Intelligence Profile: **Royal**

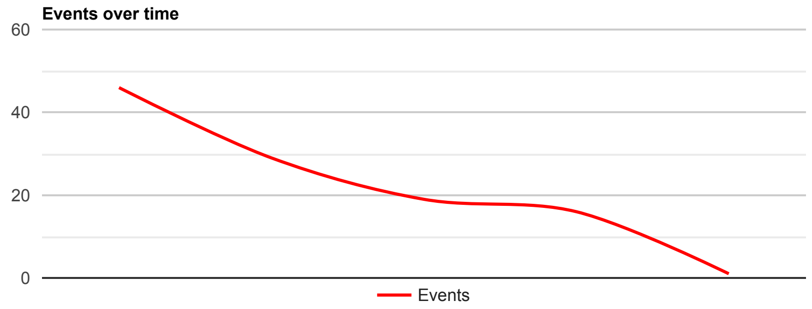
TLP:GREEN

eCrime.ch

Name	**Royal**
Alternative Names	Conti Team One · DEV-0846 · Royal Ransom

Events tracked

First Event	**2022-11-03**
Last Event	**2023-03-02**
Dates active	**119 days**
Total Events	**111**



Description

Royal ransomware is a type of malicious software that encrypts a victim's files and demands payment in exchange for the decryption key. The Royal ransomware is believed to be operated by a threat actor group known as Conti Team One, which has been active since 2020.

Royal is a sophisticated cybercriminal group that primarily targets corporate and government organizations worldwide. The group typically gains access to a victim's system by exploiting vulnerabilities or by tricking employees into clicking on malicious links or attachments. Once inside the system, Royal exfiltrates sensitive data and deploys the Royal ransomware to encrypt the victim's files, demanding payment in exchange for the decryption key.

According to security researchers, Royal actors are believed to be based in Russia. Royal is known for its use of advanced techniques, including the use of double extortion, where they threaten to leak stolen data if the ransom is not paid.
— Source: ChatGPT

Since approximately September 2022, cyber criminals have compromised U.S. and international organizations with a Royal ransomware variant. FBI and CISA believe this variant, which uses its own custom-made file encryption program, evolved from earlier iterations that used "Zeon" as a loader. After gaining access to victims' networks, Royal actors disable antivirus software and exfiltrate large amounts of data before ultimately deploying the ransomware and encrypting the systems. Royal actors have made ransom demands ranging from approximately $1 million to $11 million USD in Bitcoin. In observed incidents, Royal actors do not include ransom amounts and payment instructions as part of the initial ransom note. Instead, the note, which appears after encryption, requires victims to directly interact with the threat actor via a .onion URL (reachable through the Tor browser). Royal actors have targeted numerous critical infrastructure sectors including, but not limited to, Manufacturing, Communications, Healthcare and Public Healthcare (HPH), and Education.
— Source: Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA)

Leak Site

Impacted Countries

United States 69
Top 10 impacted sectors
- Law Practice 5
- Insurance 3
- Industrial Automation 2
- Oil and Energy 2
- Information Technology and Services 2
- Food and Beverage Manufacturing 2
- Building Materials 2
- Financial Services 2
- Construction 2
- IT Services and IT Consulting 2

Canada 10
Top 10 impacted sectors
- Retail 1
- IT Services and IT Consulting 1
- Financial Services 1
- Business Supplies and Equipment 1
- Mining 1
- Wholesale Building Materials 1
- Appliances, Electrical, and Electronics Manufacturing 1
- Motor Vehicle Manufacturing 1
- Airlines and Aviation 1
- Construction 1

Germany 5
Top 5 impacted sectors
- Machinery Manufacturing 1
- Architecture and Planning 1
- Higher Education 1
- Industrial Machinery Manufacturing 1

Brazil 4
Top 4 impacted sectors
- Software Development 1
- Environmental Services 1
- Retail 1
- Construction 1

Italy 3
Top 3 impacted sectors
- Food Production 1
- Education 1

Mexico 3
Top 3 impacted sectors
- Environmental Services 1
- Mechanical or Industrial Engineering 1
- Retail Groceries 1

Australia 3
Top 3 impacted sectors
- Financial Services 1
- Higher Education 1
- Education Administration Programs 1

United Kingdom 2
Top 2 impacted sectors
- Spectator Sports 1
- Motor Vehicle Manufacturing 1

Portugal 2
Top 2 impacted sectors
- Computer Hardware Manufacturing 1
- Automotive 1

