Replicating a Study of Ransomware in Germany

ANNA-MARIE ORTLOFF, University of Bonn, Germany
MAIKE VOSSEN, University of Bonn, Germany
CHRISTIAN TIEFENAU, University of Bonn, Germany

Ransomware is a pertinent threat to businesses and end user data. While several attacks on enterprises are reported and give insights into the prevalence of such ransomware attacks, this prevalence in the general population is hard to estimate since they are not monitored by an official entity. A 2019 study by Simoiu et al. surveyed a representative sample of American consumers to estimate it for the US population. One year later, we aimed to replicate this effort for a representative German population (N=963) to study the spread of ransomware in a different context. Our findings suggest some differences between the two samples concerning payment methods and the participants' way of dealing with ransomware. Other aspects, like the ransom amounts and behavioral changes after an attack, were largely similar. We extend prior work by examining disagreements and uncertainty in judging whether a ransomware attack occurred for participants and researchers alike.

CCS Concepts: • **Human-centered computing** → *Empirical studies in HCI*; • **Security and privacy** → **Usability in security and privacy**; **Malware and its mitigation**.

Additional Key Words and Phrases: ransomware, replication, representative study

ACM Reference Format:
Anna-Marie Ortloff, Maike Vossen, and Christian Tiefenau. 2021. Replicating a Study of Ransomware in Germany. In *European Symposium on Usable Security 2021 (EuroUSEC '21), October 11–12, 2021, Karlsruhe, Germany*. ACM, New York, NY, USA, 23 pages. https://doi.org/10.1145/3481357.3481508

1 INTRODUCTION

Ransomware is a type of malware that restricts users' access to their computer and demands payment, a so-called "ransom", in exchange for re-granting access. Since the beginning of the 21st century, these attacks have become more and more popular [25], up to the year 2021, when they were expected to cause costs of around 20 billion dollars worldwide for 2021 [31]. Recently, the rate of attacks towards enterprise and municipal targets have increased [9, 23, 32] because they can be a lucrative target [8]. To understand the threat and find ways to prevent such attacks, organizations and researchers document the cases. This is a challenging task since the environments and attack vectors can be different in every case. While the majority of the available incident reports document attacks on large victims, only recently, the first study observing the prevalence of ransomware among consumers was published [40]. It is hard to estimate the prevalence of ransomware in the general population since most reports on the problem are published by security companies and only include data generated from the user base of their product [23, 32]. Almost half of surveyed EU citizens were concerned about cyber extortion, another term for ransomware, in 2017 [18]. Analyzing this target group is important since end users do not take as many measures to protect themselves from an attack [42], so

Manuscript submitted to ACM

they are more affected if they encounter ransomware. Understanding this group's methods and perceptions can help develop countermeasures that mitigate the effects for them.

Previous work measured the prevalence of ransomware among the US population by surveying a representative sample about their experiences and reactions to ransomware attacks [40]. They found mitigation methods of end users (e.g., restarting the computer, restoring a backup, or even paying the ransom) and that there is a victimization rate of 2-3% of the US population that results in possibly millions of ransomware attacks each year [40]. Cultural differences [6, 34], as well as further development of both ransomware and protection techniques against it, may affect these results in a different population. Understanding the prevalence in different countries can contribute to the body of knowledge concerning the distribution and ways of attacking by identifying adapted patterns specific to certain cultures. It is important to monitor the state of ransomware infections in different populations to gauge the dimension of the threat that it presents.

In this work, we conducted a similar survey to Simoiu et al. [40] with a representative German sample two years after the original study took place. In the following, we report on our process of translating and adjusting the survey for use in a German population. We describe the results of our survey in terms of similarities and differences with the original work. Finally, we extend prior work by discussing two further methodological aspects. One was using a compound question in the original survey, the effect of which we examine through an A/B test. The second was the uncertainty in judging whether a participant had experienced a ransomware attack or a different computer problem.

2 RELATED WORK

Ransomware is a kind of malware whereby either the complete system is blocked, or data on the local hard drive is encrypted. Users are then blackmailed into paying a ransom in exchange for access to their data or restoration of prior system functionality [17]. Infections with ransomware often arise through spam emails or unintentionally downloading exploit kits by clicking on malicious links or ads online. Other sources are personal server vulnerabilities, as well as unprotected remote maintenance [9]. Al-rimy et al. present a taxonomy of ransomware and an overview of general detection and mitigation and prevention mechanisms [2].

One can distinguish two main types of ransomware. While locker ransomware locks the affected device, preventing its usage, but leaving the data on it untouched, crypto-ransomware encrypts the data, thus preventing users from accessing it, even though the device retains its functionality [2, 38]. Additionally, scareware variants exist that pretend to be ransomware, even though data is merely obfuscated and not encrypted [2, 7].

Recent ransomware attacks are increasingly directed towards companies and public institutions. In Germany, reports in 2018 show that 81% of ransomware attacks are targeted on businesses, while at the same time, the total amount of ransomware attacks decreased by 20% [9, 32]. Likewise, the number of municipal targets has increased [23]. However , ransomware is a pertinent threat for consumers as well. Their risk is immediate and concrete to them because their private data, possibly personal memorabilia, is not available to them anymore [10].

There is much previous work on how to detect ransomware before it interferes with device usage, e.g., by monitoring API usage [13, 24], file system [24] or registry events [1] and using dynamic analysis and different machine learning techniques [19] to classify ransomware. However, these strategies are not available to end users directly due to their technical sophistication. There are some basic protection strategies for end users that are repeatedly presented [21, 38]. These include installing anti-malware systems and keeping them up to date, installing security updates, as well as regularly backing up data to a storage device that is disconnected from the network [21]. While the former cannot

prevent all infections with malware, they do provide some protection, especially against known ransomware strains [30]. With a backup, users can avoid paying a ransom to access their data in case of an attack.

It is hard to understand the true extent of ransomware attacks on personal and industry devices. Many reports and numbers in the area stem from companies that market security products, such as Symantec or Kaspersky [23, 32]. Naturally, only users of their proprietary software are included in that data. Since there is also still a non-negligible percentage of people who do not use such software when using the internet [16, 44], this is not representative of the general population. In addition, ransomware incidents are also rarely reported to the police [11], which further inhibits the assessment of prevalence independently of software providers.

Furthermore, it is not clear whether users recognize threats when they occur. In 2009, under 55% of surveyed American and 35% of South Korean users reported knowledge of spyware, malware, and techniques to protect against them [15]. Concerning mental models, users perceive malware as entirely different from other software and show less knowledge about malware [41]. When using smartphones, risky security behavior is common [22], and users do not necessarily understand the risks of their behavior and lack knowledge about protection strategies [3]. Consequently, we have to assume that users cannot correctly identify threats, such as ransomware when they occur.

Previous work has investigated and found cultural differences in several different aspects of security and privacy-related behavior. This includes differences in the use of and knowledge about online protection measures between the U.S. and South Korea [15], cultural differences in security awareness campaigns [6], and in social network behavior in the U.S. [14] and between American and German users [27]. Information disclosed on social networks can facilitate spear-phishing attacks, which are a source of ransomware. Cultural markers can also be used in the context of Computer Network Attack Attribution [39]. In general, previous work supports the need for cross-cultural studies of security issues [34].

2.1 The Original Study

To fill this gap, Camelia Simoiu, Christopher Gates, Joseph Bonneau, and Sharad Goel conducted a study surveying a representative sample of 1,180 American adults in 2017. Their goal was to find out the distribution and characteristics of ransomware attacks in the general population in the U.S. [40]. Their five-part survey consisted of a demographic section, a section to establish whether the participants had experienced a ransomware infection, follow-up questions regarding the possible ransomware attack, a section questioning the participants about their security habits and if they have changed those regarding the former infection and a general IT knowledge quiz.
The responses of the self-reported ransomware victims were then examined and classified under a conservative and an inclusive regime: Only those responses that gave sufficient information to confirm "beyond reasonable doubt" that the participant experienced ransomware were included in the conservative regime, whereas the inclusive regime also included cases with an ambiguous or no description.

Simoiu et al. estimated a victimization rate of 2-3% per year for the U.S. population and examined ransomware characteristics and participant behaviors and risk perceptions after a ransomware attack. Many ransomware attacks impersonated law enforcement entities, and most ransomware attacks in their sample locked users' computers (74%). Fewer users suffered from encrypted files (35%). This distribution of ransomware types may also account for cryptocurrencies not being the primary reported payment method, even though a rise in their popularity has been hypothesized to promote ransomware [38]. Ransomware victims reported some intentions to change their behavior after an attack and were more likely to believe that they would experience another attack but less likely to pay the ransom. Additionally,

the authors used machine learning techniques to generate an eight-question questionnaire used in predictive risk assessment concerning ransomware infections.

The threat of ransomware may be different depending on the country of both victims and attackers. In this work, we present the results of a replication study of Simoiu et al. with a representative sample of German citizens.

3 METHODOLOGY

In this section, we describe our methodology and the changes we made to adjust Simoiu et al.'s survey to a German population. Additionally, we explain any modifications to the procedure and evaluation of data.

3.1 Definition of ransomware attacks

Like Simoiu et al., we define ransomware as malware that restricts users' access to their data or device, often through either encryption of data or locking the computer [40]. While they do not explicitly state that ransomware includes a ransom demand, this is implicitly assumed through the name of this type of malware. "Fake" ransomware differs from actual ransomware in that while users are notified that their computer has been locked or their data have been encrypted, this is not the case. This tactic attempts to scare users into paying the ransom.

3.2 Adjustments for a German population

The original questionnaires were included in the supplemental material of the study [40], but for a replication with German participants, a translation was necessary. One author first translated the questionnaire into German, and another author vetted this. We further validated the translation by piloting the questionnaire with 25 native German speakers, who then gave us feedback regarding its comprehensibility. We incorporated their feedback when sufficiently well-founded and did not change the meaning compared to the original English questionnaire. We changed the demographic part to fit usual German standards. Additionally, we made some changes to remedy issues with the original question design. We provide the changed questions in the appendix, both in German, as they were distributed and back-translated to English. One of these issues involved allowing participants to choose multiple options regarding demanded payment methods (question 3.4), since this was reported for some ransomware strains [25]. We also added an option for the participants to indicate that they have not taken any countermeasures (question 3.13). Question 2.2. was originally a compound question: The participants were asked if they had seen one of the described warning messages and suspected those messages to be scams. However, if participants are asked about two topics in one question, it is unclear to which proportion the topics contribute to the answer [5, 12]. To investigate the effect of the compound question but still retain comparability with the original study, we randomly divided the participants into two groups. The first group was shown the original question, while the second group saw a separated version of the compound question. They were first asked whether they had experienced any of the scenarios and, in the case of an affirmative answer, whether they had suspected a scam. Finally, due to a misunderstanding of the original study procedure, question 2.20, which asked participants to assess the probability that they would be victims of another ransomware attack, and the likelihood that they would pay the ransom was only displayed to those participants who previously stated that they had experienced a ransomware attack. Unfortunately, this means that we cannot compare the risk perceptions of German ransomware victims and non-victims and are limited to comparisons with the American sample. The completed questionnaire was then implemented using Qualtrics and distributed via the Splendid Research platform[1]. It was chosen

[1]https://www.splendid-research.com/en

since YouGov, the platform used in the original study, was not available in Germany. Splendid Research also maintains a representative panel for Germany and allows for stratified sampling. Their university's institutional review board had approved the original study. Since we did not significantly change the survey content, we did not additionally apply for approval of our university's IRB.

