Royal Ransomware

Analysis of one of the most active ransomware groups in late 2022 and early 2023

Date: January 10, 2023
Contents
1. Executive Summary .................................................................................................................................. 3
2. Technical Analysis .................................................................................................................................. 3
3. Threat Hunt Opportunities ................................................................................................................... 6
4. TTPs ...................................................................................................................................................... 6
5. References ............................................................................................................................................ 7
1. Executive Summary

The Royal ransomware threat actor group, initially tracked as DEV-0569, first emerged in early 2022 and has been especially active since the end of the same year. Royal ransomware was first observed by security researchers in September 2022 and since then multiple attacks were detected, targeting organizations across the globe, but mostly in U.S., Brazil and Europe. It was among the most active ransomware groups in December 2022 and has already announced its first victim of 2023: DSBJ, a Chinese company that manufactures components for IoT and telecommunications equipment.

Security researchers have noticed that the group was probably created by one of the former Conti teams (“Conti Team One”) and used the Zeon encryptor in some attacks. The group employs the double extortion tactic by gaining access to a victim’s environment, encrypting their data as well as exfiltrating sensitive data and demanding a ransom to decrypt files. The files are encrypted using the Advanced Encryption Standard (AES) and given the extension .royal. In recent attacks, the encrypted files also had the extension .royal_*.

The initial attack vectors are specifically designed and tailored for individual targets, including some unusual techniques. Their techniques for initial infection include malicious advertisements, phishing links that point to a malware payload, fake software installers and fake forum pages to lure potential victims. The group’s phishing techniques include callback phishing, where they impersonate various service providers and software providers in emails that look like subscription renewals. The phishing emails contain phone numbers that the victim should contact to cancel their subscription. Upon calling the number, the threat actors convince the victim to install remote access software. This remote access software would serve as initial access to the target network.

In a recent campaign, the ransomware actors used a compiled remote desktop malware, which was used to drop the tools that were later used to infiltrate the victim’s system. There have been instances where the threat actor used QakBot and Cobalt Strike for lateral movement, while NetScan was used to look for any network connected systems. Once they infiltrated the system, the ransomware actors used tools like Nsudo, PowerTool and Process Hacker to disable any security-related services running in the system. The ransomware actors used PsExec to execute the malware and to spread the malware to other machines in the network. The group also relies heavily on defense evasion techniques such as using encrypted binaries and disabling antivirus solutions.

In this report, we analyze the Royal ransomware payload in Section 2; present threat hunt opportunities in Section 3; and share details of the Royal ransomware group’s tactics, techniques and procedures (TTPs) in Section 4.

2. Technical Analysis

The Royal ransomware payload is a 64-bit executable written in C++ that is not packed and that imports several interesting DLLs, as shown in Figure 1.

![Figure 1 – Royal ransomware executable and DLLs](image)

The ransomware uses the Windows Restart Manager DLL to check if any of the files targeted to be encrypted are being used by other processes. The malware uses API calls such as RmStartSession, RmGetList and RmShutDown (shown in Figure 2) to start the session, get the list of processes using the resource and kill those processes using the resource.
The ransomware supports three arguments for execution: -path, -ep and -id. The last argument is mandatory while the other two are optional. The -path parameter (shown in Figure 3) is used to specify the path to be encrypted, -ep is used to specify the percentage of the file that needs to be encrypted and -id is a unique number used by the ransomware group to identify its victims.

The command executed to run the payload is as follows: cmd.exe /c "c:\windows\temp\royal.exe -id <32-bit victim ID>"

The ransomware will not run if no value is specified for the -id parameter. The ransomware will then attempt to delete volume shadow copies using the following command: vssadmin.exe delete shadows /all /quiet.

Once the shadow copies are deleted, the malware then decrypts a list of file extensions. Files with the following extensions would be excluded from encryption: .exe, .dll, .bat, .lnk, .royal. Similarly, a list of folders is also decrypted which are to be excluded from encryption: windows, $recycle.bin, google, royal perflogs, mozilla, tor browser, boot, $windows.~ws, $windows.~bt, windows.old.
The Royal ransomware uses a multi-threaded encryption mechanism. The GetNativeSystemInfo API is used to get the number of processors available in a target machine. The threads for encryption are then created using this value.

```c
unsigned long local_18 = DAT_1402cf920 * (ulonglong)0xfffffffffffffffff88;
GetNativeSystemInfo((LPSYSTEM_INFO *)&local_18);

uVar2 = 0;
if (GetSystemInfo((SYSTEM_INFO *)&local_18, sizeof(SYSTEM_INFO)) != NULL) {
    *ppVar2 = (DWORD *)((long long)param_1 + 0x30); // thread count
    if (local_44.dwNumberOfProcessors * 2 != 0) {
        while (uVar3 < (uint *)((long long)param_1 + 0x30)) {
            *ppVar2 = ppVar2 + 1;
            uVar3 = uVar3 + 1;
        }
    }
    return;
}
```

