



HM Government



Office for
Nuclear Regulation

NUCLEAR CYBER SECURITY CASE FILE



OFFICIAL SENSITIVE
SENSITIVE NUCLEAR INFORMATION

Restricted Access Only

Attention Agents: Urgent Mission Briefing



Agents, we are facing an imminent threat to the UK's critical infrastructure. Our intelligence indicates a sophisticated cyber attack targeting the national power grid. Recent operations have led us to apprehend a key suspect, codenamed John Doe, who is allegedly affiliated with a notorious cyber hacking group known as DarkNet Syndicate. This group has a history of targeting nuclear facilities worldwide, and our analysis suggests that the UK is their next target.

DarkNet Syndicate is notorious for employing a wide array of malicious techniques, including viruses, worms, trojans, botnets, spyware, ransomware, rootkits, and adware. They are adept at using sophisticated malware to infiltrate systems and disrupt operations. Additionally, the group frequently utilises social engineering tactics such as impersonation, phishing, and pretexting to gain unauthorised access to sensitive networks and information. They have also been known to exploit vulnerabilities in software and hardware systems to achieve their objectives.

During the arrest, we seized a mobile phone and a laptop belonging to John Doe. Unfortunately, the mobile phone was damaged during the apprehension, but we have successfully recovered fragments of encrypted messages. These messages indicate detailed plans and communications with multiple operatives within the group.

John Doe possesses a map of the UK, possibly indicating strategic targets for their operation. Your mission is to decrypt these intercepted messages and extract critical intelligence to thwart their plans. Various cipher techniques have been employed, suggesting a high level of encryption proficiency among the group members.

The security of our nation's energy supply is at stake. Your task is crucial in deciphering these communications and identifying the exact nature of the impending threat. Time is of the essence. We must act swiftly and decisively to neutralise this threat before it jeopardises our national security.

Are you ready to accept this mission and protect our country from this imminent cyber threat?

Please uncover...

Project Name	
Date	
Time	
Power Station	
Malware Type	
Access Method	
Suspect Identities	

Here is all the information we know about the malware DarkNet Syndicate typically uses and their common attack methods.

Malware

Virus: A malicious program that attaches itself to legitimate files, corrupting or modifying data.

Worm: A self-replicating malware that spreads across networks.

Trojan: A malicious program disguised as a legitimate application.

Botnet: A network of compromised computers controlled by a hacker.

Spyware: Software that secretly monitors user activity and gathers information without consent.

Ransomware: Malicious software that encrypts a user's data, demanding payment for the decryption key.

Rootkit: A set of software tools used by a hacker to gain control over a system without detection.

Adware: Software that automatically displays or downloads advertising material, often unwanted.

Attack Methods

Impersonation: Pretending to be someone else to gain trust or access to sensitive information or systems.

Phishing: Sending deceptive emails, messages, or websites that appear legitimate to trick individuals into revealing sensitive information.

Pretexting: Creating a fabricated scenario to manipulate individuals into divulging confidential information or performing actions that compromise security.

Vulnerability Exploitation: Identifying and exploiting weaknesses or vulnerabilities in software, hardware, or network configurations to gain unauthorised access or compromise systems.

Brute Force Attacks: Attempting to gain access to systems or data by trying all possible combinations of usernames, passwords, or encryption keys until the correct one is found.

Exhibit #1 : Map

This map was found rolled up in Doe's desk drawer.

