

A white icon inside a square frame, depicting a person's head and shoulders above three horizontal lines representing a list or profile.

PROFILE

Royal Ransomware

ZEROFOX INTELLIGENCE

P-2022-12-19a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Ransomware

December 19, 2022



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 12:00 PM (EST) on December 16, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Royal Ransomware

Executive Summary

ZeroFox Intelligence has observed an uptick in activity from the Royal Ransomware group (Royal), especially in the past two months. Royal gains access to victim networks by conducting targeted callback phishing attacks with the goal of convincing a victim to install remote access software, which is used to gain access to a corporate network. The group deploys Cobalt Strike for persistence, credential harvesting, lateral movement through a Windows domain, data stealing, and device encryption. Recently, the U.S. Department of Health and Human Services issued an advisory warning healthcare organizations in particular to be wary of Royal ransomware based on historic ransomware targeting of the healthcare industry.

Details

Royal has been active since January 2022 and is a private group without any ransomware affiliates. It does not follow the Ransomware-as-a-Service model but does utilize the double extortion technique. It initially gains access to victim networks by conducting targeted callback phishing attacks wherein threat actors impersonate food delivery and software providers in emails purporting to be subscription renewals. The emails contain phone numbers controlled by the threat actors that the victim can contact to cancel the alleged subscription. From there, actors use social engineering to persuade the victim to install remote access software over the phone, which is then used to gain access to a corporate network. In one case, initial access was gained by exploiting a vulnerability in a custom web application.

The group deploys Cobalt Strike for persistence, credential harvesting, lateral movement through a Windows domain, data stealing, and device encryption. Royal was also observed targeting virtual machines by directly encrypting virtual disk files (VMDK). Royal's encryption is a 64-bit Windows executable written in C++. It is launched via the command line and appears to use a mix of RSA and AES algorithms from the OpenSSL library. The encryptor then appends the [.]royal extension to file



names; once encrypted, ransom notes are either printed on network printers or created on encrypted Windows devices. Ransom notes are named “README[.]TXT” and include a link to the victim's private Tor negotiation page, where demands typically range from USD 250,000 to over USD 2 million.

Analyst Commentary

Royal Ransomware, although not branded as such at the time, first became active in January 2022 and comprises a vetted and experienced team of ransomware actors from previous operations. It is a private group without any ransomware affiliates, meaning it does not follow the Ransomware-as-a-Service model. Royal does follow the double extortion model, and it maintains its own ransomware leak site.¹

In November 2022, Microsoft reported that the threat cluster tracked as “DEV-0569” was delivering Royal Ransomware after gaining access to compromised networks via a BATLOADER-delivered Cobalt Strike Beacon implant.²

On December 7, 2022, the U.S. Department of Health and Human Services issued an advisory warning healthcare organizations in particular to be wary of Royal ransomware. The advisory indicated that any time Royal has targeted the healthcare industry, that it claimed to have published 100 percent of the victims’ extracted data.³

Ransomware Evolution

When it first started, Royal utilized other ransomware operations’ encryptors, such as BlackCat, before shifting to its own encryptors. Royal initially used the Zeon encryptor to generate ransom notes.⁴ Below is a mapping of Royal’s early tactics, techniques, and procedures (TTPs) to the MITRE ATT&CK framework based on the analysis of an early sample:

¹

[hXXps://www.bleepingcomputer\[.\]com/news/security/new-royal-ransomware-emerges-in-multi-million-dollar-attacks/](https://www.bleepingcomputer.com/news/security/new-royal-ransomware-emerges-in-multi-million-dollar-attacks/)

²

[hXXps://www.microsoft\[.\]com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/](https://www.microsoft.com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/)

³ [hXXps://www.hhs\[.\]gov/sites/default/files/royal-ransomware-analyst-note.pdf](https://www.hhs.gov/sites/default/files/royal-ransomware-analyst-note.pdf)

⁴ [hXXps://tria\[.\]ge/220224-17djraca3](https://tria[.]ge/220224-17djraca3)



Source: [hXXps://tria\[.\]ge/220224-l7djraca3](https://tria[.]ge/220224-l7djraca3)

In September 2022, the ransomware gang rebranded itself to “Royal” and began using that name in ransom notes generated by its new encryptor.⁵

Initial Access and TTPs

Royal gains initial access to victim networks by conducting targeted callback phishing attacks wherein threat actors impersonate food delivery and software providers in emails purporting to be subscription renewals. These phishing emails contain phone numbers that the victim can contact to cancel the alleged subscription; however, the number belongs to a service hired by the threat actors.⁶