3.3 Sampling

Splendid Research provides quotas representing demographic characteristics for the German population. Quotas were available for gender, age, highest level of education, monthly income, and state of residence. We did not ask for participants' race or ethnicity in the survey due to this being an especially delicate issue in Germany for historical reasons. So, contrary to the original study, we did not sample based on this criterion.

Splendid Research did not provide adjustment weights, and previous work suggests that using adjustment weights does not necessarily improve the generalizability of the results [36]. In the original paper, using weights also did not change the interpretation of the results [40]. Rather than calculating weights with a procedure, we could not be sure to be similar to the one in the original study. We instead report unweighted values. Nevertheless, the percentages of participation are close to the quotas which represent the sampling frame.

3.4 Study procedure

The recruiting platform contacted participants who, at some point previously, had signed up to participate in the Splendid Research Panel. The platform aimed to fulfill specific quotas of demographics concerning age, gender, location (state), education, and monthly household income to generate a stratified sample, which is representative of the German population. Participants were informed of the study procedure and their rights and then gave informed consent, before continuing with the study. They first answered demographic questions, as well as questions on their device usage. Participants who did not own a private computer were excluded from the survey, like in the original study [40], since the survey focused on end users experiencing ransomware attacks. Ransomware attacks on company-owned devices may be managed by staff and not the device user themself.

The next part of the survey focused on establishing whether participants had previously experienced a ransomware attack. Since our analysis is based mainly on this part of the survey, we provide more detail by presenting several detailed definitions of ransomware, leading to participants' self-assessment of whether they had experienced this sort of attack. It contained the A/B testing of the compound question detailed above. Participants were also shown some example screenshots of ransomware, see Figure 1, and asked whether they had encountered similar messages. We additionally enquired about experiencing individual aspects of ransomware, like timers or encrypted files. In the case of an affirmative self-assessment concerning ransomware, participants were asked to describe their experience in free text. If participants expressed uncertainty about having experienced a ransomware attack, they received a more detailed textual definition of ransomware. If they denied experiencing ransomware but nevertheless experienced one of the typical scenarios for ransomware, we asked for more details about their judgment process.

The next part of the survey asked for details on the experienced ransomware attack, such as the attack time, name of the ransomware strain, payment method, and currency. Participants had to state whether they paid the ransom and their reason for the decision. Furthermore, we asked about the aftermath of the ransomware attack, such as how participants removed the ransomware, their information sources during the attack, and changed behavior due to the attack. We

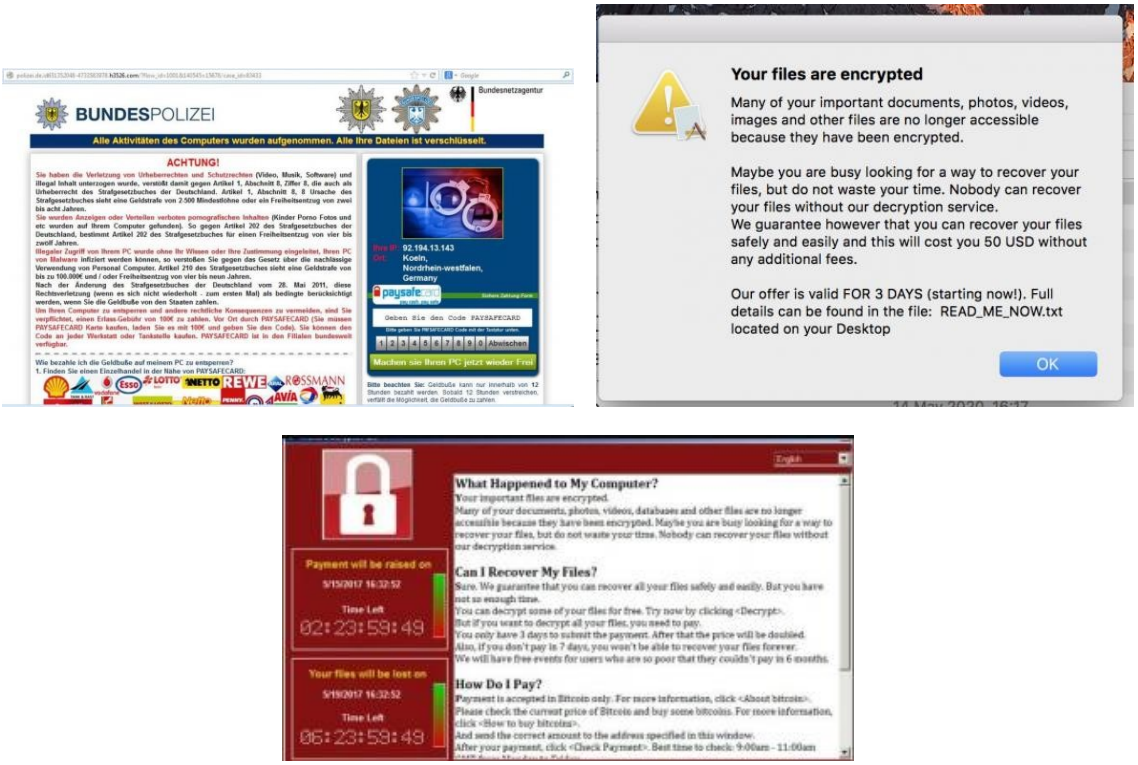


Fig. 1. Example screenshots of ransomware presented to study participants.

queried the participants' risk perceptions concerning being infected with ransomware again and their probability of paying a ransom.

The fourth part focused on participants' behavior before the ransomware attack. Finally, the fifth section of the survey was an eight-question computer knowledge quiz intended to measure how tech-savvy the respondents were.

Participants could provide a contact email for possible follow-up of their response, but this was entirely voluntary. Splendid Research reimburses participants for taking part in surveys like ours with between one and three euros, depending on the length and duration of the survey [2]. We paid 2.45€ for each survey response, so it is assumed that the participants received slightly less.

3.5 Classifying ransomware victimization

Two researchers independently coded the responses from those participants who classified themselves as having experienced ransomware. Like Simoiu et al., we used a conservative and an inclusive regime and used the reasoning they described to categorize responses. We used both free-text answers and answers to other questions from section 2 and 3 of the survey, such as the year of the ransomware attack, payment method, or method of ransomware removal, to form our judgments. Answers rated as ransomware under the conservative regime provided sufficient evidence to confirm that

[2] https://www.splendid-research.com/en/market-research-participate.html

the participant experienced a ransomware attack. The inclusive regime also included participants whose descriptions were vague or did not fit with the rest of their answers. Some participants also reported different types of malware, such as tech support scam, malware using blackmail without a ransom demand, or scareware, where the computer was not actually compromised. Still, participants were nevertheless notified of it and received a ransom demand. These were not considered to be ransomware under any of the regimes, but we nevertheless noted the occurrence of such scareware, which we labeled "fake ransomware." On the first pass through the data, the inter-rater agreement measured using Cohen's Kappa for two raters was 0.55 for the conservative regime and 0.59 for the inclusive regime. Since the regimes can also jointly be viewed as a single ordinal variable representing the amount of evidence corroborating a ransomware attack, we believe that calculating a weighted Kappa is appropriate in this case. In this case, the conservative regime represents the most evidence. The inclusive regime has less evidence. The rest of the answers are classified as having insufficient evidence to be considered ransomware. When using equal weights for Kappa, agreement improved very slightly to 0.57 and a bit more to 0.67 when using squared weights. Differences in ratings were then resolved through discussion among the raters.

4 RESULTS

We present the results of our replication of Simoiu et al.'s study on ransomware with a German population. Like the original study, we focus on describing our sample's experience of ransomware, and present it alongside the original study results to enable a comparison. However, since the two samples differed in more than merely the location, we did not conduct formal hypothesis tests to compare them. In addition, we focus on uncertainty in recognizing ransomware, both in participants and in the researchers themselves. The freely available software Gnu R [33] was used for statistics. Any participant utterances were translated from German by the authors. When the German utterance contained spelling or grammatical errors, we inferred the meaning for our translation where possible, rather than introducing incoherent mistakes into the English translation.

4.1 Participants

A total of 963 German participants started the survey between September 9th and September 30th, 2020, using the survey platform Splendid Research. The participants were required to be between 18 and 69 years old (platform-specific limitations). They had to own a private computer since we were interested in how people without assistance from their workplace handled ransomware. Additionally, ransomware attacks on company devices would be counted as incidents in a business context, whereas we were interested in attacks on consumers. We excluded 17 participants because they did not own a private computer, three because they did not provide informed consent and four because they did not provide any self-assessment whether they had experienced ransomware or not, and one person because they took more than 24 hours (119 hours 7.5 minutes) for the survey. Since some questions refer to previous questions, and we do not know when this participant took breaks, we do not know whether this participant could have provided valid responses. On the other hand, even though 31 participants did not finish the whole survey, we only excluded one of them since they did not provide any information about the ransomware attack they experienced, preventing us from classifying it. The rest of the participants did not experience a ransomware attack. Consequently, only the IT quiz is missing for all but two, which failed to continue to the last page of the survey after answering all questions. Since we did not evaluate these data for this work, we retain these participants in our sample. This resulted in 937 valid preliminary responses. The participants were recruited to represent the German population regarding age, gender, state, and the highest level of education. During the coding process, we excluded eight further participants based on their free-text responses being

	Participation	Quota
Gender		
Male	45.2%	49%
Female	53.1%	51%
Diverse	0.1%	
Prefer not to say	1.6%	
Age		
18-29 years	13.9%	20%
30-39 years	19.7%	18%
40-49 years	22.1%	21%
50-59 years	24.7%	24%
60-69 years	19.6%	17%
Monthly household gross income		
Below 1,300€	18.4%	16.3%
1,300 - 1,699€	10.5%	9.1%
1,700 - 2,600€	23.7%	20.6%
2,600 - 3,600€	20.0%	17.8%
3,600 - 5,000€	18.6%	17.5%
5,000 - 18,000€	8.1%	18.6%
Over 18,000€	0.1%	0.1%
Prefer not to say	0.6%	-
Highest level of education		
Still in education	0.8%	3.6%
Without school-leaving qualification	1.5%	4.4%
Certificate of Secondary Education	23.1%	29.6%
General Certificate of Secondary Education	33.0%	29.9%
General Certificate of Education	41.2%	32.5%
Prefer not to say	0.4%	-

Table 1. Demographics relating to survey participation and quota. Location information is left out, since this is not comparable to previous work.

nonsensical. Such responses indicate a possible malicious intent to manipulate the survey results. All other numbers are based on the set of 929 valid participants. The survey duration was between 1.3 minutes and 9 hours 18.3 minutes (Median= 5.9 minutes). Participants were on average 46.8 years old (SD=13.4). These calculations are based on the midpoints of the given age ranges. The numbers of male (424) and female (489) participants were roughly equal, and 16 people either reported their gender as diverse or not at all. More detailed information on the demographics of our sample can be found in Table 1.

The most frequent operating system on participants' private computers was Windows (85.6%), followed by MacOS (8.3%) and Linux (1.6%). The remaining participants reported various operating systems, such as Android, IOS, Chrome, multiple operating systems, or unknown. The most frequently used browser was Google Chrome (41.9%), followed by Mozilla Firefox (31.3%) and Microsoft Edge (9.1%). Among the other browsers reported were Microsoft Internet Explorer, Safari, and Opera, and some instances where participants did not know. This is in accordance with desktop browser usage statistics as collected by Statcounter[3], providing another indicator of the representativeness of our sample.

