However this option was very quickly discarded as it became very clear that all access codes to the central server and to the secret agents' smartphones had been overwritten by the hacker making it impossible for anyone at the MI6 to use the network. The attack was hence an **active attack** and it was imperative to identify and fix the security breach to avoid additional confidential data to be accessed, edited or even deleted by the hacker.

The Network Forensics Team then decided to **review the computer logs** of the firewall to see if any suspicious activity had been detected and blocked by the firewall.

A few hours before the attack, the firewall detected a flood of suspicious traffic originating from 6 different IP addresses. The MI6 was clearly targeted by a **Distributed Denial of Service attack (dDoS Attack).** This unusual volume of traffic first slowed down the central server but did not result in the server crashing. The **firewall** quickly noticed this unusual volume of traffic and automatically blocked any traffic originating from these 6 IP addresses. The Network Forensics Team is not 100% sure whether this dDoS attack was related to the hacking attack. They believe it may have been scheduled at the same time of the attack to create a distraction and generate a high volume of log files, making the work of the Network Forensics Team more tedious.

Reviewing the log files also made it clear that an unidentified external user/hacker had tried to login to the central server remotely using a **brute force attack**. An automated piece of software was used to generate and try more than 10,000 passwords on the username 007jbond over just a few minutes. It appears that the **firewall** then picked up on this unusual activity and blocked the IP address of the external user. The hacker was not successful in guessing James Bond's password (username: 007jbond) as our secret agent has always followed the **MI6 network policy/code of conduct** and is using a **very strong password** consisting of:

- More than 8 characters
- Including lowercase and uppercase letters
- Including letters, numbers and punctuation signs

After reviewing the log files from the firewall, the Network Forensics Teams decided focus on the log files of the Anti-virus and Anti-malware software installed on the MI6 central server. They came up with the following findings:

Date:	Log:
18/10-12:15	**Automatic update of Anti-virus database** to the latest known viruses signatures
18/10-12:21	**Full scan of MI6 Central Server**
18/10-12:33	Klog.exe file detected – Suspected **Key logger/spyware** file. File transferred to quarantine for 30 days before deletion.
18/10-12:46	w0rm.101 – Suspected **self-replicating file (worm)** File transferred to quarantine for 30 days before deletion.
18/10-13:16	**Full scan complete** no other suspicious files/viruses detected.

The **self-replicating worm** (w0rm.101 file) detected by the anti-virus is not a real cause of concern. Its aim would have been to clog up the server and the network with unnecessary data/traffic. But it could not be used to let someone hack into the network.

The **key logger spyware** (Klog.exe) is a more serious issue. It had not been detected during the previous day full scan so it has only been on the server for less than 24 hours. It may have recorded any keyboard entry made on the central server over the last 24 hours. The log files of the central server shows that 3 authorised users did log in to the server during these 24 hours. However one of the users used a **fingerprint scanner** instead of a traditional username and password to log in. The other two users used their **username and password** to login. It's likely that their username and password had been recorded and automatically communicated to an external hacker by the key logger software.

The MI6 uses a range of user roles for different types of users on the network. Each user role comes with different **User Access Levels**. When reviewing the User Access Levels of the two users whose passwords may have been compromised by the key logger software, it appears that both users only had **read-only access** to the mission files which have been deleted during the hacking attack. A user accessing the server using these credentials would not have had the required **Read/Write access** to be able to delete any of the mission files. The Network Forensics Team has now reset the two passwords but is convinced the hacker must have used another approach to hack into the central server and gain full access to the mission files.

Only a very few employees of the MI6 have full Admin access to the central server. The Network Forensics Team decided to interview each one of them to see if they may have been victim of a **social engineering strategy**. The team asked each employee to think about all their social interactions within and outside the MI6 over the last few days. The aim was to find out if they had been approached by anyone trying to befriend them or eventually threaten them in order to get them to reveal some sensitive information about the network system and/or to reveal their login details. However all employees from the MI6 are **fully trained** regarding social engineering strategies and have confirmed that they have not revealed any sensitive information to anyone within or outside the MI6.

