Everything You Need to Know About Royal Ransomware

avertium.com/resources/threat-reports/everything-you-need-to-know-about-royal-ransomware

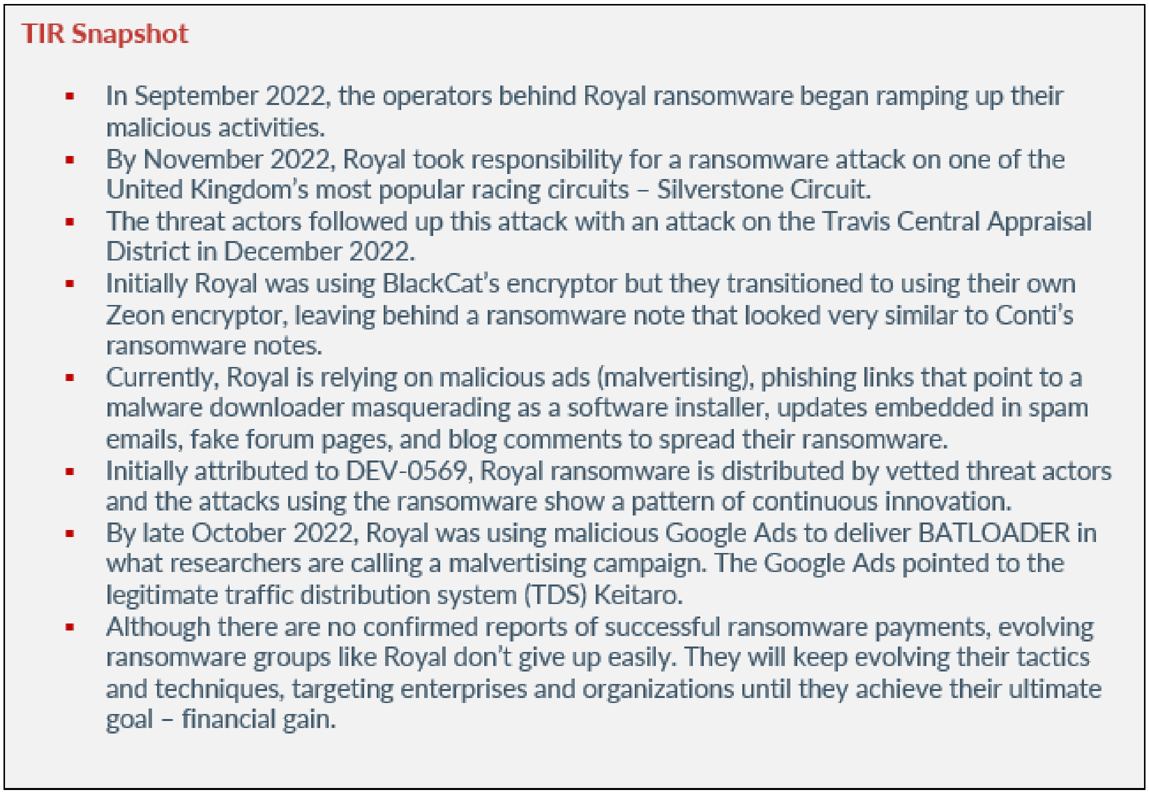
KNOW THY SELF. KNOW THY ENEMY:
Avertium
Threat Intelligence Report
EVERYTHING YOU NEED TO KNOW ABOUT ROYAL RANSOMWARE

Executive Summary

After emerging in January 2022, Royal ransomware is a ransomware strain that is being distributed by ransomware threat actors from previous operations. Initially, Microsoft attributed the distribution of Royal ransomware to DEV-0569 – a temporary name given by the tech company. Now, researchers are stating that the threat actors behind Royal ransomware have officially branded themselves with the name Royal (the name left behind in recent ransomware notes) and they are primarily focused on targeting entities within the U.S

The ransomware operation uses unusual techniques to breach networks before encrypting them with malware and demanding ransom payments. Some Royal ransomware campaigns distribute the malware via malicious attachments, and some distribute the malware via malicious advertisements.

Although Royal is a newer ransomware operation, researchers believe the threat actors behind it are very experienced due to evidence of previously seen tactics and techniques. Let’s take a look at Royal, their tactics and techniques, and what organizations can do to protect themselves and keep their cyber environments safe.