[3]https://gs.statcounter.com/browser-market-share/desktop/germany

	Current Work		Original Work	
	All victims	2019 / 2020	All victims	Last 12 months
Self-reported	18.9%	2.7%	14%	5%
Re-classified (inclusive)	13.7%	1.7%	9%	3%
Re-classified (conservative)	8.3%	1.2%	6%	2%

Table 2. Proportions of ransomware victimization for the German population compared to the original study under the conservative and inclusive classification schemes. The "all victims" column for the German population includes respondents who reported experiencing a ransomware attack at any time in the past; the "2019/2020" column includes respondents who reported attacks within 1 - 1.75 years of the survey date.

4.2 Compound Question

We were interested in the effect the compound question 2.2 had on participants' responses. Roughly half (45.4%) of the participants received the original version of the question asking whether they had previously experienced a scenario, such as the one described, that they found suspicious. The other participants (54.6%) were first asked whether they experienced the scenario and whether they found it suspicious in the case of an affirmative answer. The two groups' answers to question 2.2 did not differ statistically significant when compared using a χ^2-test, $\chi^2(4)=5.93$, p=.20. Nevertheless, 34 participants (6.7% of group B, 14.3% of those who answered affirmatively to the first question) experienced one or both of the described scenarios, but did not find them suspicious, showing some potential for misunderstanding the compound question. Depending on which question component is more important to participants, they could have either answered the compound question in the affirmative when weighting experiencing the scenario as more important or negatively when deeming the suspicion more important. Finally, participants could have chosen the "unsure" option due to uncertainty about the question phrasing.

4.3 Comparison of ransomware attacks in Germany and the U.S.

We compare the characteristics of ransomware attacks experienced by our participants in Germany to those experienced by US-based participants in Simoiu et al.'s survey in 2018, two years before.

Victimization rates (see Table 2) were generally higher in our sample but lower in the most recent time period, even though we took reports from the last 1.75 years into account, and not merely the last year. This deviation from the methodology of previous work occurred due to reporting issues since most of our participants could not remember the month of the attack but only the year.

In the following, we report on ransomware as classified under the inclusive regime, like previous work [40]. As seen in Figure 2, the distribution of ransomware types was similar, and police impersonation was also widespread in our German sample. We were not always able to clearly categorize reports of ransomware as crypto or locker ransomware. Sometimes, we could not assign a ransomware categorization at all, or participants reported experiencing characteristics of both types. Nevertheless, we see similarity to previous work in that locker ransomware was more prevalent for police impersonation than non-police impersonation ransomware. Overall, locker ransomware is more common than crypto-ransomware.

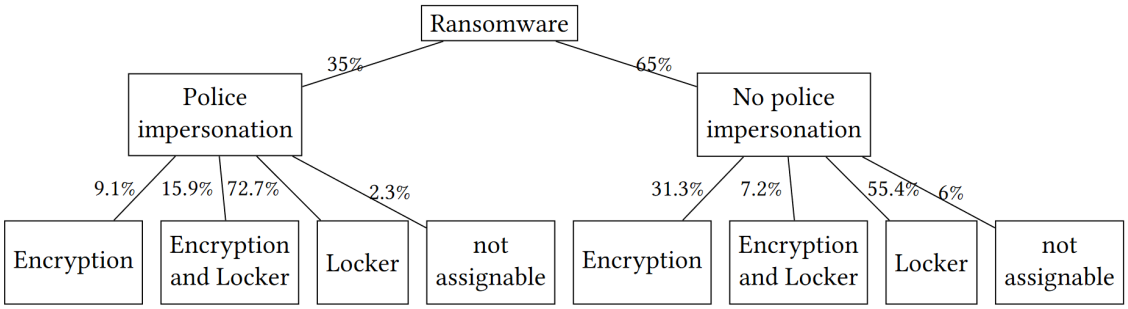


Fig. 2. Distribution of ransomware attributes (impersonation of law enforcement, locker, encryption) in German sample. Categories are not mutually exclusive.

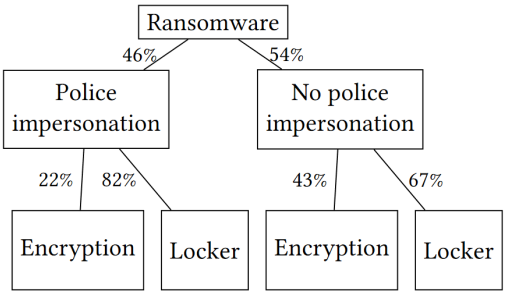


Fig. 3. Distribution of ransomware attributes (impersonation of law enforcement, locker, encryption) in the original work. Categories are not mutually exclusive.

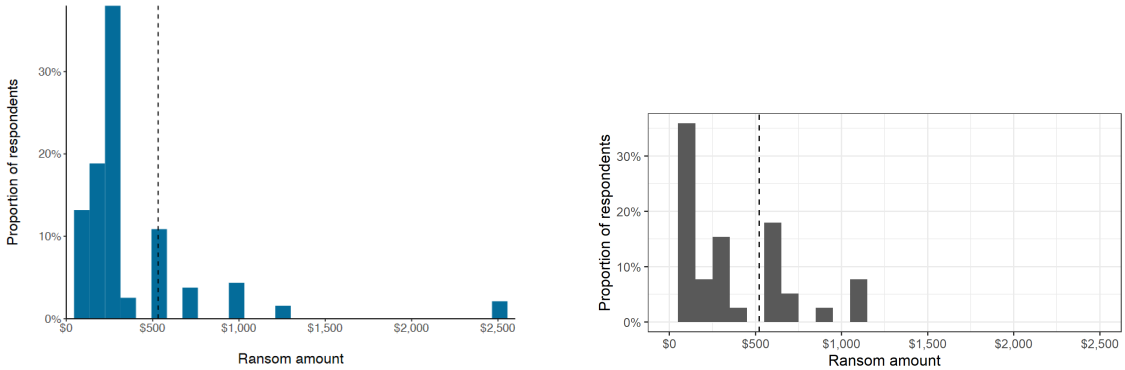
The payment methods which our German participants reported, see Table 3, differed from previous work. Many people did not remember the payment method requested in the ransomware attack they experienced, and if they did, both cryptocurrencies and using bank transfers were far more prevalent. However, it is necessary to keep in mind that our reported percentages represent an upper rather than a lower bound on actual payment because we allowed the selection of multiple answers in this question. Payment methods summarised under "Other" consisted of two people reporting that they were asked to download or buy software, one naming Western Union as a specific service for bank transfers, and one person who did not encounter a payment possibility in their ransomware.

The distribution of ransom amounts, see Figure 4, was fairly similar to previous work. Most ransom demands encompassed lower values, but there were some high ransom demands above 1,000 Dollars. Note that most ransom demands were round, whole numbers, but reported in Euro by participants. This is a sign that ransomware is localized to account for users' currency. To be able to compare them to the Dollar amounts which were reported by Simoiu et al., we sourced average conversion rates per year for all the years in which ransomware attacks were reported by participants from the European Central Bank[4]. We then converted the Euro values to Dollars using the average conversion rate of the year of attack. The median value in Euro was exactly the same as the median value in Dollar in the Simoiu study (250) but differed after conversion. Five participants reported ransomware amounts in cryptocurrencies, two in Bitcoin

[4]https://www.ecb.europa.eu/stats/policy_and_exchange_rates/euro_reference_exchange_rates/html/index.en.html

Method of payment	Proportion	Proportion Original
Cryptocurrency	26%	12%
Bank transfer	25%	14%
Online payment service provider	17%	NA
Pre-paid cash voucher	16%	42%
Credit card	12%	NA
Premium text message	4%	7%
Don't remember	24%	10%
Not displayed	NA	15%
Other	3%	NA

Table 3. Distribution of payment methods. Multiple answers were permitted for the current survey, but only one for the original work.



(a) Original (N=66). The median and mean reported ransom is $250, and $530 respectively.

(b) Replication (N=40). Amounts named in Euro converted to US-Dollar. The median and mean reported ransom is $272, and $522 respectively.

Fig. 4. Histograms of reported ransom amounts for respondents recalling an amount (in Euro or Dollar for the replication). The dashed line represents the mean. The maximum amount reported ($8,000 for the original, $6,960 for the replication) is omitted from the plot.

(2,000 and 200) and three in non-specified cryptocurrencies (100, 350, 500). Since exchange rates of these currencies are subject to a high amount of fluctuation, and participants did not report exact dates and in three cases not the specific cryptocurrency of the ransom demand, we did not include these values in our graph.

Methods of dealing with ransomware concerning the final strategy used by participants to remove ransomware from their computer are reported in Table 4. We found that merely restarting the computer is used as a strategy much less frequently in our sample than in Simoiu et al.'s sample. During our classification process, if a participant did not provide enough detail on the ransomware attack in free-text comments and other answers, we classified instances where restarting the computer sufficed to remove the ransomware as scareware, rather than ransomware under the inclusive regime. This may have contributed to this decrease. On the other hand, restoring the computer from a backup was reported more frequently. This is interesting given that regularly backing up computers is not that common. While the number of young adults who regularly backed up their computer increased from 2012 to 2016, there were still 18%

Method	Proportion	Proportion Original
Restored computer from backup	34%	22%
Found and used programm/tool	22%	18%
Removed by someone else	17%	13%
Could not remove	9%	NA
Restarted computer	6%	30%
Reformatted computer	4%	5%
Removed using AV software	2%	5%
Paid ransom	2%	4%
Other means	4%	3%

Table 4. Self-reported means of dealing with the attack, final strategy used to remove ransomware.

who never made backups, and only 12% did so weekly, or more often [35]. In a convenience sample of 319 international participants, 20% of computers did not have a backup, and the existing backups were not necessarily complete [26].

Other strategies are reported in roughly similar proportions. In our sample, seven people paid the ransom, but only one of them named this as their successful strategy to remove the ransomware. For five participants, data was restored after paying the ransom, and for two, it was not. There were no interesting reasons given for paying the ransom beyond "I don't know".

The ransomware victims in our sample reported roughly similar behavioral changes after the attack, see Table 5. The most notable change is that updating anti-virus products is reported much less frequently. This is probably due to a rephrasing in our translation. The original work used "Updated AV product," and their survey phrasing encompassed both updating and changing anti-virus products. For unambiguousness, we rephrased this item to include only changes, so the decrease may be due to users not changing but updating their anti-virus products. Browsing more carefully is slightly less common in our sample while starting to backup data is reported slightly more frequently. This is interesting since backups are already the primary strategy to deal with ransomware attacks.

4.4 Uncertainty in classifying ransomware

In the original study, the authors reported an inter-rater agreement of κ=0.53 for the conservative regime and 0.66 for the inclusive regime. For our data, the first round of coding with two authors yielded κ=0.55 and 0.59 for conservative and inclusive regimes, respectively. When using a weighted Kappa, which is more appropriate for ordinal data, such as these, agreement changed slightly to 0.57 when using equal weights and 0.67 when using squared weights. Both the authors of the original study, as well as ourselves, reached consensus after additional discussion. This suggests that both in the original study, and in our replication, it was not straightforward for the researchers to decide whether a participant was actually a ransomware victim based on their self-reports.

