Organisations Under Ransomware Attacks

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. 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. **What industry does your organisation operate in?**
   Mark only one oval.

   - ◯ Healthcare
   - ◯ Technology
   - ◯ Finance/Insurance
   - ◯ Government Services
   - ◯ Education
   - ◯ Other: _____

3. **Has your organisation been under a ransomware* attack?** *
   *In a ransomware attack device's screen and/or files get locked and a payment is demanded to release them. This can occur on a computer or a smart phone.
   Mark only one oval.

   - ◯ Yes
   - ◯ No *Stop filling out this form.*

Basic attack information

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

   _____
   Example: December 15, 2012

5. **What operating system(s) were the infected devices(s) or system running?**
   Check all that apply.

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

6. **How did the ransomware first get into the network?** *
   Mark only one oval.

   - ◯ Clicking a link in an email *Skip to question 7.*
   - ◯ Clicking a link on a website *Skip to question 17.*
   - ◯ Opening an attachment in an email *Skip to question 12.*
   - ◯ Attaching an unknown device e.g. USB stick *Skip to question 24.*
   - ◯ Downloading some software *Skip to question 20.*
   - ◯ Downloading a file through a sharing network, e.g. torrents... *Skip to question 22.*
   - ◯ Exploiting a vulnerable part or weakness *Skip to question 23.*
   - ◯ Other: _____ *Skip to question 24.*

Skip to question 24.

Malicious link in an email

7. **Who was the sender identified as?**
   Mark only one oval.

   - ◯ Colleague
   - ◯ Official authority
   - ◯ Other official (e.g. bank, tax, gas)
   - ◯ Applicant (job/studies)
   - ◯ Other person from recipient's contact list
   - ◯ Other: _____

8. **Sender email address**

   _____

9. **Describe the contents of the message**

10. **What browser was used to open the link in the email?**

11. **What website did the link direct to?**

Skip to question 24.

Malicious attachment in an email

12. **Who was the sender identified as?**
Mark only one oval.

- ◯ Official authority
- ◯ Other official (e.g. bank, tax, gas)
- ◯ Applicant (job/studies)
- ◯ Colleague
- ◯ Other person from recipient's contact list
- ◯ Other: _____

13. **Sender email address**

14. **Describe the contents of the message**

15. **State the type of the attachment (e.g. .doc, .xlsx)**

16. **How did the malware spread from the file?**
Mark only one oval.

- ◯ File had a hidden .exe extension and executed when opened
- ◯ Malware was hidden in file macros
- ◯ Other: _____

Skip to question 24.

Malicious Link

17. **What browser was used?**

_____

18. **What website was the malicious link on?**

_____

19. **What website did the link direct to?**

_____

Skip to question 24.

Malicious Software

20. **Name the software that was downloaded**

_____

21. **What website was the software downloaded from?**

_____

Skip to question 24.

File Sharing Network

22. **Describe the attacked file sharing network**

_____

_____

_____

_____

_____

Skip to question 24.

Vulnerability Exploit

23. **Describe the vulnerability that was exploited**

Skip to question 24.

More Attack Details

24. **From whom did the attack start?** *
Mark only one oval.

- ◯ Registered user
- ◯ Guest/Temporary user
- ◯ Intruder
- ◯ Unknown
- ◯ Other: _____

25. **What device was attacked first?** *
Mark only one oval.

- ◯ Organisation owned device
- ◯ Personal device
- ◯ Unknown
- ◯ Other: _____

26. **How many devices were infected during the attack?** *

27. **How did the malware propagate in the network?**
*if ransomware infected multiple devices/systems

28. **If there was an anti-virus software running, name the software**

29. **What were the first signs of the device(s) being infected?**
Check all that apply.

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

30. **What was the effect of the attack?** *
Check all that apply.

- [ ] Screen blocked
- [ ] Files encrypted
- [ ] Files removed
- [ ] Data stolen
- [ ] MBR / MFT corrupted
- [ ] Other: _____

31. **What was the name of the ransomware used?**
The ransomware name may be used as the extension of the encrypted files.

_____

32. **How long were the files and/or device(s) locked?** *
Mark only one oval.

- ◯ Hours
- ◯ Days
- ◯ Weeks

33. **Were you able to recover the files and/or access to the device(s)?** *
Mark only one oval.

- ◯ Yes *Skip to question 34.*
- ◯ No *Skip to question 35.*

Stop filling out this form.

Recovery

34. **How were the files and/or access to the device(s) recovered?**
Mark only one oval.

- Ransom was paid
- Data was recovered from backup
- Relevant authorities were contacted for advise
- Reverse engineering
- Other: _____

Skip to question 36.

Not Recovered

35. **What was the reason for not being able to recover the files?**
Mark only one oval.

- Ransom was not paid, and it was not possible to recover files or gain access
- Ransom was paid, but the attackers did not provide the decryption key or method to unlock the device
- Ransom was paid, 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 details about your organisation's 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 participate in a brief interview, fill in your email address below.

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

36. **Email address (optional)**

_____