Dark Web Profile: Royal Ransomware - SOCRadar® Cyber Intelligence Inc.

By Cem Sarı

Published: 2023-01-09 · Archived: 2026-04-10 03:12:19 UTC

By SOCRadar Research

[Update] November 14, 2023: See the subheading: "CSA Update from CISA and FBI: Royal Ransomware's Possible Rebranding to 'Blacksuit'"

Ransomware attacks have been rising in recent years, with the frequency of attacks increasing. In 2021, several high-profile ransomware attacks made headlines, such as the attack on the Colonial Pipeline. This attack resulted in the temporary shutdown of the pipeline, which caused fuel shortages and panic buying in some areas. This incident could have led to a crisis within the country.

In addition to targeting large companies, ransomware attacks are frequently directed at small businesses, hospitals, and other organizations with less robust cybersecurity measures.

In November 2022, the **Royal Ransomware** group was the most actively operating ransomware group, and the group is continuing to damage organizations.

Daily Dark Web's infographic of Ransomware activities in November 2022 (Source: Daily Dark Web)

Who is Royal Ransomware Group?

Royal Ransomware strain was first detected on DEV-0569's (threat actor) operations in September 2022. The actors behind the Royal are composed of experienced individuals from other ransomware operations, such as Conti, and operate independently without any affiliates. Royal Ransomware group operates professionally rather than adopting Ransomware-as-a-Service as most other groups work.

According to SOCRadar's dark web team's findings, Royal Ransomware primarily targets the manufacturing industry. It could be because of the **broad attack surface** area, such as various specialized equipment and managed software used in the field. Plus, the limited IT and security workforce may have led to factories becoming easy targets for cybercriminals. In addition, the probability of getting paid the ransom is high for ransomware groups considering that the extended downtime will increase the damage to facilities.

Targeted industries of Royal Ransomware

How Royal Ransomware Group Attacks?

According to BleepingComputer, Royal Ransomware attacks used a technique called callback phishing, which involves tricking victims into believing they need to take some action, such as returning a phone call or opening an email attachment.

An example of Royal's callback phishing mail (Source: Bleeping Computer)

When the victim reaches Royal, the group uses social engineering techniques to persuade the victim to install their remote access software -a malware downloader that poses legitimate applications like Zoom and Microsoft Teams– and get initial access to the network of the victim's organization.

Diagram of DEV-0569's attack chain, which is a threat actor that uses Royal Ransomware actively (Source: Microsoft)

SOCRadar Researchers took a sample and analyzed Royal Ransomware, which is detailed in the "**Analysis of Royal Ransomware**" section below.

In addition, the group generally uses the **double-extortion method**, which means they also exfiltrate sensitive data before encrypting it for ransom. Also, the group's ransom demand ranges between $250,000 to over $2 million.

Which Countries Did Royal Ransomware Target?

Royal ransomware group's victims are commonly from **Europe** and the **American** continent.

Affected countries by Royal Ransomware

SOCRadar researchers analyzed about 70 observed claims from Royal Ransomware since September 2022 and found that around 69% of the attacks were made against organizations in the United States.

Royal Ransomware's percentage distribution of target countries from its latest attacks

Findings on Royal Ransomware

Since it has damaged about 75 organizations and continues its operations actively, SOCRadar researchers browsed open sources. They examined the Royal Ransomware sample obtained from the Malware bazaar platform to learn which activities are happening after it starts working on infected systems. The findings of the sample can be seen below: (You can find the IOCs of Royal Ransomware used in the analysis at the Appendixes section)

Several anti-analysis techniques were encountered when the Royal Ransomware ran step by step. After these stages were passed, it was seen that the process compares three arguments: **"-path," "-id," and "-ep."**

The"-id" parameter could be for the **victim ID**, "-path" could be for the **directory path**, and the "-ep" parameter, as we observed, refers to the **encryption percentage** of the file.

"-path", "-id", and "-ep" parameters used in Royal Ransomware

Also, the program skips the encryption process for all the files with extensions "dll," "bat," "royal," or "exe."

Skipping files with extensions dll, bat, exe, and royal.

Skipping files with extensions dll, bat, exe, and royal.

The program encrypts files using AES and IV and changes the extension of files with ".royal."

AES and IV key generation processes (Source: TrendMicro)

When the encryption process starts, the first "README.TXT" file, which contains the ransom note, is created under the C:Program Files directory.

