Coauthored by:

Product ID: AA23-061A

March 2, 2023

#StopRansomware: Royal Ransomware

SUMMARY

***Note**: This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.*

Actions to take today to mitigate cyber threats from ransomware:

- Prioritize remediating known exploited vulnerabilities.
- Train users to recognize and report phishing attempts.
- Enable and enforce multifactor authentication.

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint CSA to disseminate known Royal ransomware IOCs and TTPs identified through FBI threat response activities as recently as January 2023.

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.

FBI and CISA encourage organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of ransomware incidents. For a downloadable copy of IOCs, see AA23-061A.stix (STIX, 115 kb).

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office at fbi.gov/contact-us/field-offices. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at Report@cisa.dhs.gov.

TECHNICAL DETAILS

Note: *This advisory uses the MITRE ATT&CK® for Enterprise framework, version 12. See MITRE ATT&CK for Enterprise for all referenced tactics and techniques.*

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.[1] 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.

Initial Access

Royal actors gain initial access to victim networks in a number of ways including:

- **Phishing.** According to third-party reporting, Royal actors most commonly (in 66.7% of incidents) gain initial access to victim networks via successful phishing emails [T1566].
    - According to open-source reporting, victims have unknowingly installed malware that delivers Royal ransomware after receiving phishing emails containing malicious PDF documents [T1566.001], and malvertising [T1566.002].[2]
- **Remote Desktop Protocol (RDP).** The second most common vector Royal actors use (in 13.3% of incidents) for initial access is RDP compromise.
- **Public-facing applications.** FBI has also observed Royal actors gain initial access through exploiting public-facing applications [T1190].
- **Brokers.** Reports from trusted third-party sources indicate that Royal actors may leverage brokers to gain initial access and source traffic by harvesting virtual private network (VPN) credentials from stealer logs.

Command and Control

Once Royal actors gain access to the network, they communicate with command and control (C2) infrastructure and download multiple tools [T1105]. Legitimate Windows software is repurposed by Royal operators to strengthen their foothold in the victim's network. Ransomware operators often use open-source projects to aid their intrusion activities; Royal operators have recently been observed using `Chisel`, a tunneling tool transported over HTTP and secured via SSH [T1572], to communicate with their C2 infrastructure. FBI has observed multiple Qakbot C2s used in Royal ransomware attacks, but has not yet determined if Royal ransomware exclusively uses Qakbot C2s.

Lateral Movement and Persistence

Royal actors often use RDP to move laterally across the network [T1021.001]. Microsoft Sysinternals tool `PsExec` has also been used to aid lateral movement. FBI has observed Royal actors using remote monitoring and management (RMM) software, such as AnyDesk, LogMeIn, and Atera, for persistence in the victim's network [T1133]. In some instances, the actors moved laterally to the domain controller. In one confirmed case, the actors used a legitimate admin account to remotely log on to the domain controller [T1078]. Once on the domain controller, the threat actor deactivated antivirus protocols [T1562.001] by modifying Group Policy Objects [T1484.001].

Exfiltration

Royal actors exfiltrate data from victim networks by repurposing legitimate cyber pentesting tools, such as Cobalt Strike, and malware tools and derivatives, such as Ursnif/Gozi, for data aggregation and exfiltration. According to third-party reporting, Royal actors' first hop in exfiltration and other operations is usually a U.S. IP address.

Note: In reference to Cobalt Strike and other tools mentioned above, a tool repository used by Royal was identified at IP: 94.232.41[.]105 in December 2022.

Encryption

Before starting the encryption process, Royal actors:

- Use Windows Restart Manager to determine whether targeted files are currently in use or blocked by other applications [T1486].[1]
- Use Windows Volume Shadow Copy service (`vssadmin.exe`) to delete shadow copies to inhibit system recovery.[1]

FBI has found numerous batch (`.bat`) files on impacted systems which are typically transferred as an encrypted 7zip file. Batch files create a new admin user [T1078.002], force a group policy update, set pertinent registry keys to auto-extract [T1119] and execute the ransomware, monitor the encryption process, and delete files upon completion—including Application, System, and Security event logs [T1070.001].

Malicious files have been found in victim networks in the following directories:

- `C:\Temp\`
- `C:\Users\<user>\AppData\Roaming\`
- `C:\Users\<users>\`
- `C:\ProgramData\`

Indicators of Compromise (IOC)

See table 1 and 2 for Royal ransomware IOCs that FBI obtained during threat response activities as of January 2023. **Note**: Some of the observed IP addresses are several months old. FBI and CISA recommend vetting or investigating these IP addresses prior to taking forward-looking action, such as blocking.

