Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

2023-01: ACSC Ransomware Profile - **Royal**

24 January 2023

Context: *Royal is a ransomware variant first observed in September 2022, used by cybercriminals to conduct ransomware attacks against multiple sectors and organisations worldwide, including Australia. Once gaining access to a victim's environment, cybercriminals use this ransomware for similar purposes to other variants such as encrypting their data, and extorting a ransom to return access to the sensitive files. This product provides information related to Royal's background, threat activity, and mitigation advice.*

The Australian Cyber Security Centre (ACSC) is providing this information to enable organisations to undertake their own risk assessments and take appropriate actions to secure their systems and networks. The ACSC will only revise and update this document in the event of further significant information coming to light.

Key Points

- Royal ransomware restricts access to corporate files and systems by encrypting them into a locked and unusable format. Victims receive instructions on how to engage with the threat actors after encryption.
- Royal ransomware threat actors have successfully deployed ransomware on corporate systems in a variety of countries and sectors, including in Australia, where the ACSC is aware of multiple victims.
- Royal ransomware threat actors are known to implement the 'double extortion' technique by uploading samples of stolen victim data obtained through the attack and threatening to sell and/or release additional information if their ransom demands are not met.
- Threat actors involved in the deployment of the Royal ransomware use a range of vectors to gain initial access into victim networks, including callback phishing and exploitation of unpatched vulnerabilities.

Background

First detected in September 2022, Royal ransomware is likely associated with Russian-speaking cybercrime actors. According to open-source reporting, Royal is related to a previous ransomware variant, Zeon. Similarities between Royal and Conti have also been reported; however, it is unclear if the actors responsible for developing Royal are the same as those linked to Conti. The Royal ransomware group operate independently rather than adopting a Ransomware-as-a-Service (RaaS) model. Royal ransomware threat actors have successfully deployed ransomware to target networks worldwide, including in Australia, where the ACSC is aware of multiple Australian victims.

Threat activity

The ACSC is aware of an increase in domestic and global Royal activity in 2022 and use of Royal ransomware has continued into 2023. This includes the targeting of Australian critical infrastructure, notably including an educational institute in 2022. As of 10 January 2023, Royal ransomware threat actors claimed to have compromised at least 70 organisations worldwide.

Tactics, Techniques and Procedures

Threat actors deploying Royal ransomware notably use a technique called callback phishing, which involves tricking victims into taking action, such as returning a phone call or opening an email attachment. When the victims call the number from the phishing message, the threat actor uses social engineering techniques to persuade the victim to install their remote access software, a malicious downloader that poses as legitimate applications to gain initial access into the victim organisation. Threat actors use a range of other initial access vectors, including:

- Exploiting known vulnerabilities or common security misconfigurations
- Making malicious downloads appear authentic by hosting fake installer files on legitimate software download sites
- Using Google Ads in a campaign to blend in with normal ad traffic
- Using contact forms located on an organisation's website to distribute phishing links

Royal ransomware threat actors have been observed using well-known malware variants including Bokbot, Qakbot and BATLOADER after gaining access into the system. Threat actors also have been observed using Cobalt Strike for network access and lateral movement.

The Royal ransomware encrypts the network shares found in the local network as well as the local drives. A command line parameter called "-id" identifies the victim which is also written in the ransom note. The files are encrypted using the OpenSSL AES algorithm, with the key and Initialisation Vector (IV) being encrypted using the RSA public key that is hard-coded in the ransomware executable. The extension of the encrypted files is changed to ".royal".

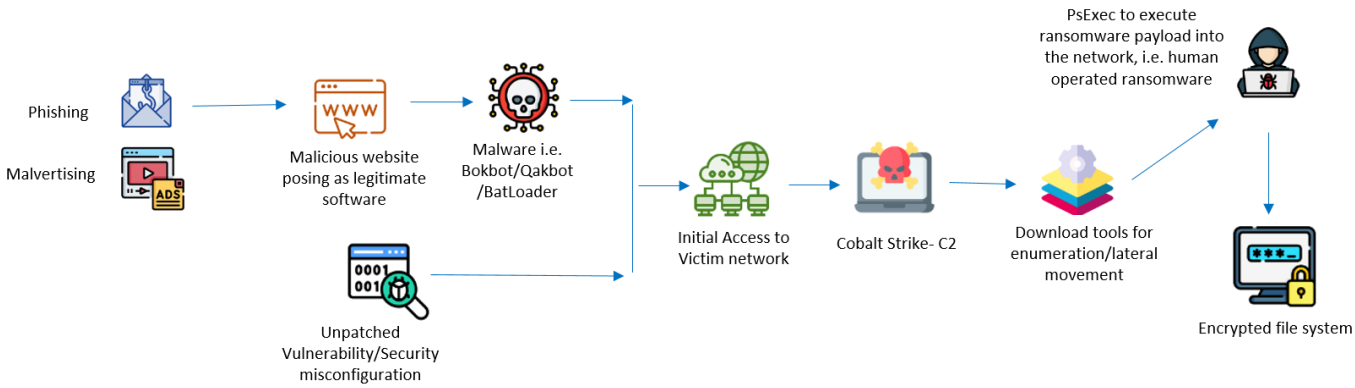

Figure-1: Royal Ransomware Infection Chain

Other observable Tactics, Techniques and Procedures (TTPs) associated with Royal ransomware activity include but are not limited to:

