Contract Research for SentinelOne

Exploring the Psychological Mechanisms used in Ransomware Splash Screens

FINAL REPORT
July 2017

Prepared By:

Dr. Lee Hadlington,
De Montfort University

Prepared for

SentinelOne

1. Overview

The present study examined a selection of 76 ransomware splash screens collected from a variety of sources. These splash screens were analysed according to surface information, including aspects of visual appearance, the use of language, cultural icons, payment and payment types. The results from the current study showed that, whilst there was a wide variation in the construction of ransomware splash screens, there was a good degree of commonality, particularly in terms of the structure and use of key aspects of social engineering used to elicit payment from the victims. There was the emergence of a sub-set of ransomware that, in the context of this report, was termed 'Cuckoo' ransomware. This type of attack often purported to be from an official source requesting payment for alleged transgressions.

2. Introduction

In the last few months several high-profile global cyber attacks have brought about an increased awareness of the scourge of ransomware on businesses and individuals (for example see http://www.bbc.co.uk/news/technology-39920141). Ransomware has been previously defined as:

> "*a piece of pernicious software that exploits a user's computer vulnerabilities to sneak into the victim's computer and encrypt all his/her files; then the attacker keeps the files locked unless the victim agrees to pay a ransom*" (Liao, 2008; p. 361).

A great deal of research has been conducted on the underlying technical mechanisms associated with ransomware (see Liao, 2008; Luo & Liao, 2007). However, detailed explorations examining the content of the initial ransomware splash screens and the underlying psychological techniques employed by the attackers to obtain payment have been severely lacking.

In this present study, the concept of a 'splash screen' is operationalised as the initial warning screen that alerts the victim to the attack, and is seen as the online equivalent to the ransom note (see images 1-8 in this report). A detailed exploration of these ransomware splash screens offers a variety of potential benefits, not least the capacity to stimulate further research in this area. A better understanding of the psychological techniques used by attackers in these splash screens could provide individuals with critical information to be used as part of their decision-making process. This could also include relevant signposting towards further help from cybersecurity professionals and law enforcement, an action that attackers are keen to dissuade victims from doing. From the research perspective, such an exploration could highlight potential categories for ransomware splash screens aligned to their use of particular tactics and associated levels of sophistication. This may provide a useful framework for security professionals and law enforcement officers alike, and allow for a more consistent discussion between groups when tackling such cybercrimes.

2.1 Is "Psychology" contained within Ransomware Splash Screens?

In principle, without interviewing the designers of ransomware attacks, we cannot say for definite if they have consciously incorporated key psychological principles to enhance their chances of being paid. However, irrespective of this conscious design and knowledge of the attacker, the impact on the victim remains the same. In the context of the current research key tenets taken from aspects of social engineering will be used to frame critical psychological components included in the ransomware attack. These aspects can be mapped jointly onto multiple facets of ransomware splash screens, including both the visual appearance and the language that is being used.

The concept of social engineering is viewed as the use of manipulation, persuasion, and influence by an attacker to obtain sensitive information (Uebelacker & Quiel, 2014). In the current discussion, the use of social engineering techniques is also seen as a mechanism to leverage payment from victims. Hadnagy (2010) provides an excellent overview of the key mechanisms used in social engineering, but in the context of the present study the focus will be on three key principles detailed below.

- **Scarcity**: in this instance people find objects or opportunities more attractive if they are rare, scarce or hard to obtain. Scarcity is often matched with the use of urgency, usually linked to a time-critical offer which means people are quick to react and will make fundamental errors in decision-making.
- **Authority**: individuals are more willing to respond to requests, or follow directions, from someone they view as being in authority. This is usually irrespective of whether the individual in question actually holds authority – if we believe they do, we will follow their instructions. An example of this is legal authority, a principle that is based on the individual being a member of law enforcement or a government body.
- **Liking**: this is a straightforward concept and details the fact that if you get someone to like you, they will likely comply with your requests. Examples of this in this study include the use of humour as well as a conversational tone in the ransomware splash screens.

2.2 Aims and Objectives

The present study aims to provide the first attempt at exploring the content of ransomware splash screens. Inferences about the underlying psychological principles that might be used to elicit payment from victims will be made. The sample of ransomware splash screens will also be explored for their shared features as well as individual nuances. It is hoped that this initial exploration will highlight critical elements contained in ransomware splash screens that could be used to help victims make better, more informed decisions. Similarly it is suggested that this report will provide security professionals, law enforcement officials and academic researchers a basis for further research in this area.

3. Methodology

In the context of the current report, the main focus was the content of the initial splash screens that provided the victim with information about the attack. To limit the scope and breadth of the current report, no further additional files were examined linked into the splash screen. The exploration of the splash screens focused on the content including but not limited to:

- Visual and aesthetic
- Use of language and overt use of social engineering techniques
- Use of imagery or cultural icons
- Information related to payment type and content

The sample used in the present study consisted of 76 ransomware splash screens which were collected by the research team at SentinelOne, a leading endpoint security company based in the U.S., between April 1 – June 30, 2017. The sample included splash screens from a variety of sources including:

- Testing using collected live malware samples
- 'ID Ransomware' website[1]
- 'Bleeping Computer' forum[2]
- 'Windows Club'[3]
- VirusTotal[4]
- Malekal malware database[5]

Splash screens were analysed for content based on the elements introduced in sections 2.1 and 3. Where a particular feature was detected, this was recorded, feeding into the quantitative data for the present study. A further

[1] ID Ransomware - https://id-ransomware.malwarehunterteam.com/
[2] Bleeping Computer forum - https://www.bleepingcomputer.com/forums/
[3] The Windows Club - http://www.thewindowsclub.com/
[4] VirusTotal – http://www.virustotal.com
[5] Malekal website - http://malwaredb.malekal.com/

qualitative exploration of aspects of the language used was also incorporated, and this focused on the use of mechanisms that could be used to persuade the victim to pay the ransom.

4. Results

In the context of the overview of the ransomware splash screens, several key trends were observed, and some novel aspects were also identified for discussion.

4.1 Payment

In general, Bitcoin (BTC) was the attackers preferred mechanism for payment, with 75% of ransomware splash screens asking for payment in BTC. In an associated element, 39% of the ransomware splash screens actively provided clear instructions on how the victim could buy Bitcoins. A smaller proportion of the ransomware splash screens advised the victim to download the Tor web browser to buy Bitcoins from other sources. In some individual cases the victims were asked to pay in other forms, such as MoneyPak or Western Union, but these represented just two of the sample in the current study.