While we cannot infer what caused the disagreements for Simoiu and their colleagues, we will attempt to interpret our difficulties in decision-making. We found that many participants did not provide detailed answers to free text questions. For example, the number of words (simplistically defined as space separated groups of characters) in answers to question 7 in part 2, which asked participants to describe the most recent ransomware attack they experienced, ranged between 0 and 84, with a median of only 12. Answers were frequently not helpful, such as "I don't know," "I

Habit	Proportion	Proportion Original
Purchased AV product	43%	44%
More careful browsing	39%	65%
Started to backup data	34%	26%
Enable automatic updates	24%	24%
Changed OS configurations	23%	20%
Backup data more regularly	15%	22%
Changed AV product	13%	31%
Changed OS	9%	10%
Changed default browser	8%	12%
Encrypted hard drive	3%	0%

Table 5. Behavioral changes following the attack for ransomware victims. Multiple answers were permitted. "Enable automatic updates" refers to updates to the OS, browser, antivirus, and other programs. Examples of configuration changes are disabling Windows Script Host, restricting login access, enabling the "show file extension" feature in Windows. The original work used "Updated AV product" instead of "Changed AV product." Their survey phrasing encompassed both updates and changes, and 31% of their participants took up this habit. For unambiguousness, we rephrased this item to only "Changed AV product."

don't remember," or very short, such as "police forged," "Bundeskriminalamt" (German Federal Criminal Office), or "The screen was locked like with a board." This made it hard to infer ransomware characteristics.

Whereas this question was the main free text one we used in determining ransomware victimization, this finding is aggravated for the other free text questions. They asked participants how they decided whether to pay the ransom (0-48 words, median=6), about the resources they used to determine their course of action (0-34 words, median=1), and for their assumptions on how they became infected with ransomware (0-34 words, median=2).

Participants also frequently reported not remembering many aspects of the ransomware attack, such as the year it took place, the amount of payment requested, and if there was a timer, among other things. Out of 176 valid participants who claimed to have experienced a ransomware attack, only 34 participants remembered the name of the ransomware, and in all but four cases, it was one of the examples included in the question phrasing. One participant named multiple ransomware strains, one of which was not among the examples. Six additional participants provided a description in place of an actual name, e.g., "malware federal office" or "BKA Trojaner" (German Federal Criminal Office trojan). This could also be an artifact of the ransomware strains not publicizing their names to their victims.

The coding researchers weighted these various aspects of participants' responses differently during their initial classification, leading to disagreements. Another critical point of discussion for us was the method that participants used to get rid of the ransomware. During the first round of coding, we disagreed about whether malware that could be removed by simply restarting the computer could be considered ransomware. After reviewing the definition, we identified two conditions: First, the computer must be blocked from use (commonly either by encryption of data or locking), and second, there must be a ransom demand. Consequently, when the participant was able to remove the ransomware by restarting the computer (without mentioning using safe mode), we thereafter did not rate this instance as ransomware since condition one was unsatisfied but instead labeled it as scareware.

We were not the only ones uncertain about whether to consider an experience a ransomware attack or not. The participants themselves were also unsure about this: 108 (11%) of them were unsure whether they had experienced ransomware after we provided a short explanation and questions on experiencing different aspects of ransomware

Participant Judgment Certainty	Researcher Judgment		
	Not Ransomware	Ransomware (inclusive)	Ransomware (strict)
Uncertain	7 [41%]	7 [41%]	3 [18%]
Certain	42 [26%]	43 [27%]	74 [47%]

Table 6. Participant judgment certainty and researcher judgment of ransomware victimization status. Number of participants and percentages per certainty bracket in square bracket

attacks. Even after an additional, more detailed explanation, 45 (42%) of the previously unsure participants were still undecided. For the rest, the further explanation helped 17 (16%) decide that they had been ransomware victims and 43 (40%) that they had not.

At the same time, our judgments did not always match the participants' ones. As can be seen in Table 6, over a quarter of those participants who were sure that they had experienced a ransomware attack actually had not, according to the researchers' judgment.

Other participants were uncertain about their judgment, meaning that they first stated they were unsure and only after a further explanation believed they had experienced ransomware. Researchers judged a higher proportion of the uncertain participants to have not actually experienced ransomware than those who were sure that that they had, see Table 6, so those participants' uncertainty was somewhat justified. However, this finding was not significant under a Fisher's exact test ($p = 0.25$), which we calculated due to expected frequencies below 5 in one of the cells [20].

5 LIMITATIONS

In the following, we describe some limitations of our study.

We cannot pinpoint the origin of differences to the time of the survey, location of participants, or methodology. Some differences, such as the more frequent demand of ransom in Euro instead of Dollar, are probably due to our German sample. We encountered some issues with translation in reproducing the original study, so some differences we found may be the result of a slightly different methodology. These could include the decrease in the prevalence of changing the used anti-virus product after becoming a ransomware victim. This decrease could be due to a change in phrasing in the German version of the survey.

It was difficult for us to find screenshots in German that closely resembled ransomware depictions used in the original study. Consequently, only one of three screenshots was in German, so that a language barrier may have impeded our participants' judgments regarding their ransomware experience.

Like the original study, all our data is self-reported and may suffer from biases accordingly. People tend to report their security practices optimistically [37], so behavioral changes may be over-reported. This is a result of the trade-off between generalizability and ecological validity. Small scale studies can measure real behavior [29] but are hard to implement for large, representative samples.

6 CONCLUSION

In our replication of Simoiu et al.'s work, we found some differences between the German and American populations, e.g., concerning the payment method and the participants' way of dealing with the ransomware [40]. Additionally, in our German sample, ransomware in 2019/2020 (a 20 month period) was only about half as prevalent than in the American sample in a 12-month period prior to 2018. Other aspects, such as the amounts of ransom demanded and the

behavioral changes after a ransomware attack, were largely similar. We slightly modified their survey and observed the effect of separating a previously used compound question into two separate component questions. However, we did not find a significant difference, even though some participants answered the two parts of a compound question differently. Additionally, we reported on uncertainty in categorizing attacks as ransomware, both on the researchers' and on the participants' sides.

This uncertainty should be considered in further work examining participants' perceptions of different types of malware. If even researchers disagree about classifying malware, it is even more challenging for end users to judge this. A broader focus on experiencing IT security incidents in general could be helpful. To gain input from users who are unsure about their experience, this could be addressed in a future replication by also presenting the questions in part 3 of the survey to those unsure participants. This could allow researchers to judge whether an experience was in fact related to ransomware, rather than relying only on participants' assessment, which can differ from researchers' judgments, as we found in this study.

Finally, our survey and the original study gauged the prevalence of ransomware on desktop devices, but ransomware also threatens other device classes, such as mobile devices [4, 28] or Internet of Things applications [43]. The magnitude of this threat and its visibility for end users remains to be investigated.

REFERENCES

[1] Mohammad Mehdi Ahmadian and Hamid Reza Shahriari. 2016. 2entFOX: A framework for high survivable ransomwares detection. In *Proceedings of the 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*. 79–84. https://doi.org/10.1109/ISCISC.2016.7736455

[2] Bander Ali Saleh Al-rimy, Mohd Aizaini Maarof, and Syed Zainudeen Mohd Shaid. 2018. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security* 74 (2018), 144 – 166. https://doi.org/10.1016/j.cose.2018.01.001

[3] Mansour Alsaleh, Noura Alomar, and Abdulrahman Alarifi. 2017. Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. *PloS one* 12, 3 (2017). https://doi.org/10.1371/journal.pone.0173284

[4] Nicoló Andronio, Stefano Zanero, and Federico Maggi. 2015. HelDroid: Dissecting and Detecting Mobile Ransomware. In *Research in Attacks, Intrusions, and Defenses*, Herbert Bos, Fabian Monrose, and Gregory Blanc (Eds.). Springer International Publishing, Cham, 382–404.

[5] Earl R Babbie and Lucia Benaquisto. 2009. *Fundamentals of social research*. Cengage Learning.

[6] Maria Bada, Angela Sasse, and Jason Nurse. 2015. Cyber Security Awareness Campaigns: Why do they fail to change behaviour?. In *Proceedings of the International Conference on Cyber Security for Sustainable Society*. 118–131.

[7] Pranshu Bajpai, Aditya Sood, and Richard Enbody. 2018. A key-management-based taxonomy for ransomware. In *Proceedings of the 2018 APWG Symposium on Electronic Crime Research (eCrime)*. 1–12. https://doi.org/10.1109/ECRIME.2018.8376213

[8] Bloomberg. 2021. Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom. https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom. Accessed: 2021-05-21.

[9] Bundesamt für Sicherheit in der Informationstechnik [n.d.]. Ransomware: Bedrohungslage, Prävention & Reaktion. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.html. Accessed: 2021-01-21.

[10] Bundesamt für Sicherheit in der Informationstechnik 2019. Schadhafte SPAM-Mails im Namen mehrerer Bundesbehörden. https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/Spam-Bundesbehoerden_181219.html. Accessed: 2021-01-21, Published on 2019-12-18.

[11] Bundeskriminalamt 2019. Bundeslagebild Cybercrime 2018. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2018.html. Accessed: 2021-01-21.

[12] Karoline Busse, Julia Schäfer, and Matthew Smith. 2019. Replication: No One Can Hack My Mind Revisiting a Study on Expert and Non-Expert Security Practices and Advice. In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS'19)*. USENIX Association, Santa Clara, CA. https://www.usenix.org/conference/soups2019/presentation/busse

[13] Zhi-Guo Chen, Ho-Seok Kang, Shang-Nan Yin, and Sung-Ryul Kim. 2017. Automatic Ransomware Detection and Analysis Based on Dynamic API Calls Flow Graph. In *Proceedings of the International Conference on Research in Adaptive and Convergent Systems* (Krakow, Poland) *(RACS '17)*. Association for Computing Machinery, New York, NY, USA, 196–201. https://doi.org/10.1145/3129676.3129704

[14] Ersin Dincelli and Sanjay Goel. 2017. Can privacy and security be friends? a cultural framework to differentiate security and privacy behaviors on online social networks. In *Proceedings of the 50th Hawaii International Conference on System Sciences*.

[15] Tamara Dinev, Jahyun Goo, Qing Hu, and Kichan Nam. 2009. User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal* 19, 4 (2009), 391–412. https://doi.org/10.1111/j.1365-2575.2007.00289.x arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1365-2575.2007.00289.x

[16] Matias Dodel and Gustavo Mesch. 2018. Inequality in digital skills and the adoption of online safety behaviors. *Information, Communication & Society* 21, 5 (2018), 712–728. https://doi.org/10.1080/1369118X.2018.1428652 arXiv:https://doi.org/10.1080/1369118X.2018.1428652

[17] Claudia Eckert. 1965. *IT Sicherheit: Konzepte - Verfahren- Protokolle* (10 ed.). De Gruyter Studium, Berlin.

[18] European Commission. 2017. Europeans' Attitudes towards Cyber Security. 464a Wave EB87.4 (2017).

[19] Damien Warren Fernando, Nikos Komninos, and Thomas Chen. 2020. A Study on the Evolution of Ransomware Detection Using Machine Learning and Deep Learning Techniques. *IoT* 1, 2 (2020), 551–604. https://doi.org/10.3390/iot1020030

[20] Andy Field, Jeremy Miles, and Zoë Field. 2012. *Discovering Statistics Using R*. Sage Publications.

[21] Steven Furnell and David Emm. 2017. The ABC of ransomware protection. *Computer Fraud & Security* 2017, 10 (2017), 5 – 11. https://doi.org/10.1016/S1361-3723(17)30089-1

[22] Beth H. Jones and Amita Goyal Chin. 2015. On the efficacy of smartphone security: A critical analysis of modifications in business students' practices over time. *International Journal of Information Management* 35, 5 (2015), 561 – 571. https://doi.org/10.1016/j.ijinfomgt.2015.06.003

[23] Kaspersky Security Bulletin. 2019. Story of the year 2019: Cities under ransomware siege. https://securelist.com/story-of-the-year-2019-cities-under-ransomware-siege/95456/. Accessed: 2021-01-21.

