Coauthored by:

Product ID: AA23-061A

November 13, 2023

#StopRansomware: Royal Ransomware Update

SUMMARY

Update November 13, 2023

This CSA is being re-released to add new TTPs, IOCs, and information related to Royal Ransomware activity.

End of Update

***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 June 2023.

Since approximately September 2022, cyber threat actors have compromised U.S. and international organizations with Royal ransomware. 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

U.S. organizations: 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.

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restrictions. For more information on the Traffic Light Protocol, see cisa.gov/tlp/.

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.

Update November 13, 2023

Since September 2022, Royal has targeted over 350 known victims worldwide and ransomware demands have exceeded 275 million USD. Royal conducts data exfiltration and extortion prior to encryption and then publishes victim data to a leak site if a ransom is not paid. Phishing emails are among the most successful vectors for initial access by Royal threat actors. There are indications that Royal may be preparing for a re-branding effort and/or a spinoff variant. Blacksuit ransomware shares a number of identified coding characteristics similar to Royal. A previous joint CSA for Royal ransomware was published on March 2, 2023. This joint CSA provides updated IOCs identified through FBI investigations.

End Update

FBI and CISA encourage organizations to implement the recommendations found in the Mitigations section of this CSA to reduce the likelihood and impact of ransomware incidents.

For a downloadable copy of IOCs, see:

- AA23-XXXA.stix (STIX, XXX kb).
- ***November 13, 2023***: AA23-XXXA.stix (STIX, XXX kb).

TECHNICAL DETAILS

Note: *This advisory uses the MITRE ATT&CK® for Enterprise framework, version 13. 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 several 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 threat actors gain initial access through exploiting public-facing applications [T1190].
- **Brokers.** Reports from trusted third-party sources indicate that Royal threat 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 a 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 within 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 observed multiple Qakbot C2s used in Royal ransomware attacks but is yet to determine if Royal ransomware exclusively uses Qakbot C2s.

Lateral Movement and Persistence

Royal threat actors often use RDP to move laterally across a network [T1021.001]. Microsoft's Sysinternals tool `PsExec` has also been used to aid lateral movement. FBI observed Royal threat 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 threat actors moved laterally to the domain controller. In one confirmed case, the threat 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 threat actors exfiltrate data from victim networks by repurposing legitimate cyber penetration testing 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 threat 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 threat 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 Tables 1 and 2 for Royal ransomware IOCs obtained by FBI during threat response activities as of January 2023.

Update November 13, 2023

See Tables 3 and 4 for Royal and Blacksuit Ransomware IOCs as of June 2023. See Table 5 for a list of legitimate software used by Royal and Blacksuit threat actors identified through FBI investigations as of June 2023.

End Update

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**
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

Update November 13, 2023

Table 3: Royal Ransomware Associated Files, Tools and Hashes as of June 2023

Name	Description
C:\Users\Public\conhost.exe client 149.28.73.161:443 R:149.28.73.161:43657:socks	Executed on the victim's machine, uses a Chisel client to tunnel traffic through port 443 instead of port 43657.
royal_w	Encryption extension
%PROGRAMDATA%	Ransomware Filepath
%TEMP%\execute.bat	
InstallerV20.8.msi	
Name	**SHA 256 Hash Value**
windows_encryptor.exe	85087f28a84205e344d7e8e06979e6622fab0cfe1759fd24e38cd0390bca5fa6

%PROGRAMDATA%\wine.exe	5b08c02c141eab94a40b56240a26cab7ff07e9a6e760dfde8b8b053a3526f0e6
%USERPROFILE%\Downloads\run1.bat	bc609cf53dde126b766d35b5bcf0a530c24d91fe23633dad6c2c59fd1843f781
%USERPROFILE%\Downloads\run2.bat	13c25164791d3436cf2efbc410caec6b6dd6978d7e83c4766917630e24e1af10
%USERPROFILE%\Downloads\run3.bat	2b93206d7a36cccdf7d7596b90ead301b2ff7e9a96359f39b6ba31bb13d11f45
%USERPROFILE%\Downloads\run4.bat	84e1efbed6bb7720caea6720a8bff7cd93b5d42fb1d71ef8031bfd3897ed4435
%USERPROFILE%\Downloads\sc.bat	e0dbe3a2d07ee10731b68a142c65db077cfb88e5ec5c8415e548d3ede40e7ffc
%USERPROFILE%\Downloads\sr.bat	34a98f2b54ebab999f218b0990665485eb2bb74babdf7e714cc10a306616b00c
runanddelete.bat	342b398647073159dfa8a7d36510171f731b760089a546e96fbb8a292791efee
InstallerV8.1.ms	3e6e2e0de75896033d91dfd07550c478590ca4cd4598004d9e19246e8a09cb97
f827.exe	5654f32a4f0f2e900a35761e8caf7ef0c50ee7800e0a3b19354b571bc6876f61
f24dc8ea.msi	91605641a4c7e859b7071a9841d1cd154b9027e6a58c20ec4cadafeaf47c9055
defw10.bat	fb638dba20e5fec72f5501d7e0627b302834ec5eaf331dd999763ee925cbc0f9
ll.exe	f0197bd7ccd568c523df9c7d9afcbac222f14d344312322c04c92e7968859726
Royal Ransomware Hash	b987f738a1e185f71e358b02cafa5fe56a4e3457df3b587d6b40e9c9de1da410
Name	**MD5 Hash Value**
b34v2.dll	a51b1f1f0636bff199c0f87e2bb300d42e06698b
1.exe	d93f1ef533e6b8c95330ba0962e3670eaf94a026
34.dll	9e19afc15c5781e8a89a75607578760aabad8e65
ll.exe	9a92b147cad814bfbd4632b6034b8abf8d84b1a5
Royal Ransomware Hash	a4ef01d55e55cebdd37ba71c28b0c448a9c833c0