First file that contains ransom note observed in C:Program Files

Royal's Ransom note (Source: BleepingComputer)

The URL link in the ransom note directs the victim to the Contact page of Royal:

Contact form page of Royal

The Royal group uses another page to share their claims:

Royal's page that they share their claims and links of their exfiltrated files

Security researchers observed that the group first used BlackCat's encryptors and Zeon's ransom notes. These notes changed to Royal's ransom notes in September 2022.

Zeon ransom note (Source: BleepingComputer)

Additionally, the ransom note used by Royal ransomware was similar to that used by Conti –observed as Zeon after Conti stopped operating- and the code used to decrypt files was also used by Conti.

CSA Update from CISA and FBI: Royal Ransomware's Possible Rebranding to 'Blacksuit'

CISA and the FBI have issued an update for the joint Cybersecurity Advisory (CSA) on Royal Ransomware as part of the #StopRansomware initiative. Emphasizing the widespread impact across critical infrastructure sectors, including manufacturing, communications, healthcare and public healthcare (HPH), and education, CISA has revised the CSA to enhance guidance for organizations.

The update reveals that Royal Ransomware has targeted over 350 known victims globally since September 2022, with ransom demands surpassing $275 million.

Moreover, and most importantly, there are indications that Royal Ransomware may undergo **re-branding** or introduce **a spinoff variant**, **Blacksuit**. The speculation stems from the fact that Blacksuit Ransomware shares several identified coding characteristics similar to Royal Ransomware.

The updated CSA offers additional insights into tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) for both Royal ransomware variants and Blacksuit. FBI investigations identified these TTPs and IOCs as recently as June 2023.

For extensive details, consult the advisory on CISA's website.

Royal Ransomware Malware Analysis

Executive Summary

Threat Identifiers	
Name	Royal Ransomware
Threat Type	Ransomware
Detections	Full List (**VirusTotal**)
Tor Address	• hxxp[:]//royal2xthig3ou5hd7zsliqagy6yygk2cdelaxtni2fyad6dpmpxedid[.]onion • hxxp[:]//royal4ezp7xrbakkus3oofjw6gszrohpodmdnfbe5e4w3og5sm7vb3qd[.]onion
Noticeable Behaviors	Ransomware skips the encryption process for all the files with extensions “dll, bat, royal, exe.“ Those sub-folders and files are not encrypted by the ransomware. “Windows, Royal, Perflogs, Tor browser, Boot, $recycle.bin, Windows.old, $window.~ws, $windows.~bt, Mozilla, Google”
Conclusion	The attacks of this group occur more often, and their pattern should be kept in mind to be safe. The group mainly uses callback phishing to get initial access to its victims. Organizations should provide cybersecurity awareness training for their employees to prevent attacks from callback phishing.

Royal ransomware is a recent threat that appeared in 2022 and was particularly active during recent months. The ransomware deletes all Volume Shadow Copies and avoids specific file extensions and folders. It encrypts the network shares found in the local network and the local drives. A parameter called “-id” that identifies the victim and is also written in the ransom note must be specified in the command line.

The files are encrypted using the AES algorithm (OpenSSL), with the key and IV being encrypted using the RSA public key that is hard-coded in the executable. The malware can fully or partially encrypt a file based on the file’s size and the “-ep” parameter. The extension of the encrypted files are changed to “.royal.”

Ransomware Composition

When run as an administrator, Royal ransomware runs two sub-processes and terminates them after. Terminations could be because the tool used for analysis may be detected by the parent process, or it could terminate itself by detecting the virtual machine environment. This will be answered in the static analysis section.

The findings gathered using Sysmon, Process Monitor and Event Viewer can be seen in the table below:

Process Name	Command Line
vssadmin.exe	delete shadows /all /quiet
conhost.exe	??C:WINDOWSsystem32conhost.exe 0xffffffff -ForceV1
slui.exe	??C:WINDOWSSystem32slui.exe -Embedding

vssadmin.exe

Volume Shadow Copy Service or VSS is a Windows service that allows taking manual or automatic backup copies (snapshots) of computer files or volumes, even when they are in use. It is executed as a Windows service called the Volume Shadow Copy service.

conhost.exe

Microsoft provides the conhost.exe (Console Windows Host) file and is usually legitimate and completely safe. conhost.exe needs to run to allow Command Prompt to work with Windows Explorer. One of its features is that it gives you the ability to drag and drop files/folders straight into Command Prompt.

Static Analysis

Overview

File Name	Royal.exe
File Size	3.013 KB
File Type	Win32.exe
MD5	df0b88dafe7a65295f99e69a67db9e1b

SHA-1	db3163a09eb33ff4370ad162a05f4b2584a20456
SHA-256	f484f919ba6e36ff33e4fb391b8859a94d89c172a465964f99d6113b55ced429

The ransomware was written in C++ and was not packed even with an entropy value of '6.60303', which is thought to be 82% packed malware first. Let's examine the strings and see if we can find anything during the analysis. You can see the entropy value in the screenshot below.