[24] Amin Kharaz, Sajjad Arshad, Collin Mulliner, William Robertson, and Engin Kirda. 2016. UNVEIL: A large-scale, automated approach to detecting ransomware. In *Proceedings of the 25th USENIX Security Symposium*. 757–772.

[25] Amin Kharraz, William Robertson, Davide Balzarotti, Leyla Bilge, and Engin Kirda. 2015. Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. In *Detection of Intrusions and Malware, and Vulnerability Assessment*, Magnus Almgren, Vincenzo Gulisano, and Federico Maggi (Eds.). Springer International Publishing, Cham, 3–24.

[26] Matjaž Kljun, John Mariani, and Alan Dix. 2016. Toward Understanding Short-Term Personal Information Preservation: A Study of Backup Strategies of End Users. *Journal of the Association for Information Science and Technology* 67, 12 (2016), 2947–2963. https://doi.org/10.1002/asi.23526 arXiv:https://asistdl.onlinelibrary.wiley.com/doi/pdf/10.1002/asi.23526

[27] Hanna Krasnova, Natasha F. Veltri, and Oliver Günther. 2012. Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture. *Business & Information Systems Engineering* 4, 3 (June 2012), 127–135. https://doi.org/10.1007/s12599-012-0216-6

[28] Nada Lachtar, Duha Ibdah, and Anys Bacha. 2019. The Case for Native Instructions in the Detection of Mobile Ransomware. *IEEE Letters of the Computer Society* 2, 2 (2019), 16–19. https://doi.org/10.1109/LOCS.2019.2918091

[29] Fanny Lalonde Lévesque, M Fernandez, José, and Anil Somayaji. 2014. Risk prediction of malware victimization based on user behavior. In *2014 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE)*. 128–134. https://doi.org/10.1109/MALWARE.2014.6999412

[30] Zandile Manjezi and Reinhardt A. Botha. 2019. Preventing and Mitigating Ransomware. In *Information Security*, Hein Venter, Marianne Loock, Marijke Coetzee, Mariki Eloff, and Jan Eloff (Eds.). Springer International Publishing, Cham, 149–162.

[31] Steve Morgan. 2019. Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/. Accessed: 2021-01-21.

[32] Brigid O'Gorman, Candid Wueest, Dick O'Brien, Gillian Cleary, Hon Lau, John-Paul Power, Mayee Corpin, Orla Cox, Paul Wood, and Scott Wallace. 2019. *ISTR Internet Security Threat Report*. Technical Report. Symantec. 61 pages. https://docs.broadcom.com/doc/istr-24-2019-en

[33] R Core Team. 2020. *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing, Vienna, Austria. https://www.R-project.org/

[34] Elissa Redmiles. 2019. "Should I Worry?" A Cross-Cultural Examination of Account Security Incident Response. In *Proceedings of the 2019 IEEE Symposium on Security and Privacy*. 920–934. https://doi.org/10.1109/SP.2019.00059

[35] Elissa M. Redmiles and Eszter Hargittai. 2018. New Phone, Who Dis? Modeling Millennials' Backup Behavior. *ACM Trans. Web* 13, 1, Article 4 (Dec. 2018), 14 pages. https://doi.org/10.1145/3208105

[36] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2019. How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1326–1343. https://doi.org/10.1109/SP.2019.00014

[37] Elissa M. Redmiles, Ziyun Zhu, Sean Kross, Dhruv Kuchhal, Tudor Dumitras, and Michelle L. Mazurek. 2018. Asking for a Friend: Evaluating Response Biases in Security User Studies. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (Toronto, Canada) *(CCS '18)*. Association for Computing Machinery, New York, NY, USA, 1238–1255. https://doi.org/10.1145/3243734.3243740

[38] Ronny Richardson and Max M North. 2017. Ransomware: Evolution, mitigation and prevention. *International Management Review* 13, 1 (2017), 10.

[39] Charmaine Sample. 2013. Applicability of cultural markers in computer network attack attribution. In *Proceedings of the 12th European Conference on Information Warfare and Security*, Rauno Kuusisto and Erkki Kurkinen (Eds.). University of Jyvaskyla, Finland, 361–369.

[40] Camelia Simoiu, Joseph Bonneau, Christopher Gates, and Sharad Goel. 2019. "I was told to buy a software or lose my computer. I ignored it": A study of ransomware. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA. https://www.usenix.org/conference/soups2019/presentation/simoiu

[41] Eric Spero, Milica Stojmenović, Zahra Hassanzadeh, Sonia Chiasson, and Robert Biddle. 2019. Mixed Pictures: Mental Models of Malware. In *Proceedings of the 17th International Conference on Privacy, Security and Trust (PST)*. IEEE, 3.

[42] Symantec. 2017. Internet Security Threat Report Vol.22. https://docs.broadcom.com/doc/istr-22-2017-en. Accessed: 2021-01-21.

[43] Ibrar Yaqoob, Ejaz Ahmed, Muhammad Habib ur Rehman, Abdelmuttlib Ibrahim Abdalla Ahmed, Mohammed Ali Al-garadi, Muhammad Imran, and Mohsen Guizani. 2017. The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks* 129 (2017), 444 – 458. https://doi.org/10.1016/j.comnet.2017.09.003 Special Issue on 5G Wireless Networks for IoT and Body Sensors.

[44] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. 2020. Examining the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3313831.3376570

A QUESTIONNAIRES

Survey as presented to participants through Splendid Research in German, and back-translated to English, to ensure comprehension of a wider audience.

A.1 Survey in German

Teil 1: Demografie und Geräteinformationen

- Q1 Wie alt sind Sie?
  [Unter 18 Jahre / 18 bis 29 Jahre / 30 bis 39 Jahre / 40 bis 49 Jahre / 50 bis 59 Jahre / 60 bis 69 Jahre / Über 69 Jahre]
- Q2 Welches Geschlecht haben Sie?
  [Weiblich / Männlich / Divers / Keine Angabe]
- Q3 Was ist Ihr höchster Bildungsabschluss?
  [Grundschulabschluss / Hauptschulabschluss / Realschulabschluss (Mittlere Reife) / Gymnasium(Abitur) / Abgeschlossene Ausbildung / Fachhochschulabschluss / Hochschulabschluss]
- Q4 In welchem Beschäftigungsverhältnis stehen Sie derzeit?
  [Berufstätig in Vollzeit / Berufstätig in Teilzeit / Arbeitssuchend / Nicht erwerbstätig / Arbeitsunfähig / Selbstständig / Student/in / Schüler/in / Rentner/in]
- Q5 Wie hoch ist Ihr monatliches Haushaltsnettoeinkommen?
  [Unter 1.300 Euro / 1.300-1.699 Euro / 1.700-2.600 Euro / 2.600-3.600 Euro / 3.600-5.000 Euro / 5.000-18.000 Euro / Über 18.000 Euro]
- Q6 In welchem Bundesland leben Sie?
  [Baden-Württemberg / Bayern / Berlin / Brandenburg / Bremen / Hamburg / Hessen / Mecklenburg-Vorpommern / Niedersachsen / Nordrhein-Westfalen / Rheinland-Pfalz / Saarland / Sachsen / Sachsen-Anhalt / Schleswig-Holstein / Thüringen]
- Q7 In welchem Bereich arbeiten oder studieren Sie?
  [Architektur, Ingenieurwesen und Mathematik / Kunst und Design / Gebäude- und Bodenreinigung / Wirtschaft und Finanzen / Gemeinde- und Sozialdienst / Computer- und Informationstechnologie / Baugewerbe / Bildungs- und Bibliotheksswesen / Unterhaltung und Sport / Land-, Forst- und Tierwirtschaft und Gartenbau / Gastronomie / Gesundheitswesen / Installation, Wartung und Reparatur / Rechtswesen / Sozialwissenschaften / Management / Medien und Kommunikation / Militär und Polizei / Büro und Verwaltung / Pflegedienstleistungen / Rohstoffgewinnung, Produktion und Fertigung / Vertrieb / Transport und Logistik]
- Q8 Nutzen Sie in diesem Moment Ihren privaten Computer, um an dieser Umfrage teilzunehmen?
  [Ja, Nein]
- Q9 Welches Betriebssystem ist auf Ihrem privaten Computer installiert?
  [Windows / MacOS / Linux / Das weiß ich nicht. / Andere: [Freetext]]
- Q10 Welchen Internetbrowser nutzen Sie üblicherweise auf Ihrem privaten Computer?
  [Google Chrome / Microsoft Internet Explorer / Firefox / Microsoft Edge / Safari / Opera / Das weiß ich nicht. / Andere: [Freetext]]

Teil 2: Zur Feststellung, ob eine Ransomware-Attacke stattgefunden hat

- Information Text: Es gibt viele verschiedene Arten von Schadsoftware, die versuchen, an Geld von Nutzern zu gelangen. Sie lassen sich dabei grob in zwei Kategorien einteilen: a) Irreführende Anwendungen, die vortäuschen beispielsweise Antiviren-Software zu sein und b) Ransomware oder Erpressungssoftware. Bitte beantworten Sie die nachfolgenden Fragen, damit wir einschätzen können, ob Sie bereits Erfahrungen mit dieser Art von Schadsoftware gemacht haben.
- Q1A (Variant A) Gefälschte Antiviren-Software alarmiert für gewöhnlich den Nutzer über einen Sicherheitsvorfall oder ein Risiko auf dessen Computer und fordert ihn auf, das Problem zu beheben (z.B. eine Support-Hotline anzurufen oder Antiviren-Software herunterzuladen). Haben Sie jemals eines der folgenden Szenarien erlebt, bei denen Sie den Verdacht hatten, dass es sich dabei um einen Betrugsversuch handelt?
  [Eine Sicherheitsmeldung oder eine Warnung wurde eingeblendet, die Sie dazu aufgefordert hat, eine Support-Hotline anzurufen. / Eine Sicherheitsmeldung oder eine Warnung wurde eingeblendet, die Sie dazu aufgefordert hat, Software herunterzuladen oder zu kaufen. / Ich habe beide Szenarien bereits erlebt. / Ich habe keine dieser Szenarien erlebt. / Ich bin mir unsicher.]
- Q1B (Variant B) Gefälschte Antiviren-Software alarmiert für gewöhnlich den Nutzer über einen Sicherheitsvorfall oder ein Risiko auf dessen Computer und fordert ihn auf, das Problem zu beheben (z.B. eine Support-Hotline anzurufen oder Antiviren-Software herunterzuladen). Haben Sie jemals eines der folgenden Szenarien erlebt?

[Eine Sicherheitsmeldung oder eine Warnung wurde eingeblendet, die Sie dazu aufgefordert hat, eine Support-Hotline anzurufen. / Eine Sicherheitsmeldung oder eine Warnung wurde eingeblendet, die Sie dazu aufgefordert hat, Software herunterzuladen oder zu kaufen. / Ich habe beide Szenarien bereits erlebt. / Ich habe keine dieser Szenarien erlebt. / Ich bin mir unsicher.]