When a victim calls the number, the threat actors use social engineering to persuade the victim to install remote access software, which is then used to gain initial access to a corporate network. One Royal Ransomware victim shared that the threat actors breached their network by exploiting a vulnerability in their custom web application. Royal also deploys Cobalt Strike for persistence, credential harvesting, lateral movement through the Windows domain, data stealing, and device encryption.⁷

When encrypting files, the Royal encryptor appends the [.]royal extension to file names. Another victim indicated that Royal targeted virtual machines by directly encrypting their virtual disk files (VMDK). Once encrypted, the threat actors print the ransom notes on network printers or create them on encrypted Windows devices. These ransom notes are named “README[.]TXT” and include a link to the victim's private Tor negotiation page at [royal2xthig3ou5hd7zsliaqgy6yygk2cdelaxtni2fyad6dpmpxedid\[.\]onion](https://royal2xthig3ou5hd7zsliaqgy6yygk2cdelaxtni2fyad6dpmpxedid[.]onion). The victim's name is appended to the [.]onion extension.⁸

⁵

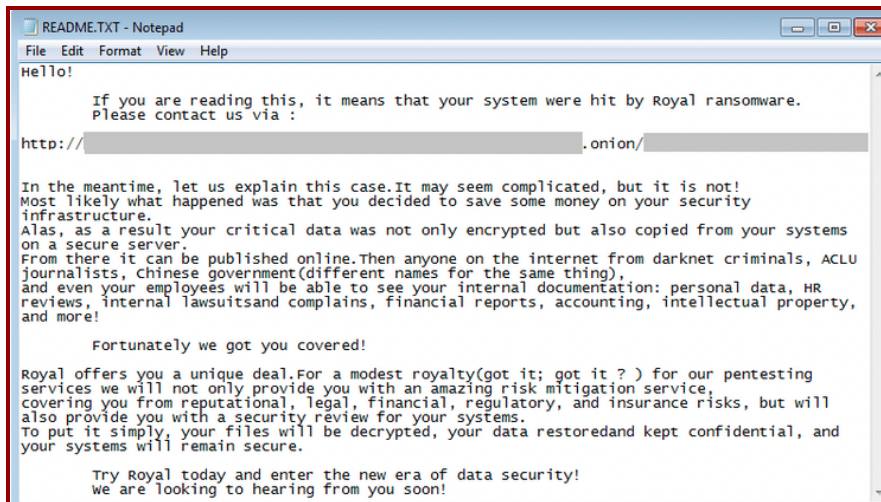
[hXXps://www.bleepingcomputer\[.\]com/news/security/new-royal-ransomware-emerges-in-multi-million-dollar-attacks/](https://www.bleepingcomputer[.]com/news/security/new-royal-ransomware-emerges-in-multi-million-dollar-attacks/)

⁶

[hXXps://www.bleepingcomputer\[.\]com/news/security/new-royal-ransomware-emerges-in-multi-million-dollar-attacks/](https://www.bleepingcomputer[.]com/news/security/new-royal-ransomware-emerges-in-multi-million-dollar-attacks/)

⁷ Ibid.

⁸ Ibid.



Source: [hXXps://www.fortinet\[.\]com/blog/threat-research/ransomware-roundup-royal-ransomware](https://www.fortinet.com/blog/threat-research/ransomware-roundup-royal-ransomware)

The ransomware gang will then provide the ransom demand, which typically ranges from USD 250,000 to over USD 2 million. They will also commonly decrypt some files for the victims to prove that their decryptor is working, as well as share file lists of the stolen data.⁹

Encryption Process

Royal Ransomware's encryption is a 64-bit Windows executable written in C++. It is launched via the command lines *GetCommandLineW* API and *CommandLineToArgvW*, suggesting that it is designed to be run via an operator after initial access has been secured by another method. There are three parameters required to initiate the encryption process: 1) "-path" determines what is to be encrypted—whether a single directory or an entire drive; 2) "-id" appears to be how the group identifies each victim and can be any 32-character string; and 3) "-ep" is the parameter for encryption percentage. Furthermore, preparation is done by deleting any shadow copies. The process creates lists of elements to be excluded during file and folder fetching.¹⁰ The encryption has the capability to infect and encrypt shared resources inside an internal network by using NetShareEnum seeking the "ADMIN\$" and "IPC\$" records.¹¹

Royal appears to use a mix of RSA and AES algorithms from the OpenSSL library. The AES key is generated and protected by an RSA public key.¹² Encrypted files are renamed and given the [.]royal file extension. The ransom note is called "README[.]txt."

