FIRMUS ADVISORY

ROYAL RANSOMWARE

27th NOVEMBER 2023

Level 15, Hampshire Place, No 1, Jalan Mayang Sari, Off Jalan Tun Razak, 50450 Kuala Lumpur
+603-6411-2626 | info@firmussec.com

Summary

Started to emerge in early 2022, the Royal ransomware is still active and currently impacting organizations across the globe, including the South East Asia region. The ransomware thrive due to its unique approach to evade anti-ransomware defenses using the partial encryption concept. The ransomware has the ability to to encrypt a pre-determined portion of the file content and base its partial encryption on a flexible percentage encryption that makes it difficult for anti-ransomware solutions to detect. To add fuel to the fire, Royal ransomware is a multi-threaded ransomware where it employs multiple threads to accelerate the encryption process. Lastly, Royal ransomware have various methods of deployment, making it very versatile in terms of gaining a foothold in the victim's environment. To conclude, organizations need to be extra aware of this ransomware because of its ability to avoid anti-ransomware tools, its ability to quickly decrypt the endpoints and its ability to enter the victim's network throughout various methods. These three traits make it a very deadly ransomware to pay extra attention to.

Technical Details

Royal ransomware is said to have developed from earlier versions of Zeon ransomware. Not only that, it also have similarities with BlackCat ransomware. However, based on the threat intelligence resources, Royal ransomware is more active compared to others where in November 2022, it was reported to be the most profilic ransomware in the e-crime threat landscape, overtaking the famous LockBit ransomware. The differentiator between Royal ransomware and other similar ransomware is the encryption algorithm and the attack vectors. Royal ransomware have its own custom-made file encryption program where the foundation of the program is based on the early version of Zeon ransomware. Next, Royal ransomware have various attack vectors that has been uniquely identified as the techniques, tactics and procedures (TTP) for this ransomware attack. Both of these factors are used as the Indicator of Compromised (IoC) and Indicator of Attack (IoA) to check and hunt for Royal ransomware by cyber-security experts.

Royal ransomware operations start in various ways. They have several initial access methods such as phishing campaigns to gain access into the victim's network. After accessing the network, the Royal actors will proceed on disabling anti-virus software and then exfiltrate large amount of data. Afterwards, they will deploy the ransomware into the environment and then started to encrypt the system by a specific percentage to avoid detection. Then a ransom note will be given where it does not give any ransom amounts or payment instructions. Instead, only a .onion URL is given so that the victim can communicate to the threat actor directly. There are approximately around 350 known victims of the Royal ransomware. If the ransomware is not paid, the data will be publish to a leak site. However, based on our threat intelligence, the official Royal ransomware group onion site is currently offline as of early November 2023.

Indicator of Compromise

IoC	Description
.royal	➢ Royal ransomware encrypted file extension
.royal_w	➢ Royal ransomware encrypted file extension
.royal_u	➢ Royal ransomware encrypted file extension
README.TXT	➢ Royal ransom note

Malicious Domain
➢ sombrat[.]com ➢ gororama[.]com ➢ softeruplive[.]com ➢ altocloudzone[.]live ➢ ciborkumari[.]xyz ➢ myappearinc[.]com ➢ parkerpublic[.]com ➢ pastebin.mozilla[.]org/Z54Vudf9/raw ➢ tumbleproperty[.]com ➢ myappearinc[.]com/acquire/draft/c7lh0s5jv

Royal Ransomware Binary (SHA256)
➢ 50bcbfa58da3e713b4ca12edef4dc06358e8986cad15928aa30c44fe4596488
➢ 9db958bc5b4a21340ceeeb8c36873aa6bd02a460e688de56ccbba945384b1926
➢ c24c59c8f4e7a581a5d45ee181151ec0a3f0b59af987eacf9b363577087c9746
➢ 5fda381a9884f7be2d57b8a290f389578a9d2f63e2ecb98bd773248a7eb99fa2
➢ 312f34ee8c7b2199a3e78b4a52bd87700cc8f3aa01aa641e5d899501cb720775
➢ f484f919ba6e36ff33e4fb391b8859a94d89c172a465964f99d6113b55ced429
➢ 7cbfea0bff4b373a175327d6cc395f6c176dab1cedf9075e7130508bec4d5393