Just over half of the total sample contained the requested ransom amount (55%) in the initial splash screen. The payments requested for the ransom ranged from a minimum 0.001 BTC ($30 USD) to a maximum of 13 BTC ($4,980 USD) in one example. Controlling for this one extreme amount, the average amount requested by attackers was 0.47 BTC ($1,164 USD). In several cases the ransom amount was seen to increase exponentially as time between the onset of the attack and payment elapsed. In general, attackers doubled the ransom amount after a certain time period, increasing the aspects of time criticality.

4.2 Time Criticality

The feature of time criticality (e.g. noting a deadline for payment that the victim must adhere to before consequences to their data occur) appeared in over half of the sample (57%) and is one of the key features used in social engineering attacks to persuade a victim to act quickly. In the context of the social engineering framework presented by Hadnagy (2010) this aspect of time criticality links into the notion of scarcity, which in turn creates a sense of urgency. For instance, an attacker might indicate that if payment is not made by a certain time, their files could be deleted, the requested ransom might increase or their files will be published on the Internet. This obviously pushes the need to make a decision quickly. It is also noted that the messages accompanying the ransomware splash screen often include a warning that the attackers are the only individuals who can provide the necessary private unlock key, hence increasing the notion of scarcity even more.

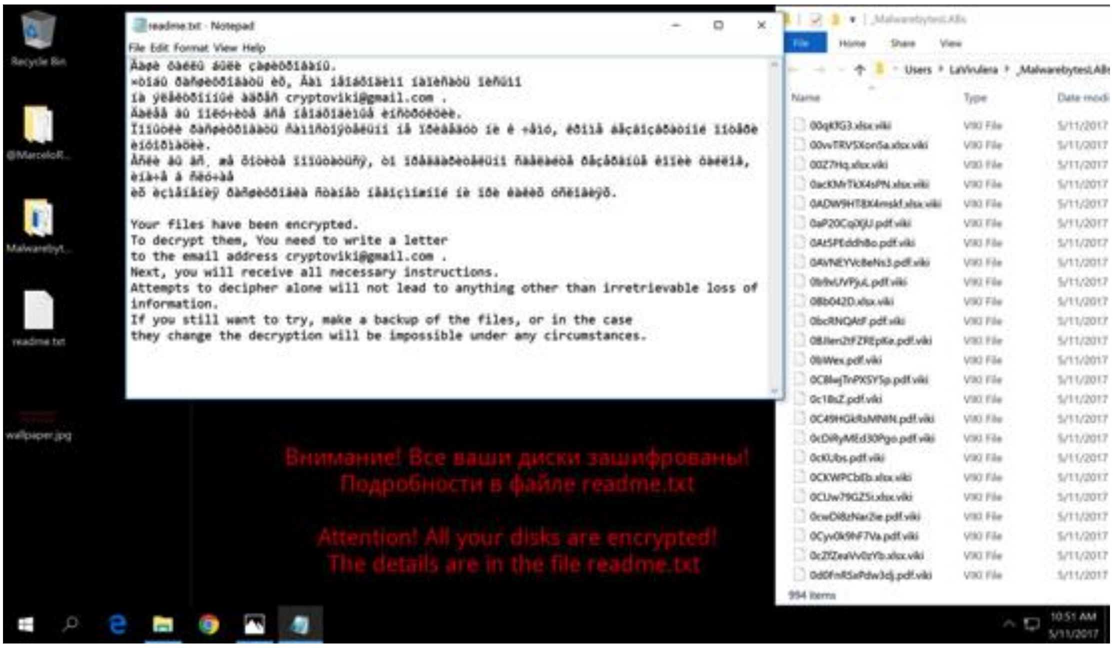
In terms of the specific time allowed to pay the ransom, there was a large range in the sample, and the consequences for not paying within the set time were also varied. The shortest time-period detailed in the sample for the payment of the ransom was just 10 hours in one example and, given the length of time it can take a victim to obtain Bitcoins, this could present a challenge. However, this short time-period was an isolated case; the majority of attackers requested payment within a 72-hour time period (36%), with 16% requesting payment in 48 hours and 16% in 96 hours. Just under a quarter (23%) of splash screens that included an aspect of time criticality for the payment of the ransom gave victims longer than 96 hours to pay the ransom. Just a small proportion (6%) requested payment in less than 12 hours.

In terms of the consequences for not paying, or missing the deadline for payment, a variety of elements came up in the sample. The most likely one was that the files would be deleted and the victim would not be able to gain access to them again, perhaps the consequence most typically associated with a ransomware attack. However, other aspects emerged in the sample, with several of the splash screens making the overt threat to publish the contents of the locked files on the Internet. This could be particularly damaging to companies where sensitive information is being held, hence providing the attackers with another form of leverage. This aspect could be loosely mapped into the social engineering mechanism of scarcity and, in particular, the sub-aspect of urgency – only a quick reaction will prevent sensitive files from being released onto the web. Other attackers levied aspects of urgency by threatening to increase the ransom if the initial sum was not paid in the time allocated, or threatening to delete a file each hour after the payment deadline.

4.3 Visual Presentation

In the context of the visual elements attached to the ransomware splash screens, there was a great deal of variation in terms of both the complexity and presentation. The majority of the splash screens were very heavily text-based in terms of content, and a few implemented the use of icons and images taken from popular media and films. A number of the splash screens (15%) were very basic text files or notepad files and contained very limited information about the attack (see image 1). The instructions usually referred the victim to other documents that had been installed on the computer as part of the attack, or asked them to visit a webpage (usually Tor-based) to get further information.

Image 1: An example of the more basic and rudimentary notepad-based splash screens.



```
Âàøè ôàéëû áûëè çàøèôðîâàíû.
×òîáû ðàñøèôðîâàòü èõ, Âàì íåîáõîäèìî îòïðàâèòü ïèñüìî
íà ýëåêòðîííûé àäðåñ cryptoviki@gmail.com .
Äàëåå âû ïîëó÷èòå âñå íåîáõîäèìûå èíñòðóêöèè.
Ïîïûòêè ðàñøèôðîâàòü ñàìîñòîÿòåëüíî íå ïðèâåäóò íè ê ÷åìó, êðîìå áåçâîçâðàòíîé ïîòåðè
èíôîðìàöèè.
Åñëè âû âñ¸ æå õîòèòå ïîïûòàòüñÿ, òî ïðåäâàðèòåëüíî ñäåëàéòå ðåçåðâíûå êîïèè ôàéëîâ,
èíà÷å â ñëó÷àå
èõ èçìåíåíèÿ ðàñøèôðîâêà ñòàíåò íåâîçìîæíîé íè ïðè êàêèõ óñëîâèÿõ.

Your files have been encrypted.
To decrypt them, You need to write a letter
to the email address cryptoviki@gmail.com .
Next, you will receive all necessary instructions.
Attempts to decipher alone will not lead to anything other than irretrievable loss of
information.
If you still want to try, make a backup of the files, or in the case
they change the decryption will be impossible under any circumstances.
```

