Dark Web Profile: Royal Ransomware

socradar.io/dark-web-profile-royal-ransomware/

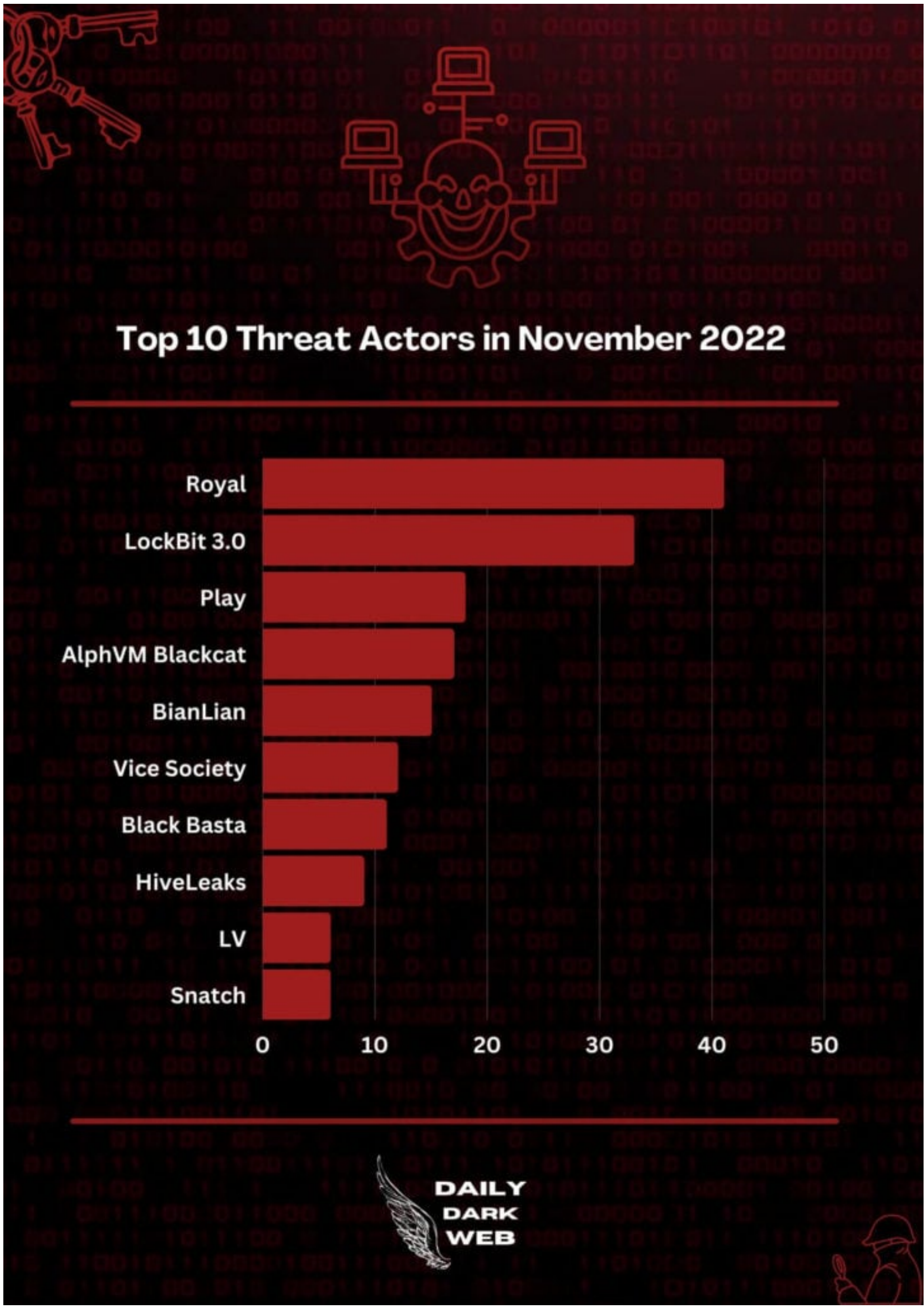
January 9, 2023

By SOCRadar Research

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.

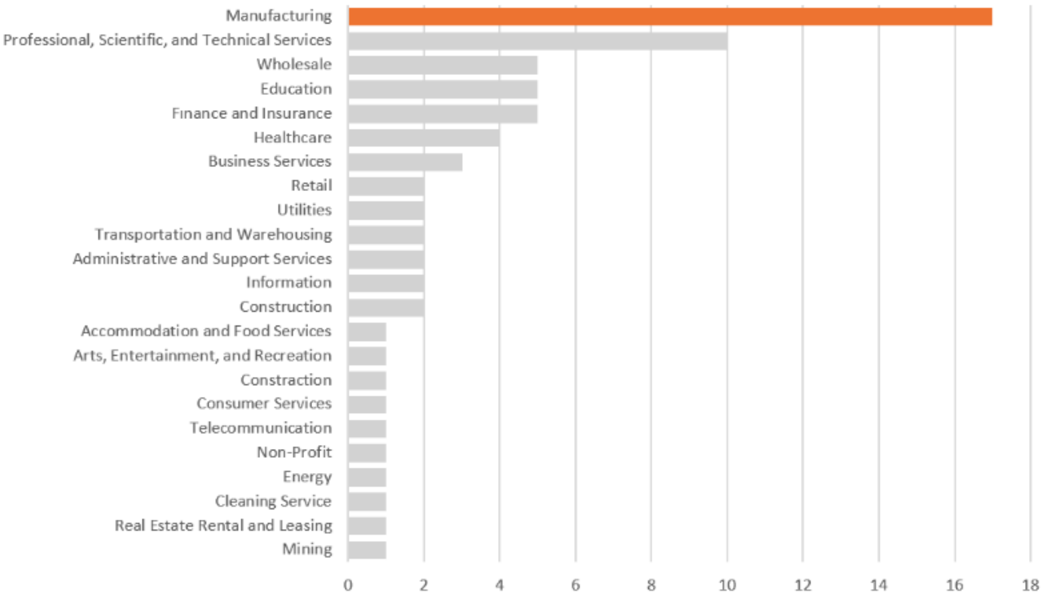


Daily Dark Web's infographic of Ransomware activities in November 2022 (Source: Daily Dark Web)

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.

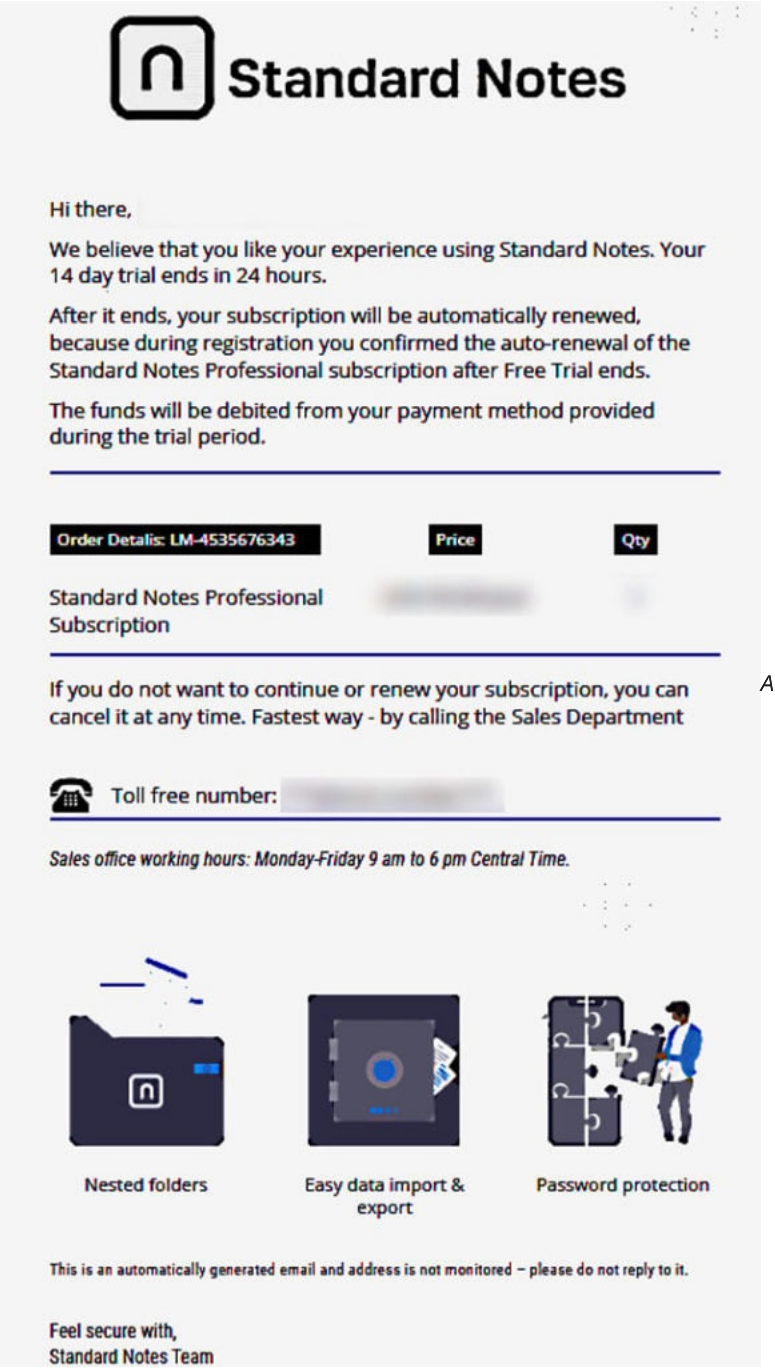
According to SOCRadar's dark web team's findings, Royal Ransomware primarily targets the manufacturing industry. It could be because of the **broad attack surface** area, such as various specialized equipment and managed software used in the field. Plus, the limited IT and security workforce may have 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.



Standard Notes

Hi there,

We believe that you like your experience using Standard Notes. Your 14 day trial ends in 24 hours.

After it ends, your subscription will be automatically renewed, because during registration you confirmed the auto-renewal of the Standard Notes Professional subscription after Free Trial ends.

The funds will be debited from your payment method provided during the trial period.

Order Details: LM-4535676343	Price	Qty
Standard Notes Professional Subscription	[redacted]	[redacted]

If you do not want to continue or renew your subscription, you can cancel it at any time. Fastest way - by calling the Sales Department

☎ Toll free number: [redacted]

Sales office working hours: Monday-Friday 9 am to 6 pm Central Time.

Nested folders

Easy data import & export

Password protection

This is an automatically generated email and address is not monitored – please do not reply to it.

Feel secure with,
Standard Notes Team

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.

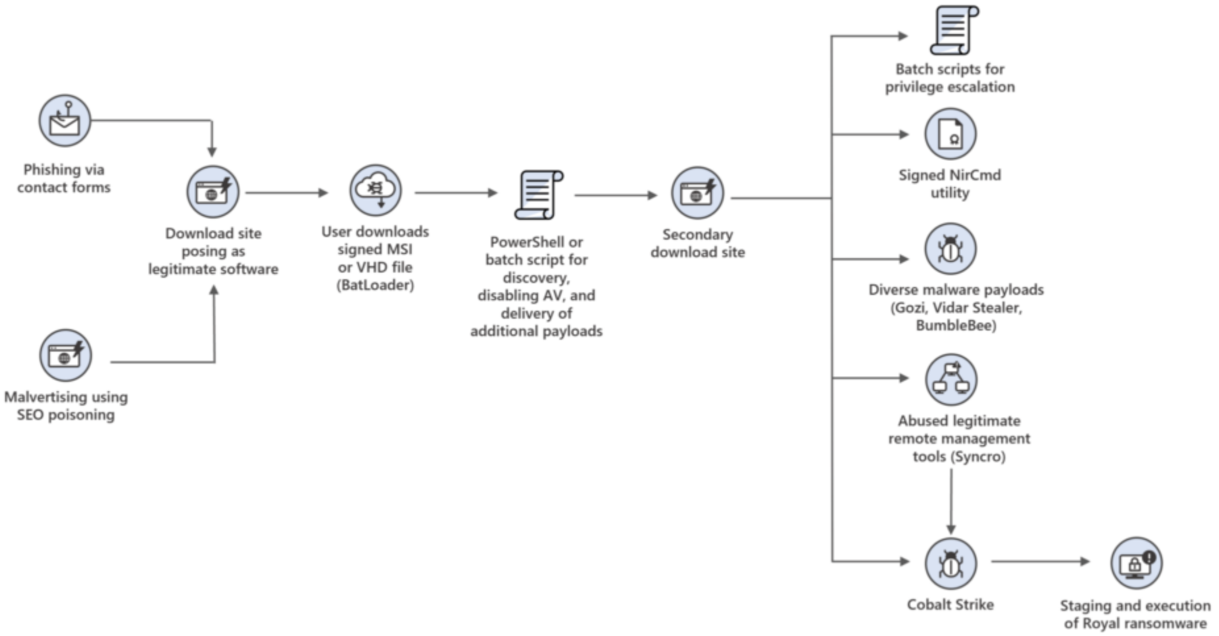

Phishing via contact forms
Malvertising using SEO poisoning
Download site posing as legitimate software
User downloads signed MSI or VHD file (BatLoader)
PowerShell or batch script for discovery, disabling AV, and delivery of additional payloads
Secondary download site
Batch scripts for privilege escalation
Signed NirCmd utility
Diverse malware payloads (Gozi, Vidar Stealer, BumbleBee)
Abused legitimate remote management tools (Syncro)
Cobalt Strike
Staging and execution of Royal ransomware

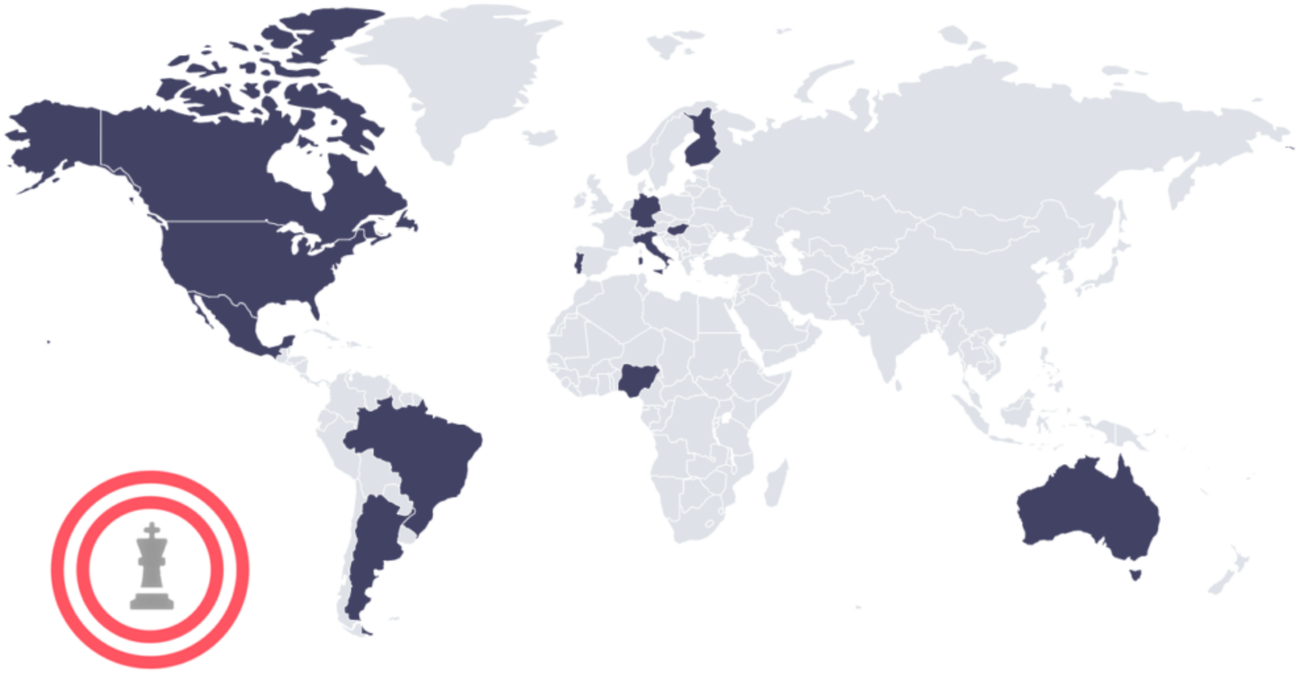
Diagram of DEV-0569's attack chain, which is a threat actor that uses Royal Ransomware actively (Source: Microsoft)

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.