➢ 2598e8adb87976abe48f0eba4bbb9a7cb69439e0c133b21aee3845dfccf3fb8f

Variant	Royal Ransomware Hash
Royal Windows Variant	➢ 595c869f8ec7eaf71fef44bad331d81bb934c886cdff99e1f013eec7acdaf8c9
Royal Linux Variant	➢ b57e5f0c857e807a03770feb4d3aa254d2c4c8c8d9e08687796be30e2093286c
Royal Linux Variant	➢ b64acb7dcc968b9a3a4909e3fddc2e116408c50079bba7678e85fee82995b0f4
Royal Linux Variant	➢ b64acb7dcc968b9a3a4909e3fddc2e116408c50079bba7678e85fee82995b0f4
Royal Linux Variant	➢ 12a6d61b309171b41347d6795002247c8e2137522a756d35bb8ece5a82fc3774

Tool	SHA 256
AV tamper	➢ 8A983042278BC5897DBCDD54D1D7E3143F8B7EAD553B5A4713E30DEFFDA16375
TCP/UDP Tunnel over HTTP (Chisel)	➢ 8a99353662ccae117d2bb22efd8c43d7169060450be413af763e8ad7522d2451
Ursnif/Gozi	➢ be030e685536eb38ba1fec1c90e90a4165f6641c8dc39291db1d23f4ee9fa0b1
Exfil	➢ B8C4AEC31C134ADBDBE8AAD65D2BCB21CFE62D299696A23ADD9AA1DE082C6E20
Remote Access (AnyDesk)	➢ 4a9dde3979c2343c024c6eeeddff7639be301826dd637c006074e04a1e4e9fe7

PowerShell Toolkit Downloader	➢ 4cd00234b18e04dcd745cc81bb928c8451f6601affb5fa45f20bb11bfb5383ce
PsExec (Microsoft Sysinternals)	➢ 08c6e20b1785d4ec4e3f9956931d992377963580b4b2c6579fd9930e08882b1c
Keep Host Unlocked (Don't Sleep)	➢ f8cff7082a936912baf2124d42ed82403c75c87cb160553a7df862f8d81809ee
Ransomware Executable	➢ d47d4b52e75e8cf3b11ea171163a66c06d1792227c1cf7ca49d7df60804a1681
Windows Command Line (NirCmd)	➢ 216047C048BF1DCBF031CF24BD5E0F263994A5DF60B23089E393033D17257CB5
System Management (NSudo)	➢ 19896A23D7B054625C2F6B1EE1551A0DA68AD25CDDBB24510A3B74578418E618

IP Addresses
➢ 102.157.44[.]105 ➢ 105.158.118[.]241 ➢ 105.69.155[.]85 ➢ 113.169.187[.]159 ➢ 134.35.9[.]209 ➢ 139.195.43[.]166 ➢ 139.60.161[.]213 ➢ 148.213.109[.]165 ➢ 163.182.177[.]80 ➢ 181.141.3[.]126 ➢ 181.164.194[.]228 ➢ 185.143.223[.]69 ➢ 186.64.67[.]6 ➢ 186.86.212[.]138

- 190.193.180[.]228
- 196.70.77[.]11
- 197.11.134[.]255
- 197.158.89[.]85
- 197.204.247[.]7
- 197.207.181[.]147
- 197.207.218[.]27
- 197.94.67[.]207
- 23.111.114[.]52
- 41.100.55[.]97
- 41.107.77[.]67
- 41.109.11[.]80
- 41.251.121[.]35
- 41.97.65[.]51
- 42.189.12[.]36
- 45.227.251[.]167
- 5.44.42[.]20
- 61.166.221[.]46
- 68.83.169[.]91
- 81.184.181[.]215
- 82.12.196[.]197
- 98.143.70[.]147
- 140.82.48[.]158
- 147.135.36[.]162
- 147.135.11[.]223
- 152.89.247[.]50
- 172.64.80[.]1
- 179.43.167[.]10
- 185.7.214[.]218
- 193.149.176[.]157
- 193.235.146[.]104
- 209.141.36[.]116
- 45.61.136[.]47
- 45.8.158[.]104