- Exfiltrating data through RClone to publicly available cloud file-sharing services
- Using software tools such as PCHunter, PowerTool and Process Hacker to disable any security-related services running in the system
- Using Virtual Hard Disk (VHD) and PowerShell to install legitimate remote management tools for first-stage payloads and persistence on the network
- Using PsExec tool to execute ransomware payload into other systems in the network
- Skipping specific file extensions (.dll, .bat,.royal, or .exe) for encryption
- Deleting all volume shadow copies that contain system backups

Post-Exploitation

During the post exploitation phase, Royal threat actors usually exfiltrate sensitive data from victim systems. Once Royal threat actors complete data exfiltration, they execute the ransomware payload to encrypt the file system and deliver a ransom note to the victims. Threat actors are known to implement the 'double extortion' technique by threatening to release victim data in part if the ransom is not paid. This ransom note may be sent to printers on the victim network or a file called README.txt, is stored in every location where files are encrypted. The ransom note also contains an advertisement of Royal ransomware actors "penetration testing" services that the actors will allegedly provide once the ransom has been paid. Royal ransomware threat actors maintain the communication with victims through a chat based platform hosted on The Onion Router (TOR) network.

Assistance

The ACSC monitors a range of activity involving the Royal ransomware variant. The ACSC is able to provide assistance and advice if required. Organisations that have been impacted or require assistance in regards to a Royal ransomware incident can contact the ACSC via 1300 CYBER1 (1300 292 371), or by submitting a report to cyber.gov.au.

Mitigations

The ACSC recommends organisations implement the following mitigations:

- Implement multifactor authentication to prevent actors from accessing valid accounts with stolen credentials
- Implement network segmentation and network traffic filtering to prevent actors from directly connecting to remote access services they have established for persistence
- Configure the Windows Registry to require User Access Control (UAC) approval for any PsExec operations requiring administrator privileges to reduce the risk of lateral movement by PsExec
- Implement hypervisor log monitoring and ensure that logs are processed on a separate system
- Implement application whitelisting (at least in monitor mode to capture unusual activity)
- Perform daily backups and keep them offline and encrypted

The below table maps the mitigations to the techniques leveraged by the actor and to the resources to implement these mitigations to protect your infrastructure.

Technique	Procedure	Mitigations
Initial Access [TA0001]		
Phishing [T1566]	Threat actors send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems.	Restrict Web-Based Content [M1021] Determine if certain websites or attachment types (ex: .scr, .exe, .pif, .cpl, etc.) that can be used for phishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk.

Exploit Public-Facing Application [T1190]	Threat actors search for and opportunistically exploit vulnerabilities in internet facing applications and devices to gain access to victim networks.	Update Software [M1051] Establish processes to identify, assess and patch vulnerabilities affecting internet facing applications and devices within appropriate timeframes. This allows organisations to address security vulnerabilities before they are discovered and exploited by actors. See also: • Assessing Security Vulnerabilities and Applying Patches Exploit Protection [M1050] Security applications that look for behaviour can be used to mitigate some exploitation behaviour. Many of these protections depend on the architecture and target application binary for compatibility.
Drive-by Compromise [T1189]	Actors gain access to a system via a user visiting a website that is used to host the adversary controlled content or malware such as Bokbot, Qakbot or BatLoader.	Exploit Protection [M1050] Security applications that look for behaviour can be used to mitigate some exploitation behaviour. Many of these protections depend on the architecture and target application binary for compatibility. Filter Network Traffic [M1037] Prevent network traffic from unknown or untrusted origins from accessing remote services on internal systems. This prevents actors from directly connecting to remote access services they have established for persistence.
Valid Accounts [T1078]	Actors have obtained credentials for valid accounts and gain access victim networks.	Multi-factor authentication [M1032] Require multifactor authentication for all user accounts, particularly privileged accounts. This prevents actors from accessing valid accounts with stolen credentials. See also: • Multi-factor Authentication - Technique D3-MFA • Implementing Multi-Factor Authentication

		• Strategies to Mitigate Cyber Security Incidents – Mitigation Details User training [M1017] Educate users to avoid password reuse. This prevents actors from obtaining credentials through public breaches or by compromising non-corporate systems. See also: • Creating Strong Passphrases
Persistence [TA0003]		
External Remote Services [T1133]	Actors have used commercial remote access software to persist on victim systems.	Filter Network Traffic [M1037] Prevent network traffic from unknown or untrusted origins from accessing remote services on internal systems. This prevents actors from directly connecting to remote access services they have established for persistence. See also: • Inbound Traffic Filtering - Technique D3-ITF Network Segmentation [M1030] Segment networks and restrict traffic for remote access services where possible. This limits the ability of threat actors moving laterally within compromised networks. Utilising network segmentation as a form of defence in depth also prevents actors from connecting to external remote access services that they have established for persistence via compromised systems within victim networks. See also: • Broadcast Domain Isolation - Technique D3-BDI • Implementing Network Segmentation and Segregation