TIR Snapshot

- In September 2022, the operators behind Royal ransomware began ramping up their malicious activities.
- By November 2022, Royal took responsibility for a ransomware attack on one of the United Kingdom's most popular racing circuits – Silverstone Circuit.
- The threat actors followed up this attack with an attack on the Travis Central Appraisal District in December 2022.
- Initially Royal was using BlackCat's encryptor but they transitioned to using their own Zeon encryptor, leaving behind a ransomware note that looked very similar to Conti's ransomware notes.
- Currently, Royal is relying on malicious ads (malvertising), phishing links that point to a malware downloader masquerading as a software installer, updates embedded in spam emails, fake forum pages, and blog comments to spread their ransomware.
- Initially attributed to DEV-0569, Royal ransomware is distributed by vetted threat actors and the attacks using the ransomware show a pattern of continuous innovation.
- By late October 2022, Royal was using malicious Google Ads to deliver BATLOADER in what researchers are calling a malvertising campaign. The Google Ads pointed to the legitimate traffic distribution system (TDS) Keitaro.
- Although there are no confirmed reports of successful ransomware payments, evolving ransomware groups like Royal don't give up easily. They will keep evolving their tactics and techniques, targeting enterprises and organizations until they achieve their ultimate goal – financial gain.

royal ransomware attacks

SILVERESTONE CIRCUIT

In September 2022, the operators behind Royal ransomware began ramping up their malicious activities. They were observed by our technology partner, AdvIntel, utilizing other ransomware operation's encryptors, such as BlackCat.

By November 2022, Royal took responsibility for a ransomware attack on one of the United Kingdom's most popular racing circuits – Silverstone Circuit. The attack held up dozens of Formula One races and motorcycle events. Details regarding the attack were not disclosed, but Emsisoft threat analyst Brett Callow stated that because Royal's ransomware is secure, its encryption cannot be broken. Callow also stated that unlike current ransomware groups, Royal uses multiple ransomware types and uses **the .Royal** extension for encrypted files rather than using randomly generated extensions.

TRAVIS CENTRAL APPRAISAL DISTRICT

The threat actors followed up this attack with an attack on the Travis Central Appraisal District in December 2022. The agency provides appraisal values for properties. As a result of the attack, the agency's servers, website, and email were shut down for more than two weeks. However, because the agency diversified where its information was stored, it was able to continue operations.

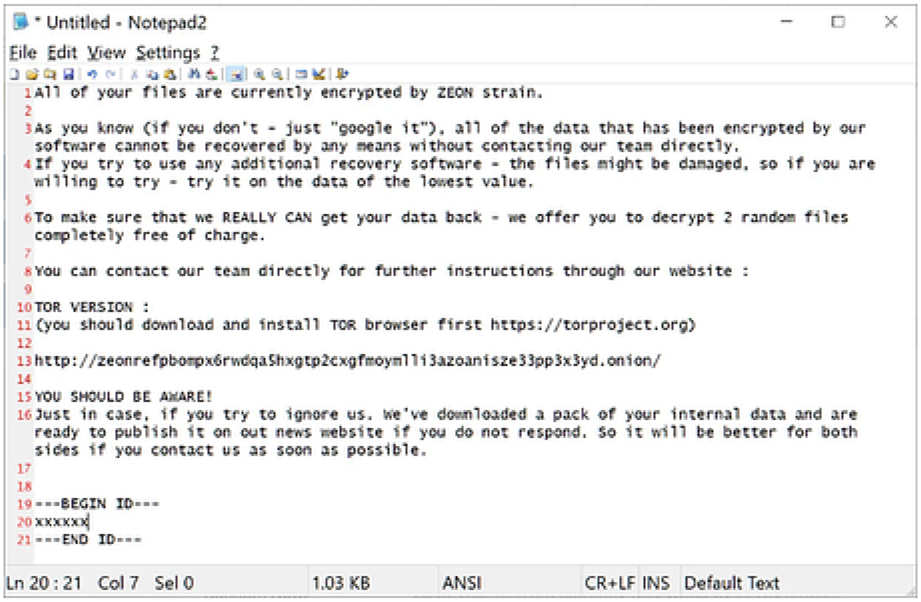
HC3

Also in December 2022, the Department of Health and Human Services Cybersecurity Coordination Center (HC3) warned that Royal based ransomware attacks were steadily increasing. Ransom demands from the threat actor ranged from $250,000 to more than $2 million. HC3 also stated that Royal should be considered a threat to the health and public health sectors due to the ransomware group victimizing the healthcare community.