➢ 5.181.234[.]58 ➢ 5.188.86[.]195 ➢ 77.73.133[.]84 ➢ 89.108.65[.]136 ➢ 94.232.41[.]105 ➢ 47.87.229[.]39

Batch Script	Hash Value
2.bat	➢ 585b05b290d241a249af93b1896a9474128da969
3.bat	➢ 41a79f83f8b00ac7a9dd06e1e225d64d95d29b1d
4.bat	➢ a84ed0f3c46b01d66510ccc9b1fc1e07af005c60
8.bat	➢ c96154690f60a8e1f2271242e458029014ffe30a
kl.bat	➢ 65dc04f3f75deb3b287cca3138d9d0ec36b8bea0
gp.bat	➢ 82f1f72f4b1bfd7cc8afbe6d170686b1066049bc7e5863b51aa15ccc5c841f58
r.bat	➢ 74d81ef0be02899a177d7ff6374d699b634c70275b3292dbc67e577b5f6a3f3c
runanddelete.bat	➢ 342B398647073159DFA8A7D36510171F731B760089A546E96FBB8A292791EFEE

Royal Ransomware Associated Files	
File	**SHA 256**
windows_encryptor.exe	➢ 85087f28a84205e344d7e8e06979e6622fab0cfe1759fd24e38cd0390bca5fa6
%PROGRAMDATA%\wine.exe	➢ 5b08c02c141eab94a40b56240a26cab7ff07e9a6e760dfde8b8b053a3526f0e6
%USERPROFILE%\Downloads\run1.bat	➢ bc609cf53dde126b766d35b5bcf0a530c24d91fe23633dad6c2c59fd1843f781

%USERPROFILE%\Downloads\run2.bat	➢ 13c25164791d3436cf2efbc410caec6b6dd6978d7e83c4766917630e24e1af10
%USERPROFILE%\Downloads\run3.bat	➢ 2b93206d7a36cccdf7d7596b90ead301b2ff7e9a96359f39b6ba31bb13d11f45
%USERPROFILE%\Downloads\run4.bat	➢ 84e1efbed6bb7720caea6720a8bff7cd93b5d42fb1d71ef8031bfd3897ed4435
%USERPROFILE%\Downloads\sc.bat	➢ e0dbe3a2d07ee10731b68a142c65db077cfb88e5ec5c8415e548d3ede40e7ffc
%USERPROFILE%\Downloads\sr.bat	➢ 34a98f2b54ebab999f218b0990665485eb2bb74babdf7e714cc10a306616b00c
runanddelete.bat	➢ 342b398647073159dfa8a7d36510171f731b760089a546e96fbb8a292791efee
InstallerV8.1.ms	➢ 3e6e2e0de75896033d91dfd07550c478590ca4cd4598004d9e19246e8a09cb97
f827.exe	➢ 5654f32a4f0f2e900a35761e8caf7ef0c50ee7800e0a3b19354b571bc6876f61
f24dc8ea.msi	➢ 91605641a4c7e859b7071a9841d1cd154b9027e6a58c20ec4cadafeaf47c9055
defw10.bat	➢ fb638dba20e5fec72f5501d7e0627b302834ec5eaf331dd999763ee925cbc0f9
ll.exe	➢ f0197bd7ccd568c523df9c7d9afcbac222f14d344312322c04c92e7968859726
Royal Ransomware Hash	➢ b987f738a1e185f71e358b02cafa5fe56a4e3457df3b587d6b40e9c9de1da410
File	**MD5 Hash Value**
b34v2.dll	➢ a51b1f1f0636bff199c0f87e2bb300d42e06698b