Table 4: Blacksuit Ransomware Associated Files, Tools, and Hashes as of June 2023

Name	SHA-1 Hash Values
sys32.exe	30cc7724be4a09d5bcd9254197af05e9fab76455
esxi_encryptor	861793c4e0d4a92844994b640cc6bc3e20944a73

Royal and Blacksuit threat actors have been observed using legitimate software and open source tools during ransomware operations. Threat actors have been observed using open source network tunneling tools such as Chisel and Cloudflared, as well as Secure Shell (SSH) Client, OpenSSH, and MobaXterm to establish SSH connections. The publicly available credential stealing tool Mimikatz and password harvesting tools from Nirsoft have also been found on victim systems. Legitimate remote access tools AnyDesk, LogMein, and Atera Agent have also been observed as backdoor access vectors. Some legitimate software and open source tools can be found in Table 5.

Table 5: Legitimate Files and Tools Used by Royal and Blacksuit Ransomware

Name	Description
C:\Program Files\OpenSSH\ssh-agent.exe C:\Program Files\OpenSSH\sshd.exe	SSH Client
%USERPROFILE%\Downloads\WinRAR.exe	Compression tool
%APPDATA%\MobaXterm\	Toolbox for remote computing
\Program Files (x86)\Mobatek\	Toolbox for remote computing
\Program Files (x86)\Mobatek\MobaXterm\	Toolbox for remote computing
b34v2.dll	ColbaltStrike Beacon
34.dll	CobaltStrike Beacon
mimikatz.exe	Mimikatz credential harvester
dialuppass.exe	Nirsoft password harvesting utility
iepv.exe	Nirsoft password harvesting utility
mailpv.exe	Nirsoft password harvesting utility
netpass.exe	Nirsoft password harvesting utility
routerpassview.exe	Nirsoft password harvesting utility
AdFind.exe	ADFind tool
LogMeIn	Remote access tool
Atera	Remote access tool
C:\Program Files\Eraser\Eraser.exe	Anti-Forensics Tool used by TA

advanced_ip_scanner.exe	Reconnaissance Tool used by TA
Name	**SHA 256 Hash Value**
conhost.exe (chisel_windows_1_7_7.exe)	b9ef2e948a9b49a6930fc190b22cbdb3571579d37a4de56564e41a2ef736767b
%USERPROFILE%\Downloads\svvhost.exe \Users\Administrator\AppData\Local\Temp\cloudflared.exe	c429719a45ca14f52513fe55320ebc49433c729a0d2223479d9d43597eab39fa
nsudo.exe	19896a23d7b054625c2f6b1ee1551a0da68ad25cddbb24510a3b74578418e618

End Update

MITRE ATT&CK TECHNIQUES

See table 6 for all referenced threat actor tactics and techniques included in this advisory.

Table 6: 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: Spear phishing 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 Services: 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, TTPs, and yield goals that all organizations across critical infrastructure sectors should implement.

> These mitigations apply to all critical infrastructure organizations and network defenders. FBI and CISA recommend that software manufactures incorporate secure-by-design and -default principles and tactics into their software development practices limiting the impact of ransomware techniques (such as threat actors leveraging backdoor vulnerabilities into remote software systems) thus strengthening the security posture for their customers.
>
> For more information on secure by design, see CISA's Secure by Design webpage and joint guide.

- **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, or the cloud).
- **Require all accounts** with password logins (e.g., service account, admin accounts, and domain admin accounts) **to comply** with the National Institute for Standards and Technology's (NIST's) 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.
- **Reduce the threat of malicious actors** using remote access tools by applying mitigations in joint Guide to Securing Remote Access Software.
- **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 (PoLP) [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 PoLP (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's and Multi-State Information Sharing and Analysis Center's (MS-ISAC's) joint Ransomware Guide.
  Note: The joint Ransomware Guide provides preparation, prevention, and mitigation best practices as well as a ransomware response checklist.

- 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 threat 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, and 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 threat 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 the FBI's Internet Crime Complaint Center (IC3) at Ic3.gov, a local FBI Field Office, or CISA via the agency's Incident Reporting System or its 24/7 Operations Center at report@cisa.gov or (888) 282-0870.

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. CISA and FBI do not endorse any commercial entity, product, company or service, including any entities, products, or services linked within this document's subjects. Any reference to specific commercial entities, 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.

VERSION HISTORY

March 02, 2023: Initial version.

November 13, 2023: Updates noted throughout.