Внимание! Все ваши диски зашифрованы!
Подробности в файле readme.txt

Attention! All your disks are encrypted!
The details are in the file readme.txt

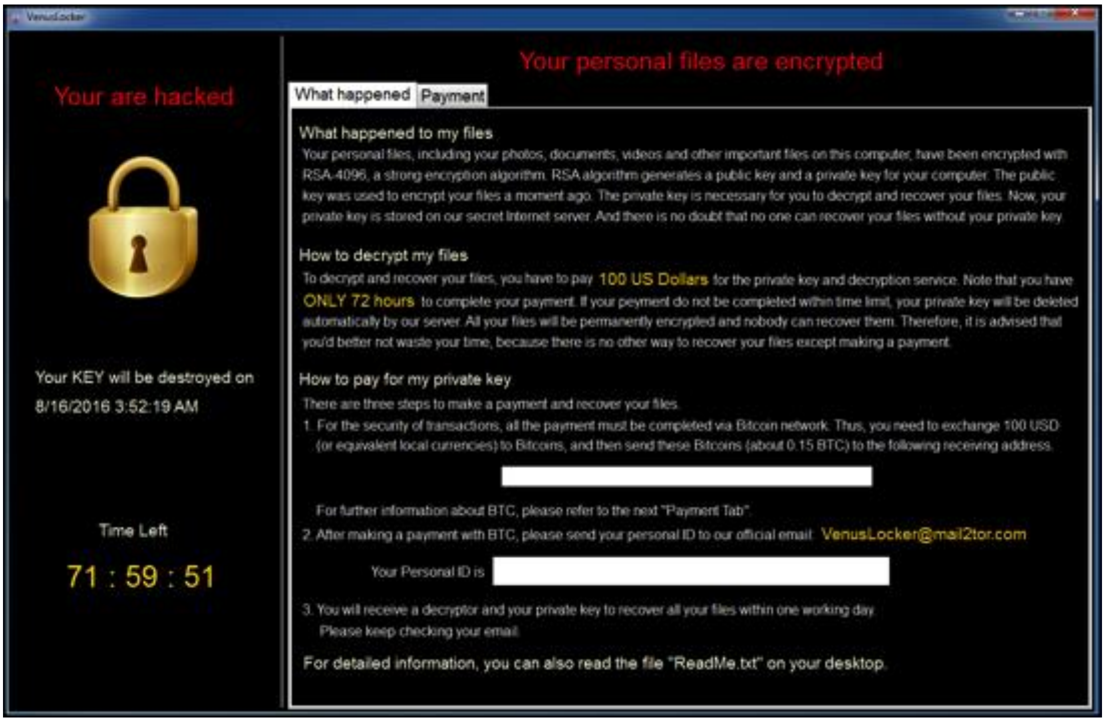
Name	Type	Date modi
00qKfG3.xlsx.viki	VIKI File	5/11/2017
00vvTRVSXonSa.xlsx.viki	VIKI File	5/11/2017
00Z7Hq.xlsx.viki	VIKI File	5/11/2017
0acKMrTkX4sPN.xlsx.viki	VIKI File	5/11/2017
0ADW9HT8X4mskf.xlsx.viki	VIKI File	5/11/2017
0aP20Cq0lJU.pdf.viki	VIKI File	5/11/2017
0AtSPEddhBo.pdf.viki	VIKI File	5/11/2017
0AVNEYVcBeNs3.pdf.viki	VIKI File	5/11/2017
0b9vUVPjuL.pdf.viki	VIKI File	5/11/2017
0Bb042D.xlsx.viki	VIKI File	5/11/2017
0bcRNQAtF.pdf.viki	VIKI File	5/11/2017
0BJlen2tFZREpKe.pdf.viki	VIKI File	5/11/2017
0biWex.pdf.viki	VIKI File	5/11/2017
0CBlwjTnPXSY5p.pdf.viki	VIKI File	5/11/2017
0c18sZ.pdf.viki	VIKI File	5/11/2017
0C49HGkRsMNIN.pdf.viki	VIKI File	5/11/2017
0cDiRyMEd30Pgo.pdf.viki	VIKI File	5/11/2017
0ckUbs.pdf.viki	VIKI File	5/11/2017
0CKWPCbEb.xlsx.viki	VIKI File	5/11/2017
0CUw79GZSi.xlsx.viki	VIKI File	5/11/2017
0cwDi8zNarZie.pdf.viki	VIKI File	5/11/2017
0Cyv0k9hF7Va.pdf.viki	VIKI File	5/11/2017
0c2fZeaVv0zYb.xlsx.viki	VIKI File	5/11/2017
0d0FnRSaPdw3dj.pdf.viki	VIKI File	5/11/2017

994 items

A set of more advanced ransomware splash screens emerged from the sample, these being typified by the inclusion of detailed information related to the attack, payment details and contact details. They were also logically structured and presented information clearly to the victim, usually in a sequential order. This could be linked back to aspects of social engineering, in particular that of authority. An informative splash screen gives the victim an impression of a group that is well organised and knows what they are doing. In turn, this generates a level of confidence in the victim that payment of the ransom will eventually lead to them getting their files back. More research in this area needs to explore this in a more direct manner, and again this suggestion is speculation based on the existing research in the area. The splash screens conforming to this latter configuration generally followed a set pattern (see image 2) and included a detailed description of the attack, how the individual could obtain Bitcoins for payment, how to pay, as well as a backup option for payment if the initial option was unavailable. This three-tiered approach to communicating ransomware to the victim was frequently replicated throughout the sample.

For the attacker, there is a potential benefit for using such an approach. For example, it increases the potential for payment as it allows the victim to fully understand what has been done and how they can get their files back. The way the ransom screen is organized provides the victim with all the relevant information they need in a self-contained box which means the victim does not have to move between windows or websites, hence reducing aspects of cognitive load (Sweller, 1988). This, in turn, reduces confusion for the victim and increases the likelihood of payment. However, this element is purely conjectural and the limited data for the current sample prevents any clear conclusions in this regard.

Image 2: An example of the more complex splash screen; note the use of the lock icon and countdown timer.