1.exe	➢ d93f1ef533e6b8c95330ba0962e3670eaf94a026
34.dll	➢ 9e19afc15c5781e8a89a75607578760aabad8e65
ll.exe	➢ 9a92b147cad814bfbd4632b6034b8abf8d84b1a5
Royal Ransomware Hash	➢ a4ef01d55e55cebdd37ba71c28b0c448a9c833c0

Legitimate Files and Tools used by Royal ransomware	
Name	**Description**
C:\Program Files\OpenSSH\ssh-agent.exe	➢ SSH Client
C:\Program Files\OpenSSH\sshd.exe	➢ SSH Client
%USERPROFILE%\Downloads\WinRAR.exe	➢ Compression tool
%APPDATA%\MobaXterm\	➢ Toolbox for remote computing
\Program Files (x86)\Mobatek\	➢ Toolbox for remote computing
\Program Files (x86)\Mobatek\MobaXterm\	➢ Toolbox for remote computing
b34v2.dll	➢ ColbaltStrike Beacon
34.dll	➢ CobaltStrike Beacon
mimikatz.exe	➢ Mimikatz credential harvester
dialuppass.exe	➢ Nirsoft password harvesting utility
iepv.exe	➢ Nirsoft password harvesting utility
mailpv.exe	➢ Nirsoft password harvesting utility
netpass.exe	➢ Nirsoft password harvesting utility

routerpassview.exe	➢ Nirsoft password harvesting utility
AdFind.exe	➢ ADFind tool
LogMeIn	➢ Remote access tool
Atera	➢ Remote access tool
C:\Program Files\Eraser\Eraser.exe	➢ Anti-Forensics Tool used by Threat Actor
advanced_ip_scanner.exe	➢ Reconnaissance Tool used by Threat Actor
Name	**SHA 256**
conhost.exe (chisel_windows_1_7_7.exe)	➢ b9ef2e948a9b49a6930fc190b22cbdb3571579d37a4de56564e41a2ef736767b
%USERPROFILE%\Downloads\svvhost.exe \Users\Administrator\AppData\Local\Temp\cloudflared.exe	➢ c429719a45ca14f52513fe55320ebc49433c729a0d2223479d9d43597eab39fa
nsudo.exe	➢ 19896a23d7b054625c2f6b1ee1551a0da68ad25cddbb24510a3b74578418e618

Royal Ransomware Tactics, Techniques and Procedures (TTPs)

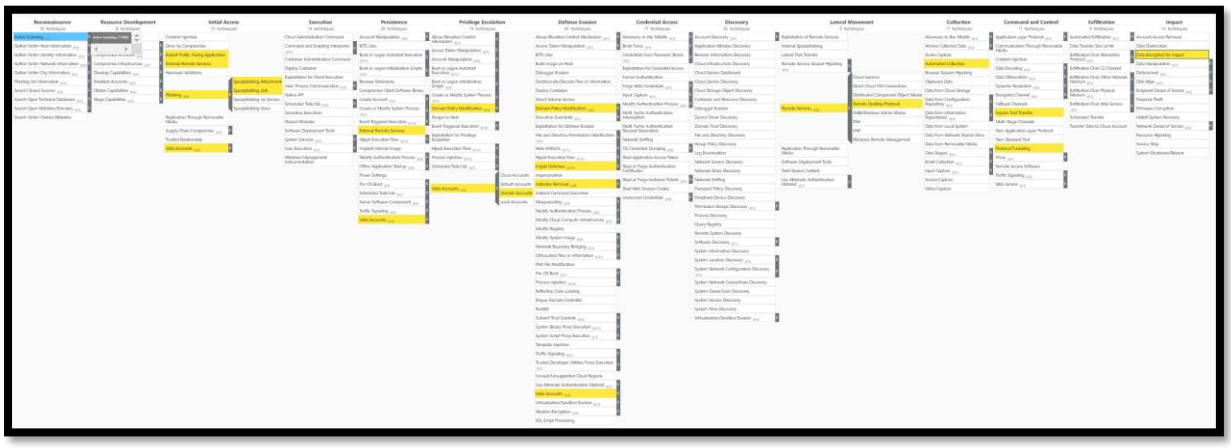

Figure 1: MITRE Attack Navigator (ROYAL RANSOMWARE)

Initial Access

T1190: Exploit Public-Facing Application

Royal ransomware threat actor target to exploit weaknesses in a public-facing applications to gain initial access to the network. It could be a known vulnerability, misconfiguration, or a software bug.