Hijack Execution Flow [T1574]	Actors execute their own malicious payloads by hijacking the way operating systems run programs. Actors may use these mechanisms to elevate privileges or evade defences.	Restrict File and Directory Permissions [M1022] Restrict access by setting directory and file permissions that are not specific to users or privileged accounts. Restrict Library Loading [M1044] Prevent abuse of library loading mechanisms in the operating system and software to load untrusted code by configuring appropriate library loading mechanisms and investigating potential vulnerable software.
Execution [TA0002]		
System Services: Service Execution [T1569.002]	Actors have used the legitimate Windows Sysinternals tool PsExec [S0029] to execute malicious content.	Enable Attack Surface Reduction (ASR) on Microsoft Windows 10, and configure ASR to block process creations originating from PsExec commands. Note: PsExec is commonly used for legitimate system administration tasks. Organisations should consider how this mitigation could impact business practices before implementing. See also: • Hardening Microsoft Windows 10 version 21H1 Workstations
Command and Scripting Interpreter [T1059]	Threat actor abuse command and script interpreters such as windows command shell or PowerShell to execute commands, scripts, or binaries.	Privileged Account Management [M1026] When PowerShell is necessary, restrict PowerShell execution policy to administrators. Be aware that there are methods of bypassing the PowerShell execution policy, depending on environment configuration.
Exfiltration [TA0010]		
Exfiltration Over Web Service [T1567]	Actors have exfiltrated sensitive data and threatened to publicly release it. Actors have exfiltrated data to legitimate and publicly available web	Encrypt Sensitive Information [M1041] Encrypt sensitive data at rest. This prevents actors from accessing sensitive data even if they can access the systems storing the data. Network Segmentation [M1030]

	services, and in some cases have used legitimate tools such as RClone.	Segment networks to separate sensitive data, and services that provide access to sensitive data, from corporate environments. This prevents adversaries from compromising vulnerable systems, such as desktop environments, and immediately accessing and exfiltrating sensitive data. See also: • Broadcast Domain Isolation - Technique D3-BDI • Implementing Network Segmentation and Segregation Restrict Web-Based Content [M1021] Restrict access to web-based storage services from corporate networks, except where required for legitimate business activity. This prevents actors from directly uploading sensitive data to blocked web-based storage services.
Lateral Movement [TA0008], Privilege Escalation [TA0004], Discovery [TA0007]		
Various	Actors have deployed post-exploitation tools such as PCHunter, PowerTool, GMER, NetScan and Process Hacker on victim networks. These techniques are commonly used to move laterally through victim networks, harvest credentials, elevate privileges, exfiltrate data and deploy additional tools such as encryption binaries.	Network Segmentation [M1030] Segment networks and restrict or monitor certain types of traffic that are commonly used for lateral movement or reconnaissance. This prevents actors from moving laterally in networks and accessing sensitive systems or data. See also: • Broadcast Domain Isolation - Technique D3-BDI • Implementing Network Segmentation and Segregation Privileged Account Management [M1026] Restrict administrative privileges to operating systems and applications based on user duties. This reduces actors' ability to elevate privilege, move laterally in networks, bypass security controls and access sensitive data. See also:

		• Restricting Administrative Privileges Update Software [M1051] Patch applications and operating systems and keep them up to date. This prevents actors from exploiting known vulnerabilities in applications and operating systems to elevate privilege, bypass security controls and move laterally in networks. Limit Software Installation [M1033] Restrict access to installing or executing unapproved software. This prevents actors from using unapproved software on corporate devices to perform some of their objectives. See also: • System Patching
Impact [TA0040]		
Data Encrypted for Impact [T1486]	Actors have used Royal ransomware to encrypt valuable data, disrupt operations, and extort payment from victims.	Backup Data [M1053] Perform daily backups and keep them offline and encrypted. Test recovery and integrity procedures to make sure data and operations can be quickly and reliably restored. This will allow business operations to be recovered if data is encrypted, reducing the impact of a ransomware attack. Note that backups will not mitigate risks where sensitive data is exfiltrated and released. See also: • Data backup and restoration

Document Change Log

Version	Date	Change summary
1	24 January 2023	First Published

ACSC Australian Cyber Security Centre

Traffic Light Protocol

TLP Level	Restriction on access and use
TLP:RED	**Not for disclosure, restricted to participants only.** Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER+STRICT	**Limited disclosure, restricted to participants' organization.** Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization. Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.
TLP:AMBER	**Limited disclosure, restricted to participants' organization and its clients** Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only. Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect their organization and its clients and prevent further harm.
TLP:GREEN	**Limited disclosure, restricted to the community.** Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. Unless otherwise specified, TLP:GREEN information may not be shared outside of the cybersecurity or cyber defense community.
TLP:CLEAR	**Disclosure is not limited.** Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Recipients may share this information without restriction. Information is subject to standard copyright rules.