Your are hacked

Your KEY will be destroyed on
8/16/2016 3:52:19 AM

Time Left
71 : 59 : 51

Your personal files are encrypted

What happened to my files

Your personal files, including your photos, documents, videos and other important files on this computer, have been encrypted with RSA-4096, a strong encryption algorithm. RSA algorithm generates a public key and a private key for your computer. The public key was used to encrypt your files a moment ago. The private key is necessary for you to decrypt and recover your files. Now, your private key is stored on our secret Internet server. And there is no doubt that no one can recover your files without your private key.

How to decrypt my files

To decrypt and recover your files, you have to pay 100 US Dollers for the private key and decryption service. Note that you have ONLY 72 hours to complete your payment. If your peyment do not be completed within time limit, your private key will be deleted automatically by our server. All your files will be permanently encrypted and nobody can recover them. Therefore, it is advised that you'd better not waste your time, because there is no other way to recover your files except making a payment.

How to pay for my private key

There are three steps to make a payment and recover your files.

1. For the security of transactions, all the payment must be completed via Bitcoin network. Thus, you need to exchange 100 USD (or equivalent local currencies) to Bitcoins, and then send these Bitcoins (about 0.15 BTC) to the following receiving address.

   For further information about BTC, please refer to the next "Payment Tab".

2. After making a payment with BTC, please send your personal ID to our official email: VenusLocker@mail2tor.com

   Your Personal ID is

3. You will receive a decryptor and your private key to recover all your files within one working day. Please keep checking your email.

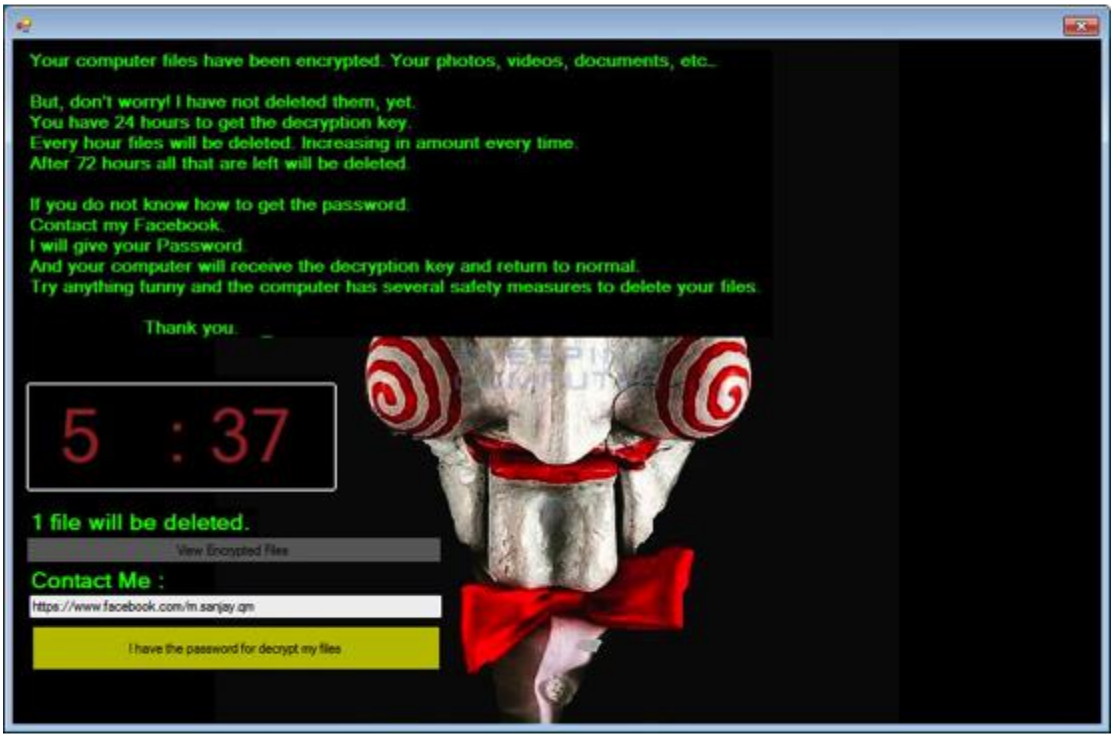
For detailed information, you can also read the file "ReadMe.txt" on your desktop.

4.3.1. Use of Symbols and Culturally Iconic Images

One interesting element that came through in the exploration of the splash screens was the use of a variety of images. One sub-category of these included very simple icons, such as the use of lock icons, shields and badges. In several instances, the ransomware splash screen included logos taken from prominent law enforcement agencies, including the crest of the U.S. Federal Bureau of Investigations (FBI) (see image 7 further in the report). Such use of these specific images again links into the social engineering aspect of authority, particularly when the same image was used in a ransomware splash screen purporting to have detected pornography and/or copyrighted material on the victim's computer. This was also noted in splash screens where trademark logos from Windows and Microsoft were used to enhance the appearance of the attack. Both mechanisms were used in '*cuckoo*' ransomware attacks that will be discussed in more detail later on in this report (see section 4.3.2).

One of the most prominent pop cultural images used was that of “Jigsaw”, a character that appears in the *Saw* horror movie series (see image 4 below). The character acts as a spokesperson for an often-unseen attacker, and has a menacing appearance. The use of such imagery is interesting as it almost gives a substance to what is generally seen as a faceless crime, although it is noted that just a few of the splash screens used this image. Another image that was often used in the samples was the Guy Fawkes mask, used most notably with the hacking group Anonymous (see image 5 below). Again, this symbol is used to enhance the authority element associated with social engineering, with many individuals (irrespective of their technical background) having some familiarity with Anonymous and their associated exploits. The use of these pop cultural icons is an interesting element of the ransomware splash screen and, as yet, is something that has not been fully explored in the context of research. It would be useful to understand how the victims of such attacks perceive such cultural symbols and how they feed into the decision-making process aligned with paying the ransom.

Image 4: The use of the Jigsaw character from the Saw film series – this symbol was noted in several of the splash screens.



Your computer files have been encrypted. Your photos, videos, documents, etc..

But, don't worry! I have not deleted them, yet.
You have 24 hours to get the decryption key.
Every hour files will be deleted. Increasing in amount every time.
After 72 hours all that are left will be deleted.

If you do not know how to get the password.
Contact my Facebook.
I will give your Password.
And your computer will receive the decryption key and return to normal.
Try anything funny and the computer has several safety measures to delete your files.