T1566.001: Phishing: Spear Phishing Attachment

The Royal ransomware threat actor sends spearphishing emails with malicious malware attached to gain access to victim systems. The email will be curated specifically for the individual or the company in order to make the victim open the malicious attachment. Royal ransomware threat actor uses malicious PDF attachments sent via email.

T1566.002: Phishing: Spear Phishing Link

A spearphishing email with a malicious link is a tactic which will download the malware contained in the email to avoid defenses that inspect email attachments. Royal ransomware threat actor uses malvertising links via emails and public-facing sites to lure victims.

T1133: External Remote Services

The threat actor gains initial access through a variety of remote monitoring and management software. They exploit remote services such as VPN, Citrix and other access mechanisms that allow users to connect to internal enterprise network resources from external locations.

Command and Control

T1105: Ingress Tool Transfer

Once the Royal ransomware threat actor set a foothold inside the environment, they will use C2 infrastructure to download multiple tools to the compromised environment. This technique can be used to spread malicious tools between victim devices within the environment.

T1572: Protocol Tunneling

The threat actor tunnel network communication to and from victim system by using encrypted SSH tunnel to communicate to the C2 server. The traffic will be concealed which makes it hard to be detected. This technique is usually used to avoid detection, network filtering and sometimes used to enable access to unreachable systems.

Privilege Escalation

T1078.002: Valid Accounts: Domain Accounts

Domain accounts are accounts that are managed by Active Directory Domain Services where access and permissions are configured across systems and services that are part of the domain. The Royal ransomware threat actor utilizes this technique to create new admin user accounts to gain higher privilege in the victim's environment.

Defense Evasion

T1562.001: Impair Defenses: Disable or Modify Tools

Royal ransomware threat actor will disable antivirus protocols to avoid detection of their malware tools and activities.

T1484.001: Domain Policy Modification: Group Policy Modification

Royal ransomware threat actor altered Group Policy Objects in order to bypass antivirus protocols.

T1070.001: Indicator Removal: Clear Windows Event Logs

The main purpose of this technique is to hide the activity of intrusion. The threat actor deletes shadow files, system, and security logs after data exfiltration to cover up their digital footprint.

T1021.001: Remote Services: Remote Desktop Protocol

Royal ransomware threat actor uses valid accounts to move laterally through the domain controller using RDP. They can perform actions as the logged-on user.

T1119: Automated Collection

Once the Royal ransomware threat actor established themselves within the environment, they will use registry keys to auto-extract and collect files.

Impact

T1486: Data Encrypted for Impact

Royal ransomware threat actor encrypted data to interrupt the availability of the system and network resources. What makes it unique is that this ransomware can control the percentage of the encryption, where they can choose which and how much data they want to encrypt.

Mitigations

In order to respond to Royal ransomware, FIRMUS implies that all organizations execute the mitigation listed below to improve their security posture.

Conduct Compromise Assessment on all Organization's assets

Conducting a compromise assessment is a proactive and essential step for organizations to avoid ransomware and strengthen their overall cybersecurity posture. A compromise assessment involves examining an organization's network and systems to identify any signs of compromise or unauthorized activity. By conducting this, FIRMUS believes that current the organization will be more secure because vulnerabilities will be identified and resolved before getting exploited. Compromised Assessments will also check whether the organization is compromised or not by Royal ransomware or any other threats.