- Q1B_FollowUp Hatten Sie bei den beschriebenen Szenarien, die Sie erlebt haben, den Verdacht, dass es sich dabei um einen Betrugsversuch handeln könnte?
  [Ja,ich hatte den Verdacht,dass es sich um einen Betrugsversuch gehandelt haben könnte. / Nein, ich hatte nicht den Verdacht, dass es sich um einen Betrugsversuch gehandelt haben könnte.]
- Information Text: Ransomware ist eine weitere Art von Schadsoftware, die entweder Ihren Computer sperrt oder Ihre Dateien verschlüsselt. Wird Ihr Computer mit Ransomware infiziert, werden Ihnen Meldungen wie unten abgebildet angezeigt. Diese werden Sie darüber informieren, dass Sie ein Lösegeld zahlen müssen, um den Zugriff auf Ihren Computer und/oder Ihre Dateien wiederherzustellen sowie Anweisungen geben, wie Sie dies tun können.
- Q2 Haben Sie schon einmal eine ähnliche Meldung wie auf den abgebildeten Beispielen gesehen, die Sie benachrichtigt hat, dass Ihr Computer gesperrt oder Ihre Daten verschlüsselt wurden und die Sie dazu aufgefordert hat, ein Lösegeld zu zahlen? Anmerkung: Diese Art von Meldungen ist typisch für Ransomware und wird Sie explizit darauf hinweisen, dass Ihr Computer gesperrt oder Ihre Dateien verschlüsselt wurden. Sie werden Sie dabei nicht anweisen, sich Antivirus-Software herunterzuladen.
  [Ja, ich habe schon einmal eine Meldung gesehen, die mich darüber benachrichtigt hat, dass mein Computer gesperrt oder meine Daten verschlüsselt wurden. / Nein, ich habe noch nie eine Meldung gesehen, die mich darüber benachrichtigt hat, dass mein Computer gesperrt oder meine Daten verschlüsselt wurden.]
- Q3 Manchmal enthält eine Ransomware-Meldung ein Zeitlimit (typischerweise ein Timer, der herunterzählt), was bedeuten soll, dass sobald dieses Zeitlimit endet, der Zugang zu Ihrem Computer oder Ihre Dateien für immer verloren sei, oder aber, dass sich dann der Lösegeldbetrag erhöhe. Haben Sie schon einmal eine Meldung gesehen, die damit droht, dass Sie das Lösegeld innerhalb einer gesetzten Frist zahlen müssten, oder haben Sie einen solchen Timer schon einmal gesehen?
  [Ja, ich habe bereits Benachrichtigungen mit Zeitlimits oder einem Timer gesehen, die mich dazu aufgefordert haben, innerhalb einer Frist das Lösegeld zu zahlen. / Nein, ich habe noch nie eine Benachrichtigung mit einem Zeitlimit oder einem Timer gesehen.]
- Q4 Manche Ransomware-Varianten können Ihre Daten verschlüsseln, so dass Sie nicht mehr auf sie zugreifen können. In diesem Fall könnten Sie sehen, dass sich in allen Ordnern (1) Dateien mit Namen wie "HOW_TO_DECRYPT_FILES.TXT" oder (2) Dateien mit seltsamen Dateiendungen wie ".locky" befinden. Wurden Dateien von Ihnen bereits auf diese Art verschlüsselt, so dass Sie nicht mehr darauf zugreifen konnten?
  [Ja, Vorfälle wie (1) oder (2) habe ich schon erlebt oder ich habe ähnliche Meldungen darüber erhalten, dass meine Dateien verschlüsselt worden seien. / Nein, meine Dateien wurden noch nie derart verschlüsselt, dass ich nicht mehr auf sie zugreifen konnte.]
- Q5 Bitte lesen und beantworten Sie diese Frage sorgfältig! Haben Sie jemals eine Ransomware-Attacke erfahren, die Sie darüber informiert hat, dass Ihr Computer gesperrt oder Ihre Dateien verschlüsselt worden seien und Sie dazu aufgefordert hat, ein Lösegeld zu zahlen, um wieder Zugang zu Ihrem Computer oder Ihren Dateien zu erhalten?
  [Nein, ich habe noch nie eine Ransomware-Attacke auf meinen persönlichen Computer erlebt. / Ja, ich habe bereits eine Ransomware-Attacke auf meinen persönlichen Computer erlebt. / Ich bin mir unsicher.]
- Information Text (If Q5 was answered with "Ich bin mir unsicher."): Bitte helfen Sie uns, zu verstehen, warum Sie bei der letzten Frage die Option „Ich bin mir unsicher" ausgewählt haben. Im Folgenden gehen wir zu diesem Zweck noch einmal genauer auf das Thema Ransomware ein.Ransomware ist eine Art von Schadsoftware, die entweder Ihren Computer für Sie sperrt oder Ihre Daten verschlüsselt. Ransomware weist den User auch immer daraufhin, dass sein Computer gesperrt oder seine Daten verschlüsselt wurden, üblicherweise mit einer großen Pop-up-Meldung, die nur schwer oder gar nicht zu schließen ist. Ein häufig verwendeter Trick der Angreifer ist es, sich dabei als Strafverfolgungsbehörde auszugeben und dem Nutzer vorzuwerfen, er habe das Gesetz gebrochen, indem er sich entweder urheberrechtlich geschütztes Material (wie Musik oder Software) heruntergeladen oder illegales digitales Material (wie Pornografie) angesehen hätte. Die Ransomware fordert dann ein Lösegeld vom Nutzer, um dessen Computer oder Daten wieder freizugeben und gibt dem Nutzer Instruktionen, wie dieses Lösegeld auszurichten sei. Ransomware fordert den Nutzer hingegen nicht dazu auf, sich weitere Software (z.B. Antivirus-Software) herunterzuladen.

- Information Text (If "Ja" in Q2-Q4 but "No" in Q5): Sie haben zuvor angegeben, dass Sie noch nie eine Ransomware- Attacke auf ihren persönlichen Computer erlebt haben, aber mindestens ein Szenario, das üblich für Ransomware-Attacken ist. Warum meinen Sie, dass es sich bei dieser Erfahrung/diesen Erfahrungen nicht um Ransomware gehandelt hat? Im Folgenden gehen wir zu diesem Zweck noch einmal genauer auf das Thema Ransomware ein. Ransomware ist eine Art von Schadsoftware, die entweder Ihren Computer für Sie sperrt oder Ihre Daten verschlüsselt. Ransomware weist den User auch immer daraufhin, dass sein Computer gesperrt oder seine Daten verschlüsselt wurden, üblicherweise mit einer großen Pop-up-Meldung, die nur schwer oder gar nicht zu schließen ist. Ein häufig verwendeter Trick der Angreifer ist es, sich dabei als Strafverfolgungsbehörde auszugeben und dem Nutzer vorzuwerfen, er habe das Gesetz gebrochen, indem er sich entweder urheberrechtlich geschütztes Material (wie Musik oder Software) heruntergeladen oder illegales digitales Material (wie Pornografie) angesehen hätte. Die Ransomware fordert dann ein Lösegeld vom Nutzer, um dessen Computer oder Daten wieder freizugeben und gibt dem Nutzer Instruktionen, wie dieses Lösegeld auszurichten sei. Ransomware fordert den Nutzer hingegen nicht dazu auf, sich weitere Software (z.B. Antivirus-Software) herunterzuladen.

- Q6 (If Q5 was answered with "Ich bin mir unsicher."): Bitte bestätigen Sie, ob Sie jemals eine Ransomware-Attacke auf Ihren persönlichen Computer erlebt haben. Das wäre dann der Fall, wenn Sie eine Benachrichtigung erhalten haben, dass Ihr Computer gesperrt oder Ihre Daten verschlüsselt worden seien, die nur schwer oder gar nicht zu schließen war und die Sie dazu aufgefordert hat, ein Lösegeld zu entrichten, um wieder Zugang zu Ihrem Computer oder Ihren Dateien zu erhalten. Bitte wählen Sie „Ja" aus, wenn Sie eine solche Nachricht erhalten haben, unabhängig davon, ob Sie das Lösegeld gezahlt haben oder nicht. *[Nein, ich habe noch nie eine Ransomware-Attacke auf meinen persönlichen Computer erlebt. / Ja,ich habe bereits eine Ransomware-Attacke auf meinen persönlichen Computer erlebt. / Ich bin mir immer noch unsicher.]*
- Q7 (If Q5 and Q6 was answered with "Ja"): Bitte beschreiben Sie die Ransomware-Attacke, die Sie persönlich erlebt haben. Erinnern Sie sich an den Wortlaut der Benachrichtigung und an die genauen Instruktionen, die Ihnen gegeben wurden? Wie sah die Benachrichtigung/Ihr Bildschirm aus? Wurde irgendeine Funktion Ihres Computers deaktiviert? Bitte geben Sie so viele Details wie möglich an. [Freitext]

Teil 3: Details der Ransomware-Attacke

The following questions were shown to respondents who reported experiencing a ransomware attack (i.e., selected "Yes" in Q7 or Q10 in the previous section). Die folgenden Fragen beziehen sich auf die Ransomware-Attacke, die Sie erfahren haben. Sollten Sie bereits mehrere Attacken erlebt haben, beantworten Sie die Fragen bitte hinsichtlich des Vorfalls, der als letztes passiert ist.

