Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Royal Ransomware Targets Organizations with Custom Encryption and Double Extortion Tactics

Date of Publication

March 3, 2023

Admiralty Code

A1

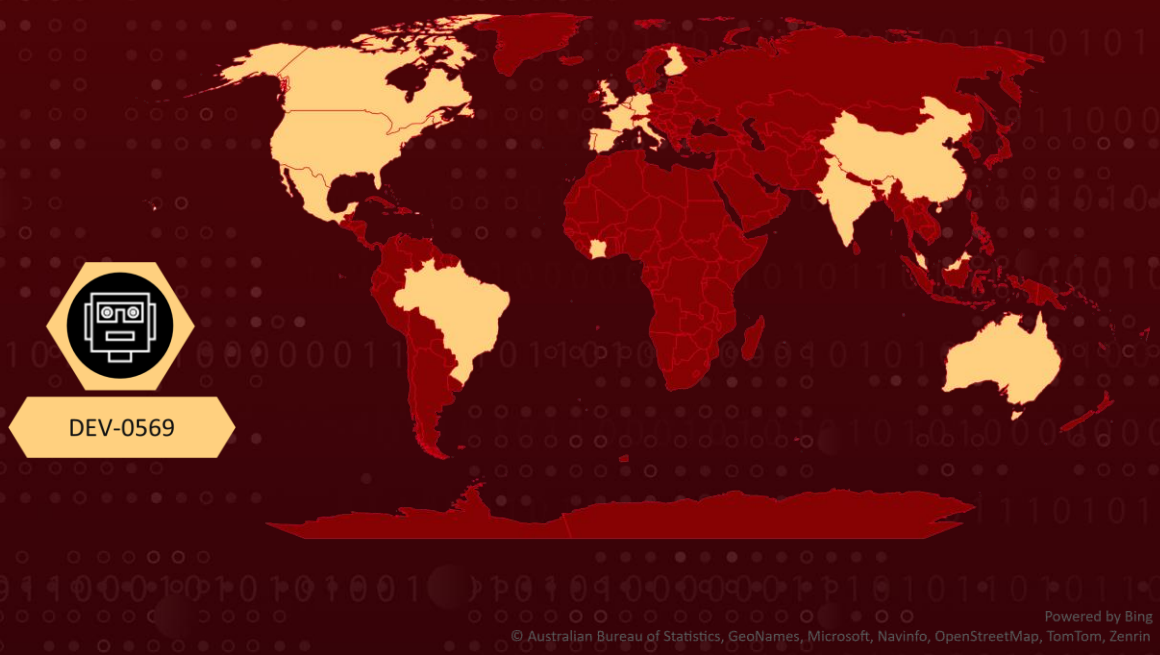
TA Number

TA2023116

Summary

Attack Begin: September 2022
Affected Industry: Industrial, Engineering, Transportation, Education, Retail, Government, Aerospace, Defense, Gas Utilities, Food Products, Consumer, Pharmaceuticals, Automotive, Legal, Renewable Electricity, Insurance, Airlines, Media, Financial, Technology, Storage & Peripherals, HealthCare, Hotels, Real estate, Telecommunications, Building Materials, Electrical Equipment, Banks, Manufacturing
Attack Countries: France, Spain, United States, Brazil, Mexico, India, Germany, Italy, Canada, Australia, Portugal, United Kingdom, Netherlands, China, Trinidad and Tobago, Belgium, Puerto Rico, Finland, Cote d'Ivoire, Malaysia
Threat Actor: DEV-0569
Attack: Royal ransomware uses custom encryption and double extortion tactics to target organizations since Sep 2022, gaining access via phishing or RDP, and using RDP, PsExec and legitimate tools for lateral movement and data exfiltration.

Attack Regions



Attack Details

#1 Since September 2022, threat actors have been attacking both US and international organizations using a version of ransomware called Royal. This ransomware is unique because it employs a custom-made file encryption program and uses double extortion tactics. This involves threatening to release encrypted data publicly if the victim does not pay a ransom, which ranges from $1 million to $11 million USD in Bitcoin.

#2 The Royal ransomware partially encrypts files by selecting a specific percentage of data in a file, which allows cybercriminals to lower the encryption percentage for larger files to avoid detection. The actors often gain initial access through phishing emails or RDP compromise. Once they have gained access, they communicate with a command-and-control infrastructure and download multiple tools.