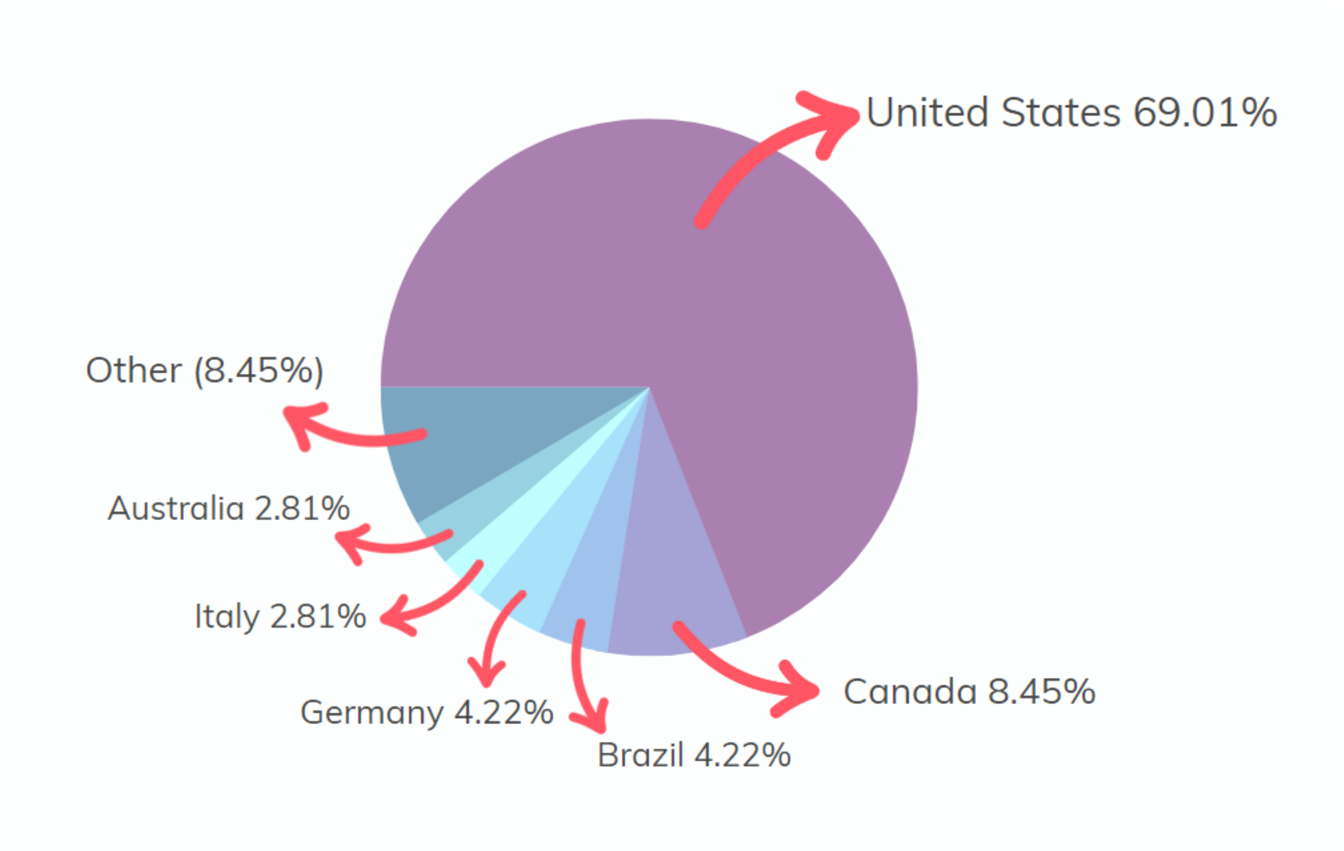
Which Countries Did Royal Ransomware Target?

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.



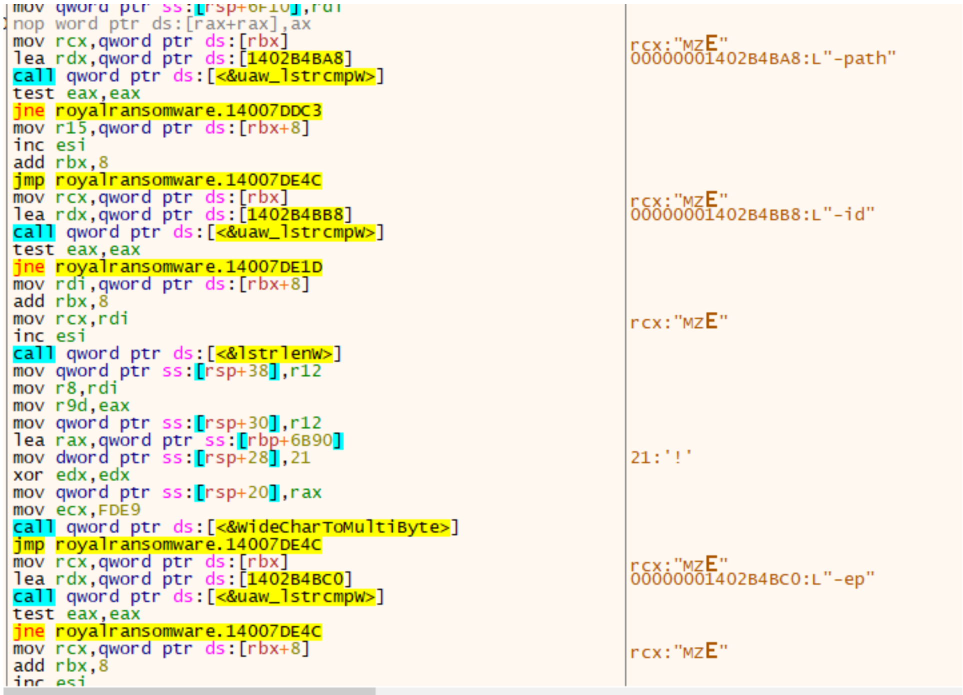
Royal Ransomware's percentage distribution of target countries from its latest attacks

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."**

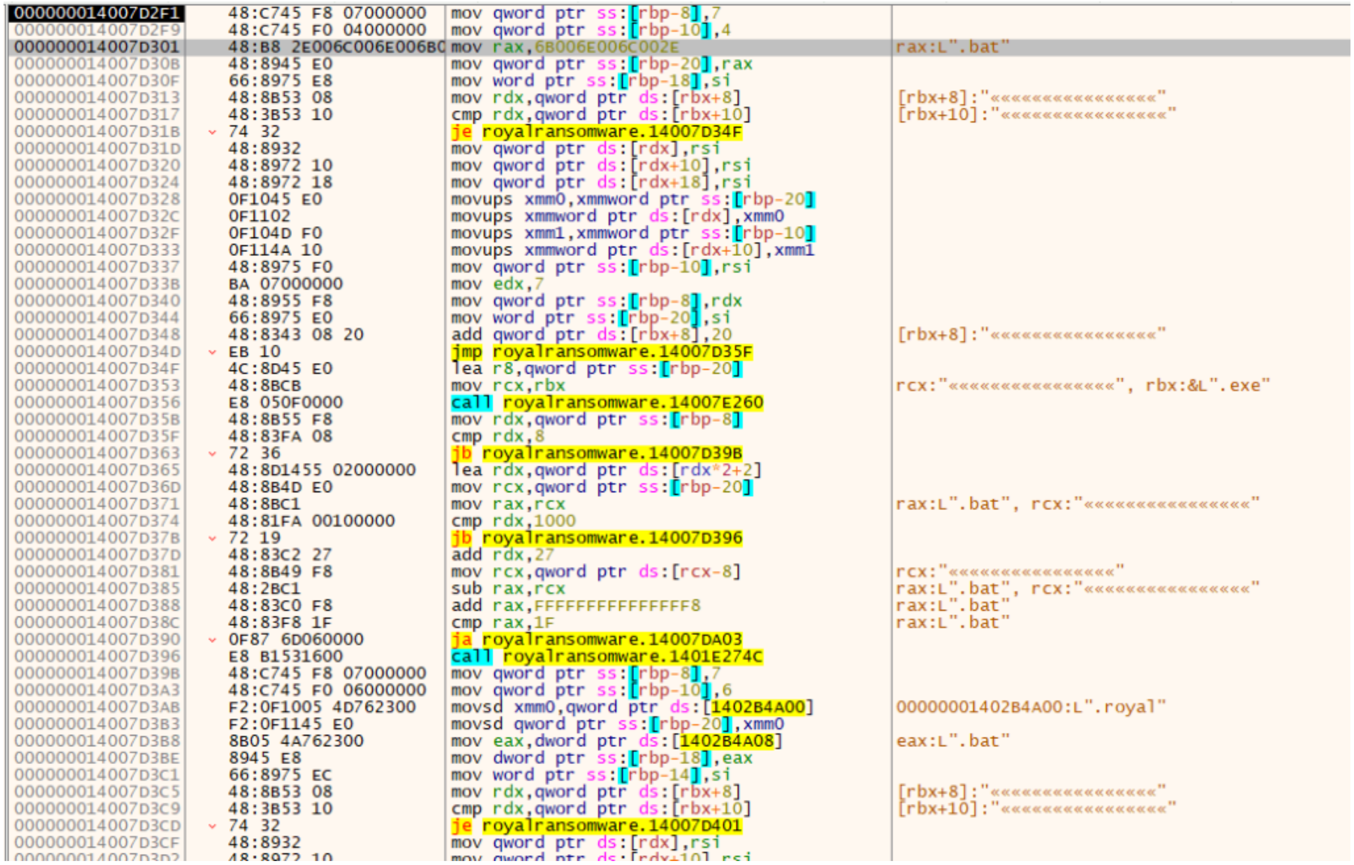
The"-id" parameter could be for the **victim ID**, "-path" could be for the **directory path**, and the "-ep" parameter, as we observed, refers to the **encryption percentage** of the file.



```
mov qword ptr ss:[rsp+6F10],rdi
nop word ptr ds:[rax+rax],ax
mov rcx,qword ptr ds:[rbx]                          rcx:"MZE"
lea rdx,qword ptr ds:[1402B4BA8]                    00000001402B4BA8:L"-path"
call qword ptr ds:[<&uaw_lstrcmpW>]
test eax,eax
jne royalransomware.14007DDC3
mov r15,qword ptr ds:[rbx+8]
inc esi
add rbx,8
jmp royalransomware.14007DE4C
mov rcx,qword ptr ds:[rbx]                          rcx:"MZE"
lea rdx,qword ptr ds:[1402B4BB8]                    00000001402B4BB8:L"-id"
call qword ptr ds:[<&uaw_lstrcmpW>]
test eax,eax
jne royalransomware.14007DE1D
mov rdi,qword ptr ds:[rbx+8]
add rbx,8
mov rcx,rdi                                         rcx:"MZE"
inc esi
call qword ptr ds:[<&lstrlenW>]
mov qword ptr ss:[rsp+38],r12
mov r8,rdi
mov r9d,eax
mov qword ptr ss:[rsp+30],r12
lea rax,qword ptr ss:[rbp+6B90]
mov dword ptr ss:[rsp+28],21                        21:'!'
xor edx,edx
mov qword ptr ss:[rsp+20],rax
mov ecx,FDE9
call qword ptr ds:[<&WideCharToMultiByte>]
jmp royalransomware.14007DE4C
mov rcx,qword ptr ds:[rbx]                          rcx:"MZE"
lea rdx,qword ptr ds:[1402B4BC0]                    00000001402B4BC0:L"-ep"
call qword ptr ds:[<&uaw_lstrcmpW>]
test eax,eax
jne royalransomware.14007DE4C
mov rcx,qword ptr ds:[rbx+8]                        rcx:"MZE"
add rbx,8
inc esi
```

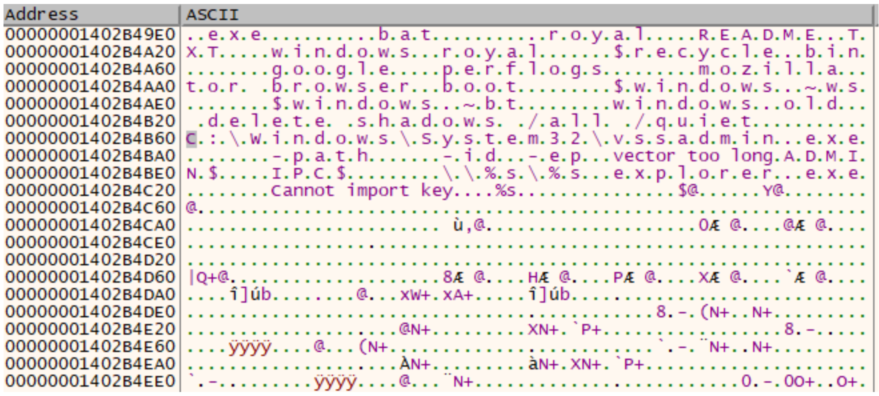
“-path”, “-id”, and “-ep” parameters used in Royal Ransomware

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



```
000000014007D2F1   48:C745 F8 07000000   mov qword ptr ss:[rbp-8],7
000000014007D2F9   48:C745 F0 04000000   mov qword ptr ss:[rbp-10],4
000000014007D301   48:B8 2E006C006E006BC mov rax,6B006E006C002E          rax:L".bat"
000000014007D30B   48:8945 E0            mov qword ptr ss:[rbp-20],rax
000000014007D30F   66:8975 E8            mov word ptr ss:[rbp-18],si
000000014007D313   48:8B53 08            mov rdx,qword ptr ds:[rbx+8]    [rbx+8]:"««««««««««««««««"
000000014007D317   48:3B53 10            cmp rdx,qword ptr ds:[rbx+10]   [rbx+10]:"««««««««««««««««"
000000014007D31B   74 32                 je royalransomware.14007D34F
000000014007D31D   48:8932               mov qword ptr ds:[rdx],rsi
000000014007D320   48:8972 10            mov qword ptr ds:[rdx+10],rsi
000000014007D324   48:8972 18            mov qword ptr ds:[rdx+18],rsi
000000014007D328   0F1045 E0             movups xmm0,xmmword ptr ss:[rbp-20]
000000014007D32C   0F1102                movups xmmword ptr ds:[rdx],xmm0
000000014007D32F   0F104D F0             movups xmm1,xmmword ptr ss:[rbp-10]
000000014007D333   0F114A 10             movups xmmword ptr ds:[rdx+10],xmm1
000000014007D337   48:8975 F0            mov qword ptr ss:[rbp-10],rsi
000000014007D33B   BA 07000000           mov edx,7
000000014007D340   48:8955 F8            mov qword ptr ss:[rbp-8],rdx
000000014007D344   66:8975 E0            mov word ptr ss:[rbp-20],si
000000014007D348   48:8343 08 20         add qword ptr ds:[rbx+8],20     [rbx+8]:"««««««««««««««««"
000000014007D34D   EB 10                 jmp royalransomware.14007D35F
000000014007D34F   4C:8D45 E0            lea r8,qword ptr ss:[rbp-20]
000000014007D353   48:8BCB               mov rcx,rbx                     rcx:"««««««««««««««««", rbx:&L".exe"
000000014007D356   E8 050F0000           call royalransomware.14007E260
000000014007D35B   48:8B55 F8            mov rdx,qword ptr ss:[rbp-8]
000000014007D35F   48:83FA 08            cmp rdx,8
000000014007D363   72 36                 jb royalransomware.14007D39B
000000014007D365   48:8D1455 02000000    lea rdx,qword ptr ds:[rdx*2+2]
000000014007D36D   48:8B4D E0            mov rcx,qword ptr ss:[rbp-20]
000000014007D371   48:8BC1               mov rax,rcx                     rax:L".bat", rcx:"««««««««««««««««"
000000014007D374   48:81FA 00100000      cmp rdx,1000
000000014007D37B   72 19                 jb royalransomware.14007D396
000000014007D37D   48:83C2 27            add rdx,27
000000014007D381   48:8B49 F8            mov rcx,qword ptr ds:[rcx-8]    rcx:"««««««««««««««««"
000000014007D385   48:2BC1               sub rax,rcx                     rax:L".bat", rcx:"««««««««««««««««"
000000014007D388   48:83C0 F8            add rax,FFFFFFFFFFFFFFF8        rax:L".bat"
000000014007D38C   48:83F8 1F            cmp rax,1F                      rax:L".bat"
000000014007D390   0F87 6D060000         ja royalransomware.14007DA03
000000014007D396   E8 B1531600           call royalransomware.1401E274C
000000014007D39B   48:C745 F8 07000000   mov qword ptr ss:[rbp-8],7
000000014007D3A3   48:C745 F0 06000000   mov qword ptr ss:[rbp-10],6
000000014007D3AB   F2:0F1005 4D762300    movsd xmm0,qword ptr ds:[1402B4A00]   00000001402B4A00:L".royal"
000000014007D3B3   F2:0F1145 E0          movsd qword ptr ss:[rbp-20],xmm0
000000014007D3B8   8B05 4A762300         mov eax,dword ptr ds:[1402B4A08]      eax:L".bat"
000000014007D3BE   8945 E8               mov dword ptr ss:[rbp-18],eax
000000014007D3C1   66:8975 EC            mov word ptr ss:[rbp-14],si
000000014007D3C5   48:8B53 08            mov rdx,qword ptr ds:[rbx+8]    [rbx+8]:"««««««««««««««««"
000000014007D3C9   48:3B53 10            cmp rdx,qword ptr ds:[rbx+10]   [rbx+10]:"««««««««««««««««"
000000014007D3CD   74 32                 je royalransomware.14007D401
000000014007D3CF   48:8932               mov qword ptr ds:[rdx],rsi
000000014007D3D2   48:8972 10            mov qword ptr ds:[rdx+10],rsi
```

