1 Executive Summary

This redacted report presents the findings of the Project Silver Seagull investigation conducted on behalf of Gloucester City Council. The investigation was conducted between 23/12/2021 and 12/01/2022 and was authorised by Civica UK Ltd, on behalf of Gloucester City Council.

1.1 Investigation Summary

On 20/12/2021 Gloucester City Council were made aware of systems not operating as expected and staff being unable to connect remotely to servers. Civica UK Ltd were contacted and instigated an initial investigation which identified that Gloucester City Council were the subject of a ransomware attack by a group known as Conti.

Conti ransomware is operated as Ransomware-as-a-Service (RaaS) and means that there are operators and affiliates. Operators are the group behind the creation and maintenance of the ransomware. The affiliates are trusted parties who compromise the networks of victims and facilitate the deployment of the ransomware and exfiltration of data, with any ransom payment split between the two parties. If the victim fails to pay the ransom then any exfiltrated data is published on the Conti leak site and made available for anyone to download. It was evident that the threat actor had done their best to cover their tracks and used the ransomware in a destructive manner to impede any investigation.

Evidence of data exfiltration was identified on the host `DC-VS-PTC`, with the `Rclone` tool being present. `Rclone` provides an easy and effective way of copying data to an array of cloud storage providers and private servers, therefore is popular among threat actors. The firewall logs for the Gloucester City Council environment show that 226.5GB of data was exfiltrated to 126 different IP addresses which relate to the cloud application `Mega.nz`. `Rclone` and `Mega.nz` are known tools utilised by the Conti threat actor. The data exfiltration took place between 15/12/2021 9:47:57 and 16/12/2021 23:29:42. Due to the nature of `Rclone`, no data staging is required and data can be taken from either local or network locations. Therefore, it cannot be determined what data was taken however the threat actor is seen to move laterally to the file server `DC-VS-V601` seconds before the exfiltration commences, and it is therefore highly likely that the data captured by the threat actor is from the host `DC-VS-V601`, which is the main file server for Gloucester City Council.

The earliest malicious activity by the threat actor was identified as 24/11/2021, when a spearphishing email was sent to `REDACTED@gloucester.gov.uk` at 14:58. The user thereafter clicked the malicious link and downloaded a malicious zip file, attributed to Bazarloader malware, to the host `GCC004208`. The next stage involved a trojan being downloaded which is attributed as IcedID malware, confirming `GCC004208` as patient zero. Some internal reconnaissance of the users' endpoint was thereafter conducted with no further malicious activity identified until 14/12/2021. It is highly likely this delay was due to a disconnect between the threat actor group responsible for the initial access and the

threat actor group responsible for the further compromise.

On 14/12/2021, malicious activity restarted with the Bazarloader malware executing. It is then hypothesised that credential elevation was gained to the wider environment when a member of IT staff logged on remotely to the endpoint `GCC004208` to assist with a Citrix issue. A short time after the IT remote logon a user is seen to RDP to the host `APPVLIVHKP40` and deploy a Cobalt Strike beacon, which was installed as a Windows Service to ensure persistence. Further RDP connections and Cobalt Strike deployments followed with the activity taking place between 14/12/2021 and 18/12/2021. Cobalt Strike is a popular tool for adversary simulation and although distribution is tightly controlled, there are non-legitimate copies which are used by threat actors for malicious purposes. Deployment of Cobalt Strike was done in two ways, firstly by pushing out an executable via SMB to the `$Admin` share which created a new service on the infected hosts. Deployment was also identified via executing encoded PowerShell commands.

The threat actor installed AnyDesk on the host `DC-VS-PTC`. AnyDesk is a remote access tool which is popular with ransomware actors. It is highly likely this was installed as a persistence mechanism to ensure continued access to the Gloucester City Council environment. Forensic artefacts also identified Atera which is a Remote Monitoring and Management (RMM) application. Atera was found on the hosts `APPVTSTHKP02` and `Webvlivhkp16`. The purpose of installing this is to gain remote control of the host and install further software. Atera was used to install a legitimate remote access tool called Splashtop which could allow the threat actor a remote connection to any host on the network with it installed. Atera was first installed within the environment on 15/12/2021.

A number of the tools were utilised by the threat actor throughout this attack including `Process Hacker`, `Netscan` and `Power Tool`. The Conti ransomware binary was executed by threat actor at 21:18:07 on 18/12/2021.

It should be noted that the effectiveness of this investigation was significantly affected due to the lack of a centralised SIEM and no Endpoint Detection and Response (EDR) tool being deployed within the Gloucester City Council estate prior to the incident taking place.

Based on the artefacts recovered during this investigation it is recommended that any recovery in respect of restoration of backups is considered from two specific points. Should recovered hosts be in the form of an entire server rebuild (bare metal, without forensically wiping local storage), the recommended recovery date is 24/11/2021, prior to the malicious email being received. If the preferred remediation option is to rebuild the database (leaving the OS and applications intact) the suggested restore for backups date is 13/12/2021.

Note - This report has been redacted, NCC will not be liable for any reliance on this report by third parties due to the disclosure.