#3 To move laterally across the network, the Royal ransomware actors frequently use RDP and the Microsoft Sysinternals tool PsExec. Remote monitoring and management (RMM) software is used to persist in the victim's network. They often use legitimate pen-testing and malware tools and derivatives to exfiltrate data. In the past, this ransomware was deployed by a threat actor known as DEV-0569.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
TA0010 Exfiltration	TA0040 Impact	T1016 System Network Configuration Discovery	T1021 Remote Services
T1021.001 Remote Desktop Protocol	T1027 Obfuscated Files or Information	T1036 Masquerading	T1046 Network Service Discovery
T1057 Process Discovery	T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1059.003 Windows Command Shell
T1059.005 Visual Basic	T1070 Indicator Removal	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
T1105 Ingress Tool Transfer	T1119 Automated Collection	T1133 External Remote Services	T1135 Network Share Discovery
T1189 Drive-by Compromise	T1190 Exploit Public-Facing Application	T1195 Supply Chain Compromise	T1204 User Execution
T1204.002 Malicious File	T1218 System Binary Proxy Execution	T1218.005 Mshta	T1218.007 Msiexec
T1219 Remote Access Software	T1484 Domain Policy Modification	T1484.001 Group Policy Modification	T1486 Data Encrypted for Impact
T1489 Service Stop	T1490 Inhibit System Recovery	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder

T1558 Steal or Forge Kerberos Tickets	T1562 Impair Defenses	T1562.001 Disable or Modify Tools	T1566 Phishing
T1566.001 Spearphishing Attachment	T1566.002 Spearphishing Link	T1567 Exfiltration Over Web Service	T1569 System Services
T1569.002 Service Execution	T1572 Protocol Tunneling	T1574 Hijack Execution Flow	T1584 Compromise Infrastructure
T1587 Develop Capabilities	T1587.001 Malware	T1593 Search Open Websites/Domains	T1593.002 Search Engines
T1608 Stage Capabilities	T1608.001 Upload Malware		

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	102.157.44[.]105 105.158.118[.]241 105.69.155[.]85 113.169.187[.]159 134.35.9[.]209 139.195.43[.]166 139.60.161[.]213 148.213.109[.]165 163.182.177[.]80 181.141.3[.]126 181.164.194[.]228 185.143.223[.]69 186.64.67[.]6 186.86.212[.]138 190.193.180[.]228 196.70.77[.]11 197.11.134[.]255 197.158.89[.]85 197.204.247[.]7 197.207.181[.]147 197.207.218[.]27 197.94.67[.]207

TYPE	VALUE
IPV4	23.111.114[.]52 41.100.55[.]97 41.107.77[.]67 41.109.11[.]80 41.251.121[.]35 41.97.65[.]51 42.189.12[.]36 45.227.251[.]167 5.44.42[.]20 61.166.221[.]46 68.83.169[.]91 81.184.181[.]215 82.12.196[.]197 98.143.70[.]147 140.82.48[.]158 147.135.36[.]162 147.135.11[.]223 152.89.247[.]50 172.64.80[.]1 179.43.167[.]10 185.7.214[.]218 193.149.176[.]157 193.235.146[.]104 209.141.36[.]116 45.61.136[.]47 45.8.158[.]104 5.181.234[.]58 5.188.86[.]195 77.73.133[.]84 89.108.65[.]136 94.232.41[.]105 47.87.229[.]39
Domains	ciborkumari[.]xyz sombrat[.]com gororama[.]com softeruplive[.]com altocloudzone[.]live ciborkumari[.]xyz myappearinc[.]com parkerpublic[.]com pastebin.mozilla[.]org/Z54Vudf9/raw tumbleproperty[.]com myappearinc[.]com/acquire/draft/c7lh0s5jv