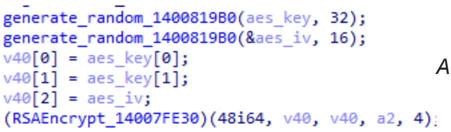
Skipping files with extensions dll, bat, exe, and royal.



```
Address           ASCII
00000001402B49E0  ..e.x.e...........b.a.t...........r.o.y.a.l.....R.E.A.D.M.E...T.
00000001402B4A20  X.T.....w.i.n.d.o.w.s...r.o.y.a.l.......$.r.e.c.y.c.l.e...b.i.n.
00000001402B4A60  ........g.o.o.g.l.e.....p.e.r.f.l.o.g.s.........m.o.z.i.l.l.a...
00000001402B4AA0  t.o.r. .b.r.o.w.s.e.r...b.o.o.t.........$.w.i.n.d.o.w.s...~.w.s.
00000001402B4AE0  ........$.w.i.n.d.o.w.s...~.b.t.........w.i.n.d.o.w.s...o.l.d...
00000001402B4B20   .d.e.l.e.t.e. .s.h.a.d.o.w.s. ./.a.l.l. ./.q.u.i.e.t..........
00000001402B4B60  C.:.\.w.i.n.d.o.w.s.\.S.y.s.t.e.m.3.2.\.v.s.s.a.d.m.i.n...e.x.e.
00000001402B4BA0  ........-.p.a.t.h.......-.i.d...-.e.p...vector too long.A.D.M.I.
00000001402B4BE0  N.$.....I.P.C.$.........\.\.%.s.\.%.s...e.x.p.l.o.r.e.r...e.x.e.
00000001402B4C20  ........Cannot import key....%s...............$@......Y@........
00000001402B4C60  @...............................................................
00000001402B4CA0  ........................ù,@.....................OÆ @....@Æ @....
00000001402B4CE0  ................................................................
00000001402B4D20  ................................................................
00000001402B4D60  |Q+@....................8Æ @....HÆ @....PÆ @....XÆ @....`Æ @....
00000001402B4DA0  ....î]úb........@...xW+.xA+.....î]úb............................
00000001402B4DE0  ..........................................8.-.(N+..N+..........
00000001402B4E20  ........................@N+.........XN+.`P+...............8.-....
00000001402B4E60  ....ÿÿÿÿ....@...(N+........................`.-.¨N+..N+..........
00000001402B4EA0  ........................ÀN+.........àN+.XN+.`P+.................
00000001402B4EE0  `.-.........ÿÿÿÿ....@...¨N+....................0.-.00+..0+.
```

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

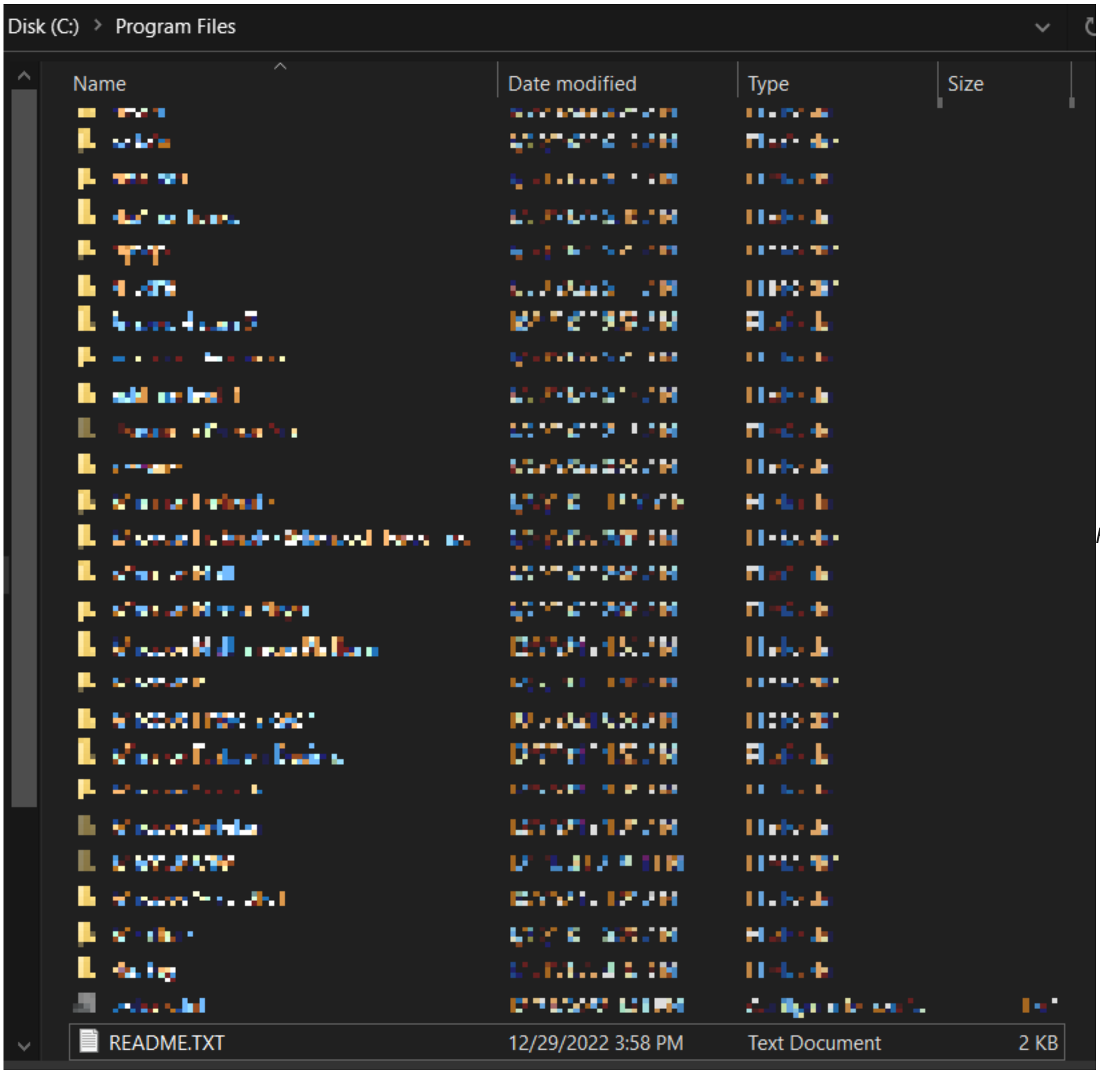
The program encrypts files using AES and IV and changes the extension of files with ".royal."



```
generate_random_1400819B0(aes_key, 32);
generate_random_1400819B0(&aes_iv, 16);
v40[0] = aes_key[0];
v40[1] = aes_key[1];
v40[2] = aes_iv;
(RSAEncrypt_14007FE30)(48i64, v40, v40, a2, 4);
```

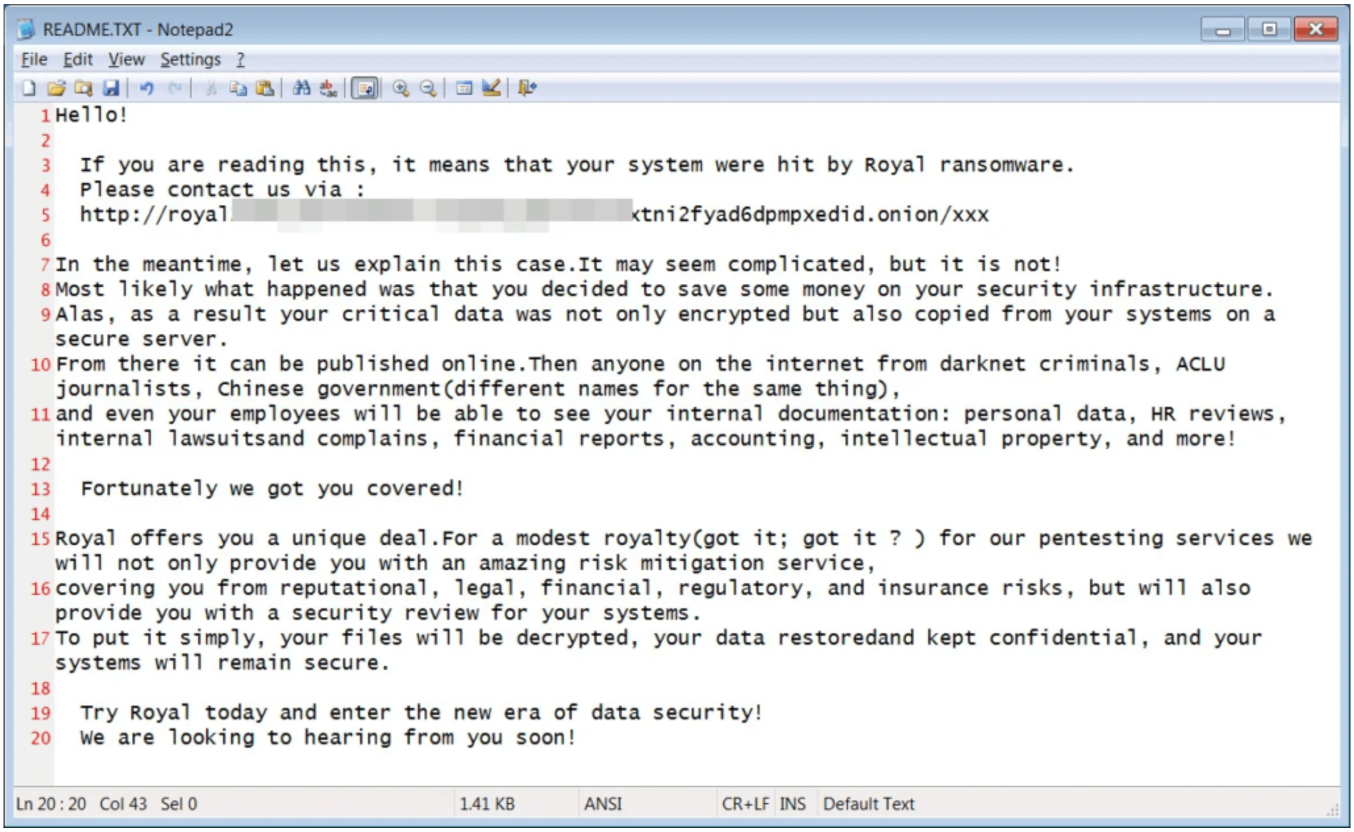
AES and IV key generation processes (Source: TrendMicro)

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



Name	Date modified	Type	Size
README.TXT	12/29/2022 3:58 PM	Text Document	2 KB

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



Hello!

 If you are reading this, it means that your system were hit by Royal ransomware.
 Please contact us via :
 http://royal[redacted]xtni2fyad6dpmpxedid.onion/xxx

In the meantime, let us explain this case.It may seem complicated, but it is not!
Most likely what happened was that you decided to save some money on your security infrastructure.
Alas, as a result your critical data was not only encrypted but also copied from your systems on a secure server.
From there it can be published online.Then anyone on the internet from darknet criminals, ACLU journalists, Chinese government(different names for the same thing),
and even your employees will be able to see your internal documentation: personal data, HR reviews, internal lawsuitsand complains, financial reports, accounting, intellectual property, and more!

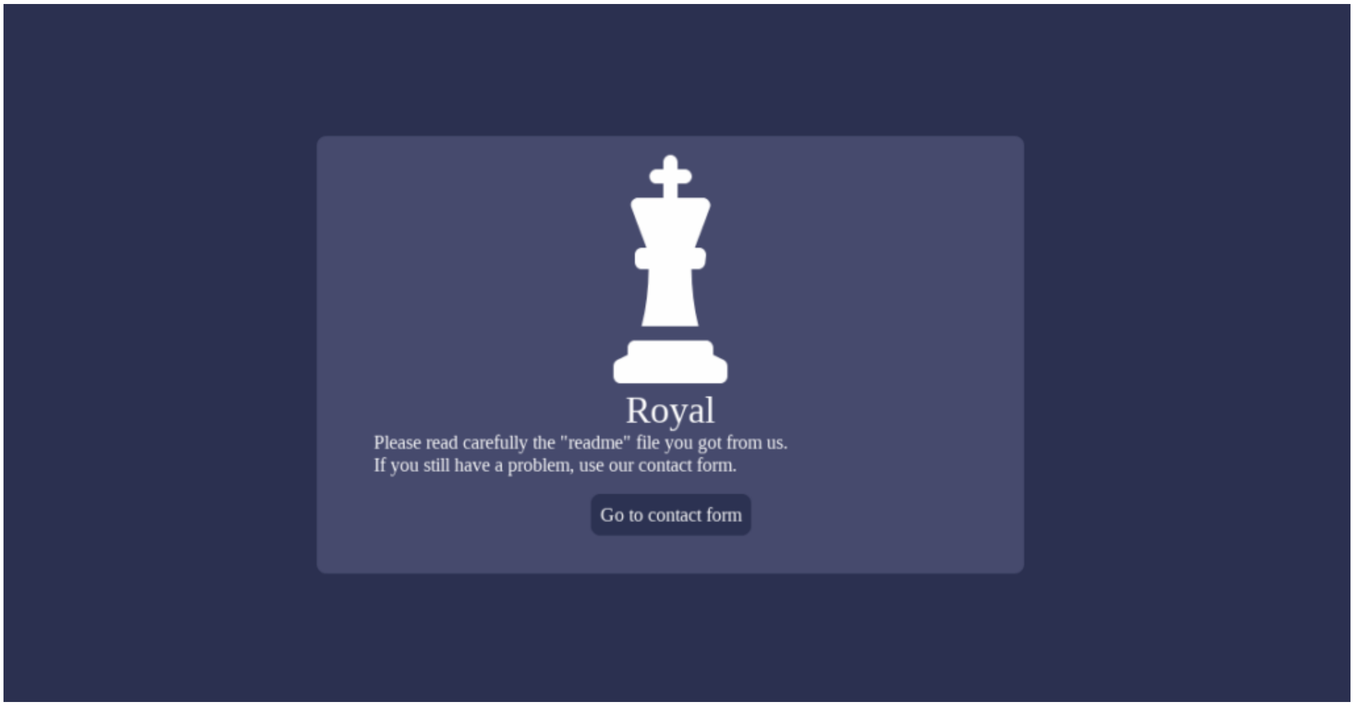
 Fortunately we got you covered!

Royal offers you a unique deal.For a modest royalty(got it; got it ?) for our pentesting services we will not only provide you with an amazing risk mitigation service,
covering you from reputational, legal, financial, regulatory, and insurance risks, but will also provide you with a security review for your systems.
To put it simply, your files will be decrypted, your data restoredand kept confidential, and your systems will remain secure.

 Try Royal today and enter the new era of data security!
 We are looking to hearing from you soon!

