Mphasis
The Next Applied

New Royal Ransomware Emerges in Multi-million-dollar Attacks

Severity: High

Date: 6th March 2023

Description

A ransomware operation named Royal is quickly ramping up, targeting corporations with ransom demands ranging from $250,000 to over $2 million. Royal is an operation that launched in January 2022 and consists of a group of vetted and experienced ransomware actors from previous operations.

Unlike most active ransomware operations, Royal does not operate as a Ransomware-as-a-Service but is instead a private group without affiliates.

Technical Details

Royal ransomware uses a unique partial encryption approach that allows the threat actor to choose a specific percentage of data in a file to encrypt. This approach allows the actor to lower the encryption percentage for larger files, which helps evade detection. In addition to encrypting files, Royal actors also engage in double extortion tactics in which they threaten to publicly release the encrypted data if the victim does not pay the ransom.

Methodology

The Royal operation has been operating in the shadows, not using a data leak site and keeping news of their attacks quiet. However, as the gang became more active this month, victims have appeared at Bleeping Computer, and a sample was uploaded to Virus Total. Royal group utilizes targeted callback phishing attacks where they impersonate food delivery and software providers in emails pretending to be subscription renewals.

These phishing emails contain phone numbers that the victim can contact to cancel the alleged subscription, but, in reality, it is a number to a service hired by the threat actors.

When a victim calls the number, the threat actors use social engineering to convince the victim to install remote access software, which is used to gain initial access to the corporate network.

A Royal victim who spoke to Bleeping Computer shared that the threat actors breached their network using a vulnerability in their custom web application, showing the threat actors are also being creative in how they gain access to a network.

Once they gain access to a network, they perform the same activities commonly used by other human-operated ransomware operations. They deploy Cobalt Strike for persistence, harvest credentials, spread laterally through the Windows domain, steal data, and ultimately encrypt devices.

When encrypting files, the Royal encryptor will append the .royal extension to the file names of encrypted files. For example, test.jpg would be encrypted and renamed to test.jpg.royal. These ransom notes are named **README.TXT** and contain a link to the victim's private Tor negotiation page at royal2xthig3ou5hd7zsliqagy6yygk2cdelaxtni2fyad6dpmpxedid.onion. XXX in the ransom note below has been redacted but is unique to the victim.

The Tor negotiation site is nothing special, simply containing a chat screen where a victim can communicate with the Royal ransomware operators. As part of these negotiations, the ransomware gang will provide the ransom demand, with ransom demands between $250,000 and over $2 million. The ransomware gang will also commonly decrypt a few files for the victims to prove their decryptor works and share file lists of the stolen data.

IOCs

197.207.181[.]147	102.157.44[.]105	147.135.11[.]223
197.207.218[.]27	105.158.118[.]241	152.89.247[.]50
197.94.67[.]207	105.69.155[.]85	172.64.80[.]1
23.111.114[.]52	113.169.187[.]159	179.43.167[.]10
41.100.55[.]97	134.35.9[.]209	185.7.214[.]218
41.107.77[.]67	139.195.43[.]166	193.149.176[.]157
41.109.11[.]80	139.60.161[.]213	193.235.146[.]104
41.251.121[.]35	148.213.109[.]165	209.141.36[.]116
41.97.65[.]51	163.182.177[.]80	45.61.136[.]47
42.189.12[.]36	181.141.3[.]126	45.8.158[.]104
45.227.251[.]167	181.164.194[.]228	5.181.234[.]58
5.44.42[.]20	185.143.223[.]69	5.188.86[.]195
61.166.221[.]46	186.64.67[.]6	77.73.133[.]84
68.83.169[.]91	186.86.212[.]138	89.108.65[.]136
81.184.181[.]215	190.193.180[.]228	94.232.41[.]105
82.12.196[.]197	196.70.77[.]11	47.87.229[.]39
98.143.70[.]147	197.11.134[.]255	140.82.48[.]158
147.135.36[.]162	197.158.89[.]85	197.204.247[.]7

Malicious Domains

- ciborkumari[.]xyz
- sombrat[.]com
- gororama[.]com
- softeruplive[.]com
- altocloudzone[.]live
- ciborkumari[.]xyz
- myappearinc[.]com
- parkerpublic[.]com
- astebin.mozilla[.]org/Z54Vudf9/raw
- tumbleproperty[.]com
- myappearinc[.]com/acquire/draft/c7lh0s5jv

Hash values

Tool	SHA256
AV tamper	8A983042278BC5897DBCDD54D1D7E3143F8B7EAD553B5A4713E30DEFFDA16375
TCP/UDP Tunnel over HTTP (Chisel)	8a99353662ccae117d2bb22efd8c43d7169060450be413af763e8ad7522d2451
Ursnif/Gozi	be030e685536eb38ba1fec1c90e90a4165f6641c8dc39291db1d23f4ee9fa0b1
Exfil	B8C4AEC31C134ADBDBE8AAD65D2BCB21CFE62D299696A23ADD9AA1DE082C6E20
Remote Access (AnyDesk)	4a9dde3979c2343c024c6eeeddff7639be301826dd637c006074e04a1e4e9fe7
PowerShell Toolkit Downloader	4cd00234b18e04dcd745cc81bb928c8451f6601affb5fa45f20bb11bfb5383ce
PsExec (Microsoft Sysinternals)	08c6e20b1785d4ec4e3f9956931d992377963580b4b2c6579fd9930e08882b1c
Keep Host Unlocked (Don’t Sleep)	f8cff7082a936912baf2124d42ed82403c75c87cb160553a7df862f8d81809ee
Ransomware Executable	d47d4b52e75e8cf3b11ea171163a66c06d1792227c1cf7ca49d7df60804a1681
Windows Command Line (NirCmd)	216047C048BF1DCBF031CF24BD5E0F263994A5DF60B23089E393033D17257CB5
System Management (NSudo)	19896A23D7B054625C2F6B1EE1551A0DA68AD25CDDBB24510A3B74578418E618

Filename	Hash Value
2.bat	585b05b290d241a249af93b1896a9474128da969
3.bat	41a79f83f8b00ac7a9dd06e1e225d64d95d29b1d
4.bat	a84ed0f3c46b01d66510ccc9b1fc1e07af005c60
8.bat	c96154690f60a8e1f2271242e458029014ffe30a
kl.bat	65dc04f3f75deb3b287cca3138d9d0ec36b8bea0
gp.bat	82f1f72f4b1bfd7cc8afbe6d170686b1066049bc7e5863b51aa15ccc5c841f58
r.bat	74d81ef0be02899a177d7ff6374d699b634c70275b3292dbc67e577b5f6a3f3c
runanddelete.bat	342B398647073159DFA8A7D36510171F731B760089A546E96FBB8A292791EFEE

Reference Links

New Royal Ransomware emerges in multi-million dollar attacks (bleepingcomputer.com)

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