Table 1: Royal Ransomware Associated Files, Hashes, and IP addresses as of January 2023

IOC	Description
.royal	Encrypted file extension
README.TXT	Ransom note
Malicious IP	**Last Activity**

102.157.44[.]105	November 2022
105.158.118[.]241	November 2022
105.69.155[.]85	November 2022
113.169.187[.]159	November 2022
134.35.9[.]209	November 2022
139.195.43[.]166	November 2022
139.60.161[.]213	November 2022
148.213.109[.]165	November 2022
163.182.177[.]80	November 2022
181.141.3[.]126	November 2022
181.164.194[.]228	November 2022
185.143.223[.]69	November 2022
186.64.67[.]6	November 2022
186.86.212[.]138	November 2022
190.193.180[.]228	November 2022
196.70.77[.]11	November 2022
197.11.134[.]255	November 2022
197.158.89[.]85	November 2022
197.204.247[.]7	November 2022
197.207.181[.]147	November 2022
197.207.218[.]27	November 2022
197.94.67[.]207	November 2022
23.111.114[.]52	November 2022
41.100.55[.]97	November 2022
41.107.77[.]67	November 2022
41.109.11[.]80	November 2022
41.251.121[.]35	November 2022
41.97.65[.]51	November 2022
42.189.12[.]36	November 2022
45.227.251[.]167	November 2022
5.44.42[.]20	November 2022
61.166.221[.]46	November 2022
68.83.169[.]91	November 2022
81.184.181[.]215	November 2022
82.12.196[.]197	November 2022
98.143.70[.]147	November 2022
140.82.48[.]158	December 2022
147.135.36[.]162	December 2022
147.135.11[.]223	December 2022
152.89.247[.]50	December 2022

172.64.80[.]1	December 2022
179.43.167[.]10	December 2022
185.7.214[.]218	December 2022
193.149.176[.]157	December 2022
193.235.146[.]104	December 2022
209.141.36[.]116	December 2022
45.61.136[.]47	December 2022
45.8.158[.]104	December 2022
5.181.234[.]58	December 2022
5.188.86[.]195	December 2022
77.73.133[.]84	December 2022
89.108.65[.]136	December 2022
94.232.41[.]105	December 2022
47.87.229[.]39	January 2023
Malicious Domain	**Last Observed**
ciborkumari[.]xyz	October 2022
sombrat[.]com	October 2022
gororama[.]com	November 2022
softeruplive[.]com	November 2022
altocloudzone[.]live	December 2022
ciborkumari[.]xyz	December 2022
myappearinc[.]com	December 2022
parkerpublic[.]com	December 2022
pastebin.mozilla[.]org/Z54Vudf9/raw	December 2022
tumbleproperty[.]com	December 2022
myappearinc[.]com/acquire/draft/c7lh0s5jv	January 2023

Table 2: Tools used by Royal operators

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
Batch Scripts	
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

MITRE ATT&CK TECHNIQUES

See table 3 for all referenced threat actor tactics and techniques included in this advisory.

Table 3: Royal Actors ATT&CK Techniques for Enterprise

Initial Access		
Technique Title	**ID**	**Use**
Exploit Public Facing Application	T1190	The actors gain initial access through public-facing applications.
Phishing: Spear phishing Attachment	T1566.001	The actors gain initial access through malicious PDF attachments sent via email.
Phishing: Spearphishing Link	T1566.002	The actors gain initial access using malvertising links via emails and public-facing sites.
External Remote Services	T1133	The actors gain initial access through a variety of RMM software.
Command and Control		
Technique Title	**ID**	**Use**
Ingress Tool Transfer	T1105	The actors used C2 infrastructure to download multiple tools.
Protocol Tunneling	T1572	The actors used an encrypted SSH tunnel to communicate within C2 infrastructure.
Privilege Escalation		
Technique Title	**ID**	**Use**
Valid Accounts: Domain Accounts	T1078.002	The actors used encrypted files to create new admin user accounts.
Defense Evasion		
Technique Title	**ID**	**Use**
Impair Defenses: Disable or Modify Tools	T1562.001	The actors deactivated antivirus protocols.
Domain Policy Modification: Group Policy Modification	T1484.001	The actors modified Group Policy Objects to subvert antivirus protocols.

Indicator Removal: Clear Windows Event Logs	T1070.001	The actors deleted shadow files and system and security logs after exfiltration.
Remote Desktop Protocol	T1021.001	The actors used valid accounts to move laterally through the domain controller using RDP.
Automated Collection	T1119	The actors used registry keys to auto-extract and collect files.
Impact		
Technique Title	**ID**	**Use**
Data Encrypted for Impact	T1486	The actors encrypted data to determine which files were being used or blocked by other applications.