Required All Accounts with Password Logins

FIRMUS recommends organizations to enforce all accounts to have login credentials. The password must comply with NIST standards for developing and managing password policies. All accounts, especially service accounts which are most likely to be exploited by Royal ransomware threat actor must have a login credential that is up to NIST standards.

Secure Remote Access Software

It is crucial to secure Remote Access software since many malwares including the Royal ransomware takes advantage of this as one of their attack vectors. In order to secure the Remote Access Software, below are the steps that can be taken:

- Audit remote access software and their configurations on devices to identify currently used or authorized RMM software.

- Implement network segmentation to minimize lateral movement and restrict access to devices, data, and applications.
- Require RMM solutions to only be used from within the network over approved remote access solutions such as VPNs or Virtual Desktop Interfaces (VDIs).
- Configure least privilege for RMM tools for common uses, like read-only monitoring.
- Keep direct access to log servers and the ability to delete or alter logs, out of reach of RMM tools.

Safeguard Mass scripting and Script Approval process

Use safeguards for mass scripting and a script approval process. For example, if an account attempts to push commands to 10 or more devices within an hour, retrigger security protocols, such as multifactor authentication (MFA), to ensure the source is legitimate.

Network Segmentation

Segment the network to prevent ransomware from getting spread. Segmentation can control the flow of traffic and restrict the ransomware from infecting further

Time-based access for accounts set at admin level and higher

Enforce Just-in-Time (JIT) access method provisions privileged when needed with Principle of Least Privilege (PoLP). This network-wide policy can automatically disable admin accounts at the active directory level when the account is not in direct need. Individual users may submit their requests through an automated process that grants them access to a specified system for a set timeframe when they need to support the completion of a certain task

Email Banner to emails

Apply email banners when receiving emails outside of the organization. This will make it easier to identify and report potentially malicious content.

Maintain offline backups

Ensure that organizations have a regularly offline maintained backup to ensure that if they got infected by the ransomware, the offline backup would not be infected. It is best to backup daily or weekly.

Implement a recovery plan

Implement a recovery plan to save several copies of sensitive or proprietary data and servers in a physically isolated, segregated, and secure location.

Apply Multi-factor Authentication (MFA)

The best practice is to apply MFA to all services that is possible, particularly on VPN, webmail and accounts that access critical systems.

Software, Firmware and Operating Systems are up to date

Ensure that all software, firmware, and OS are up to date to reduce the attack surface for the Royal ransomware threat actor to exploit.

Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool.

Implement a system that logs and reports all network traffic, including lateral movement activity, to aid in the detection of ransomware. Endpoint detection and response (EDR) tools are very good for detecting lateral connections since they know what network connections are typical and rare for each host especially when using a tool that has behavioral analysis. FIRMUS offers EDR services that can help organizations to detect vulnerabilities and existing threats inside the organization effectively with a tool that uses artificial intelligence to detect and block threats.

Summary

Royal ransomware has been in the wild for a while now and they are becoming more aggressive than before, hence making them more active than LockBit ransomware at the end of this year. However, the Royal ransomware threat actor official .onion site is still offline, but there are numerous reports from multiple threat intelligence platform including in Malaysia reported that they detected the Indicator of Compromised (IoC) of Royal ransomware in their environment. Hence, to be safe from this ransomware, FIRMUS has provided some mitigation steps on how to increase your security defenses and reduce your attack surface. FIRMUS hopes by sharing this information with the community, we could all protect our organizations and the South-East Asia region from this evolving cyber threat landscape. FIRMUS would also like to remind you that we offer EDR services and Compromised Assessments service which help strengthen an organization's security posture and at the same time, identify whether the organization has been compromised or not. Lastly, FIRMUS hopes that organizations check their current networks and assets by utilizing the Indicator of Compromise given. Feel free to contact FIRMUS for any inquiries. You Change The World, We Secure It.

Sources:

- https://unit42.paloaltonetworks.com/royal-ransomware/
- https://www.cybereason.com/blog/royal-ransomware-analysis
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a
- https://www.securityweek.com/royal-ransomware-possibly-rebranding-after-targeting-350-organizations-worldwide/