Initially Royal was using BlackCat's encryptor but they transitioned to using their own Zeon encryptor, leaving behind a ransomware note that looked very similar to Conti's ransomware notes. If you recall, Conti was notorious for targeting the healthcare sector as well. The threat actors behind the Zeon encryptor were seen impersonating healthcare patient data software back in October 2022.

Avertium's technology partner, AdvIntel confirmed that the attackers contacted healthcare employees of targeted organizations and gained access via the Zoho remote access tool. Since the middle of September 2022, Royal has been using their branded name in their ransom notes generated by a new encryptor.

Image 1: A Zeon Ransomware Note



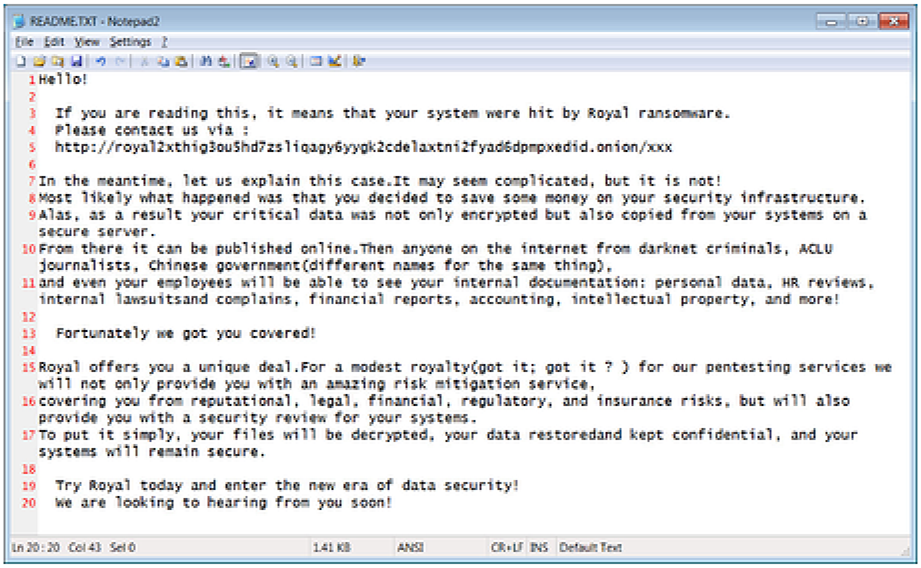
```
All of your files are currently encrypted by ZEON strain.

As you know (if you don't - just "google it"), all of the data that has been encrypted by our
software cannot be recovered by any means without contacting our team directly.
If you try to use any additional recovery software - the files might be damaged, so if you are
willing to try - try it on the data of the lowest value.

To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files
completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://zeonrefpbompx6rwdqa5hxgtp2cxgfmoymlli3azoanisze33pp3x3yd.onion/

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are
ready to publish it on out news website if you do not respond. So it will be better for both
sides if you contact us as soon as possible.


---BEGIN ID---
xxxxxx
---END ID---
```

Source: Bleeping Computer

Currently, Royal is relying on malicious ads (malvertising), phishing links that point to a malware downloader masquerading as software installers, updates embedded in spam emails, fake forum pages, and blog comments to spread their ransomware. The group's phishing attacks include callback phishing where they impersonate food delivery and software providers in emails that look like subscription renewals. The phishing emails contain phone numbers that the victim must contact to cancel the "subscription". Once the victim calls the number, they speak to threat actors who use social engineering to convince the victim to install remote access software. This remote access software is used to gain initial access to corporate networks.

Royal does not have a data leak site and they are not a ransomware-as-a-service (RaaS) with affiliates. Also, the group is low key and does not announce their attacks. The ransom note left behind is named **README.TXT** and contains a link to a private Tor negotiation page. The negotiation page consists of a chat screen for communication with Royal ransomware operators. Sometimes, Royal will decrypt a few files to prove to their victims that their decryptor works. They will also share file lists of stolen data at times.