**Figure 6 – Thread creation for encryption**

The ransomware then tries to enumerate the network shares available in the network using the NetShareEnum API. Shares ADMIN$ and IPC$ are excluded.

**Figure 7 – Network share enumeration**

The ransomware then imports a hard-coded RSA public key that is embedded in the binary in plain text format (shown in Figure 8). This is used for encrypting the AES key used for file encryption.

**Figure 8 – Embedded RSA public key**
The target files are encrypted using the OpenSSL library and the AES256 algorithm. Finally, a ransom note named README.txt is created in every directory (shown in Figure 9).

```
    1v4 = !v4 -&gt; "{longlong *(1v4 - -8)}
    1v4 = *(longlong *)(1v4 - -8);
    AB_14007c2f:
    thunk_FIN_1401b14c(1v4, uVar9);
    }
    else
        FIN_1401b156(2, 0x000, 0x000);
        nNumberofBytesToWrite =
            FIN_1407v80(0, local_1030);
/*Hello!\r\n\tIf you are reading this, it means that your system were hit
by Royal ransomware.\r\n\tPlease contact us via
\r\n\thttp://royalrthig3ouk6d2alaxml2ye665mpxedid.onion/\r\n\tIn the meantime, let us explain this case. It may be complicated,
but it is not likely what happened was that you decided to save
some money on your security infrastructure.\r\n\tAs a result your critical data was not only encrypted but also copied from your systems on a
secure server.\r\n\tFrom there it can be published online. Then anyone on the
internet from darkest criminals, ACLU journalists, Chinese
government (different names for the same thing).\r\n\tand even your employees
will be able to see your internal documentation: personal data, HR reviews,

Figure 9 – Ransom note creation

3. Threat Hunt Opportunities

- **PsExec Service Installation**: event_id = 7045 OR 7036 && service_name contains “psexesvc”

- **PsExec Remote Command Execution**: process _process_name = psexesvc.exe && process _name = cmd.exe

- **Shadow Copy Deletion**: process _name = vssadmin.exe && Commandline contains “delete*shadows”

- **Local Admin Account Created Using Net.exe**: process_name = net.exe OR net1.exe && Commandline contains “* administr*/add*”

4. TTPs
<table>
<thead>
<tr>
<th>Tactic</th>
<th>Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Access</td>
<td>T1566: Phishing</td>
</tr>
<tr>
<td></td>
<td>T1078: Valid Accounts</td>
</tr>
<tr>
<td>Discovery</td>
<td>T1083: File and Directory Discovery</td>
</tr>
<tr>
<td></td>
<td>T1016: System Network Configuration Discovery</td>
</tr>
<tr>
<td></td>
<td>T1046: Network Service Discovery</td>
</tr>
<tr>
<td></td>
<td>T1057: Process Discovery</td>
</tr>
<tr>
<td></td>
<td>T1082: System Information Discovery</td>
</tr>
<tr>
<td></td>
<td>T1135: Network Share Discovery</td>
</tr>
<tr>
<td>Execution</td>
<td>T1059: Command and Scripting Interpreter</td>
</tr>
<tr>
<td></td>
<td>T1569: System Services</td>
</tr>
<tr>
<td></td>
<td>T1204: User Execution</td>
</tr>
<tr>
<td>Defense Evasion</td>
<td>T1562: Impair Defenses</td>
</tr>
<tr>
<td></td>
<td>T1036: Masquerading</td>
</tr>
<tr>
<td>Impact</td>
<td>T1486: Data Encrypted for Impact</td>
</tr>
<tr>
<td></td>
<td>T1489: Service Stop</td>
</tr>
<tr>
<td></td>
<td>T1490: Inhibit System Recovery</td>
</tr>
</tbody>
</table>

5. References


© 2023 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents is available at www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products or service names may be trademarks or service marks of their respective owners. v01_01 January 2023