⁹

[hXXps://www.bleepingcomputer\[.\]com/news/security/new-royal-ransomware-emerges-in-multi-million-dollar-attacks/](https://www.bleepingcomputer.com/news/security/new-royal-ransomware-emerges-in-multi-million-dollar-attacks/)

¹⁰ [hXXps://www.fortinet\[.\]com/blog/threat-research/ransomware-roundup-royal-ransomware](https://www.fortinet.com/blog/threat-research/ransomware-roundup-royal-ransomware)

¹¹ [hXXps://yoro\[.\]company/research/reconstructing-the-last-activities-of-royal-ransomware/](https://yoro[.]company/research/reconstructing-the-last-activities-of-royal-ransomware/)

¹² [hXXps://securityscorecard\[.\]pathfactory\[.\]com/research/the-royal-ransomware](https://securityscorecard[.]pathfactory[.]com/research/the-royal-ransomware)



Recommendations

- Search for any of the referenced Indicators of Compromise (IOCs) throughout the corporate network.
- Block the referenced IOCs to prevent any potential attacks.
- Conduct internal training to make employees aware of social engineering attempts utilizing lures for subscription renewals, particularly around food delivery and software providers in emails.
- Subscribe to Advanced Dark Web Intelligence in the ZeroFox Platform for continued updates on new ransomware targets.
- Access the ZeroFox Platform's [Intelligence Search](#) interface to investigate IOCs and metadata related to Malware and Ransomware.



Appendix 1: Indicators of Compromise

SHA256

2598e8adb87976abe48f0eba4bbb9a7cb69439e0c133b21aee3845dfccf3fb8f
9db958bc5b4a21340ceeeb8c36873aa6bd02a460e688de56ccbba945384b1926
c24c59c8f4e7a581a5d45eel81151lec0a3f0b59af987eac9b363577087c9746
5fda381a9884f7be2d57b8a290f389578a9d2f63e2ecb98bd773248a7eb99fa2
312f34ee8c7b2199a3e78b4a52bd87700cc8f3aa01aa641e5d899501cb720775
491c2b32095174b9de2fd799732a6f84878c2e23b9bb560cd3155cbdc65e2b80
f484f919ba6e36ff33e4fb391b8859a94d89c172a465964f99d6113b55ced429
7cbfea0bff4b373a175327d6cc395f6c176dab1cedf9075e7130508bec4d5393
383eb4802490f4ffd47f7918d5cd237e69deed15f0ce2aba761f7120d7481037
c860bf644bd5e3d6f4cae67848c4fc769184ae652fcb41cac670042b185d217a
f484f919ba6e36ff33e4fb391b8859a94d89c172a465964f99d6113b55ced429
c24c59c8f4e7a581a5d45eel81151lec0a3f0b59af987eac9b363577087c9746

7cbfea0bff4b373a175327d6cc395f6c176dab1cedf9075e7130508bec4d5393
5fda381a9884f7be2d57b8a290f389578a9d2f63e2ecb98bd773248a7eb99fa2
491c2b32095174b9de2fd799732a6f84878c2e23b9bb560cd3155cbdc65e2b80
312f34ee8c7b2199a3e78b4a52bd87700cc8f3aa01aa641e5d899501cb720775

SHA-1

f5eac094d9eb8f1f691d66dlcfcla9ada6548def
66535700bbce7f90d2add7c504bc0e0523d4d71d
6b0deb67a178fe20e81691133b257df3bafa3006
04028a0a1d44f81709040c31af026785209d4343
f697230ba32c437760bf2ac36e6bb33b86684244
db3163a09eb33ff4370ad162a05f4b2584a20456
61ae4cdfb8477a58c56267870599af325e79ea71

SHA-512

861e4ad17b9flab53a94bf785b436bf3336218cld5a9dcb41047b5ea8d7de549032727c4896b
86e3ab8c7cdd410208e8999505a24dd09e9b2b75db7a4b13a3fa

MD5

846274ff97d7e0bffcc993cab1851270
33f612338b6b5e6b4fe8cbb17208795c
01492156ce8b4034c5b1027130f4cf4e
afd5d656a42a746e95926ef07933f054
df0b88dafa7a65295f99e69a67db9e1b
a96c125a0b4729e8494c696d300a7357
937d8f5da4adff6309bfa4c3b63a2708



PROFILE: ROYAL RANSOMWARE

P-2022-12-19a
TLP:CLEAR

Ransom Note

README[.]txt

File Extension

[.]royal

[.]royal_w

Process Spawned

C:\Windows\System32\vssadmin[.]exe delete shadows /all /quiet

Onion Site

royal2xthig3ou5hd7zsliqagy6yygk2cdelaxtni2fyad6dpmpxedid[.]onion



Appendix 2: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.