Image 2: Royal's Newly Branded Ransomware Note



```
Hello!

  If you are reading this, it means that your system were hit by Royal ransomware.
  Please contact us via :
  http://royal2xthig3ou5hd7zsliqagy6yygk2cdelaxtni2fyad6dpmpxedid.onion/xxx

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!
```

Source: Bleeping Computer

royal/dev-0569 tactics & techniques

As previously stated, Royal ransomware emerged in January 2022, but their attacks were not noticed by security researchers until September 2022. Initially attributed to DEV-0569, Royal ransomware is distributed by vetted threat actors and the attacks using the ransomware show a pattern of continuous innovation. Royal has displayed a consistent incorporation of new defense evasion, techniques, and various post-compromise payloads.

Since Royal emerged, the ransomware operators have evolved their delivery methods to include:

- Using Google Ads in a campaign to blend in with normal ad traffic.
- Making malicious downloads appear authentic by hosting fake installer files on legitimate looking software download sites.
- Using contact forms located on an organization’s website to distribute phishing links.

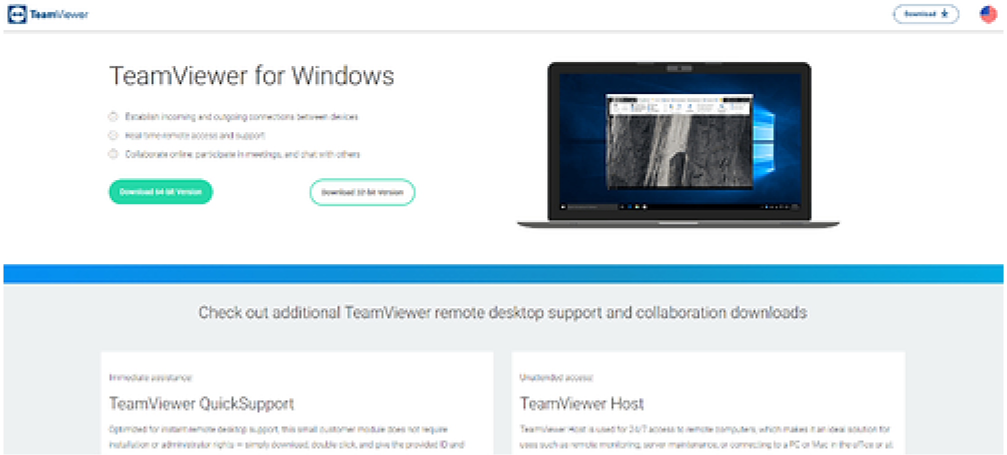
The above methods have allowed the ransomware operators to reach a greater number of targets and achieve their goal of deploying various post-compromise payloads. Microsoft stated that Royal uses signed binaries and delivers encrypted malware payloads – relying heavily on defense evasion techniques.

The group has also continued to use *Nsudo*, an open-source tool, to try and disable antivirus solutions. As previously stated, Royal has a few ways of gaining initial access and one of those ways is via malicious links delivered to their targets. The links are embedded in advertisements, fake forum pages, phishing emails, and blog comments. After the victim clicks, the links lead them to malicious files signed by Royal using a legitimate certificate.

The malicious files masquerade as installers or updates for applications such as Zoom or Microsoft teams. The victim does not know that the files are malware downloaders known as BATLOADER. When the legitimate applications are launched, BATLOADER uses MSI Custom Actions to launch malicious PowerShell activity. BATLOADER also uses the MSI Custom Actions to run batch scripts that attempt to disable security solutions, leading to the delivery of various encrypted malware payloads.

Between August and October 2022, Royal's observed activity included BATLOADER being hosted on attacker-created domains masquerading as software download sites such as *anydeskos[.]com*, and on legitimate repositories such as OneDrive and GitHub.