Another approach that a hacker could have used is by **intercepting or stealing computer data** in order to then gain access to the network. On the MI6 network, all sensitive data including login credentials are stored on the network servers. The data is **fully encrypted**. USB ports on all the servers have been disabled to prevent employees transferring data to an external device (USB Key, portable SSD drive). All backed up data is stored on a dedicated backup server and is also **fully encrypted**. Even if a hacker had access to the backup server they would not be able to decrypt the data. Regarding data theft, there has not been any report of **missing/stolen laptops or smartphones** by any of the MI6 employees. All Wi-Fi hotspots within the MI6 headquarters require an **SSID key** and Wi-Fi communications are **encrypted**. All communication outside of the MI6 and are fully **encrypted**, so once again, even if a hacker managed to intercept an MI6 communication, they would not be able to decrypt it.

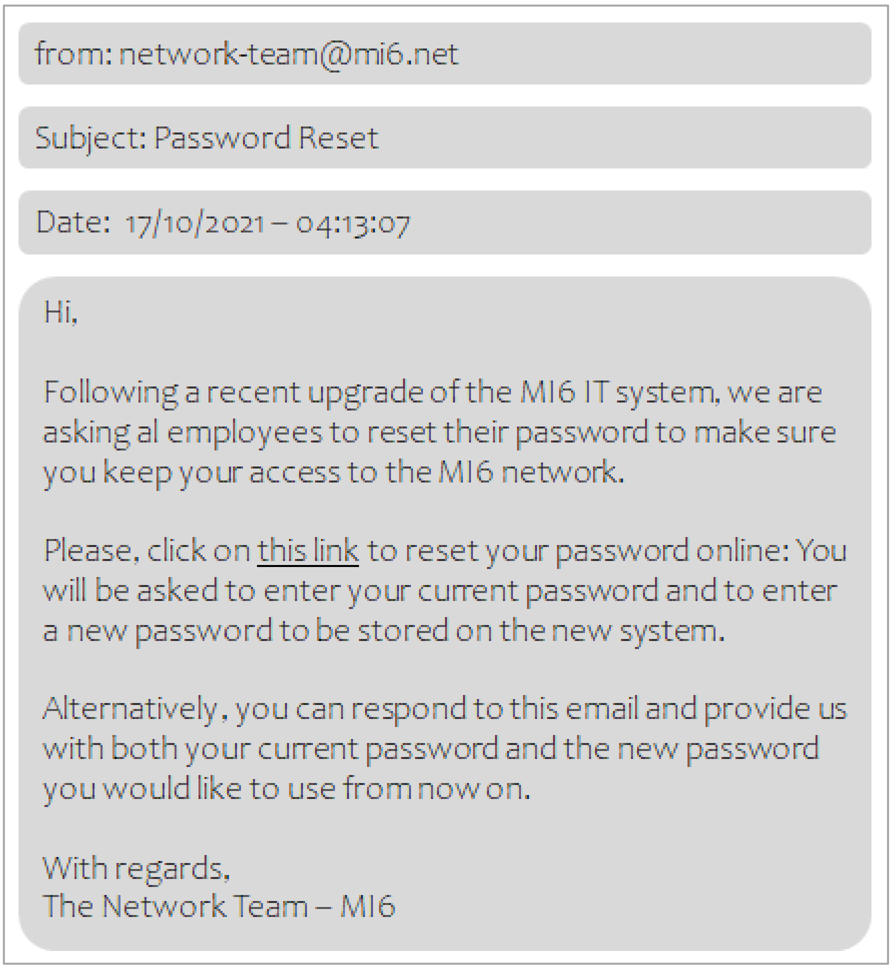
The Network Forensics Team also reviewed all login forms that can be accessed via a web browser. They first made sure that all these forms were using the **HTTPS protocol** to make sure that when users logged in remotely to the network, their login credentials were fully **encrypted**. They also reviewed the server side code used to process the web-based login requests to make sure that clear **validation checks** where implemented to block any form of **SQL injection**. For instance, login names or passwords containing special characters such as ", * or ; are automatically rejected before being processed by the server. This prevents attempts by potential hackers to inject some malicious SQL code in the username or password fields of the login form.