Malaysia 1
No sectors identified

Ivory Coast 1
No sectors identified

Finland 1
Top 1 impacted sector
Utilities 1

Trinidad and Tobago 1
Top 1 impacted sector
Insurance 1

Spain 1
Top 1 impacted sector
Industrial Machinery Manufacturing 1

Puerto Rico 1
Top 1 impacted sector
Wholesale 1

China 1
Top 1 impacted sector
Electrical/Electronic Manufacturing 1

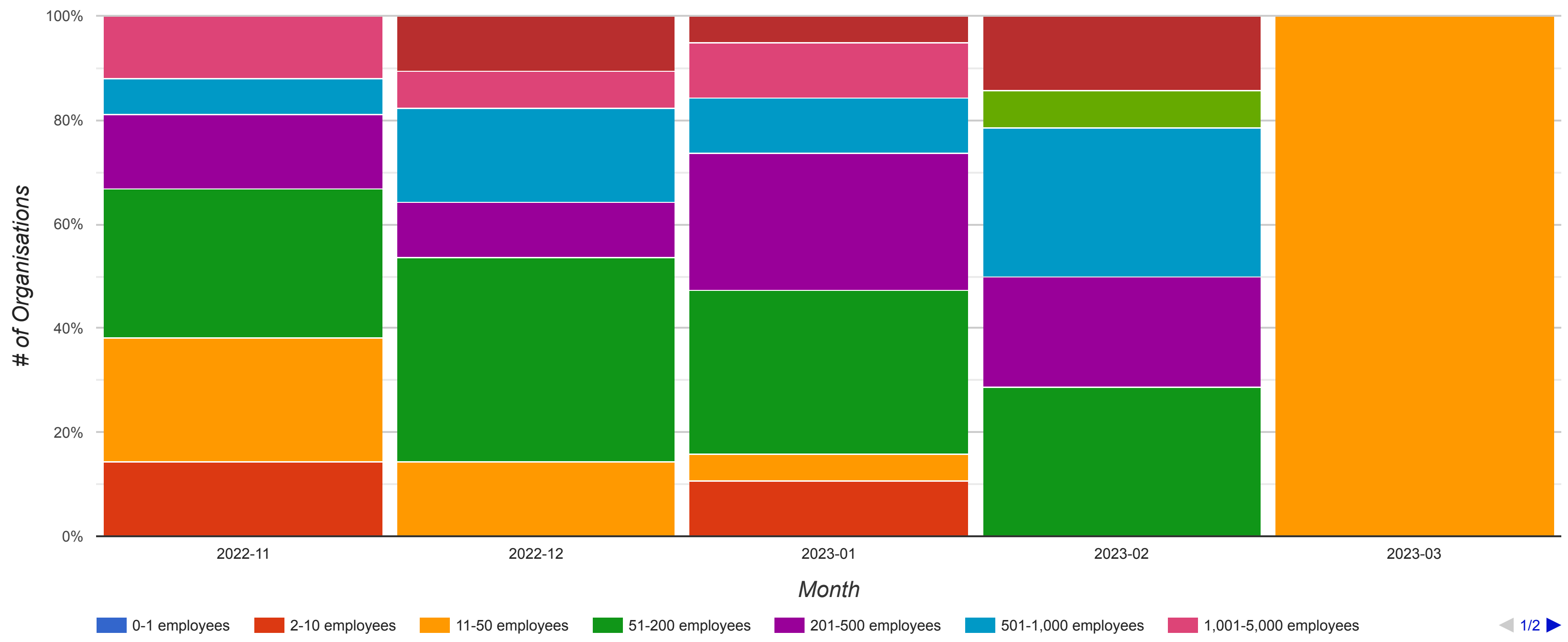
France 1
Top 1 impacted sector
Machinery 1

Belgium 1
Top 1 impacted sector
Truck Transportation 1

Netherlands 1
Top 1 impacted sector
Machinery Manufacturing 1

Company size

by employee count



Known TTPs

MITRE ATT&CK

T1001 - Data Obfuscation

T1016 - System Network Configuration Discovery

T1021.001 - Remote Desktop Protocol

T1027 - Obfuscated Files or Information

T1036 - Masquerading

T1046 - Network Service Discovery

T1048 - Exfiltration Over Alternative Protocol

T1055 - Process Injection

T1057 - Process Discovery

T1059 - Command and Scripting Interpreter

T1070.001 - Clear Windows Event Logs

T1070.004 - File Deletion

T1078 - Valid Accounts

T1078.002 - Domain Accounts

T1082 - System Information Discovery

T1083 - File and Directory Discovery

T1090 - Proxy

T1105 - Ingress Tool Transfer

T1106 - Native API

T1119 - Automated Collection

T1129 - Shared Modules

T1133 - External Remote Services

T1134.001 - Token Impersonation/Theft

T1135 - Network Share Discovery

T1140 - Deobfuscate/Decode Files or Information

T1189 - Drive-by Compromise

T1190 - Exploit Public-Facing Application

T1204 - User Execution

T1219 - Remote Access Software

T1484.001 - Group Policy Modification

T1486 - Data Encrypted for Impact

T1489 - Service Stop

T1490 - Inhibit System Recovery

T1518 - Software Discovery

T1559.001 - Component Object Model

T1560 - Archive Collected Data

T1562 - Impair Defenses

T1562.001 - Disable or Modify Tools

T1563 - Remote Service Session Hijacking

T1566 - Phishing

T1567 - Exfiltration Over Web Service

T1569.002 - Service Execution

T1572 - Protocol Tunneling

T1574 - Hijack Execution Flow

T1622 - Debugger Evasion

Known Exploited Vulnerabilities

CVE-2022-27510

Open Source Links

#StopRansomware: Royal Ransomware

Read more

Malpedia: Royal ransomware

Read more

MalwareBazaar Database: Royal

Read more

Royal ransomware spreads to Linux and VMware ESXi

Read more

ACSC Ransomware Profile - Royal

Read more

Conti Team One Splinter Group Resurfaces as Royal Ransomware with Callback Phishing Attacks

Read more

DEV-0569 finds new ways to deliver Royal ransomware, various payloads

Read more

Ransomnote Sample

```
Filename: README.TXT


Hello!

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

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!
```