Royal's Ransom note (Source: BleepingComputer)

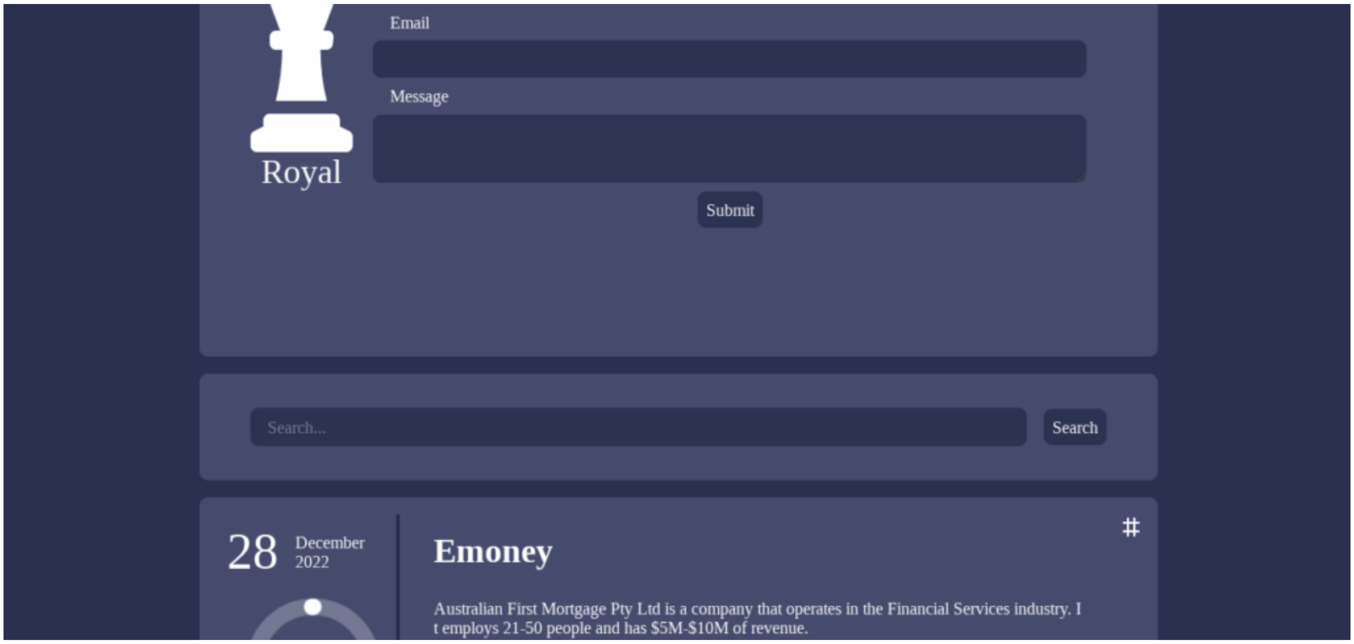
The URL link in the ransom note directs the victim to the Contact page of Royal:


Royal

Please read carefully the "readme" file you got from us.
If you still have a problem, use our contact form.

Contact form page of Royal

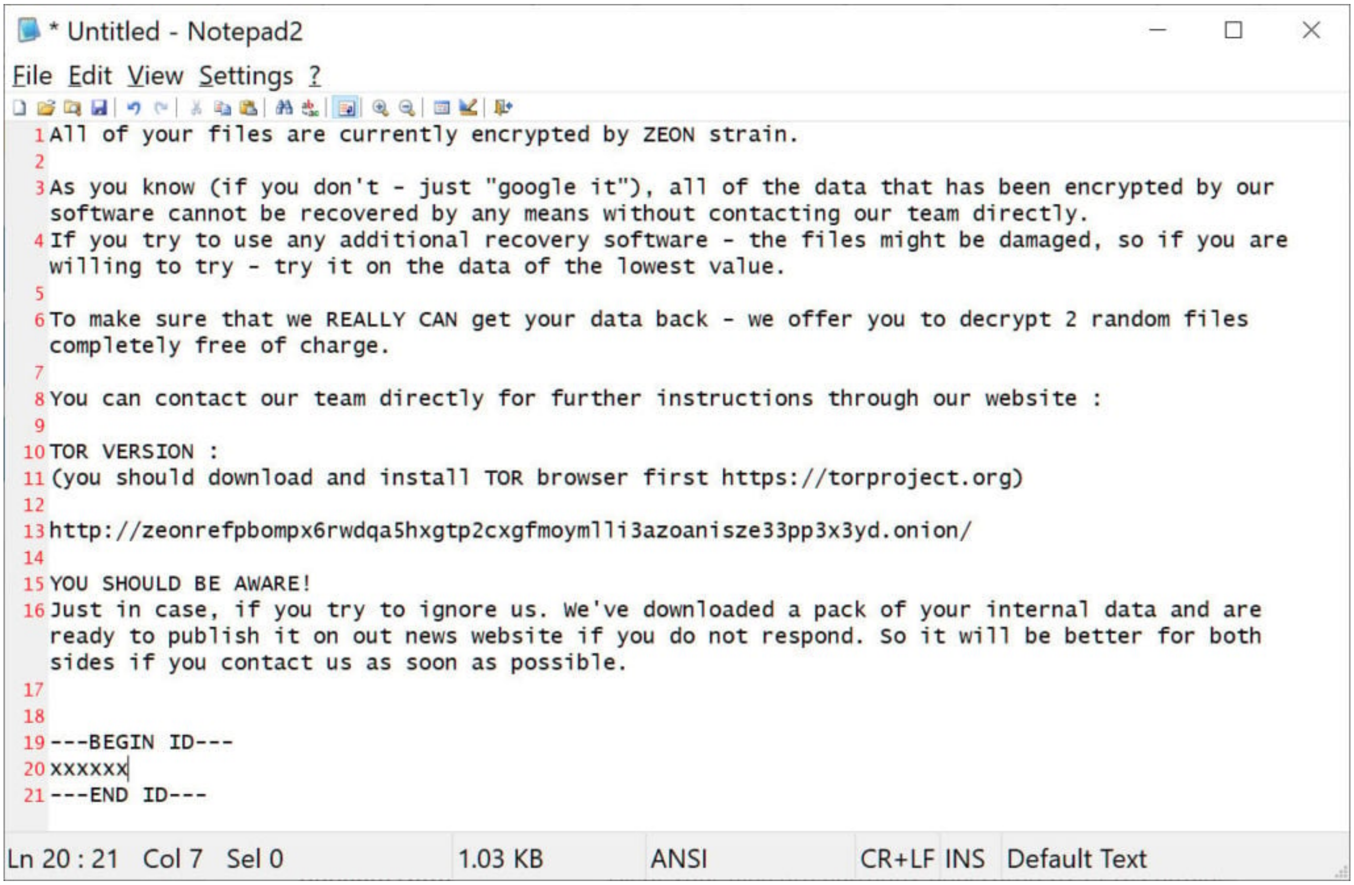
The Royal group uses another page to share their claims:



Australian First Mortgage Pty Ltd is a company that operates in the Financial Services industry. I t employs 21-50 people and has $5M-$10M of revenue.

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.



```
All of your files are currently encrypted by ZEON strain.

As you know (if you don't - just "google it"), all of the data that has been encrypted by our software cannot be recovered by any means without contacting our team directly.
If you try to use any additional recovery software - the files might be damaged, so if you are willing to try - try it on the data of the lowest value.

To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://zeonrefpbompx6rwdqa5hxgtp2cxgfmoymlli3azoanisze33pp3x3yd.onion/

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are ready to publish it on out news website if you do not respond. So it will be better for both sides if you contact us as soon as possible.


---BEGIN ID---
xxxxxx
---END ID---
```

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.

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:

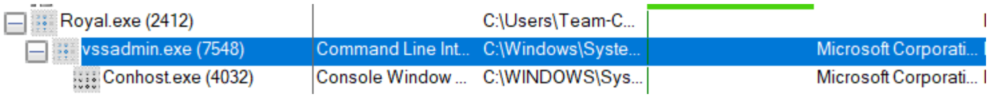
Process Name	Command Line
vssadmin.exe	delete shadows /all /quiet
conhost.exe	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1
slui.exe	\??\C:\WINDOWS\System32\slui.exe -Embedding

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.



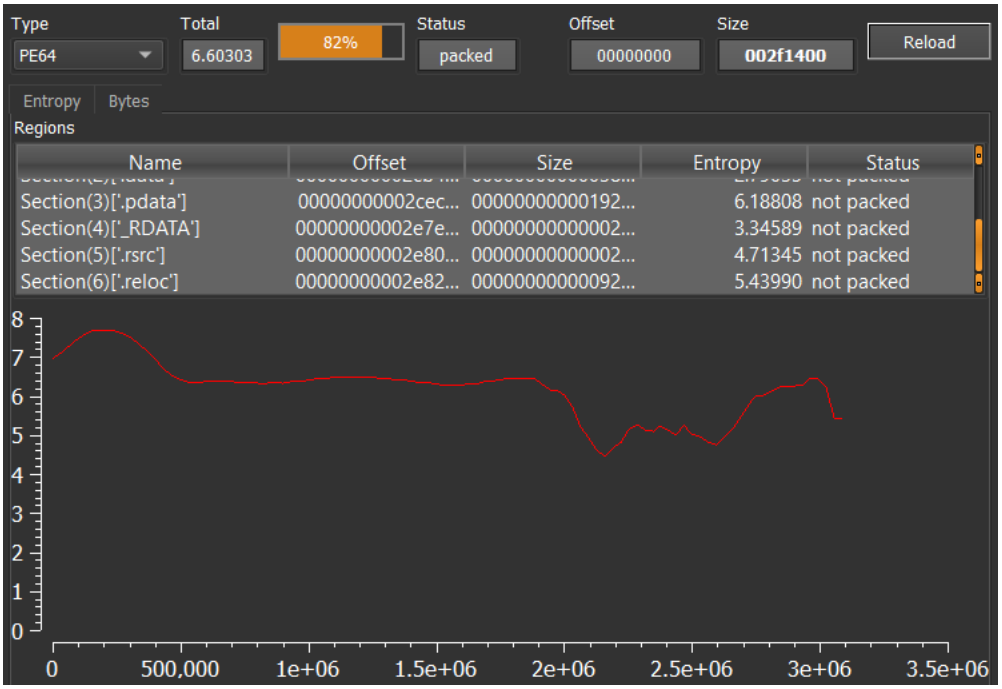
Royal.exe (2412)		C:\Users\Team-C...	
vssadmin.exe (7548)	Command Line Int...	C:\Windows\Syste...	Microsoft Corporati...
Conhost.exe (4032)	Console Window ...	C:\WINDOWS\Sys...	Microsoft Corporati...

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.

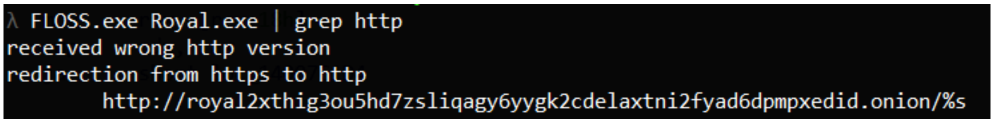


Type: PE64 | Total: 6.60303 | 82% | Status: packed | Offset: 00000000 | Size: 002f1400

Regions

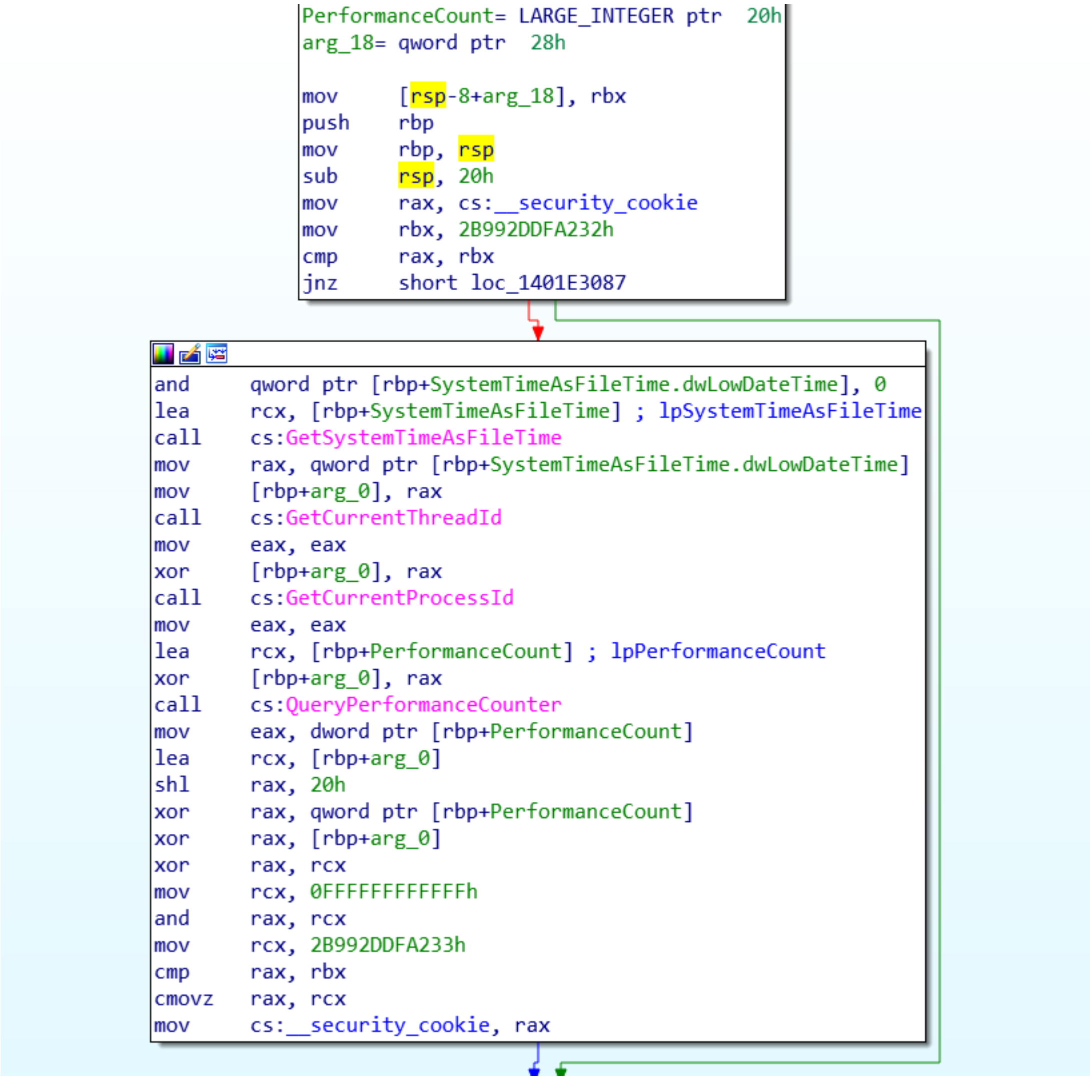
Name	Offset	Size	Entropy	Status
Section(3)['.pdata']	00000000002cec...	00000000000192...	6.18808	not packed
Section(4)['_RDATA']	00000000002e7e...	00000000000002...	3.34589	not packed
Section(5)['.rsrc']	00000000002e80...	00000000000002...	4.71345	not packed
Section(6)['.reloc']	00000000002e82...	00000000000092...	5.43990	not packed

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



```
λ FLOSS.exe Royal.exe | grep http
received wrong http version
redirection from https to http
        http://royal2xthig3ou5hd7zsliqagy6yygk2cdelaxtni2fyad6dpmpxedid.onion/%s
```

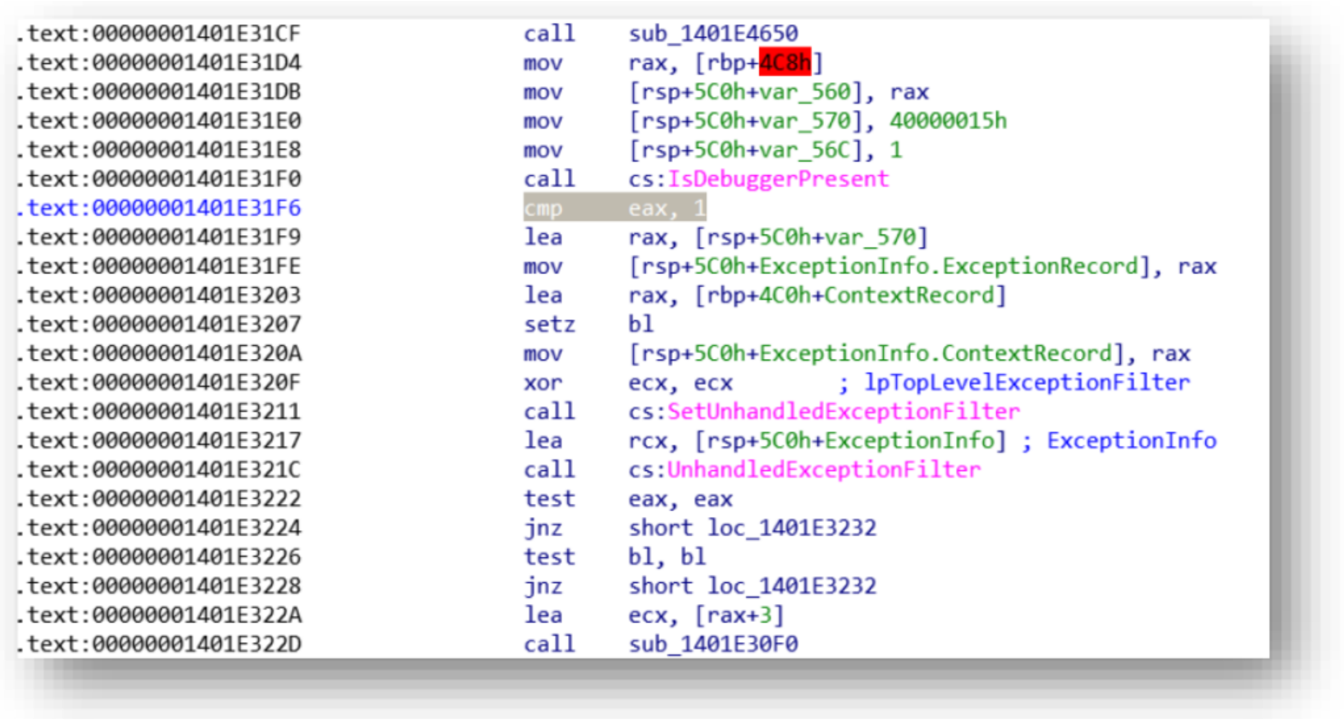
The first function call at the program's start is shown in the screenshot below:



```
PerformanceCount= LARGE_INTEGER ptr  20h
arg_18= qword ptr  28h

mov     [rsp-8+arg_18], rbx
push    rbp
mov     rbp, rsp
sub     rsp, 20h
mov     rax, cs:__security_cookie
mov     rbx, 2B992DDFA232h
cmp     rax, rbx
jnz     short loc_1401E3087
```