TYPE	VALUE
SHA256	8a983042278bc5897dbcdd54d1d7e3143f8b7ead553b5a4713e30deffda16375 8a99353662ccae117d2bb22efd8c43d7169060450be413af763e8ad7522d2451 be030e685536eb38ba1fec1c90e90a4165f6641c8dc39291db1d23f4ee9fa0b1 b8c4aec31c134adbdbe8aad65d2bcb21cfe62d299696a23add9aa1de082c6e20 4a9dde3979c2343c024c6eeeddff7639be301826dd637c006074e04a1e4e9fe7 4cd00234b18e04dcd745cc81bb928c8451f6601affb5fa45f20bb11bfb5383ce 08c6e20b1785d4ec4e3f9956931d992377963580b4b2c6579fd9930e08882b1c f8cff7082a936912baf2124d42ed82403c75c87cb160553a7df862f8d81809ee d47d4b52e75e8cf3b11ea171163a66c06d1792227c1cf7ca49d7df60804a1681 216047c048bf1dcbf031cf24bd5e0f263994a5df60b23089e393033d17257cb5 19896a23d7b054625c2f6b1ee1551a0da68ad25cddbb24510a3b74578418e618 82f1f72f4b1bfd7cc8afbe6d170686b1066049bc7e5863b51aa15ccc5c841f58 74d81ef0be02899a177d7ff6374d699b634c70275b3292dbc67e577b5f6a3f3c 342b398647073159dfa8a7d36510171f731b760089a546e96fbb8a292791efee
SHA1	585b05b290d241a249af93b1896a9474128da96941a79f83f8b00ac7a9dd06e1e225d64d95d29b1da84ed0f3c46b01d66510ccc9b1fc1e07af005c60 c96154690f60a8e1f2271242e458029014ffe30a65dc04f3f75deb3b287cca3138d9d0ec36b8bea0

Recent Breaches

www.unisco.com

www.ancora.com.br

www.dallas.k12.or.us

www.evansonline.com

www.delallo.com

Recent Breaches

www.trendsetterengineering.com

www.ics-nett.com

www.casaley.com.mx

www.servicemasterclr.com

www.traviscountytx.gov

www.ioccompany.com

www.pillar.ca

www.kazcolaw.com

www.carinya.nsw.edu.au

www.livingstonintl.com

www.autodelta.pt

www.hills-motors.co.uk

www.fh-zwickau.de

www.samuelsseafood.com

www.ruhrpumpen.com

www.tasupply.com

www.lvcdlaw.com

www.reventics.com

www.tusd1.org

www.lunainc.com

References

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a

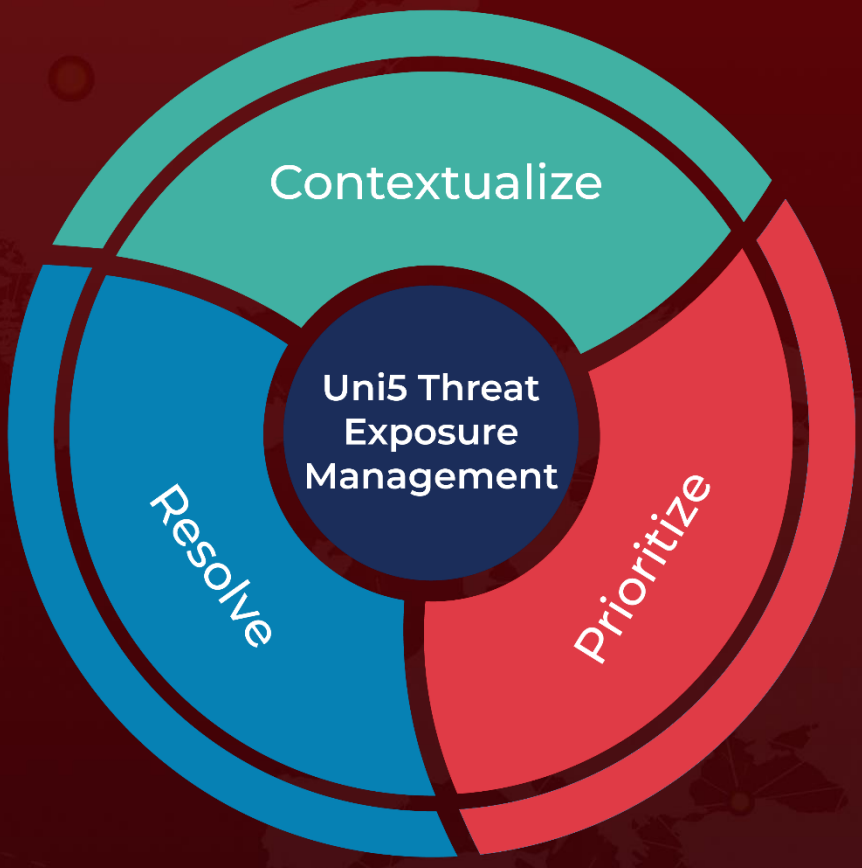
https://www.cybereason.com/blog/royal-ransomware-analysis

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

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 3, 2023 . 2:50 AM

More at www.hivepro.com