- Q1 Wann hat die Ransomware-Attacke stattgefunden? Sollten Sie sich nicht an das genaue Datum erinnern können, nennen Sie uns bitte eine ungefähre Schätzung (idealerweise Jahr und Monat der Attacke). [Freetext]
- Q2 Nennen Sie den Namen der Ransomware, sofern Sie sich daran erinnern können. Einige Beispiele sind "CryptoLocker", "CryptoWall", "Locky", "TeslaCrypt". [Freetext]
- Q3 Wie sollten Sie das Lösegeld entrichten? Also, was war die verlangte Zahlungsmethode in der Forderung? Bitte wählen Sie alle Methoden aus, die Ihnen zur Verfügung standen.
  [Kryptowährung (z.B. Bitcoin, Litecoin, Zcash) / Prepaid-System(z.B.Paysafecard von REWE, Rossmann...) / Online-Bezahldienst (z.B. PayPal) / Banküberweisung / Premium-Textnachricht an den Angreifer / Kreditkarte / Ich kann mich nicht erinnern. / Andere: [Freetext]]
- Q4 Wie hoch war der Lösegeldbetrag?
  [Lösegeldbetrag:[Freetext] / Ich kann mich nicht erinnern.]
- Q5 In welcher Währung wurde der geforderte Lösegeldbetrag angegeben?
  [Euro / Kryptowährung: [Freetext] / Ich kann mich nicht erinnern. / Andere: [Freetext]]
- Q6 Wies die Ransomware-Attacke, die Sie erlebt haben, die folgenden Charakteristiken auf? Bitte wählen Sie alle Aussagen aus, die zutreffen.
  [Ich habe eine Meldung gesehen, die mich darüber informiert hat, dass mein Computer gesperrt worden sei. / Ich habe eine Meldung gesehen, die mich darüber informiert hat, dass meine Daten oder Dateien verschlüsselt worden seien. / Mir wurde gesagt, dass ich nur dann wieder Zugriff auf meine Daten, Dateien oder meinen Computer erhalten würde, wenn ich ein Lösegeld bezahle. / Mir wurde ein Timer angezeigt und gesagt, dass ich das Lösegeld zahlen muss, bevor dieser vollständig heruntergezählt habe. / Ich habe eine Benachrichtigung einer angeblichen Strafverfolgungsbehörde (z.B. Polizei, Staatsanwaltschaft) gesehen, die mich darüber informiert hat, dass ich bei einer illegalen Online-Aktivität ertappt worden sei. / Ich habe nichts davon erlebt.]
- Q7 Wie viel Zeit wurde Ihnen anfänglich gegeben, um das Lösegeld zu zahlen? (Z.B. 24 Stunden, fünf Tage, eine Woche usw.) [Freetext]
- Q8 Haben Sie den geforderten Betrag gezahlt?
  [Ja, ich habe das geforderte Lösegeld gezahlt. / Nein, ich habe das geforderte Lösegeld nicht gezahlt.]
- Q9 Was hat Sie dazu bewegt, das Lösegeld zu zahlen oder eben nicht zu zahlen? Beschreiben Sie in kurzen Worten die Faktoren, die bei dieser Entscheidung eine Rolle gespielt haben. [Freetext]
- Q10 (If Q8 was answered with "Yes") Wurde Ihnen wieder Zugriff auf Ihre Daten/Ihren Computer gewährt, nachdem Sie das Lösegeld gezahlt hatten?
  [Ja, mein Zugriff wurde wiederhergestellt. / Nein, mein Zugriff wurde nicht wiederhergestellt. / Ich bin mir unsicher.]
- Q10 Haben Sie die Polizei über die Ransomware-Attacke informiert?
  [Ja, ich habe den Vorfall der Polizei gemeldet. / Nein, ich habe den Vorfall nicht der Polizei gemeldet.]
- Q11 Haben Sie eine (oder mehrere) der folgenden Gegenmaßnahmen ergriffen, um die Ransomware zu entfernen und den Zugang auf Ihre Daten oder Ihren Computer wiederzuerlangen? Bitte wählen Sie alle Punkte, die zutreffen.
  [Ich habe meinen Computer neugestartet. / Ich habe versucht, die Dateiendungen der verschlüsselten Dateien in ihr ursprüngliches Format zurück zu ändern und sie zu öffnen. / Ich habe meinen Computer mit Hilfe eines Backups wiederhergestellt. / Ich habe ein Programm gefunden und genutzt, um die Ransomware zu entfernen. / Ich habe ein Programm gefunden und genutzt, um meine Daten zu entschlüsseln. / Ich habe eine andere Gegenmaßnahme ergriffen: [Freetext] / Ich habe keine Gegenmaßnahmen ergriffen. / Ich kann mich nicht erinnern.]
- Q12 Konnten Sie die Ransomware erfolgreich entfernen?
  [Ja, ich konnte die Ransomware entfernen und habe keine meiner Daten oder Dateien verloren. / Ja, ich konnte die Ransomware entfernen, aber habe meine Daten oder Dateien verloren. / Nein, ich konnte die Ransomware nicht entfernen und habe weiterhin keinen Zugriff auf meine Daten oder meinen Computer.]
- Q13 Wie konnten Sie die Ransomware entfernen?
  [Ich habe das Lösegeld gezahlt. / Ich habe meinen Computer neugestartet. / Ich habe meinen Computer mit Hilfe eines Backups wiederhergestellt. /

Ich habe ein Programm gefunden und genutzt, dass die Ransomware entfernt und meine Dateien entschlüsselt hat. / Ich habe eine andere Methode angewendet, um die Ransomware zu entfernen: [Freetext] / Ich bin mir unsicher; ich habe die Ransomware nicht selbst entfernt. / Ich konnte die Ransomware nicht entfernen und hatte weiterhin keinen Zugriff auf meine Daten oder meinen Computer]

- Q14 Haben Sie sich Hilfe gesucht, um die Ransomware zu entfernen? Bitte wählen Sie alle zutreffenden Antworten aus.
  [Ich habe mir Hilfe bei meinen Freunden, Bekannten oder Verwandten gesucht. / Ich habe mir Hilfe bei meinen Kollegen gesucht. / Ich habe mir Hilfe bei einem Computer-Fachgeschäft oder einem IT-Experten gesucht. / Ich habe mir bei niemandem Hilfe gesucht.]
- Q15 Welche anderen Ressourcen haben Sie genutzt, um sich darüber zu informieren, was Ransomware ist, ob und wie man sie entfernen kann oder ob man das Lösegeld zahlen sollte? [Freetext]
- Q16 Was denken Sie, wie Sie sich mit Ransomware infiziert haben könnten? [Freetext]
- Q17 Denken Sie, eine der folgenden Aktionen könnte dazu geführt haben, dass Sie sich mit Ransomware infiziert hatten? Bitte wählen Sie alle zutreffenden Antworten aus.
  [Ich habe auf einen bösartigen Link in einer E-Mail geklickt. / Ich habe Schadsoftware heruntergeladen. / Ich habe auf eine Warnmeldung oder Benachrichtigung geklickt, die mir angezeigt wurde (aus Versehen oder mit Absicht, um sie z.B. zu schließen). / Ich habe eine Werbung angeklickt (aus Versehen oder mit Absicht), während ich im Internet gesurft oder soziale Medien genutzt habe. / Ich habe im Internet gesurft und dabei nichts angeklickt. / Anderes.]
- Q18 Haben Sie Ihr Online-Verhalten oder Ihr Verhalten im Hinblick auf die Sicherheit Ihres Computers allgemein seit der Ransom-Attacke verändert? Bitte wählen Sie alle zutreffenden Antworten aus.
  [Ich habe mein Betriebssystem gewechselt. / Ich habe angefangen, meine Daten mit einem Backup auf einer externen Festplatte oder einem Cloud-Server zu sichern. / Ich habe ein Antivirus-/Firewall-Produkt gekauft. / Ich habe die Einstellungen meines Computers geändert (z.B. die Anzeige der Dateiendungen aktiviert, Windows Script Host deaktiviert, Login eingeschränkt usw.). / Ich habe automatische Updates für mein Betriebssystem, meinen Browser, meine Antivirus-Software oder andere Programme eingestellt. / Ich habe meinen Standardbrowser gewechselt. / Ich sichere meine Daten häufiger mit einem Backup auf einer externen Festplatte oder einem File Storage Server. / Ich habe mein Antivirus-/Firewall-Produkt gewechselt. / Ich bin vorsichtiger, welche Webseiten ich besuche, was ich mir herunterlade und welche Anhänge ich öffne. / Ich aktualisiere mein Betriebssystem, meinen Browser, meine Antivirus-Software oder andere Programme häufiger. / Ich habe meine Festplatte verschlüsselt.]
- Q19 Für wie wahrscheinlich schätzen Sie es ein, dass Sie noch einmal eine Ransomware- Attacke erleben? Bitte geben Sie eine Zahl zwischen 0 und 100 an, wobei 100 bedeutet, dass Sie auf jeden Fall (also zu 100%) noch einmal eine Ransomware-Attacke erleben werden und 0 bedeutet, dass Sie auf gar keinen Fall (also zu 0%) noch einmal eine Ransomware-Attacke erleben werden. [Slider with a range from 0 to 100]
- Q20 Stellen Sie sich vor, Sie würden heute noch einmal eine Ransomware-Attacke erleben und die einzige Möglichkeit, wieder Zugriff auf Ihre Daten zu erlangen wäre, das Lösegeld (hier 300€) zu zahlen. Für wie wahrscheinlich halten Sie es, dass Sie das Lösegeld zahlen würden? Bitte geben Sie eine Zahl zwischen 0 und 100 an, wobei 100 bedeutet, dass Sie auf jeden Fall (also zu 100%) das Lösegeld zahlen würden und 0 bedeutet, dass Sie auf gar keinen Fall (also zu 0%) das Lösegeld zahlen würden. [Slider with a range from 0 to 100]

Teil 4: Sicherheitsgewohnheiten

The questions in this section were only shown to those participants that stated to have encountered a ransomware attack ("Ja" in Q5 and Q6 in "Teil 2") Bitte beantworten Sie die folgenden Fragen über Ihr Online-Verhalten direkt vor der von Ihnen erlebten Ransomware-Attacke.

- Q1 Wie viel Zeit haben Sie ungefähr jeden Tag im Internet an Ihrem privaten Computer verbracht in dem Zeitraum, in dem die Ransomware-Attacke stattfand?
  [Weniger als 1 Stunde / Zwischen 1 und 2 Stunden / Zwischen 3 und 5 Stunden / Zwischen 6 und 10 Stunden / Mehr als 10 Stunden]
- Q2 Wie viele E-Mails haben Sie täglich ungefähr auf Ihrem privaten Computer geöffnet in dem Zeitraum, in dem die Ransomware-Attacke stattfand?
  [Weniger als 5 E-Mails / Zwischen 5 und 10 E-Mails / Zwischen 11 und 20 E-Mails / Zwischen 21 und 50 E-Mails / Mehr als 50 E-Mails]
- Q3 Wie regelmäßig haben Sie Dateien von Torrent-Webseiten (z.B. "The Pirate Bay", "Extratorrent", "TorrentZ2") heruntergeladen in dem Zeitraum, in dem die Ransomware-Attacke stattfand?
  [Ich habe regelmäßig Dateien von Torrent-Webseiten heruntergeladen. / Ich habe manchmal Dateien von Torrent-Webseiten heruntergeladen. / Ich habe selten Dateien von Torrent-Webseiten heruntergeladen. / Ich habe nie Dateien von Torrent-Webseiten heruntergeladen.]
- Q4 Auf welche Weise haben Sie Dateien auf Ihrem privaten Computer gespeichert, von denen Sie nicht wollten, dass sie jemand sieht in dem Zeitraum, in dem die Ransomware-Attacke stattfand? Bitte wählen Sie alle zutreffenden Antworten aus.
  [Mein Computer war passwortgeschützt. / Alle meine sensiblen Daten befanden sich in einem passwortgeschützten Ordner. / Alle meine sensiblen Daten befanden sich in einem versteckten Ordner, der schwer zu finden war. / Ich habe Daten nur dann "versteckt", wenn ich erwartet habe, dass jemand anderes meinen Computer zeitweise benutzt. / Ich habe Daten, die niemand sehen durfte, immer sofort gelöscht. / Ich hatte keine sensiblen Daten auf meinem Computer.]
- Q5 Hatten Sie in dem Zeitraum, in dem die Ransomware-Attacke stattfand, die Gewohnheit, Ihre Daten in einem Backup auf einer externen Festplatte oder in der Cloud zu sichern? Welche der folgenden Aussagen beschreibt Ihr Verhalten am ehesten?

[Ich habe in diesem Zeitraum nie Backups gemacht. / Ich habe jährlich ein Backup gemacht. / Ich habe alle paar Monate ein Backup gemacht. / Ich habe alle paar Wochen ein Backup gemacht. / Ich habe fast täglich ein Backup gemacht.]

