



CYBER CONSIDERATIONS

- Inventory, map & update all your equipment, systems, and networks
- Segmented/offline back up of your data and systems
- Reduce Exposure to the Public-Facing Internet and Remote Access
- Change Default Passwords Immediately
- Delete old or inactive accounts (previous employees, etc.)
- Develop and Exercise Cybersecurity Incident Response and Recovery Plans
- Train your employees in cyber hygiene, phishing scams, etc.

Have a Cyber Incident Response Plan

Spear Phishing Tests

Royal Ransomware

Hello!

If you are reading this, it means that your system were hit by Royal ransomware.

Please contact us via:

<http://>

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 lawsuits and 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 restored and 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!



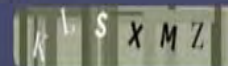
Royal

Contact from

Email

Message

Captcha



Submit

Royal Ransomware



- Compromised several appraisal districts, school districts, and county governments in Texas
- Access point is through spear phishing emails
- Encrypts data and asks for a ransom between 1 to 11 million dollars
- Will publish victim's data if ransom not paid
- One appraisal district paid approximately \$170,000 and a school district paid over \$500,000 in crypto currency to regain data access
- Back up data/files can also be encrypted
- As of 2022, has made over 275 million dollars in ransom demands

AKIRA

Well, you are here. It means that you're suffering from cyber incident right now. Think of our actions as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that there is a fair price to make it all go away.

Do not rush to assess what is happening - we did it to you. The best thing you can do is to follow our instructions to get back to your daily routine, by cooperating with us you will minimize the damage that might be done.

Those who choose different path will be shamed here publicly. The functionality of this blog is extremely simple - enter the desired command in the input line and enjoy the juiciest information that corporations around the world wanted to stay confidential.

Remember. You are unable to recover without our help. Your data is already gone and cannot be traced to the place of final storage nor deleted by anyone besides us.

```
guest@akira:~$ help
```

```
List of all commands:
```

```
leaks      - hacked companies
news       - news about upcoming data releases
contact    - send us a message and we will contact you
help       - available commands
clear      - clear screen
```

```
guest@akira:~$ █
```

AKIRA Ransomware



- Targeted organizations located in North America, UK and Europe in the government, manufacturing, technology, education, consulting, pharmaceuticals, and telecommunication sectors.
- Access point is through spear phishing emails or vulnerable software
- Has also used stolen credentials and brute-force password attacks
- Steals and encrypts data and has received more than 244 million dollars in ransom proceeds
- Back up data/files can also be encrypted

The Regulator & The Help

Federal Trade Commission (FTC)



Department of Homeland Security –
Cybersecurity and Infrastructure Security
(CISA)



Investigators - 18 U.S. Code § 1030

Federal Bureau of Investigation (FBI)



United States Secret Service (USSS)

DHS Homeland Security Investigations (HSI)



**KEY
TAKEAWAYS**

1. What part of our network is open to the public facing internet and remote access? How is it secured?
2. What systems are not running on the latest updated version and how often are these updates conducted?
3. Is our data segmented and do we have an offline back up of our data and operating systems? If so, how does it work?
4. Do we have a Cyber Incident Response Plan and when was the last time we practiced it?
5. Do we have reoccurring cyber training for our employees? Do we conduct E-mail spear phishing tests?

Resources & Reporting

Internet Crime and Complaint Center (IC3)

www.ic3.gov

DHS CISA

<https://www.cisa.gov/>

InfraGard

<https://www.infragard.org/>