Image 3: BATLOADER Masquerading as a TeamViewer Installer



TeamViewer for Windows

- Establish incoming and outgoing connections between devices
- Real-time remote access and support
- Collaborate online, participate in meetings, and chat with others

Check out additional TeamViewer remote desktop support and collaboration downloads

Immediate assistance:

TeamViewer QuickSupport

Optimized for instant remote desktop support, this small customer module does not require installation or administrator rights — simply download, double click, and give the provided ID and

Unattended access:

TeamViewer Host

TeamViewer Host is used for 24/7 access to remote computers, which makes it an ideal solution for uses such as remote monitoring, server maintenance, or connecting to a PC or Mac in the office or at

Source: Microsoft

In addition to using installer files, Royal uses file formats such as Virtual Hard Disk (VHD) to impersonate legitimate software for first-stage payloads. Royal also uses various infection chains that use PowerShell and batch scripts, ultimately leading to the download of malware payloads such as a legitimate remote management tool used for persistence on the network. The management tool also acts as an access point for the staging and spreading of ransomware.

By late October 2022, Royal was using malicious Google Ads to deliver BATLOADER in what researchers are calling a malvertising campaign. The Google Ads pointed to the legitimate traffic distribution system (TDS) Keitaro. According to Microsoft, Keitaro provides capabilities to customize advertising campaigns via tracking and ad traffic and user or device-based filtering. The TDS redirects the victim to a legitimate download site or to a malicious BATLOADER download site. By using Keitaro, Royal can filter traffic and avoid IP ranges of known security sandboxing solutions.

what organizations can do

Although there are no confirmed reports of successful ransomware payments between Royal and their victims, evolving ransomware groups like Royal don't give up easily. They will keep evolving their tactics and techniques, targeting enterprises and organizations until they achieve their ultimate goal – financial gain. Fortunately, there are ways organizations can stay safe and protect themselves from Royal:

- Enabling Microsoft Defender for Office 365 will help guard against phishing by inspecting the body of emails and URLs for patterns.
- Royal's phishing campaigns abuses legitimate services; therefore, organizations should leverage mail flow rules and capture suspicious keywords or review broad exceptions such as those related to domain-level allow lists and IP ranges.
- Also, enabling Safe Links for Microsoft Teams, emails, and Office Apps will also help keep your organization safe.
- User awareness training regarding email threats and social engineering will help build resilience against Royal. After training, provide users with a method for reporting a suspected attack.
- Organizations should maintain credential hygiene and practice the principle of least privilege. This means that an organization should provide access a user absolutely needs to do their job. Organizations should also ensure that the accounts have strong passwords and multifactor authentication.
- To prevent threat actors from stopping security services, organizations should turn on tamper-protection features.

Making sure that your organization takes proactive measures by keeping track of Indicators of Compromise (IoCs) and by keeping track of Royal's attack methods will ensure good defense against Royal ransomware.

How Avertium is Protecting Our CUSTOMERS

It's important to get ahead of the curve by being proactive with protecting your organization, instead of waiting to put out a massive fire. **Avertium offers the following services to keep your organization safe:**

- Expanding endpoints, cloud computing environments, and accelerated digital transformation have decimated the perimeter in an ever-expanding attack surface. Avertium's offers **Attack Surface Management**, so you'll have no more blind spots, weak links, or fire drills.

- **Fusion MXDR** is the first MDR offering that fuses together all aspects of security operations into a living, breathing, threat-resistant XDR solution. By fusing insights from threat intelligence, security assessments, and vulnerability management into our MDR approach, Fusion MXDR offers a more informed, robust, and cost-effective approach to cybersecurity – one that is great than the sum of its parts.

- Avertium offers **VMaaS** to provide a deeper understanding and control over organizational information security risks. If your enterprise is facing challenges with the scope, resources, or skills required to implement a vulnerability management program with your team, outsourced solutions can help you bridge the gap.

- Avertium offers **Zero Trust Architecture**, like AppGate, to stop malware lateral movement.

- Avertium offers **user awareness training** through KnowBe4**.** The service also includes Incident Response Table-Top exercises (IR TTX) and Core Security Document development, as well as a comprehensive new-school approach that integrates baseline testing using mock attacks.

avertium's recommendations

The FBI, CISA, and HHS urge all organizations to apply the following recommendations to prepare for, mitigate/prevent, and respond to ransomware incidents:

- Review the security posture of third-party vendors and those interconnected with your organization. Ensure all connections between third-party vendors and outside software or hardware are monitored and reviewed for suspicious activity.

- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (i.e., hard drive, storage device, the cloud).

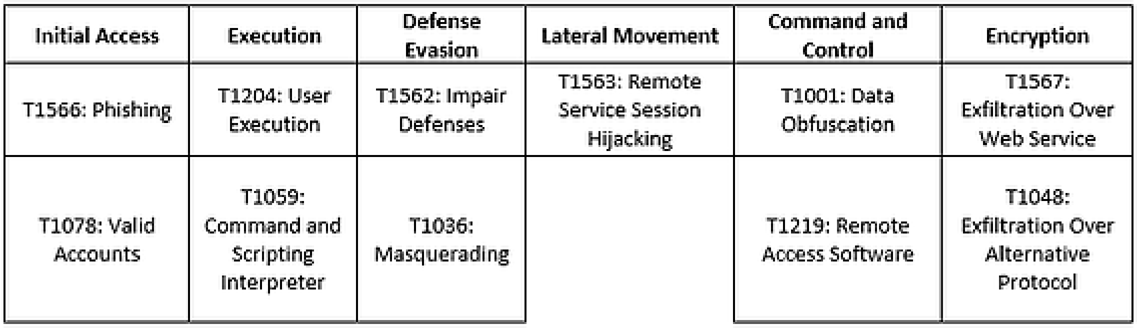
- Require all accounts with password logins (e.g., service account, admin accounts, and domain admin accounts) to comply with National Institute of Standards and Technology (NIST) standards for developing and managing password policies.

- Review domain controllers, servers, workstations, and active directories for new and/or unrecognized accounts.
- Segment networks to prevent the spread of ransomware. 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.

- Consider adding an email banner to emails received from outside your organization.

- 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.

MITRE Map



Initial Access	Execution	Defense Evasion	Lateral Movement	Command and Control	Encryption
T1566: Phishing	T1204: User Execution	T1562: Impair Defenses	T1563: Remote Service Session Hijacking	T1001: Data Obfuscation	T1567: Exfiltration Over Web Service
T1078: Valid Accounts	T1059: Command and Scripting Interpreter	T1036: Masquerading		T1219: Remote Access Software	T1048: Exfiltration Over Alternative Protocol

Indicators of Compromise (IoCs)

Hashes

- 01492156ce8b4034c5b1027130f4cf4e

- afd5d656a42a746e95926ef07933f054
- 04028a0a1d44f81709040c31af026785209d4343
- 6b0deb67a178fe20e81691133b257df3bafa3006
- 2598e8adb87976abe48f0eba4bbb9a7cb69439e0c133b21aee3845dfccf3fb8f
- 9db958bc5b4a21340ceeeb8c36873aa6bd02a460e688de56ccbba945384b1926

Supporting Documentation

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

HHS warns Royal ransomware threat targeting healthcare providers | SC Media (scmagazine.com)

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

Popular UK motor racing circuit investigating ransomware attack - The Record by Recorded Future

This sneaky ransomware gang keeps changing tactics to spread its malware | ZDNET

Microsoft: Royal ransomware group using Google Ads in campaign - The Record by Recorded Future

Microsoft Warns of Cybercrime Group Delivering Royal Ransomware, Other Malware | SecurityWeek.Com

Travis Central Appraisal District hit with ransomware, officials say (statesman.com)

H-ISAC TLP Green Threat Bulletin: Zeon Threat Group Impersonating Healthcare Patient Data Software Solutions | AHA

202212071400_Royal Ransomware Analyst Note_TLPCLEAR (hhs.gov)

APPENDIX II: Disclaimer

This document and its contents do not constitute, and are not a substitute for, legal advice. The outcome of a Security Risk Assessment should be utilized to ensure that diligent measures are taken to lower the risk of potential weaknesses be exploited to compromise data.

Although the Services and this report may provide data that Client can use in its compliance efforts, Client (not Avertium) is ultimately responsible for assessing and meeting Client's own compliance responsibilities. This report does not constitute a guarantee or assurance of Client's compliance with any law, regulation or standard.

Related Resource: 2023 Cybersecurity Landscape: 8 Lessons for Cybersecurity Professionals