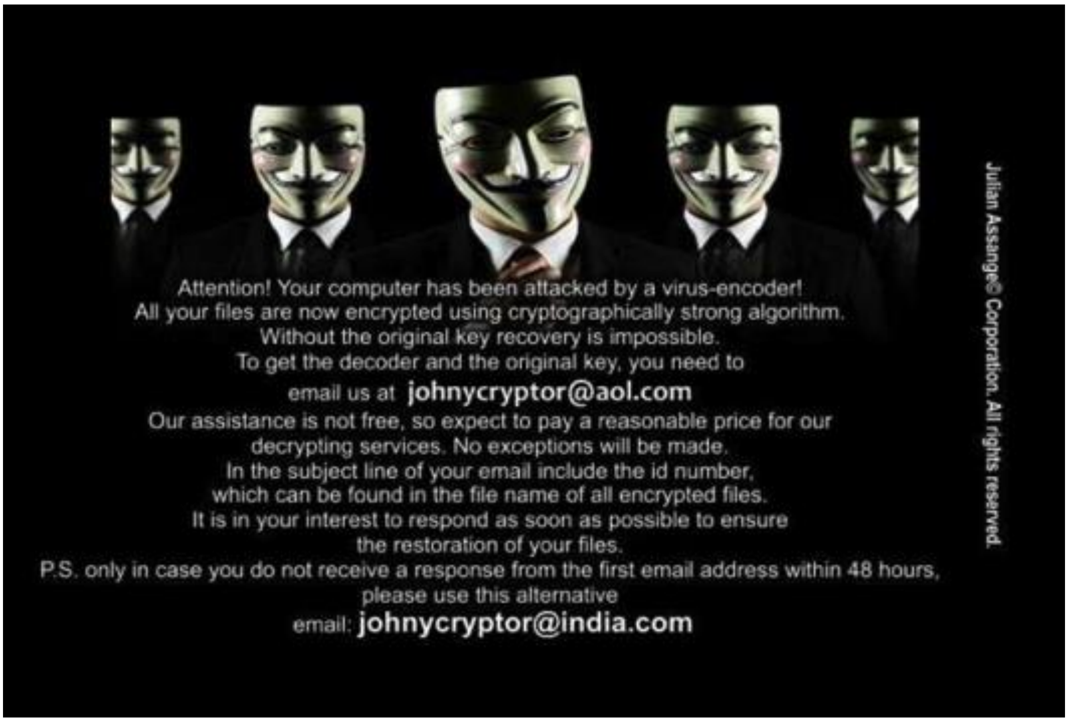
Thank you.

5 : 37

1 file will be deleted.

Contact Me : https://www.facebook.com/m.sanjay.qm

Image 5: The use of the Guy Fawkes mask appeared in several of the splash screens. This one is also conspicuous because it claims to be copyrighted by Wikileaks founder Julian Assange.



Attention! Your computer has been attacked by a virus-encoder!
All your files are now encrypted using cryptographically strong algorithm.
Without the original key recovery is impossible.
To get the decoder and the original key, you need to
email us at **johnycryptor@aol.com**
Our assistance is not free, so expect to pay a reasonable price for our
decrypting services. No exceptions will be made.
In the subject line of your email include the id number,
which can be found in the file name of all encrypted files.
It is in your interest to respond as soon as possible to ensure
the restoration of your files.
P.S. only in case you do not receive a response from the first email address within 48 hours,
please use this alternative
email: **johnycryptor@india.com**

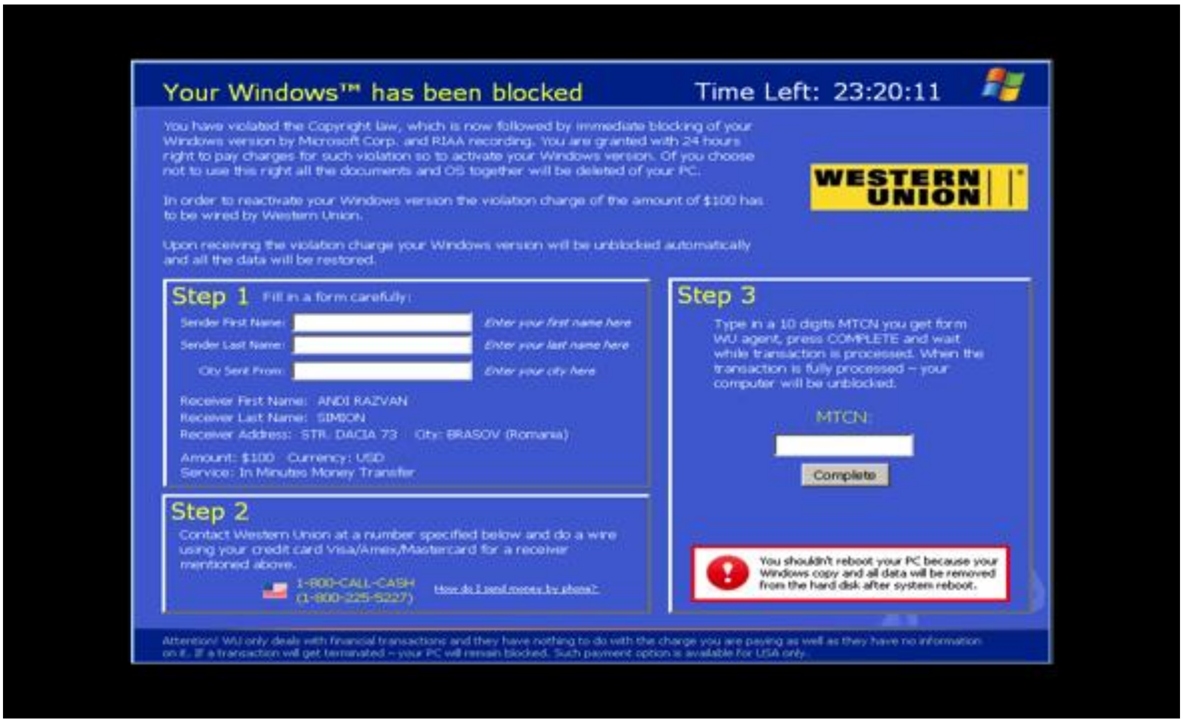
Julian Assange© Corporation. All rights reserved.

4.3.2 The 'Cuckoo' Ransomware

This term has been coined in the current report to describe ransomware that doesn't overtly ask for a 'ransom', or that appears to be from an official source. In the present sample, this type of ransomware accounted for just 9% of the total number of splash screens and, often, there were slight variations along a similar theme (see images 6 and 7 below). As can be seen, this type of ransomware attack uses several social engineering tactics already mentioned previously in this report. Primarily there is the use of official trademarks or emblems, which instils the notion of authority and credibility to the request. The language is also interesting as there is often a lot of technical information related to the relevant legal statute that has been allegedly transgressed by the victim. The examples which included the FBI emblems were even more interesting when looking at the payment options offered as they asked for Bitcoins, which would perhaps flag this as a potential scam straightaway for those who had more knowledge about this type of currency. Secondly, a variation of ransomware also offers individuals the opportunity to go into a local courthouse to pay their fine, but with the provision that this would mean it would take longer (4-5 working days) to unlock their files. This is an interesting tactic, as, for most individuals, urgency to unlock their computer and access the files on it would make the second option redundant. (Note: There is no further data to assess if victims actually chose to visit a courthouse to pay their fine, and is noted as another aspect for further research in that area.)