MITIGATIONS

FBI and CISA recommend network defenders apply the following mitigations to limit potential adversarial use of common system and network discovery techniques and to reduce the risk of compromise by Royal ransomware. These mitigations follow CISA's Cybersecurity Performance Goals (CPGs), which provide a minimum set of practices and protections that are informed by the most common and impactful threats, tactics, techniques, and procedures, and which yield goals that all organizations across critical infrastructure sectors should implement:

- **Implement a recovery plan** to maintain and retain multiple copies of sensitive or proprietary data and servers [CPG 7.3] in a physically separate, segmented, and secure location (i.e., hard drive, storage device, the cloud).
- **Require all accounts** with password logins (e.g., service account, admin accounts, and domain admin accounts) **to comply** with National Institute for Standards and Technology (NIST) standards for developing and managing password policies [CPG 3.4].
    - Use longer passwords consisting of at least 8 characters and no more than 64 characters in length [CPG 1.4].
    - Store passwords in hashed format using industry-recognized password managers.
    - Add password user "salts" to shared login credentials.
    - Avoid reusing passwords.
    - Implement multiple failed login attempt account lockouts [CPG 1.1].
    - Disable password hints.
    - Refrain from requiring password changes more frequently than once per year.
      Note: NIST guidance suggests favoring longer passwords instead of requiring regular and frequent password resets. Frequent password resets are more likely to result in users developing password patterns cyber criminals can easily decipher.

  - Require administrator credentials to install software.

- **Require multifactor authentication** [CPG 1.3] for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.
- **Keep all operating systems, software, and firmware up to date.** Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats.
- **Segment networks** [CPG 8.1]. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement.
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool.** To aid in detecting ransomware, implement a tool that logs and reports all network traffic [CPG 5.1], including lateral movement activity on a network. Endpoint detection and response (EDR) tools are useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.
- **Install, regularly update, and enable real time detection for antivirus software** on all hosts.
- **Review domain controllers, servers, workstations, and active directories** for new and/or unrecognized accounts.
- **Audit user accounts** with administrative privileges and configure access controls according to the principle of least privilege [CPG 1.5].
- **Disable unused ports.**
- **Consider adding an email banner to emails** [CPG 8.3] received from outside your organization.
- **Implement time-based access for accounts set at the admin level and higher.** For example, the Just-in-Time (JIT) access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the Zero Trust model). This is a process where a network-wide policy is set in place to automatically disable admin accounts at the Active Directory level when the account is not in direct need. Individual users may submit their requests through an automated process that grants them access to a specified system for a set timeframe when they need to support the completion of a certain task.
- **Disable command-line and scripting activities and permissions.** Privilege escalation and lateral movement often depend on software utilities running from the command line. If threat actors are not able to run these tools, they will have difficulty escalating privileges and/or moving laterally.
- **Maintain offline backups of data,** and regularly maintain backup and restoration [CPG 7.3]. By instituting this practice, the organization ensures they will not be severely interrupted, and/or only have irretrievable data.
- **Ensure all backup data is encrypted, immutable** (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure [CPG 3.3].

RESOURCES

- Stopransomware.gov is a whole-of-government approach that gives one central location for ransomware resources and alerts.
- Resource to mitigate a ransomware attack: CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide.
- No-cost cyber hygiene services: Cyber Hygiene Services and Ransomware Readiness Assessment.

REPORTING

FBI is seeking any information that can be shared, to include boundary logs showing communication to and from foreign IP addresses, a sample ransom note, communications with Royal actors, Bitcoin wallet information, decryptor files, and/or a benign sample of an encrypted file.

Additional details requested include: a targeted company Point of Contact, status and scope of infection, estimated loss, operational impact, transaction IDs, date of infection, date detected, initial attack vector, host and network based indicators.

FBI and CISA do not encourage paying ransom as payment does not guarantee victim files will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Regardless of whether you or your organization have decided to pay the ransom, FBI and CISA urge you to promptly report ransomware incidents to a local FBI Field Office, or CISA at https://www.cisa.gov/report.

DISCLAIMER

The information in this report is being provided “as is” for informational purposes only. CISA and FBI do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA or the FBI.

REFERENCES

[1] Royal Rumble: Analysis of Royal Ransomware (cybereason.com)

[2] DEV-0569 finds new ways to deliver Royal ransomware, various payloads - Microsoft Security Blog

[3] 2023-01: ACSC Ransomware Profile - Royal | Cyber.gov.au

ACKNOWLEDGEMENTS

Recorded Future, Coveware, Digital Asset Redemption, Q6, and RedSense contributed to this CSA.