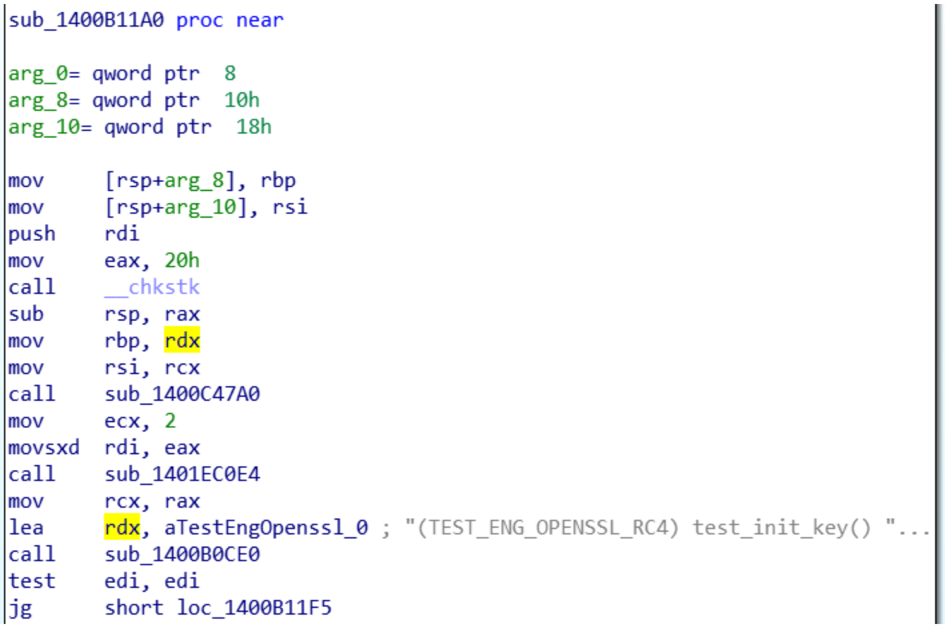
```
and     qword ptr [rbp+SystemTimeAsFileTime.dwLowDateTime], 0
lea     rcx, [rbp+SystemTimeAsFileTime] ; lpSystemTimeAsFileTime
call    cs:GetSystemTimeAsFileTime
mov     rax, qword ptr [rbp+SystemTimeAsFileTime.dwLowDateTime]
mov     [rbp+arg_0], rax
call    cs:GetCurrentThreadId
mov     eax, eax
xor     [rbp+arg_0], rax
call    cs:GetCurrentProcessId
mov     eax, eax
lea     rcx, [rbp+PerformanceCount] ; lpPerformanceCount
xor     [rbp+arg_0], rax
call    cs:QueryPerformanceCounter
mov     eax, dword ptr [rbp+PerformanceCount]
lea     rcx, [rbp+arg_0]
shl     rax, 20h
xor     rax, qword ptr [rbp+PerformanceCount]
xor     rax, [rbp+arg_0]
xor     rax, rcx
mov     rcx, 0FFFFFFFFFFFFh
and     rax, rcx
mov     rcx, 2B992DDFA233h
cmp     rax, rbx
cmovz   rax, rcx
mov     cs:__security_cookie, rax
```

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.



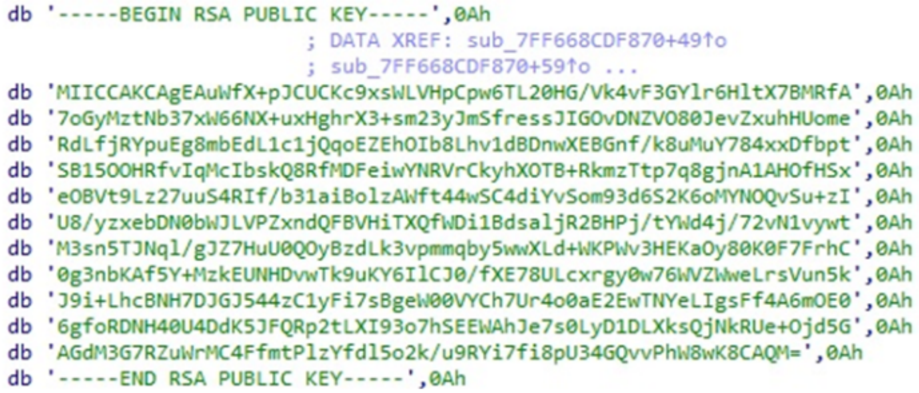
```
.text:00000001401E31CF                 call    sub_1401E4650
.text:00000001401E31D4                 mov     rax, [rbp+4C8h]
.text:00000001401E31DB                 mov     [rsp+5C0h+var_560], rax
.text:00000001401E31E0                 mov     [rsp+5C0h+var_570], 40000015h
.text:00000001401E31E8                 mov     [rsp+5C0h+var_56C], 1
.text:00000001401E31F0                 call    cs:IsDebuggerPresent
.text:00000001401E31F6                 cmp     eax, 1
.text:00000001401E31F9                 lea     rax, [rsp+5C0h+var_570]
.text:00000001401E31FE                 mov     [rsp+5C0h+ExceptionInfo.ExceptionRecord], rax
.text:00000001401E3203                 lea     rax, [rbp+4C0h+ContextRecord]
.text:00000001401E3207                 setz    bl
.text:00000001401E320A                 mov     [rsp+5C0h+ExceptionInfo.ContextRecord], rax
.text:00000001401E320F                 xor     ecx, ecx        ; lpTopLevelExceptionFilter
.text:00000001401E3211                 call    cs:SetUnhandledExceptionFilter
.text:00000001401E3217                 lea     rcx, [rsp+5C0h+ExceptionInfo] ; ExceptionInfo
.text:00000001401E321C                 call    cs:UnhandledExceptionFilter
.text:00000001401E3222                 test    eax, eax
.text:00000001401E3224                 jnz     short loc_1401E3232
.text:00000001401E3226                 test    bl, bl
.text:00000001401E3228                 jnz     short loc_1401E3232
.text:00000001401E322A                 lea     ecx, [rax+3]
.text:00000001401E322D                 call    sub_1401E30F0
```

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

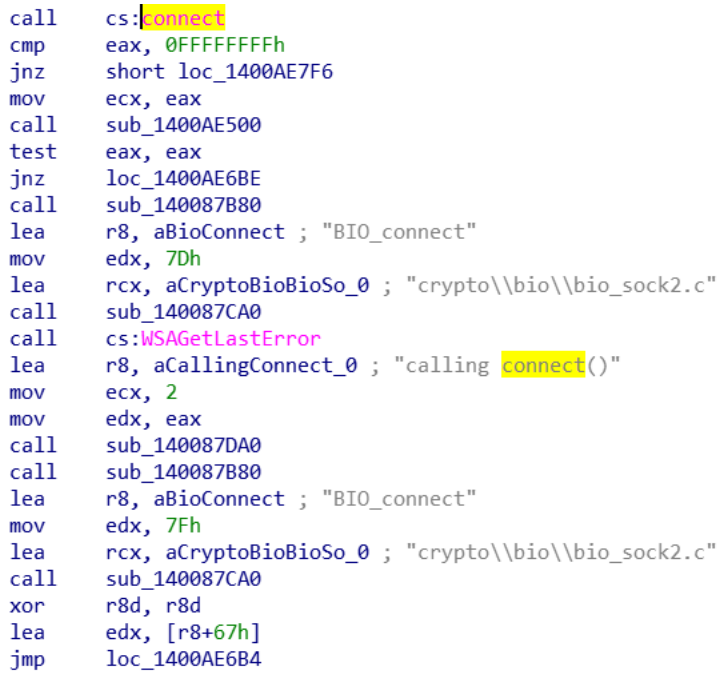


```
sub_1400B11A0 proc near

arg_0= qword ptr  8
arg_8= qword ptr  10h
arg_10= qword ptr  18h

mov     [rsp+arg_8], rbp
mov     [rsp+arg_10], rsi
push    rdi
mov     eax, 20h
call    __chkstk
sub     rsp, rax
mov     rbp, rdx
mov     rsi, rcx
call    sub_1400C47A0
mov     ecx, 2
movsxd  rdi, eax
call    sub_1401EC0E4
mov     rcx, rax
lea     rdx, aTestEngOpenssl_0 ; "(TEST_ENG_OPENSSL_RC4) test_init_key() "...
call    sub_1400B0CE0
test    edi, edi
jg      short loc_1400B11F5
```

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:



```
db '-----BEGIN RSA PUBLIC KEY-----',0Ah
                                ; DATA XREF: sub_7FF668CDF870+49↑o
                                ; sub_7FF668CDF870+59↑o ...
db 'MIICCAKCAgEAuWfX+pJCUCKc9xsWLVHpCpw6TL20HG/Vk4vF3GYlr6HltX7BMRfA',0Ah
db '7oGyMztNb37xW66NX+uxHghrX3+sm23yJmSfressJIGOvDNZVO80JevZxuhHUome',0Ah
db 'RdLfjRYpuEg8mbEdL1c1jQqoEZEhOIb8Lhv1dBDnwXEBGnf/k8uMuY784xxDfbpt',0Ah
db 'SB15OOHRfvIqMcIbskQ8RfMDFeiwYNRVrCkyhXOTB+RkmzTtp7q8gjnA1AHOfHSx',0Ah
db 'eOBVt9Lz27uuS4RIf/b31aiBolzAWft44wSC4diYvSom93d6S2K6oMYNOQvSu+zI',0Ah
db 'U8/yzxebDN0bWJLVPZxndQFBVHiTXQfWDi1BdsaljR2BHPj/tYWd4j/72vN1vywt',0Ah
db 'M3sn5TJNql/gJZ7HuU0QOyBzdLk3vpmmqby5wwXLd+WKPWv3HEKaOy80K0F7FrhC',0Ah
db '0g3nbKAf5Y+MzkEUNHDvwTk9uKY6IlCJ0/fXE78ULcxrgy0w76WVZWweLrsVun5k',0Ah
db 'J9i+LhcBNH7DJGJ544zC1yFi7sBgeW00VYCh7Ur4o0aE2EwTNYeLIgsFf4A6mOE0',0Ah
db '6gfoRDNH40U4DdK5JFQRp2tLXI93o7hSEEWAhJe7s0LyD1DLXksQjNkRUe+Ojd5G',0Ah
db 'AGdM3G7RZuWrMC4FfmtPlzYfdl5o2k/u9RYi7fi8pU34GQvvPhW8wK8CAQM=',0Ah
db '-----END RSA PUBLIC KEY-----',0Ah
```



```
call    cs:connect
cmp     eax, 0FFFFFFFFh
jnz     short loc_1400AE7F6
mov     ecx, eax
call    sub_1400AE500
test    eax, eax
jnz     loc_1400AE6BE
call    sub_140087B80
lea     r8, aBioConnect ; "BIO_connect"
mov     edx, 7Dh
lea     rcx, aCryptoBioBioSo_0 ; "crypto\\bio\\bio_sock2.c"
call    sub_140087CA0
call    cs:WSAGetLastError
lea     r8, aCallingConnect_0 ; "calling connect()"
mov     ecx, 2
mov     edx, eax
call    sub_140087DA0
call    sub_140087B80
lea     r8, aBioConnect ; "BIO_connect"
mov     edx, 7Fh
lea     rcx, aCryptoBioBioSo_0 ; "crypto\\bio\\bio_sock2.c"
call    sub_140087CA0
xor     r8d, r8d
lea     edx, [r8+67h]
jmp     loc_1400AE6B4
```

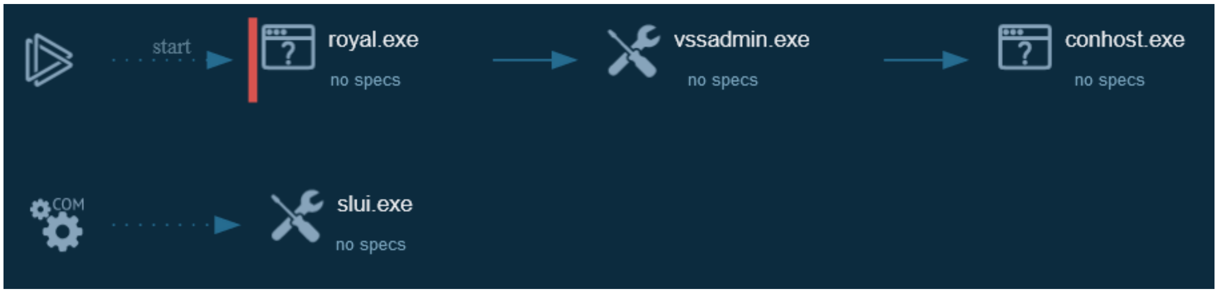
Dynamic Analysis

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.

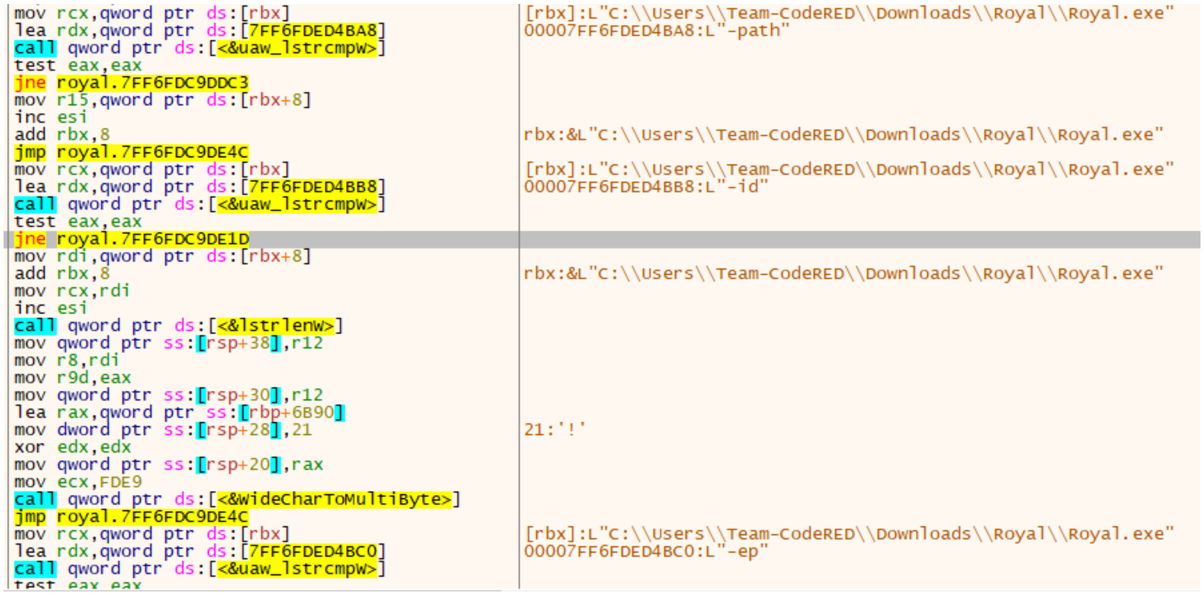
During the Debugger, when we try to move forward by putting a breakpoint on a few specific APIs, the program closes itself and performs the terminate operation. It is clearly understood that Anti-Analysis techniques, which we see in the Static analysis section, are used.