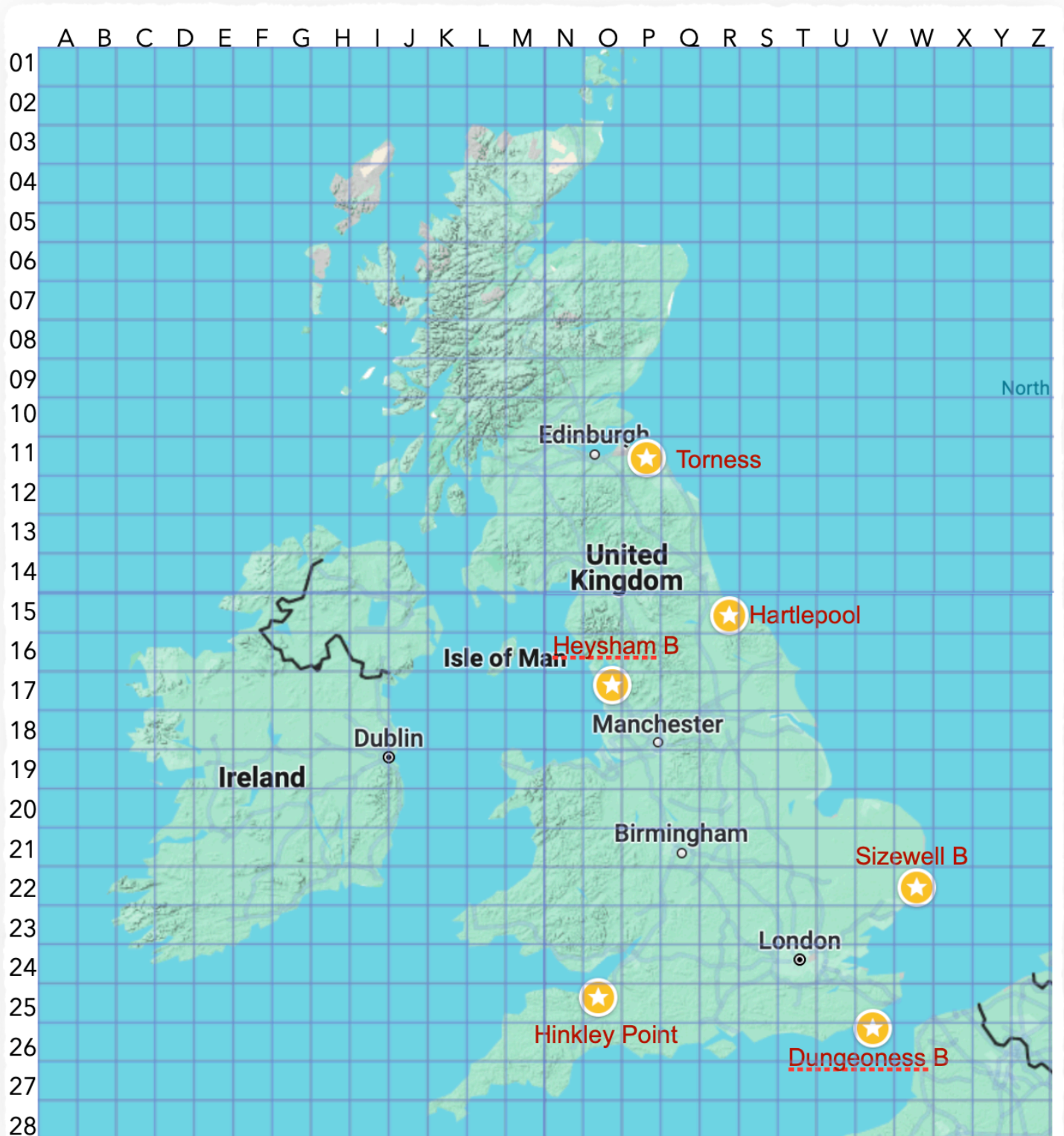




Exhibit #2 : Recovered Message Set 1

We think this is a conversation as a number we recognise to be DarkNet Syndicate's software developer.

I have an update.

...- . -.

WYVQLJA □□□□PU TVAPVU,
WYLWHYHAPVUZ JVTWSLAL,
AHYNLA D ADLUF ADV

DOLU JHU DL LEWLJA ZBJJLZZ?

AHSVU DPSS KLWSVF VU ECPP
CPP TTEPC

NVVK. DL DPSS ZVVU JVUAYVS
AOL BR LULYNF NYPK.

Exhibit #3 : Recovered Message Set 2



We think this is a conversation as a number we recognise to be DarkNet Syndicate's software developer.

12 11 23 31 53 43

NS ATCWJCE □□□□ TSNİY?

DED. YS QTWYNCNIEO VVR
YAWQB FTUCES PTDP TSNİY EQ
GRSD TPHB YHPKF AJTHQFX

BIWN HUJY MG OOQE EQ HRQL?

SO DKF, JJ DTUUHNSPF WG FS L
UCSYWLTS HUDLVS.

UECHSPY, BP TSNİY EQ ZNZNNJ
OG YHCGS SNFEGSA FM ZP
OGYANM RND.