Other examples of this type of attack included warnings that the operating system (usually Windows) had been blocked or banned due to the detection of illegal or copyrighted software and/or the detection of other spurious activities (such as visiting websites with adult content and pornographic images). Again, there is a clear lack of actionable intelligence about how successful these types of attacks are. It is assumed that they may be directed to those who are more vulnerable (e.g. the elderly), those who wish not to have such information released to family/friends, and those who have limited technical knowledge and, therefore, would be more likely to just pay the ransom right away.

Image 6: A clear example of the "Cuckoo" form of ransomware, notable in its use of the Microsoft Windows logo and colouration.



Your Windows™ has been blocked

Time Left: 23:20:11

You have violated the Copyright law, which is now followed by immediate blocking of your Windows version by Microsoft Corp. and RIAA recording. You are granted with 24 hours right to pay charges for such violation so to activate your Windows version. Of you choose not to use this right all the documents and OS together will be deleted of your PC.

In order to reactivate your Windows version the violation charge of the amount of $100 has to be wired by Western Union.

Upon receiving the violation charge your Windows version will be unblocked automatically and all the data will be restored.

Step 1 Fill in a form carefully:

Sender First Name: Enter your first name here

Sender Last Name: Enter your last name here

City Sent From: Enter your city here

Receiver First Name: ANDI RAZVAN

Receiver Last Name: SIMION

Receiver Address: STR. DACIA 73 City: BRASOV (Romania)

Amount: $100 Currency: USD

Service: In Minutes Money Transfer

Step 2

Contact Western Union at a number specified below and do a wire using your credit card Visa/Amex/Mastercard for a receiver mentioned above.

1-800-CALL-CASH (1-800-225-5227)

How do I send money by phone?

Step 3

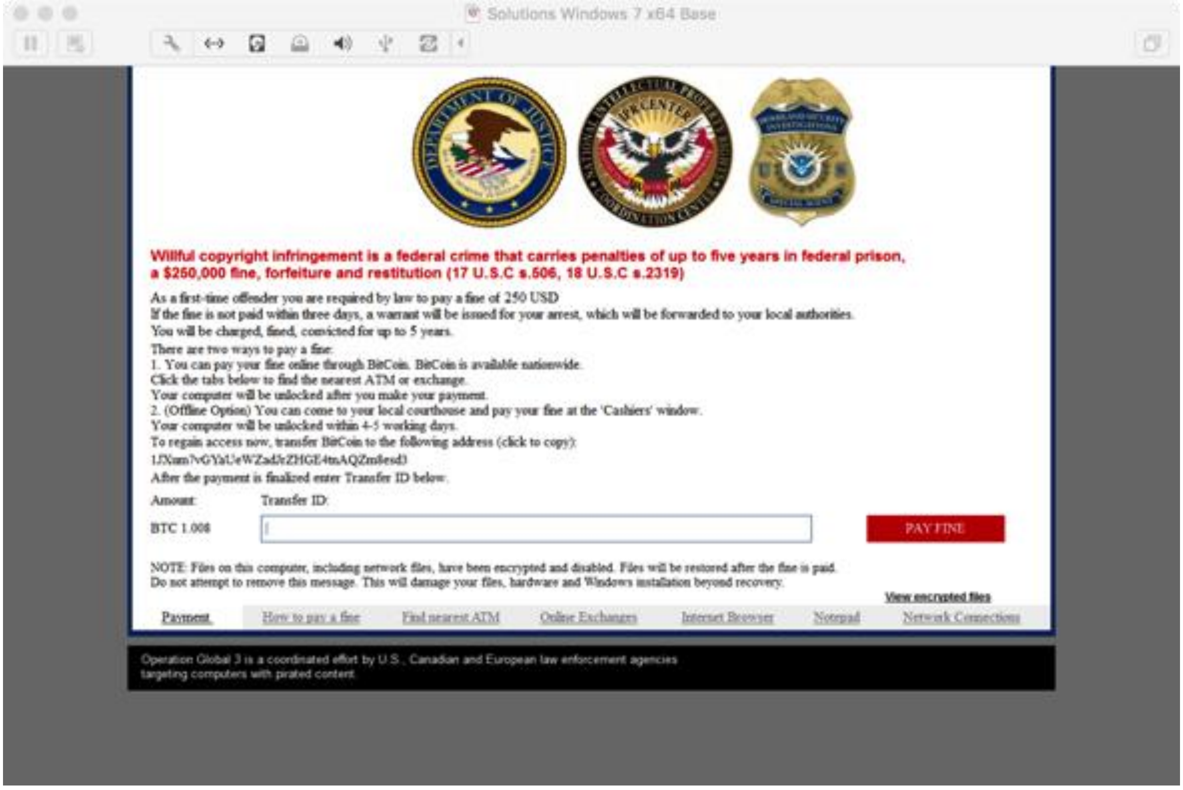
Type in a 10 digits MTCN you get form WU agent, press COMPLETE and wait while transaction is processed. When the transaction is fully processed – your computer will be unblocked.

MTCN:

You shouldn't reboot your PC because your Windows copy and all data will be removed from the hard disk after system reboot.

Attention! WU only deals with financial transactions and they have nothing to do with the charge you are paying as well as they have no information on it. If a transaction will get terminated – your PC will remain blocked. Such payment option is available for USA only.

Image 7: Another example of "Cuckoo" ransomware displaying aspects of authority in the form of key law enforcement agencies.



Willful copyright infringement is a federal crime that carries penalties of up to five years in federal prison, a $250,000 fine, forfeiture and restitution (17 U.S.C s.506, 18 U.S.C s.2319)

As a first-time offender you are required by law to pay a fine of 250 USD
If the fine is not paid within three days, a warrant will be issued for your arrest, which will be forwarded to your local authorities.
You will be charged, fined, convicted for up to 5 years.
There are two ways to pay a fine:
1. You can pay your fine online through BitCoin. BitCoin is available nationwide.
Click the tabs below to find the nearest ATM or exchange.
Your computer will be unlocked after you make your payment.
2. (Offline Option) You can come to your local courthouse and pay your fine at the 'Cashiers' window.
Your computer will be unlocked within 4-5 working days.
To regain access now, transfer BitCoin to the following address (click to copy):
1JXam7vGYaUeWZadJrZHGE4tnAQZm8esd3
After the payment is finalized enter Transfer ID below.