Command line arguments:

– path: The path to be encrypted.

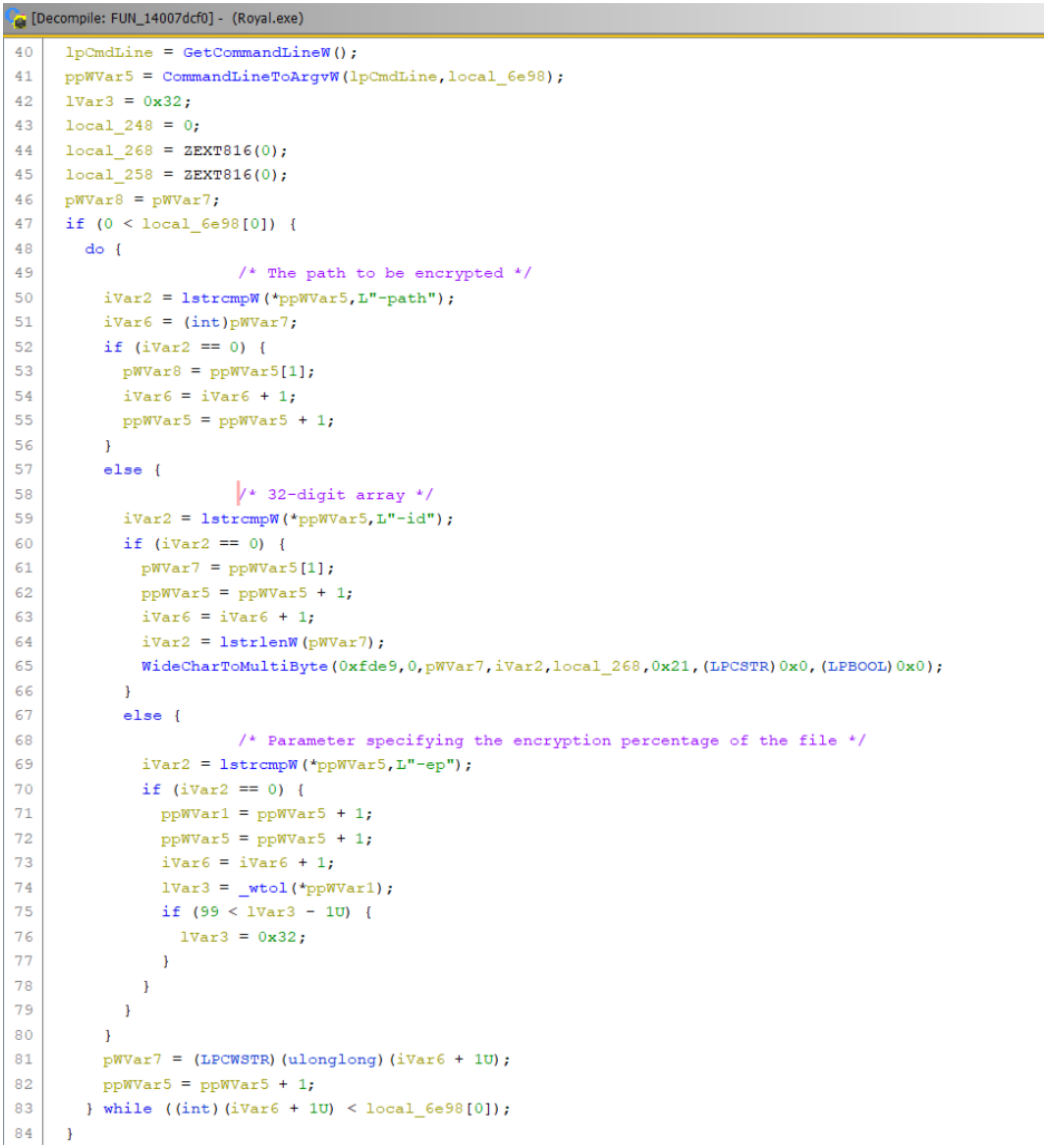
– ep: The number that represents the percentage of the file that will be encrypted.

– id: A 32-digit array.



```
mov rcx,qword ptr ds:[rbx]                  [rbx]:L"C:\\Users\\Team-CodeRED\\Downloads\\Royal\\Royal.exe"
lea rdx,qword ptr ds:[7FF6FDED4BA8]         00007FF6FDED4BA8:L"-path"
call qword ptr ds:[<&uaw_lstrcmpW>]
test eax,eax
jne royal.7FF6FDC9DDC3
mov r15,qword ptr ds:[rbx+8]
inc esi
add rbx,8                                   rbx:&L"C:\\Users\\Team-CodeRED\\Downloads\\Royal\\Royal.exe"
jmp royal.7FF6FDC9DE4C
mov rcx,qword ptr ds:[rbx]                  [rbx]:L"C:\\Users\\Team-CodeRED\\Downloads\\Royal\\Royal.exe"
lea rdx,qword ptr ds:[7FF6FDED4BB8]         00007FF6FDED4BB8:L"-id"
call qword ptr ds:[<&uaw_lstrcmpW>]
test eax,eax
jne royal.7FF6FDC9DE1D
mov rdi,qword ptr ds:[rbx+8]
add rbx,8                                   rbx:&L"C:\\Users\\Team-CodeRED\\Downloads\\Royal\\Royal.exe"
mov rcx,rdi
inc esi
call qword ptr ds:[<&lstrlenW>]
mov qword ptr ss:[rsp+38],r12
mov r8,rdi
mov r9d,eax
mov qword ptr ss:[rsp+30],r12
lea rax,qword ptr ss:[rbp+6B90]
mov dword ptr ss:[rsp+28],21                21:'!'
xor edx,edx
mov qword ptr ss:[rsp+20],rax
mov ecx,FDE9
call qword ptr ds:[<&WideCharToMultiByte>]
jmp royal.7FF6FDC9DE4C
mov rcx,qword ptr ds:[rbx]                  [rbx]:L"C:\\Users\\Team-CodeRED\\Downloads\\Royal\\Royal.exe"
lea rdx,qword ptr ds:[7FF6FDED4BC0]         00007FF6FDED4BC0:L"-ep"
call qword ptr ds:[<&uaw_lstrcmpW>]
test eax,eax
```

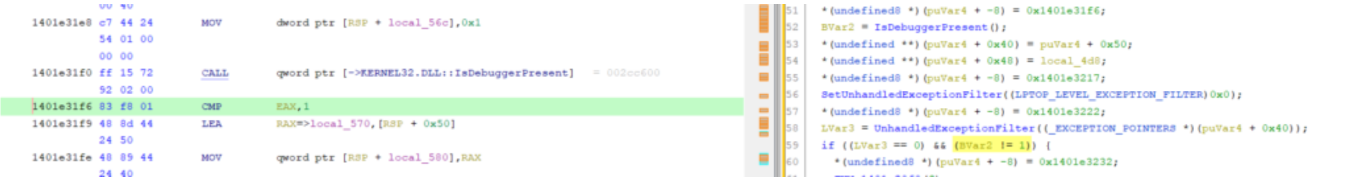
Re-examined code part where the parameters are run with Ghidra can be found below:



```
lpCmdLine = GetCommandLineW();
ppWVar5 = CommandLineToArgvW(lpCmdLine,local_6e98);
lVar3 = 0x32;
local_248 = 0;
local_268 = ZEXT816(0);
local_258 = ZEXT816(0);
pWVar8 = pWVar7;
if (0 < local_6e98[0]) {
  do {
                  /* The path to be encrypted */
    iVar2 = lstrcmpW(*ppWVar5,L"-path");
    iVar6 = (int)pWVar7;
    if (iVar2 == 0) {
      pWVar8 = ppWVar5[1];
      iVar6 = iVar6 + 1;
      ppWVar5 = ppWVar5 + 1;
    }
    else {
                  /* 32-digit array */
      iVar2 = lstrcmpW(*ppWVar5,L"-id");
      if (iVar2 == 0) {
        pWVar7 = ppWVar5[1];
        ppWVar5 = ppWVar5 + 1;
        iVar6 = iVar6 + 1;
        iVar2 = lstrlenW(pWVar7);
        WideCharToMultiByte(0xfde9,0,pWVar7,iVar2,local_268,0x21,(LPCSTR)0x0,(LPBOOL)0x0);
      }
      else {
                  /* Parameter specifying the encryption percentage of the file */
        iVar2 = lstrcmpW(*ppWVar5,L"-ep");
        if (iVar2 == 0) {
          ppWVar1 = ppWVar5 + 1;
          ppWVar5 = ppWVar5 + 1;
          iVar6 = iVar6 + 1;
          lVar3 = _wtol(*ppWVar1);
          if (99 < lVar3 - 1U) {
            lVar3 = 0x32;
          }
        }
      }
    }
    pWVar7 = (LPCWSTR)(ulonglong)(iVar6 + 1U);
    ppWVar5 = ppWVar5 + 1;
  } while ((int)(iVar6 + 1U) < local_6e98[0]);
}
```

Anti-Analysis Section

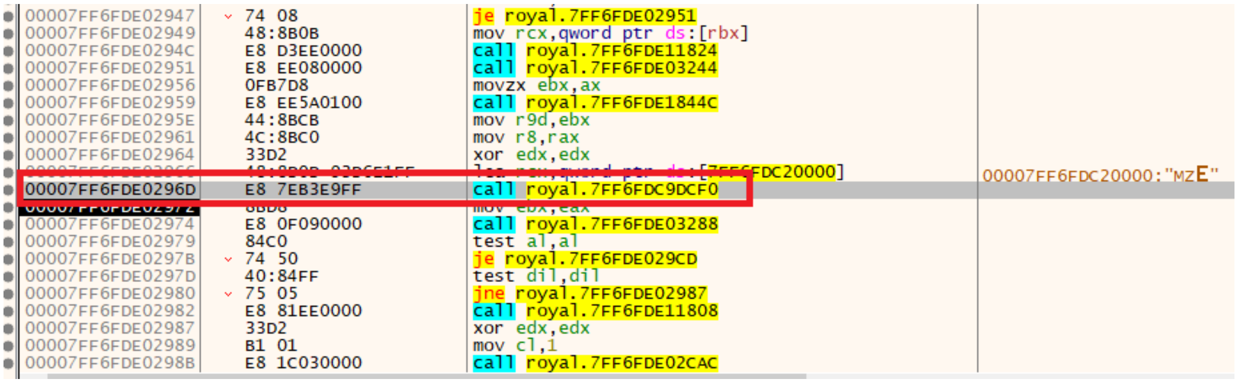
We saw the EAX Register value as 1 for IsDebuggerPresent, an important API that we constantly encounter in malware and will make the analyst's job more difficult. Let's check again with Ghidra and start looking at what we can do for an anti-analysis bypass.



```
1401e31e8 c7 44 24      MOV      dword ptr [RSP + local_56c],0x1
          54 01 00
          00 00
1401e31f0 ff 15 72      CALL     qword ptr [->KERNEL32.DLL::IsDebuggerPresent]   = 002cc600
          92 02 00
1401e31f6 83 f8 01      CMP      EAX,1
1401e31f9 48 8d 44      LEA      RAX=>local_570,[RSP + 0x50]
          24 50
1401e31fe 48 89 44      MOV      qword ptr [RSP + local_580],RAX
          24 40
```

```
*(undefined8 *)(puVar4 + -8) = 0x1401e31f6;
BVar2 = IsDebuggerPresent();
*(undefined **)(puVar4 + 0x40) = puVar4 + 0x50;
*(undefined **)(puVar4 + 0x48) = local_4d8;
*(undefined8 *)(puVar4 + -8) = 0x1401e3217;
SetUnhandledExceptionFilter((LPTOP_LEVEL_EXCEPTION_FILTER)0x0);
*(undefined8 *)(puVar4 + -8) = 0x1401e3222;
LVar3 = UnhandledExceptionFilter((_EXCEPTION_POINTERS *)(puVar4 + 0x40));
if ((LVar3 == 0) && (BVar2 != 1)) {
  *(undefined8 *)(puVar4 + -8) = 0x1401e3232;
```

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.

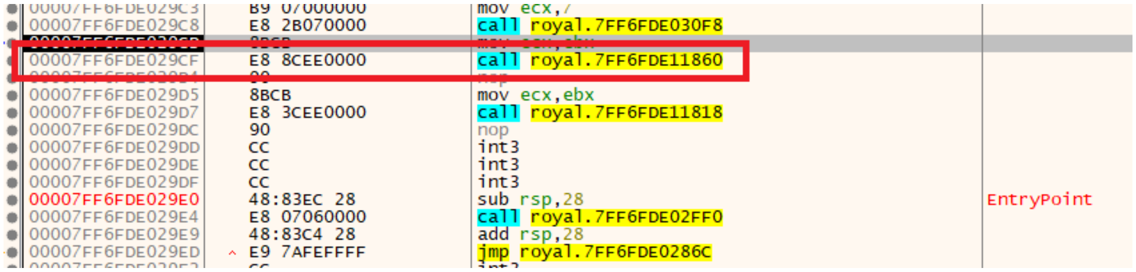


```
00007FF6FDE02947  v 74 08             je royal.7FF6FDE02951
00007FF6FDE02949    48:8B0B           mov rcx,qword ptr ds:[rbx]
00007FF6FDE0294C    E8 D3EE0000       call royal.7FF6FDE11824
00007FF6FDE02951    E8 EE080000       call royal.7FF6FDE03244
00007FF6FDE02956    0FB7D8            movzx ebx,ax
00007FF6FDE02959    E8 EE5A0100       call royal.7FF6FDE1844C
00007FF6FDE0295E    44:8BCB           mov r9d,ebx
00007FF6FDE02961    4C:8BC0           mov r8,rax
00007FF6FDE02964    33D2              xor edx,edx
00007FF6FDE02966    48:8D0D 93D6E1FF  lea rcx,qword ptr ds:[7FF6FDC20000]   00007FF6FDC20000:"MZE"
00007FF6FDE0296D    E8 7EB3E9FF       call royal.7FF6FDC9DCF0
00007FF6FDE02972    8BD8              mov ebx,eax
00007FF6FDE02974    E8 0F090000       call royal.7FF6FDE03288
00007FF6FDE02979    84C0              test al,al
00007FF6FDE0297B  v 74 50             je royal.7FF6FDE029CD
00007FF6FDE0297D    40:84FF           test dil,dil
00007FF6FDE02980  v 75 05             jne royal.7FF6FDE02987
00007FF6FDE02982    E8 81EE0000       call royal.7FF6FDE11808
00007FF6FDE02987    33D2              xor edx,edx
00007FF6FDE02989    B1 01             mov cl,1
00007FF6FDE0298B    E8 1C030000       call royal.7FF6FDE02CAC
```

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”.