When we searched for HTTP in the strings, we found an output. This onion URL may be the contact address of Royal Ransomware.

The first function call at the program's start is shown in the screenshot below:

Anti-Debugger control is provided with "IsDebuggerPresent" API. If the EAX register takes 1 as a value, the program will close itself, and it is not possible to debug with the analysis tools; that's why it is necessary to change it to 0 to run the program without closing. The anti-Debugger Bypass technique will be done during Dynamic analysis.

The function related to the OpenSSL and RC4 encryption stage is given in the image below:

The ransomware imports a hard-coded RSA public key. The OpenSSL library will be used to encrypt the files using the AES algorithm, with the AES key being encrypted using the RSA public key:

Dynamic Analysis

When executing the Royal ransomware, it takes three arguments. In this section, we will start the dynamic analysis phase by showing what they are and for what they are used.

When we run the program, it performs backup deletion -with child processes using the parameters we specified in the Ransomware Composition section- with vssadmin.exe and conhost.exe.

Conhost.exe must be run to allow Command Prompt to work with Windows Explorer. One of its features is that it will enable you to drag and drop files/folders directly into Command Prompt.

ANY.RUN Process Graph

Behavioral Information	Reads the computer name	Checks supported languages	The process checks LSA protection
royal.exe	x	PID: 1568	x
vssadmin.exe	x	x	PID: 4768
conhost.exe	PID: 4892	PID: 4892	PID: 4892
slui.exe	x	x	PID: 1672

When we examined the network activity, we could not find any interaction with blacklist IP addresses. All requested domain addresses are legal addresses and whitelist IP addresses.

Since it is a 64-bit program, let's run it step by step by marking the relevant parts using x64dbg in the virtual environment.

During the Debugger, when we try to move forward by putting a breakpoint on a few specific APIs, the program closes itself and performs the terminate operation. It is clearly understood that Anti-Analysis techniques, which we see in the Static analysis section, are used.

Command line arguments:

– path: The path to be encrypted.

– ep: The number that represents the percentage of the file that will be encrypted.

– id: A 32-digit array.

Re-examined code part where the parameters are run with Ghidra can be found below:

Anti-Analysis Section

We saw the EAX Register value as 1 for IsDebuggerPresent, an important API that we constantly encounter in malware and will make the analyst's job more difficult. Let's check again with Ghidra and start looking at what we can do for an anti-analysis bypass.

As we will see in the screenshot below, if we directly pass the function call made at the base address "00007FF6FDE0296D", the program performs the terminate operation.

Let's skip the executing process by changing the RIP address before it terminates the process using the function call and continue exploring it.

We've detected another function call that performs another terminate operation "00007FF6FDE029CF".

Let's perform the previous RIP address change at this stage as well.

It repeats the same actions. Now let's start reviewing the parts we skipped. After we got through the Anti-Analysis stages, we continued monitoring the program's operation, as seen in the image below. Once the backups have been deleted, Royal ransomware will set its exclusion paths (the files or directories spared from file encryption). The following file extensions will be excluded from being encrypted:

- .exe, .dll, .bat, .lnk, README.TXT, .royal

Next, the ransomware will set the list of directories excluded from the encryption process. These directories are the ones that contain the following strings:

– Windows, RoyalPreflogs, Tor Browser, Boot $recycle.bin, Windows.old, $windows.~ws, $windows.~bt, Mozilla, Google.

Network Activity

Ransomware will scan the network interfaces and, if possible, retrieve the different IP addresses for the target machine/machines using the "GetIpAddrTable" API call. It will specifically search for IP addresses that start with "192.10.100./ 172."

Royal ransomware will establish a socket using the API WSASocketW and associate it with a completion port using CreateIoCompletionPort. It then will use the API call tones to set the port to SMB and eventually try to connect to the instructed IP addresses via the LPFN_CONNECTEX callback function.

Ransomware will enumerate the shared resources of the given IP addresses using the API called NetShareEnum. If a shared resource is one of "ADMIN$" or "IPC$", the ransomware will not encrypt it.

Encryption

Royal ransomware's encryption is multi-threaded. To choose the number of running threads, the ransomware will use the API call GetNativeSystemInfo to collect the number of processors in a machine. It will then multiply the result by two and create the appropriate number of threads accordingly. Next, the ransomware will set the RSA public key, embedded in the binary in plain text and used for encrypting the AES key.