Amount: BTC 1.008
Transfer ID:

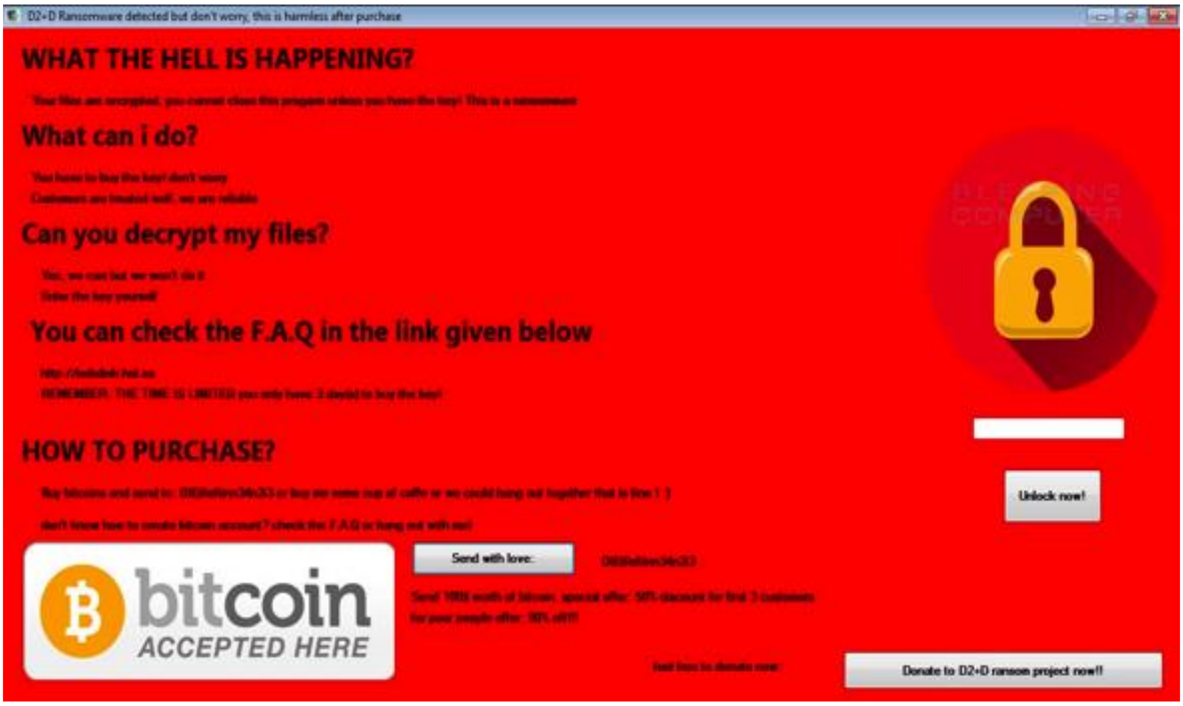
NOTE: Files on this computer, including network files, have been encrypted and disabled. Files will be restored after the fine is paid.
Do not attempt to remove this message. This will damage your files, hardware and Windows installation beyond recovery.

Operation Global 3 is a coordinated effort by U.S., Canadian and European law enforcement agencies targeting computers with pirated content

4.4 The Unusual and The Bizarre

Some of the splash screens from the sample stood out for other reasons, mainly because they contained either very random images or differed so much from the rest of the sample they deserved a more in-depth discussion. The first one that was highlighted is shown in image 8 below.

Image 8: The example of a unique splash screen that is conversational and overtly trying to establish liking, perhaps as an attempt to garner payment of the ransom.



D2+D Ransomware detected but don't worry, this is harmless after purchase

WHAT THE HELL IS HAPPENING?

Your files are encrypted, you cannot close this program unless you have the key! This is a ransomware

What can i do?

You have to buy the key! don't worry

Customers are treated well, we are reliable

Can you decrypt my files?

Yes, we can but we won't do it

Enter the key yourself

You can check the F.A.Q in the link given below

http://[illegible]

REMEMBER: THE TIME IS LIMITED you only have 3 day(s) to buy the key!

HOW TO PURCHASE?

Buy bitcoins and send to: [illegible] or buy me some cup of caffe or we could hang out together that is fine ! :)

don't know how to create bitcoin account? check the F.A.Q or hang out with me!

Send with love: [illegible]

Send 100$ worth of bitcoin, special offer: 50% discount for first 3 customers

for poor people offer: 90% off!!!

feel free to donate now:

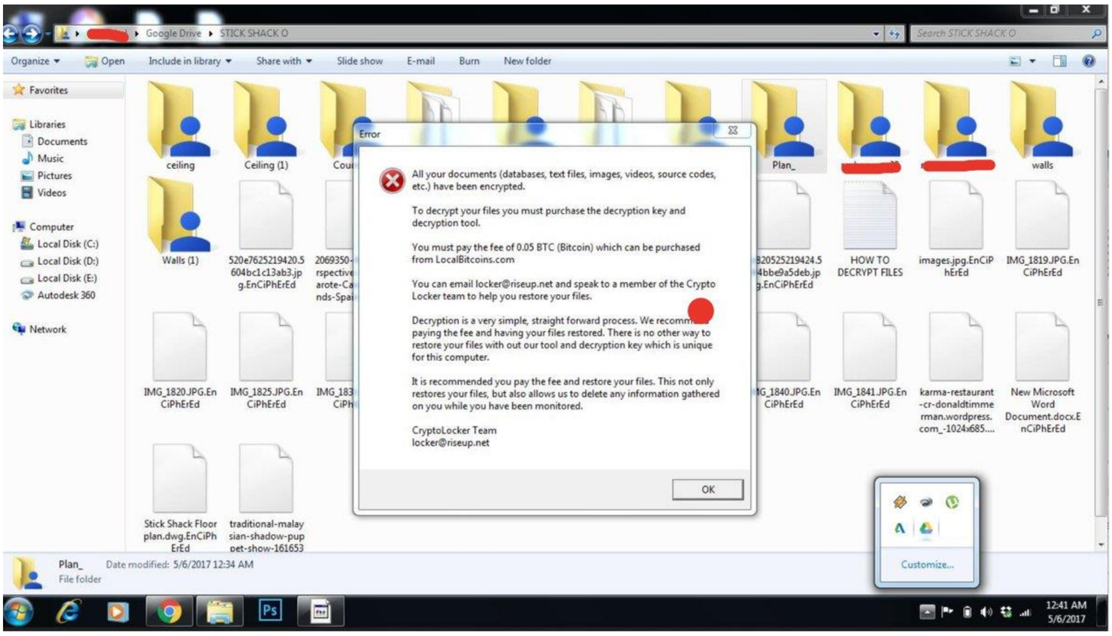
There are a variety of aspects to this splash screen that are interesting. The text attempts to be humorous and conversational, perhaps an attempt to elicit an aspect of liking, another tactic used in social engineering. The two further interesting elements are contained under the header of "How to Purchase?" where the attacker asks the victim to send Bitcoins "or buy me some cup of coffee or we could hang out together that is fine! 😉", as well as "check the F.A.Q. or hang out with me!". The final aspect of this is the option to send Bitcoins and is labelled "send with love". This splash screen is filled with paradoxes, as the attacker obviously wants the victim to pay the relevant ransom, but then also appears to want the victim to like them, attempting to engage them in conversational and interpersonal interactions. The offer to allow the victim to "donate" to the ransomware project is another element to this splash screen that makes it unusual. One final notable element is the offer of a discount for individuals who are "poor", which makes this attacker perhaps the only one to exhibit an aspect of "social conscience"; however it is also noted that if they had such an aspect to their personality they would not have initiated the attack in the first instance.

