

Your experience of a ransomware attack

Please answer the following questions regarding your experience of a ransomware attack. By answering the questionnaire you participate in our research that helps to gain a better understanding of ransomware attacks and thus prevent future attacks. Only statistical information will be gathered from this questionnaire and all participants are kept anonymous. Participation in the questionnaire is voluntary and participants are free to withdraw at any point without prejudice and without providing a reason. All data will be destroyed at the end of the project and handled according to the Data Protection Act (DPA) 1998. We are researchers at The University of Kent undertaking a project called "Ransomware Deployment Methods and Analysis". Should you have any queries or would like to contact us, please do. Henna John hsj4@kent.ac.uk or Gavin Hull gjh9@kent.ac.uk Thank you!

* Required

1. I agree to the above statement *

Check all that apply.

Yes

Basic information

2. Are you familiar with the term 'ransomware'?

Mark only one oval.

Yes

No

Maybe

3. Have you experienced a situation where your screen or files were locked and a message appeared demanding a payment? This may have occurred using a computer or a smart phone. *

Mark only one oval.

Yes *Skip to question 4.*

No *Stop filling out this form.*

General attack details

Please fill in more information about the time when hackers demanded payment to free your files or computer screen.

4. When did the attack take place? (approx.) *

Example: December 15, 2012

5. What operating system (OS) were you using at the time? *

Mark only one oval.

- Windows 10
- Windows 8
- Windows 7
- Windows XP
- MacOS
- Linux
- FreeBSD
- Android
- iOS
- Other: _____

6. What were you doing prior to the attack? *

Mark only one oval.

- Browsing the internet *Skip to question 7.*
- Downloading some new software *Skip to question 12.*
- Viewing or editing photos or videos *Skip to question 14.*
- Playing computer games *Skip to question 17.*
- Programming software or configuring hardware, such as routers *Skip to question 20.*
- Reading/writing emails using a stand-alone email client *Skip to question 9.*
- Other: _____ *Skip to question 20.*

Skip to question 20.

Visiting a website

7. What was the name of the browser you used?

8. What was the website you had visited?

Skip to question 20.

Reading an email

9. What did you do with that email? *

Mark only one oval.

- Clicked on a link *Skip to question 7.*
- Opened its attachment *Skip to question 10.*
- None of the above *Skip to question 20.*
- Other: _____ *Skip to question 20.*

Skip to question 20.

Email attachment

If you can remember the extension of the file in the attachment, or type of file, please state here.

10. What was the extension of the attachment e.g. .doc, .zip, or type of the file in the email? *

11. After downloading the attachment, did you open it? *

Mark only one oval.

- Yes
- No

Skip to question 20.

Downloaded software

12. What was software you downloaded called? *

13. Where did you download it from?

Skip to question 7.

Editing photos or videos

14. What software were you using?

15. Was it a new software package you recently downloaded? *

Mark only one oval.

- Yes*
- No

16. ***Name the website you used to download the software**

Skip to question 20.

Playing a computer game

17. **What was the name of the game you were playing?**

18. **Was the game new? ***

Mark only one oval.

Yes*

No

19. **Where did you get the game from? (please be specific)**

Skip to question 20.

More details of the attack

20. **What were the first signs of your device being infected? (check all that apply)**

Check all that apply.

- Antivirus software was disabled, or took longer to start up
- Computer crashed
- Computer restarted without my consent
- Computer started to overheat and became very slow
- Desktop was locked
- Office software, such as MS Word, Excel, etc., crashed, or failed to open files
- Screen or display started to jitter
- Some personal files went missing
- Starting up took much longer than usual
- Other: _____

21. **Did you have any anti-virus scanning software running?**

Mark only one oval.

Yes*

No

22. What was the anti-virus software called?

23. Can you remember any details of the message or ransom note given to you by the attacker? If so, please write any of it below.

24. What was the name of the ransomware used (e.g. file extension of encrypted files or given in the message)?

25. What was the effect of the attack? (check all that apply) *

Check all that apply.

- Screen blocked
- Files encrypted
- Files removed
- Other: _____

26. How long were your files/screen locked?

Mark only one oval.

- Hours
- Days
- Weeks

27. Were you able to recover the files/access to your device? *

Mark only one oval.

- Yes *Skip to question 28.*
- No *Skip to question 29.*

File recovery

28. How did you recover the files/access to the device?

Mark only one oval.

- Paid the ransom money
- Recovered data from a backup
- Contacted relevant authorities, who advised the next steps
- Other: _____

Skip to question 30.

Failed to recover files

29. Why were the files/device access not recovered?

Mark only one oval.

- Did not pay the ransom, and it was not possible to recover files or gain access
- Paid the ransom, but the attackers did not provide the decryption key or method to unlock the device
- Paid the ransom, but the decryption key or method to unlock device did not successfully recover files or access to the device
- Other: _____

Further Study

We are interested in hearing more about your experience with ransomware, and would like to contact you with further questions. This would be very beneficial for the quality of our research. If you are willing to share your story, fill in your email address below.

Note! No personal information will be stored and all data will be kept anonymous.

30. Email address (optional)