- **RSA Public Key:** —–BEGIN RSA PUBLIC KEY—– nMIICCAKCAgEAuWfX+pJCUCKc9xsWLVHpCpw6TL20HG/Vk4vF3GYlr6HltX7BMRfAn7oGyMztNb37xW66NX+uxHghrX3+sm23yJmSfr

Regarding partial encryption, Royal ransomware gives the ransomware operator a more flexible solution for evading detection than most ransomware. We assume this flexibility and the evasion potential it enables was a design goal for the creators of Royal ransomware.

Latest Attacks of the Group

Ransomware attacks on the healthcare industry increased by **81.1% in 2022** compared to 2021. Also, Health Sector Cybersecurity Coordination Center (HC3) draws attention to this issue in its latest analysis of Royal Ransomware. Some recent attacks made in the healthcare industry, such as compromising the Northwest Michigan Health Services and Happy Sapiens Dental firms, are made from Royal Ransomware. The group may likely target this sector more often in the future.

Royal's post about the Happy Sapiens Dental

One of the Royal's most significant claims is the compromise of INTRADO, an American telecommunications company with more than **10K** employees. It is unknown which data was stolen, but according to Royal, they exfiltrated internal documents, passports, and driver's licenses of **INTRADO's** employees.

Royal's claim about INTRADO

Countries affected by Royal Ransomware over time, based on our findings from around 70 observations, can be seen below:

Timeline of Royal Ransomware attacks

The SOCRadar dark web team constantly monitors ransomware activities and reports in the SOCRadar Dark Web News panel.

SOCRadar's Dark Web News panel under the Cyber Threat Intelligence module

Conclusion

The attacks of this group occur more often, and their pattern should be kept in mind to be safe. The group mainly uses callback phishing to get initial access to its victims. Organizations should provide cybersecurity awareness training for their employees to prevent attacks from callback phishing.

Employees should:

- Be cautious of unsolicited calls, texts, or emails, especially if it asks to provide personal information or login credentials.
- Be cautious when providing personal information online.
- Do not click links or download attachments from unknown sources.
- Use strong passwords and assist it using 2FA or MFA solutions.
- Keep their systems up to date, which will help protect the devices from vulnerabilities that could be exploited.

Organizations -especially those operating in the Manufacturing and Healthcare sectors- should:

- Regularly update and patch software and systems.
- Regularly back up important data and test the backups.
- Use network segmentation and access controls to limit attackers' movement within the network.
- Deploy and regularly update security software. (e.g., firewalls and antivirus)

These measures can help reduce the risk of Royal Ransomware, but no security measures are foolproof. It is vital to have a response plan in place in case of an attack.

Appendixes

Appendix 1.

Royal Ransomware (used sample's information)

- **MD5:**df0b88dafe7a65295f99e69a67db9e1b
- **SHA-1:**db3163a09eb33ff4370ad162a05f4b2584a20456
- **SHA-256: f484f919ba6e36ff33e4fb391b8859a94d89c172a465964f99d6113b55ced429**
- **File Type:**Win32 EXE

IOCs of Royal Ransomware:

- 104.86.182.8:443 (TCP)
- 20.99.133.109:443 (TCP)
- 20.99.184.37:443 (TCP)
- 23.216.147.64:443 (TCP)
- 23.216.147.76:443 (TCP)
- a83f:8110:0:0:64ca:1f00:0:0:53 (UDP)
- a83f:8110:1749:73ff:1749:73ff:1a4b:73ff:53 (UDP)
- a83f:8110:8401:0:2075:2cc:8401:0:53 (UDP)
- hxxp[:]//royal2xthig3ou5hd7zsliqagy6yygk2cdelaxtni2fyad6dpmpxedid[.]onion/%s
- README.txt

Appendix 2.

MITRE ATT&CK Techniques

Techniques	Name
T1059	Command and Scripting Interpreter
T1106	Native API
T1559.001	Inter-Process Communication: Component Object Model
T1129	Shared Modules
T1055	Process Injection
T1134	Access Token Manipulation
T1134.001	Access Token Manipulation: Token Impersonation/Theft
T1070.004	Indicator Removal: File Deletion
T1622	Debugger Evasion

T1027	Obfuscated Files or Information
T1140	Deobfuscate/Decode Files or Information
T1082	System Information Discovery
T1622	Debugger Evasion
T1057	Process Discovery
T1083	File and Directory Discovery
T1135	Network Share Discovery
T1518	Software Discovery
T1560	Archive Collected Data
T1090	Proxy