DED UWE.

Exhibit #4 : Recovered Message Set 3

We think this is a conversation as a number we recognise to be DarkNet Syndicate's network engineer.

I request an update.

AAAAA BAABA AAAAB AAAAA
BAAAB AABBB

WL BLF SZEZ ZXXVHH GL GSV
MVGDLIP?

BVH, NFOGRKOV VNKOLBVVH
XORXPVW GSV ORMP DV HVMG
LFG KIVGVMWRMT GL YV
NRXILHLUG.

TLLW DLIP, DSZG ZGGZXP RK
ZWWIVHH ZIV DV FHRMT?

10101100.11001000.00010110.11111
100

Exhibit #5 : Document

This is document was found folded up in Doe's pocket.

Roman Numerals - 1-100									
Arabic Roman	Arabic Roman	Arabic Roman	Arabic Roman	Arabic Roman	Arabic Roman	Arabic Roman	Arabic Roman	Arabic Roman	Arabic Roman
1 I	11 XI	21 XXI	31 XXXI	41 XL I	51 LI	61 LXI	71 LXXI	81 LXXXI	91 XCI
2 II	12 XII	22 XXII	32 XXXII	42 XLII	52 LII	62 LXII	72 LXXII	82 LXXXII	92 XCII
3 III	13 XIII	23 XXIII	33 XXXIII	43 XLIII	53 LIII	63 LXIII	73 LXXIII	83 LXXXIII	93 XCIII
4 IV	14 XIV	24 XXIV	34 XXXIV	44 XLIV	54 LIV	64 LXIV	74 LXXIV	84 LXXXIV	94 XCIV
5 V	15 XV	25 XXV	35 XXXV	45 XLV	55 LV	65 LXV	75 LXXV	85 LXXXV	95 XCV
6 VI	16 XVI	26 XXVI	36 XXXVI	46 XLVI	56 LVI	66 LXVI	76 LXXVI	86 LXXXVI	96 XCVI
7 VII	17 XVII	27 XXVII	37 XXXVII	47 XLVII	57 LVII	67 LXVII	77 LXXVII	87 LXXXVII	97 XCVII
8 VIII	18 XVIII	28 XXVIII	38 XXXVIII	48 XLVIII	58 LVIII	68 LXVIII	78 LXXVIII	88 LXXXVIII	98 XCVIII
9 IX	19 XIX	29 XXIX	39 XXXIX	49 XLIX	59 LIX	69 LXIX	79 LXXIX	89 LXXXIX	99 XCIX
10 X	20 XX	30 XXX	40 XL	50 L	60 LX	70 LXX	80 LXXX	90 XC	100 C
Roman Numerals - Years									
1970 MCMLXX	1980 MCMLXXX	1990 MCMXC	2000 MIM	2010 MIMX	2020 MIMXX				
1971 MCMLXXI	1981 MCMLXXXI	1991 MCMXCI	2001 MIMI	2011 MIMXI	2021 MIMXXI				
1972 MCMLXXII	1982 MCMLXXXII	1992 MCMXCII	2002 MIMII	2012 MIMXII	2022 MIMXXII				
1973 MCMLXXIII	1983 MCMLXXXIII	1993 MCMXCIII	2003 MIMIII	2013 MIMXIII	2023 MIMXXIII				
1974 MCMLXXIV	1984 MCMLXXXIV	1994 MCMXCIV	2004 MIMIV	2014 MIMXIV	2024 MIMXXIV				
1975 MCMLXXV	1985 MCMLXXXV	1995 MCMXCV	2005 MIMV	2015 MIMXV	2025 MIMXXV				
1976 MCMLXXVI	1986 MCMLXXXVI	1996 MCMXCVI	2006 MIMVI	2016 MIMXVI	2026 MIMXXVI				
1977 MCMLXXVII	1987 MCMLXXXVII	1997 MCMXCVII	2007 MIMVII	2017 MIMXVII	2027 MIMXXVII				
1978 MCMLXXVIII	1988 MCMLXXXVIII	1998 MCMXCVIII	2008 MIMVIII	2018 MIMXVIII	2028 MIMXXVIII				
1979 MCMLXXIX	1989 MCMLXXXIX	1999 MCMXCIX	2009 MIMIX	2019 MIMXIX	2029 MIMXXIX				