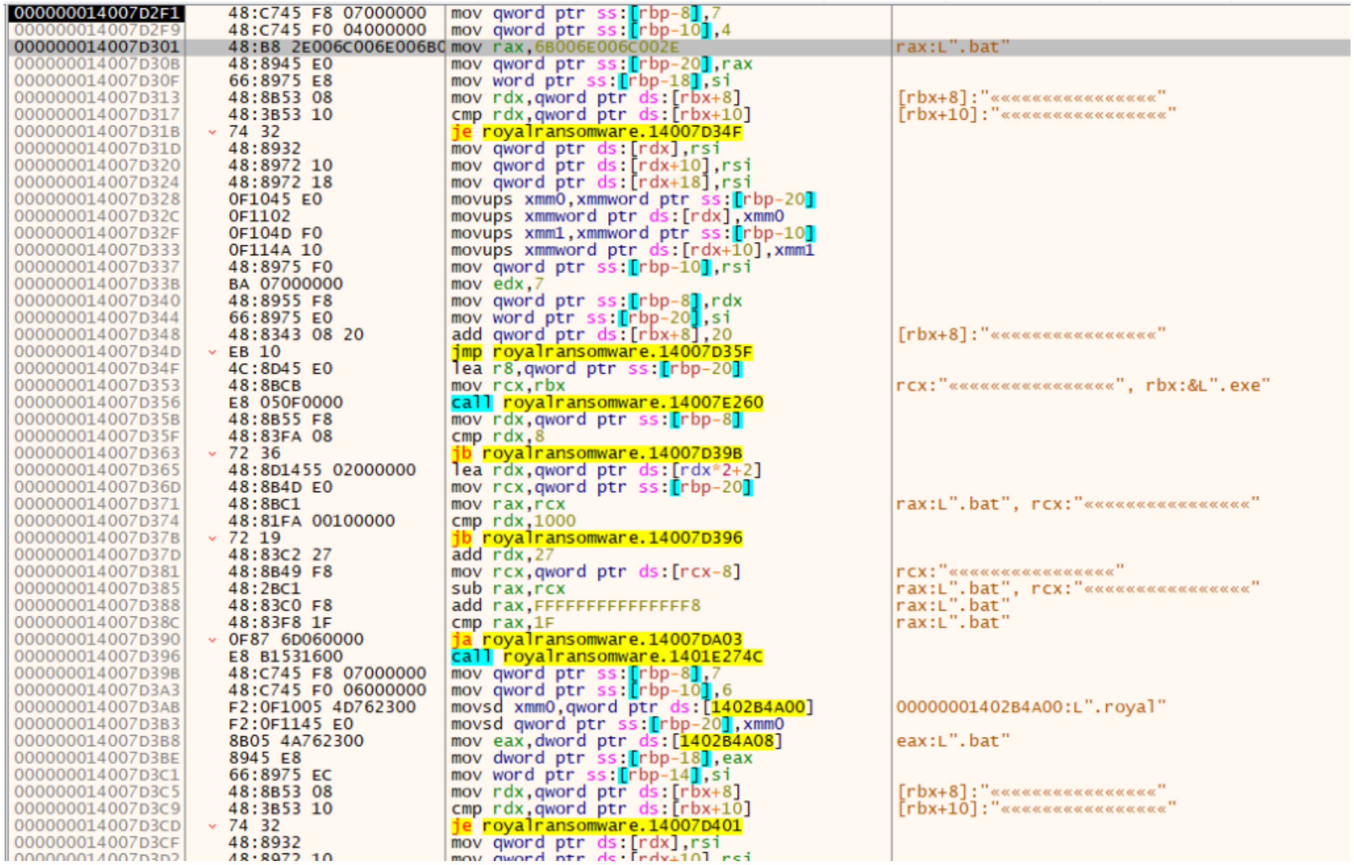
Let’s perform the previous RIP address change at this stage as well.



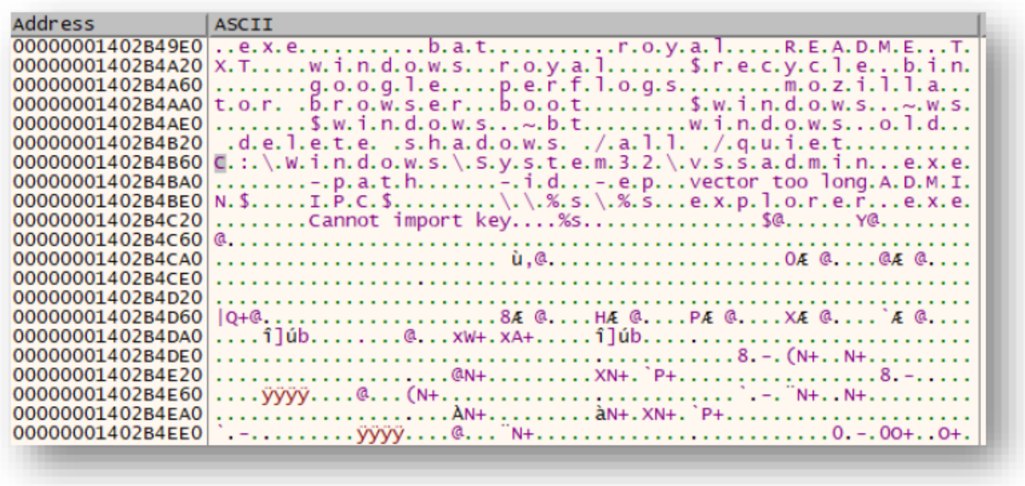
```
00007FF6FDE029C3    B9 07000000       mov ecx,7
00007FF6FDE029C8    E8 2B070000       call royal.7FF6FDE030F8
00007FF6FDE029CD    8BCB              mov ecx,ebx
00007FF6FDE029CF    E8 8CEE0000       call royal.7FF6FDE11860
00007FF6FDE029D4    90                nop
00007FF6FDE029D5    8BCB              mov ecx,ebx
00007FF6FDE029D7    E8 3CEE0000       call royal.7FF6FDE11818
00007FF6FDE029DC    90                nop
00007FF6FDE029DD    CC                int3
00007FF6FDE029DE    CC                int3
00007FF6FDE029DF    CC                int3
00007FF6FDE029E0    48:83EC 28        sub rsp,28                            EntryPoint
00007FF6FDE029E4    E8 07060000       call royal.7FF6FDE02FF0
00007FF6FDE029E9    48:83C4 28        add rsp,28
00007FF6FDE029ED  ^ E9 7AFEFFFF       jmp royal.7FF6FDE0286C
00007FF6FDE029F2    CC                int3
```

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



```
000000014007D2F1    48:C745 F8 07000000    mov qword ptr ss:[rbp-8],7
000000014007D2F9    48:C745 F0 04000000    mov qword ptr ss:[rbp-10],4
000000014007D301    48:B8 2E006C006E006BC  mov rax,6B006E006C002E                 rax:L".bat"
000000014007D30B    48:8945 E0             mov qword ptr ss:[rbp-20],rax
000000014007D30F    66:8975 E8             mov word ptr ss:[rbp-18],si
000000014007D313    48:8B53 08             mov rdx,qword ptr ds:[rbx+8]           [rbx+8]:"«««««««««««««««"
000000014007D317    48:3B53 10             cmp rdx,qword ptr ds:[rbx+10]          [rbx+10]:"«««««««««««««««"
000000014007D31B  v 74 32                  je royalransomware.14007D34F
000000014007D31D    48:8932                mov qword ptr ds:[rdx],rsi
000000014007D320    48:8972 10             mov qword ptr ds:[rdx+10],rsi
000000014007D324    48:8972 18             mov qword ptr ds:[rdx+18],rsi
000000014007D328    0F1045 E0              movups xmm0,xmmword ptr ss:[rbp-20]
000000014007D32C    0F1102                 movups xmmword ptr ds:[rdx],xmm0
000000014007D32F    0F104D F0              movups xmm1,xmmword ptr ss:[rbp-10]
000000014007D333    0F114A 10              movups xmmword ptr ds:[rdx+10],xmm1
000000014007D337    48:8975 F0             mov qword ptr ss:[rbp-10],rsi
000000014007D33B    BA 07000000            mov edx,7
000000014007D340    48:8955 F8             mov qword ptr ss:[rbp-8],rdx
000000014007D344    66:8975 E0             mov word ptr ss:[rbp-20],si
000000014007D348    48:8343 08 20          add qword ptr ds:[rbx+8],20            [rbx+8]:"«««««««««««««««"
000000014007D34D  v EB 10                  jmp royalransomware.14007D35F
000000014007D34F    4C:8D45 E0             lea r8,qword ptr ss:[rbp-20]
000000014007D353    48:8BCB                mov rcx,rbx                            rcx:"«««««««««««««««", rbx:&L".exe"
000000014007D356    E8 050F0000            call royalransomware.14007E260
000000014007D35B    48:8B55 F8             mov rdx,qword ptr ss:[rbp-8]
000000014007D35F    48:83FA 08             cmp rdx,8
000000014007D363  v 72 36                  jb royalransomware.14007D39B
000000014007D365    48:8D1455 02000000     lea rdx,qword ptr ds:[rdx*2+2]
000000014007D36D    48:8B4D E0             mov rcx,qword ptr ss:[rbp-20]
000000014007D371    48:8BC1                mov rax,rcx                            rax:L".bat", rcx:"«««««««««««««««"
000000014007D374    48:81FA 00100000       cmp rdx,1000
000000014007D37B  v 72 19                  jb royalransomware.14007D396
000000014007D37D    48:83C2 27             add rdx,27
000000014007D381    48:8B49 F8             mov rcx,qword ptr ds:[rcx-8]           rcx:"«««««««««««««««"
000000014007D385    48:2BC1                sub rax,rcx                            rax:L".bat", rcx:"«««««««««««««««"
000000014007D388    48:83C0 F8             add rax,FFFFFFFFFFFFFFF8               rax:L".bat"
000000014007D38C    48:83F8 1F             cmp rax,1F                             rax:L".bat"
000000014007D390  v 0F87 6D060000          ja royalransomware.14007DA03
000000014007D396    E8 B1531600            call royalransomware.1401E274C
000000014007D39B    48:C745 F8 07000000    mov qword ptr ss:[rbp-8],7
000000014007D3A3    48:C745 F0 06000000    mov qword ptr ss:[rbp-10],6
000000014007D3AB    F2:0F1005 4D762300     movsd xmm0,qword ptr ds:[1402B4A00]    00000001402B4A00:L".royal"
000000014007D3B3    F2:0F1145 E0           movsd qword ptr ss:[rbp-20],xmm0
000000014007D3B8    8B05 4A762300          mov eax,dword ptr ds:[1402B4A08]       eax:L".bat"
000000014007D3BE    8945 E8                mov dword ptr ss:[rbp-18],eax
000000014007D3C1    66:8975 EC             mov word ptr ss:[rbp-14],si
000000014007D3C5    48:8B53 08             mov rdx,qword ptr ds:[rbx+8]           [rbx+8]:"«««««««««««««««"
000000014007D3C9    48:3B53 10             cmp rdx,qword ptr ds:[rbx+10]          [rbx+10]:"«««««««««««««««"
000000014007D3CD  v 74 32                  je royalransomware.14007D401
000000014007D3CF    48:8932                mov qword ptr ds:[rdx],rsi
000000014007D3D2    48:8972 10             mov qword ptr ds:[rdx+10],rsi
```



```
Address           ASCII
00000001402B49E0  ..e.x.e...........b.a.t..........r.o.y.a.l.....R.E.A.D.M.E...T.
00000001402B4A20  X.T.....w.i.n.d.o.w.s...r.o.y.a.l.......$.r.e.c.y.c.l.e...b.i.n.
00000001402B4A60  ........g.o.o.g.l.e.....p.e.r.f.l.o.g.s.........m.o.z.i.l.l.a...
00000001402B4AA0  t.o.r. .b.r.o.w.s.e.r...b.o.o.t.........$.w.i.n.d.o.w.s...~.w.s.
00000001402B4AE0  ........$.w.i.n.d.o.w.s...~.b.t.........w.i.n.d.o.w.s...o.l.d...
00000001402B4B20   .d.e.l.e.t.e. .s.h.a.d.o.w.s. ./.a.l.l. ./.q.u.i.e.t..........
00000001402B4B60  C.:.\.W.i.n.d.o.w.s.\.S.y.s.t.e.m.3.2.\.v.s.s.a.d.m.i.n...e.x.e.
00000001402B4BA0  ........-.p.a.t.h.......-.i.d...-.e.p...vector too long.A.D.M.I.
00000001402B4BE0  N.$.....I.P.C.$.........\.\.%.s.\.%.s...e.x.p.l.o.r.e.r...e.x.e.
00000001402B4C20  ........Cannot import key....%s..............$@......Y@........
00000001402B4C60  @...............................................................
00000001402B4CA0  ........................ ù,@.......................0Æ @....@Æ @....
00000001402B4CE0  ................................................................
00000001402B4D20  ................................................................
00000001402B4D60  |Q+@....................8Æ @....HÆ @....PÆ @....XÆ @....`Æ @....
00000001402B4DA0  ....î]úb........@...xW+.xA+.....î]úb............................
00000001402B4DE0  ..............................................8.-.(N+..N+........
00000001402B4E20  ......................@N+.........XN+.`P+...................8.-...
00000001402B4E60  ....ÿÿÿÿ....@...(N+...........................`.-.¨N+..N+........
00000001402B4EA0  ......................ÀN+.........àN+.XN+.`P+....................
00000001402B4EE0  `.-.........ÿÿÿÿ....@...¨N+.........................0.-.00+..0+.
```

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

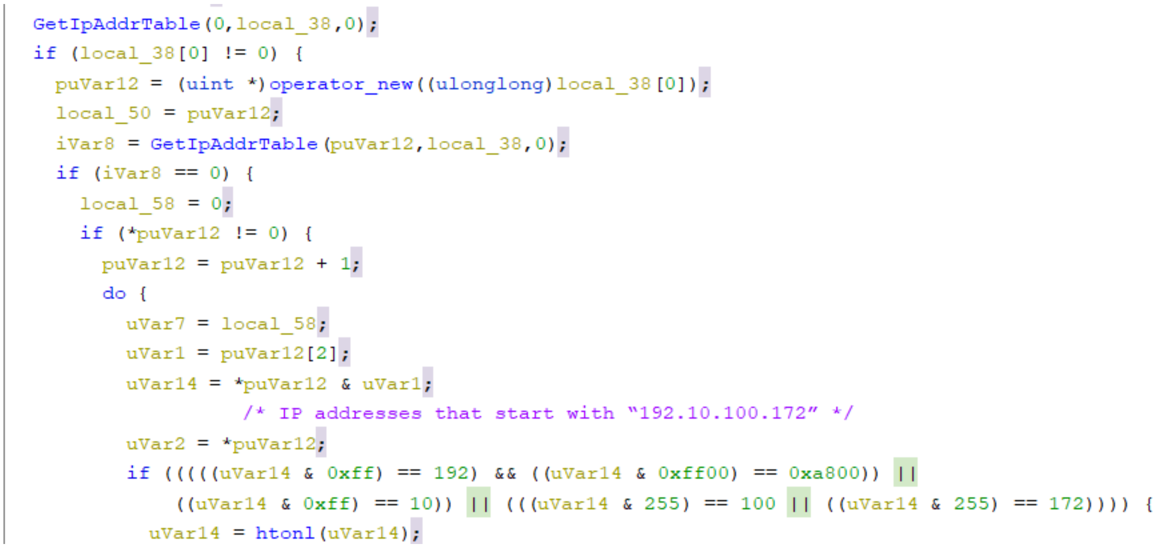
– Windows, RoyalPreflogs, Tor Browser, Boot $recycle.bin, Windows.old, $windows.~ws, $windows.~bt, Mozilla, Google.

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 "\\<IP_Address>\ADMIN$" or "\\<IP_Address>\IPC$", the ransomware will not encrypt it.