At this stage there are only a few options left for a hacker to gain access to the MI6 central server. The Network Forensics Team decided to rule out the possibility of anyone outside the MI6 **physically accessing the server room** where the central server is located. Effectively the server room, located on the top floor of the MI6 headquarters in London UK, is extremely protected using **physical security measures** including:

- Fully locked doors with 5-point locking mechanisms,
- Facial Recognition and Retina Scanner to unlock security doors,
- 24 hours CCTV recording both inside and outside the server room,
- Burglar alarm with motion sensors inside the server room,
- Security guards at the main entrance of the MI6 headquarters.

The possibility of an **insider attack** has also been considered. The MI6 conducted a review of all the employees who have **full admin access levels** on the server. These employees have been working for the MI6 for more than 20 years and their dedication to the MI6 is beyond doubt. The option of an insider attack can therefore be discarded at this stage of the investigation.

The Network Forensics Team decided to review the e-mail inboxes of all of the employees who have access to the MI6 central server. Out of the thousands of emails reviewed, one specific e-mail drew their attention:



from: network-team@mi6.net

Subject: Password Reset

Date: 17/10/2021 – 04:13:07

Hi,

Following a recent upgrade of the MI6 IT system, we are asking al employees to reset their password to make sure you keep your access to the MI6 network.

Please, click on this link to reset your password online: You will be asked to enter your current password and to enter a new password to be stored on the new system.

Alternatively, you can respond to this email and provide us with both your current password and the new password you would like to use from now on.

With regards,
The Network Team – MI6

This e-mail has not been sent by the MI6 Network Team and the link provided in this email redirects to an external website, designed to look like the official MI6 website even though it is not owned or maintained by the MI6. This email is clearly a **phishing e-mail**. The log files of the central server shows that one of employee of high rank at the MI6 did click on this link and accessed the fake MI6 website. The employee has been interviewed by the Network Forensics Team and has confirmed resetting his password as instructed in this phishing e-mail. The employee being of a very high rank at the MI6 has full admin access to the central server and to all MI6 mission files. It is very likely that the hacker gained access to the central server thanks to this phishing email. The employee’s password has now been reset by the Network Forensic Team to prevent the hacker accessing the central server again.

Review of MI6 Network Security Measures

The Network Forensics Team needs your help to complete a full review of the Network Security measures in place at the MI6. Your task is to complete the table below to describe the potential **Network Security** threats and use the information given in the Network Forensic Report to identify the **measures currently in place to minimise/prevent these threats**.

We would also like you to make additional recommendations on how the MI6 could make sure their network is fully secure.

Network Security Threats:	**Network Security Measures in place to prevent the identified threats:**
dDoS Attack (Distributed Denial of Service Attack): a malicious attempt to overwhelm a server/network by generating a flood of traffic towards this server/network. The aim is to try to crash the server or at least significantly reduce its response time when dealing with genuine requests.	The MI6 firewall is configured to detect potential dDoS attacks. It automatically can block requests from suspicious IP addresses to minimise the impact of a dDoS attack. When the firewall receives too many requests originating from a specific IP address, it automatically adds this IP address to a blocked list. Requests originating from blocked IP addresses are not forwarded to the central server.
Brute Force Attack:	

Viruses & Malware (including Viruses, Worms, Trojan Horses, spyware and key loggers, ransomware, etc.)	
Data Interception:	
Social Engineering:	

Phishing:	
Physical Access:	
SQL Injection:	