- Q6 War Ihre Festplatte verschlüsselt in dem Zeitraum, in dem die Ransomware-Attacke stattfand?
  [Ja, meine Festplatte war verschlüsselt. / Nein, meine Festplatte war nicht verschlüsselt.]
- Q7 Nehmen Sie an, Sie würden gelegentlich (z.B. alle zwei Wochen) Ihre Login-Daten auf einer Webseite eingeben. Ihr Browser bietet Ihnen an, Ihre Angaben zu speichern, um zukünftig Formulare automatisch ausfüllen zu können. Was hätten Sie generell in dem Zeitraum, in dem die Ransomware-Attacke stattfand, getan?
  [Ich hätte meine Angaben generell gespeichert. / Ich hätte meine Angaben generell nicht gespeichert.]
- Q8 Nehmen Sie an, Flash Player, Adobe Reader oder Flash benachrichtigen Sie über ein Update, das Sie herunterladen und installieren sollen. Was hätten Sie generell in dem Zeitraum, in dem die Ransomware-Attacke stattfand, getan?
  [Ich hätte die Option "Installiere Updates" gewählt. / Ich hätte die Option "Erinnere mich später" gewählt. / Ich sehe selten Benachrichtigungen solcher Software. / Ich sehe nie Benachrichtigungen solcher Software.]
- Q9 Nehmen Sie an, Sie erstellen einen neuen Account auf einer Webseite, die Sie zukünftig gelegentlich nutzen wollen (z.B. ein Vielfliegerkonto bei einer Fluggesellschaft). Wie hätten Sie in dem Zeitraum, in dem die Ransomware-Attacke stattfand, ein Passwort erstellt?
  [Ich hatte dasselbe Passwort für alle meine Accounts. / Ich hatte verschiedene Passwörter, zwischen denen ich gewechselt habe,wenn ich einen neuen Account erstellen wollte. / Ich hatte eine Vorlage für Passwörter, die ich für jeden Account ein wenig abgeändert habe. / Ich habe für jeden Account ein völlig neues Passwort erstellt und sichergestellt, dass es stark genug ist.]
- Q10 Besaßen Sie in dem Zeitraum, in dem die Ransomware-Attacke stattfand, einen eigenen Blog oder eine eigene Webseite?
  [Ja, ich hatte einen eigenen Blog oder eine eigene Webseite. / Nein, ich hatte weder einen eigenen Blog noch eine eigene Webseite.]
- Q11 Die Zwei-Faktor-Authentifizierung gilt als besonders sicher und funktioniert beispielsweise wie folgt: wenn Sie sich online anmelden, geben Sie Ihren Benutzernamen und Ihr Passwort ein. Auf Ihrem Smartphone erhalten Sie dann per SMS oder durch eine von Ihnen installierte App einen Code, den Sie dann zusätzlich bei der Anmeldung eingeben müssen. Haben Sie in dem Zeitraum, in dem die Ransomware-Attacke stattfand, die Zwei-Faktor-Authentifizierung für mindestens einen Ihrer persönlichen Accounts genutzt?
  [Ja, ich habe Zwei-Faktor-Authentifizierung für mindestens einen meiner persönlichen Accounts genutzt. / Nein, ich habe Zwei-Faktor-Authentifizierung für keinen meiner persönlichen Accounts genutzt]
- Q12 Nutzten Sie in dem Zeitraum, in dem die Ransomware-Attacke stattfand, einen Computer oder Laptop an Ihrer Arbeitsstelle?
  [Ja, ich habe an meiner Arbeitsstelle einem Computer genutzt. / Nein, ich habe an meiner Arbeitsstelle keinen Computer genutzt. / Nicht anwendbar.]
- Q13 (If Q12 was answered with 'Ja") Für welche Aufgaben haben Sie den Computer an Ihrer Arbeitsstelle in dem Zeitraum, in dem die Ransomware-Attacke stattfand, genutzt?
  [Internet oder E-Mails / Textverarbeitung oder Desktop-Publishing / Tabellenkalkulation oder Datenbanken / Kalender oder Terminplanung / Grafikbearbeitung oder Design / Programmierung / Anderes: [Freetext]]

Teil 5: IT Quiz

- Q1 Wählen Sie die größere Datenmenge.
  [Ein Kilobyte / Ein Megabyte]
- Q2 Der Begriff "Netzneutralität" steht für:
  [Das Veröffentlichen überparteilicher Inhalte auf Webseiten. / Die Art und Weise, in der Wikipedia-Redakteure angehalten sind, neue Einträge zu behandeln. / Die Gleichbehandlung digitaler Inhalte durch Internetanbieter / Die Vereinbarung unter Nutzern bestimmter Webseiten, keine überparteilichen Kommentare oder Arbeiten zu veröffentlichen.]
- Q3 Für was steht die Abkürzung "RAM"?
  [Random Access Monitoring / Running Access Mount / Random Access Memory / Random Access Mount]
- Q4 Bei welchem der folgenden Teile handelt es sich um ein E/A-Gerät?
  [CPU / Tastatur / Netzteil / USB-Anschluss]
- Q5 Sie wollen eine Banküberweisung (bei ihrer Bank "Money Bank") online durchführen. Welche der folgenden Webseiten erscheint Ihnen am sichersten zu sein?
  [http://www.MoneyBank.de / https://www.MoneyBamk.de / https://www.MoneyBank.de / https://www.MoneyBank.net.de]
- Q6 Was bezeichnet man als einen "Trojaner"?
  [Ein Programm, das sich selbst repliziert, um andere Computer zu infizieren. / Ein Programm, das jeden Tastenanschlag eines Computernutzers aufzeichnet. / Ein Programm, das sich als ein anderes Programm ausgibt. / Ein Programm, das sich jedes Mal, wenn es ein System infiziert, anders kodiert.]
- Q7 1 Byte besteht aus...
  [4 Bits. / 8 Bits. / 16 Bits. / 32 Bits.]
- Q8 Daten werden permanent gespeichert auf...
  [dem RAM. / der Festplatte. / der CPU. / dem Cache.]

A.2 Survey translated from German to English

We report the English version of the changed parts of the German survey and describe our changes. All other questions remain the same as reported by Simoiu et al. [40].

Part 1: Demographics and device details

- Q1 How old are you?
  [Under 18 years / 18 to 29 years / 30 to 39 years / 40 to 49 years / 50 to 59 years / 60 to 69 years / Over 69 years]
  Changed to reflect quotas provided by Splendid Research to facilitate recruiting
- Q2 Which gender are you?
  [Female / Male / Diverse / Prefer not to say]
  Changed to be more inclusive
- Q3 What is the highest level of education you have completed?
  [Elementary school / Certificate of Secondary Education / Secondary school certificate / General qualification for university entrance (Abitur) / completed apprenticeship / Polytechnic degree / University degree]
  Changed to reflect German education system and Splendid Research quotas
- Q4 What is your current employment status?
  [Employed full time / Employed part time / Unemployed looking for work / Not working / Not able to work / Self-employed / Student in tertiary education / Student in first and secondary education / Retired]
  Changed to reflect different meanings of student in German and added self-employed
- **Removed question on ethnicity, since it is not common to ask this in German surveys.**
- Q5 What is your monthly household income?
  [Under 1.300 Euro / 1.300-1.699 Euro / 1.700-2.600 Euro / 2.600-3.600 Euro / 3.600-5.000 Euro / 5.000-18.000 Euro / Over 18.000 Euro]
  Changed to reflect quotas provided by Splendid Research to facilitate recruiting
- Q6 In which federal state of Germany do you live?
  [Baden-Wuerttemberg / Bavaria / Berlin / Brandenburg / Bremen / Hamburg / Hesse / Mecklenburg-Western Pomerania / Lower Saxony / North Rhine-Westphalia / Rhineland-Palatinate / Saarland / Saxony / Saxony-Anhalt / Schleswig-Holstein / Thuringia]
  Changed to reflect quotas provided by Splendid Research to facilitate recruiting

Part 2: Establishing whether a ransomware attack occurred

Tested variants of the compound question in the original work (Q1A + Q1B and Q1B_FollowUp

- Q1A (Variant A) Misleading antivirus-applications usually alert the user to a security issue or vulnerability on their computer, and prompt them to act (e.g. call a tech support number, download or purchase anti-virus software) in order resolve the issue. Have you ever experienced any of the following scenarios that you suspect were scams?
  [A security alert or warning popped up, prompting you to call a tech support number. / A security alert or warning popped up, prompting you to purchase or download software. / I have experienced both the above scenarios / I have not experienced any of the above scenarios / I am not sure]
- Q1B (Variant B) Misleading antivirus-applications usually alert the user to a security issue or vulnerability on their computer, and prompt them to act (e.g. call a tech support number, download or purchase anti-virus software) in order resolve the issue. Have you ever experienced any of the following scenarios?
  [A security alert or warning popped up, prompting you to call a tech support number. / A security alert or warning popped up, prompting you to purchase or download software. / I have experienced both the above scenarios / I have not experienced any of the above scenarios / I am not sure]
- Q1B_FollowUp In the case of the described scenarios, which you have experienced, did you suspect that they were scams?
  [Yes, I suspected that they could be scams./ No, I didn't suspect that they could be scams.]
- Information Text: **Text was the same as in the original study, but images were updated to ones which were reported for somewhat recent ransomware attacks in Germany, see Figure 1**.
- Q3 Sometimes, ransomware includes a time limit (typically in the form of a timer counting down), indicating that if you don't pay before the specified time limit, then access to your computer and your files will be lost forever, or the ransom will increase. Have you ever been told that you must pay within some time limit or seen such a timer counting down?
  [Yes, I've seen messages with time limits or timers counting down, telling me I must pay before they expire. / No, I've never seen messages with time limits or timers counting down.]
  Removed mention of decryption key in the question, since this phrasing was not easy to comprehend for lay people.
- Information Text (If Q5 was answered with "I am not sure"): Please help us understand why you have selected "I am not sure". Below are some clarifications about ransomware. Ransomware is a type of malware that will either lock your computer, or encrypt your data. Ransomware will inform users that their computers are locked or their data is encrypted, typically with a large pop-up screen that is difficult or impossible to close. A common trick is to impersonate law-enforcement agencies and claim that the user has broken the law by downloading copyrighted materials such as pirated music or software, or by viewing other illegal digital materials such as pornography. Ransomware will demand money

to re-gain access to your computer and/or files, and provide instructions on how to pay. Ransomware does not tell users to download software (e.g. antivirus software) to fix the issue.
Added phrasing "or impossible", since lay people users may not know all possibilities to close pop-ups, so it may appear impossible to them.

Part 3: Ransomware Attack details

- Q3 How were you asked to pay the ransom (i.e. what was the method of payment used in the attack)? Please choose all methods that were available to you.
  [Cryptocurrency (e.g. Bitcoin, Litecoin, Zcash) / Payment voucher system (e.g.Paysafecard from REWE,Rossmann...) / Online paymentservice (e.g. PayPal) / wire transfer / premium-rate text message to attacker / credit card / I don't remember / Other: [Freetext]]
  Adjusted payment voucher examples to Germany, added online payment service and enabled selecting multiple answers
- Q11 Did you try any of of the following strategies to remove the ransomware and restore access to your computer or files? Please select all that apply.
  [I re-started my computer. / I tried to change the extension of files back to their original format and open them / I restored my computer from a backup / I found and ran a tool to remove the ransomware / I found and ran a tool to decrypt my files / I used some other strategy: [Freetext] / I did not use any of these strategies / I don't remember]
  Added option: I did not use any of these strategies
- Q14 Did you seek help from anyone else to remove the ransomware? Please select all that apply.
  [I sought help from friends, acquaintances or family. / I sought help from co-workers. / I sought help from a store specialized in computers, or another IT expert / I did not seek help from anyone.]
  Moved acquaintances from group with co-workers to group with family and friends, as co-workers were perceived to be a distinct group, as they were work-related contacts, in contrast to the others.
- **Q19 was presented as part of the question before (Q18) in the original paper and thus only shown to participants who had already experienced a ransomware attack, and not to all participants, like in the original work.**
- **Q20 was presented as part of Q18 in the original paper and thus only shown to participants who had already experienced a ransomware attack, and not to all participants, like in the original work.**

Part 4: Security habits

There were no changes to questions in this part of the survey.

Part 5: Computer knowledge quiz

There were no changes to questions in this part of the survey.