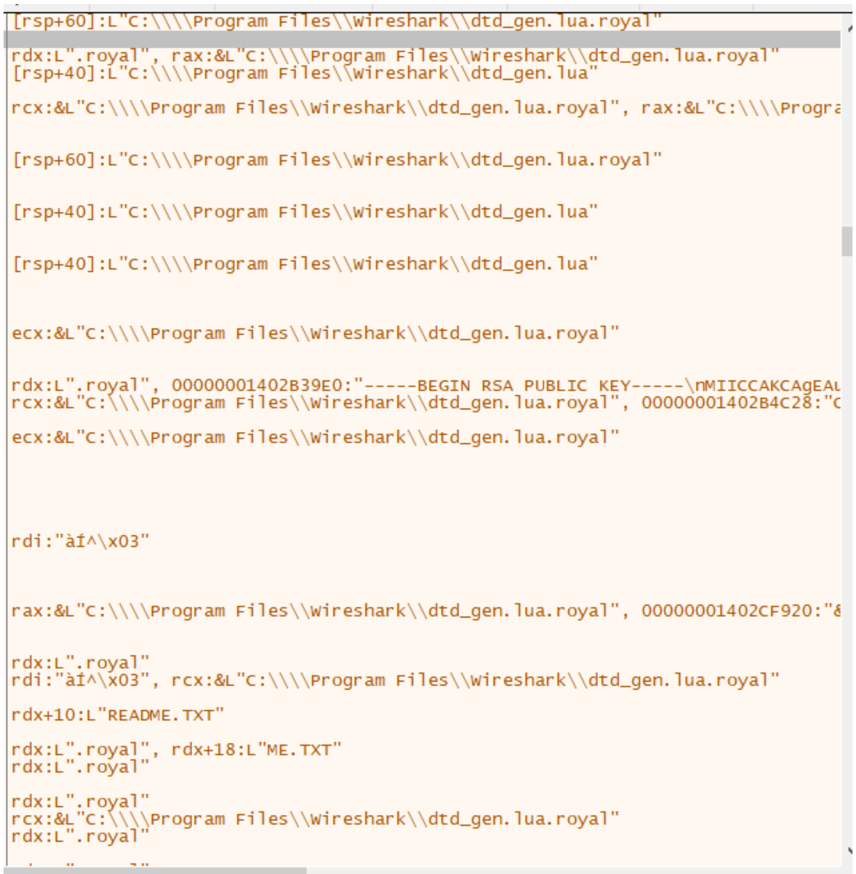


```
GetIpAddrTable(0,local_38,0);
if (local_38[0] != 0) {
  puVar12 = (uint *)operator_new((ulonglong)local_38[0]);
  local_50 = puVar12;
  iVar8 = GetIpAddrTable(puVar12,local_38,0);
  if (iVar8 == 0) {
    local_58 = 0;
    if (*puVar12 != 0) {
      puVar12 = puVar12 + 1;
      do {
        uVar7 = local_58;
        uVar1 = puVar12[2];
        uVar14 = *puVar12 & uVar1;
                  /* IP addresses that start with "192.10.100.172" */
        uVar2 = *puVar12;
        if (((((uVar14 & 0xff) == 192) && ((uVar14 & 0xff00) == 0xa800)) ||
            ((uVar14 & 0xff) == 10)) || (((uVar14 & 255) == 100 || ((uVar14 & 255) == 172)))) {
          uVar14 = htonl(uVar14);
```

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/Vk4vF3GYlr6HltX7BMRfA\n7oGyMztNb37xW66NX+uxHghrX3+sm23yJmSfres

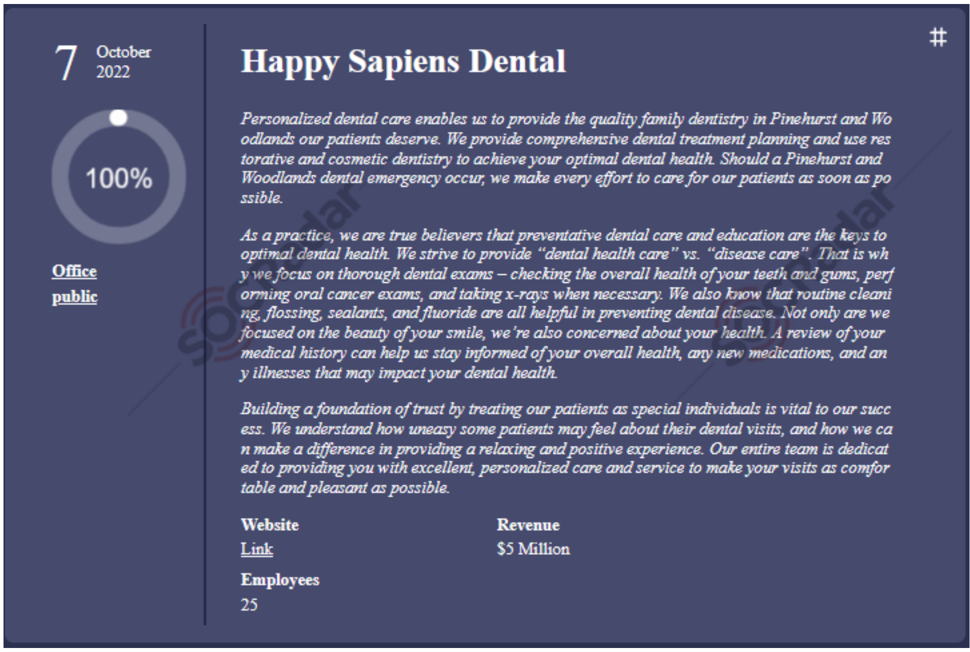


```
[rsp+60]:L"C:\\\\Program Files\\Wireshark\\dtd_gen.lua.royal"

rdx:L".royal", rax:&L"C:\\\\Program Files\\Wireshark\\dtd_gen.lua.royal"
[rsp+40]:L"C:\\\\Program Files\\Wireshark\\dtd_gen.lua"

rcx:&L"C:\\\\Program Files\\Wireshark\\dtd_gen.lua.royal", rax:&L"C:\\\\Progra

[rsp+60]:L"C:\\\\Program Files\\Wireshark\\dtd_gen.lua.royal"

[rsp+40]:L"C:\\\\Program Files\\Wireshark\\dtd_gen.lua"

[rsp+40]:L"C:\\\\Program Files\\Wireshark\\dtd_gen.lua"


ecx:&L"C:\\\\Program Files\\Wireshark\\dtd_gen.lua.royal"

rdx:L".royal", 00000001402B39E0:"-----BEGIN RSA PUBLIC KEY-----\nMIICCAKCAgEAL
rcx:&L"C:\\\\Program Files\\Wireshark\\dtd_gen.lua.royal", 00000001402B4C28:"C

ecx:&L"C:\\\\Program Files\\Wireshark\\dtd_gen.lua.royal"



rdi:"àí^\x03"


rax:&L"C:\\\\Program Files\\Wireshark\\dtd_gen.lua.royal", 00000001402CF920:"&


rdx:L".royal"
rdi:"àí^\x03", rcx:&L"C:\\\\Program Files\\Wireshark\\dtd_gen.lua.royal"

rdx+10:L"README.TXT"

rdx:L".royal", rdx+18:L"ME.TXT"
rdx:L".royal"

rdx:L".royal"
rcx:&L"C:\\\\Program Files\\Wireshark\\dtd_gen.lua.royal"
rdx:L".royal"
```

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.



7 October 2022

100%

Office

public

#

Happy Sapiens Dental

Personalized dental care enables us to provide the quality family dentistry in Pinehurst and Woodlands our patients deserve. We provide comprehensive dental treatment planning and use restorative and cosmetic dentistry to achieve your optimal dental health. Should a Pinehurst and Woodlands dental emergency occur, we make every effort to care for our patients as soon as possible.

As a practice, we are true believers that preventative dental care and education are the keys to optimal dental health. We strive to provide "dental health care" vs. "disease care". That is why we focus on thorough dental exams – checking the overall health of your teeth and gums, performing oral cancer exams, and taking x-rays when necessary. We also know that routine cleaning, flossing, sealants, and fluoride are all helpful in preventing dental disease. Not only are we focused on the beauty of your smile, we're also concerned about your health. A review of your medical history can help us stay informed of your overall health, any new medications, and any illnesses that may impact your dental health.

Building a foundation of trust by treating our patients as special individuals is vital to our success. We understand how uneasy some patients may feel about their dental visits, and how we can make a difference in providing a relaxing and positive experience. Our entire team is dedicated to providing you with excellent, personalized care and service to make your visits as comfortable and pleasant as possible.

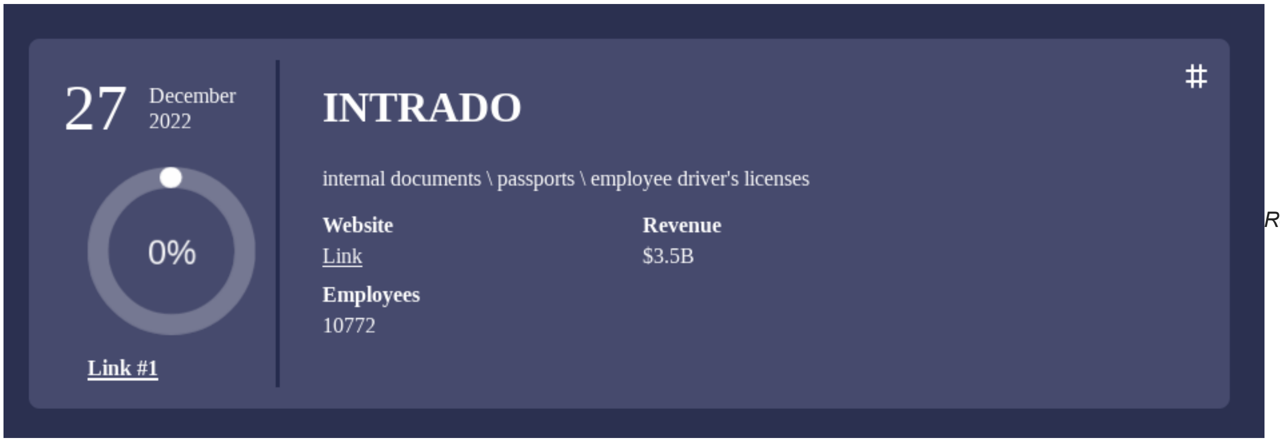
Website
Link

Revenue
$5 Million

Employees
25

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.



27 December 2022

0%

Link #1

INTRADO

internal documents \ passports \ employee driver's licenses

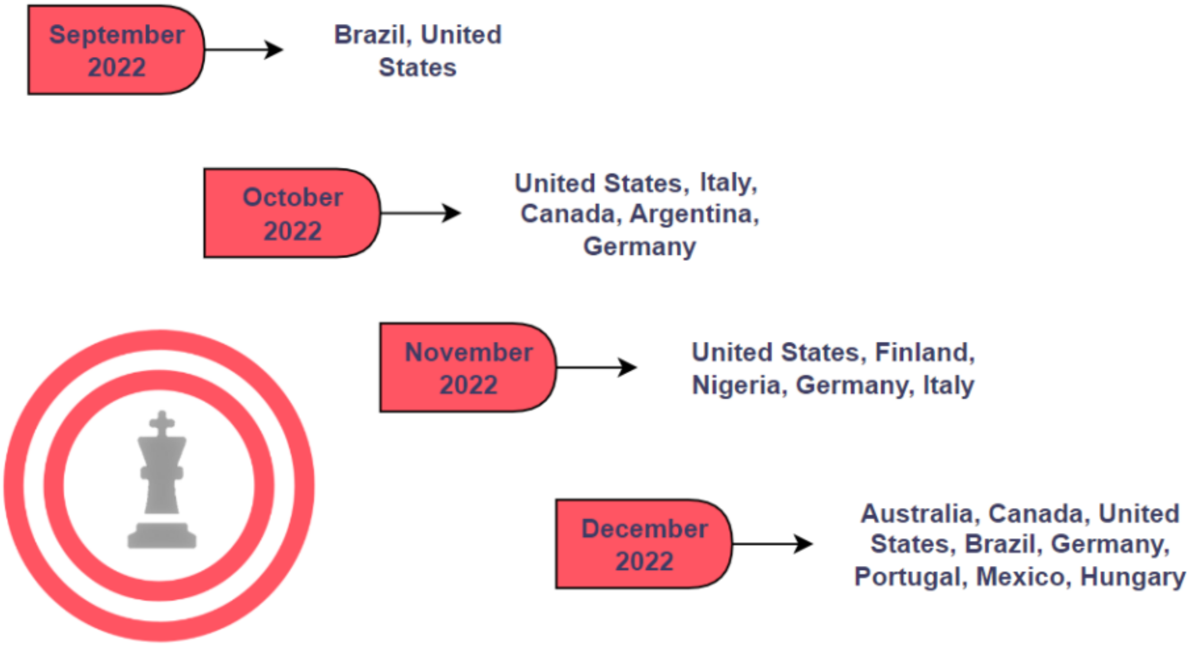
Website
Link

Revenue
$3.5B

Employees
10772

Royal's claim about INTRADO

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



September 2022 → Brazil, United States

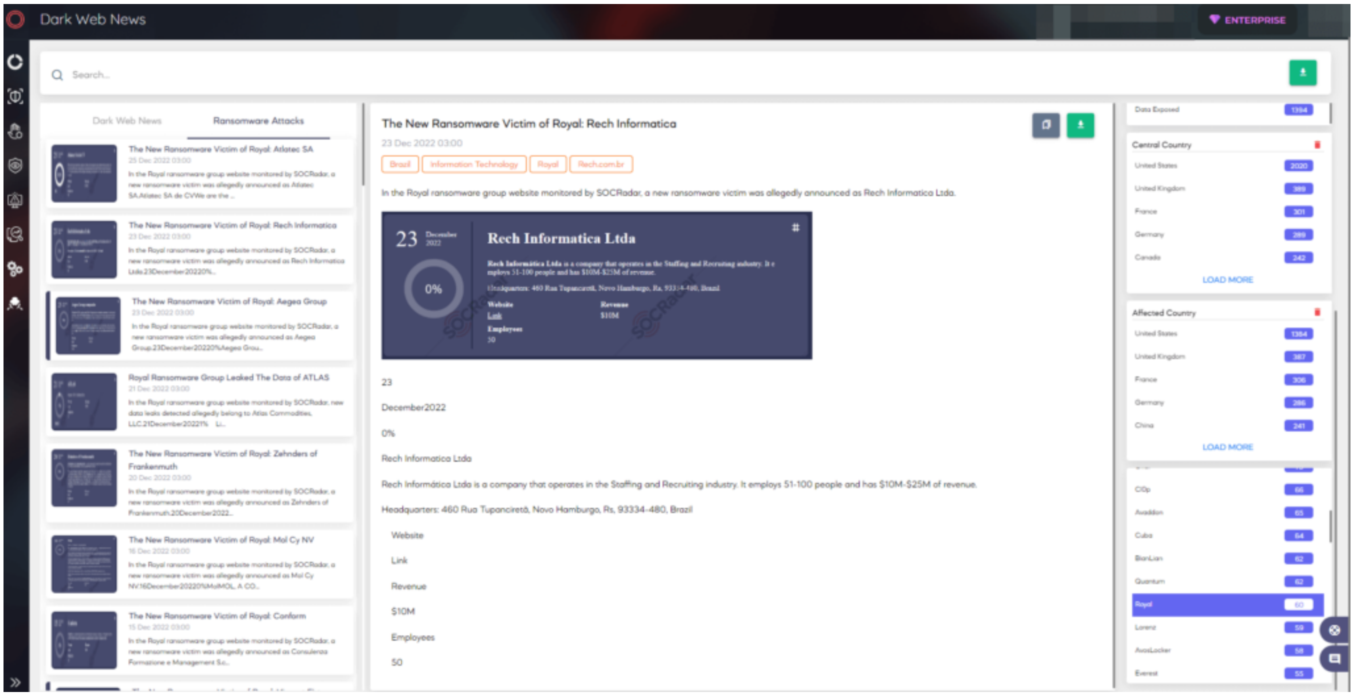
October 2022 → United States, Italy, Canada, Argentina, Germany

November 2022 → United States, Finland, Nigeria, Germany, Italy

December 2022 → Australia, Canada, United States, Brazil, Germany, Portugal, Mexico, Hungary

Timeline of Royal Ransomware attacks

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



The New Ransomware Victim of Royal: Atlatec SA
25 Dec 2022 03:00
In the Royal ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Atlatec SA.Atlatec SA de CVWe are the ...

The New Ransomware Victim of Royal: Rech Informatica
23 Dec 2022 03:00
In the Royal ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Rech Informatica Ltda.23December20220%...

The New Ransomware Victim of Royal: Aegea Group
23 Dec 2022 03:00
In the Royal ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Aegea Group.23December20220%Aegea Grou...

Royal Ransomware Group Leaked The Data of ATLAS
21 Dec 2022 03:00
In the Royal ransomware group website monitored by SOCRadar, new data leaks detected allegedly belong to Atlas Commodities, LLC.21December20221% Li...

The New Ransomware Victim of Royal: Zehnders of Frankenmuth
20 Dec 2022 03:00
In the Royal ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Zehnders of Frankenmuth.20December2022...

The New Ransomware Victim of Royal: Mol Cy NV
16 Dec 2022 03:00
In the Royal ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Mol Cy NV.16December20220%MolMOL A CO...

The New Ransomware Victim of Royal: Conform
15 Dec 2022 03:00
In the Royal ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Consulenza Formazione e Management S.c...

The New Ransomware Victim of Royal: Rech Informatica
23 Dec 2022 03:00
Brazil | Information Technology | Royal | Rech.com.br

In the Royal ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Rech Informatica Ltda.

23 December 2022
0%
Rech Informatica Ltda
Rech Informática Ltda is a company that operates in the Staffing and Recruiting industry. It employs 51-100 people and has $10M-$25M of revenue.
Headquarters: 460 Rua Tupanciretã, Novo Hamburgo, Rs, 93334-480, Brazil
Website
Link
Revenue
$10M
Employees
50

23

December2022

0%

Rech Informatica Ltda

Rech Informática Ltda is a company that operates in the Staffing and Recruiting industry. It employs 51-100 people and has $10M-$25M of revenue.

Headquarters: 460 Rua Tupanciretã, Novo Hamburgo, Rs, 93334-480, Brazil

Website

Link

Revenue

$10M

Employees

50

Data Exposed	1394

Central Country	
United States	2020
United Kingdom	389
France	301
Germany	289
Canada	242

LOAD MORE

Affected Country	
United States	1384
United Kingdom	387
France	306
Germany	286
China	241

LOAD MORE

Cl0p	66
Avaddon	65
Cuba	64
BianLian	62
Quantum	62
Royal	60
Lorenz	59
AvosLocker	58
Everest	55

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