4.5 The 'Customer Service' Angle

It seems strange to suggest that ransomware attacks have an aspect of customer service attached to them but, within the sample selected for the present study, this element became more apparent. Again, this perhaps fits into the notion of authority, and the overt notion that a well-organised and structured organisation may make victims more likely to pay the ransom by treating them like "customers." In this sample, 51% of the splash screens included some aspect of customer service, ranging from instructions on how to buy BTC, downloading Tor or key Frequently Asked Questions. In one example splash screen (see Image 9) the victim was offered the chance to 'speak to a member of the team'; this fulfils two key aims:

1. Elicits the connotation of the group being organised and;
2. An overt invitation for the victim to contact the group if they have any issues, and may fit into the pattern of liking.

Image 9: An overt display of apparent customer service, with reference to the service team available to answer any queries.



All your documents (databases, text files, images, videos, source codes, etc.) have been encrypted.

To decrypt your files you must purchase the decryption key and decryption tool.

You must pay the fee of 0.05 BTC (Bitcoin) which can be purchased from LocalBitcoins.com

You can email locker@riseup.net and speak to a member of the Crypto Locker team to help you restore your files.

Decryption is a very simple, straight forward process. We recomm[redacted] paying the fee and having your files restored. There is no other way to restore your files with out our tool and decryption key which is unique for this computer.

It is recommended you pay the fee and restore your files. This not only restores your files, but also allows us to delete any information gathered on you while you have been monitored.

CryptoLocker Team
locker@riseup.net

Many of the splash screens also provided clear instructions on how victims could obtain Bitcoins as well as included links to local sites where they could be purchased. One example even included a short video tutorial showing how to buy BTCs, demonstrating the importance of making sure the 'customer' is well informed. As discussed in brief earlier in this report, this aspect provides the victim with essential information, particularly where they have no knowledge of such payment methods or how to buy them. It also provides another mechanism for the attacker to get the ransom; simply stating that the payment needs to be given in BTCs has the potential to create confusion and further panic in the victim, leading to a delay in payment. Presenting this information in the form of Frequently Asked Questions (FAQs) is also an interesting approach and further emulates well know practices from business.

Incidentally, a wider number of the splash screens contained detailed information about the type of algorithm that had been used to encrypt the data; in several instances the splash screens referred the victim to detailed information (usually in the form of a link to Wikipedia) on this topic as well. Such algorithms were often described as 'military grade'. This could be a tactic that would suggest any attempt to circumvent the encryption process would be a fruitless endeavour. Nearly 44% of the ransomware splash screens also contained an overt warning not to tamper with encryption or try to find other help to aid in the decoding. All these are further examples of the customer service angle presented by the ransomware splash screens – from one perspective the attackers are promoting the legitimacy of their product, with supporting evidence from an external source. On the other hand, they are protecting their brand by telling the victim not to attempt to tamper with the ransomware as only they can provide the right public key.

5. Conclusion

This report presents a first attempt at exploring the underlying psychology that is hidden within ransomware splash screens. In the context of the present study there are a variety of key findings that demonstrated ransomware splash screens are not as basic as perhaps first assumed. Similarly, like ransomware attacks, the splash screens that accompany them are not all the same, and hint towards differing levels of sophistication. Attackers, whether it is by design or through imitation, are employing a variety of tactics that appear to be geared towards eliciting payment from victims. The argument presented in the current report suggests that these tactics are closely aligned to the concept of social engineering, working on aspects of fear, urgency, scarcity, authority and, in some cases, humour. Other elements emerge from the analysis, including the presentation of a customer service element to ransomware that is perhaps something of an unusual aspect. The presence of ransomware that is cleverly disguised as a formal transgression of laws or linked to the use of copyrighted programs/material is also another interesting trend within the current sample.

The key points present in this initial exploration of ransomware splash screens highlights the following:

- Not all splash screens are the same – there is a distinct difference in terms of the level of sophistication of mechanisms used to gain payment, presentation of the splash screens and provision of information for further contact. However, there is no further data to explore how such differences map to their success in terms of eliciting payment.
- The ransomware splash screens utilise key aspects of influence and persuasion, concepts that are often used in the context of social engineering, to present a convincing argument for the victim to pay their ransom.
- A small subset of ransomware splash screens served to intimidate the victim by claiming to be from an official source or law enforcement agency but that did not explicitly ask for a specific ransom be paid. These were termed ‘cuckoo’ ransomware, and utilised official branding and badges to enhance the authority element.
- A variety of images and cultural icons were used in the ransomware splash screens. The cultural icons presented overtly menacing images,

again hypothesised to create a fear response in victims. Shield and lock icons were also evident, and it is noted that such icons are also widely used by cybersecurity companies and anti-virus programs. It is unclear if this is an attempt by attackers to emulate the professional appearance of such, or is simply an *ad hoc* addition.

There are some obvious limitations to the current study, not only in terms of the inferences made between the content and the potential mechanisms being used by the attackers. More research is needed in this area, aligned to a more systematic approach to the collection and classification of ransomware splash screens. In this instance there has been a close focus on a very small proportion of the potential psychological theories that could be applied in this context, and there is a wide variety of further work that needs to be done in this area. By expanding the current work with more empirical research, a clearer understanding of why certain ransomware splash screens are more successful at eliciting a payment over others could be obtained. Such information could in turn be used to provide effective mitigation techniques for such attacks, as well as giving both investigators and victims a clearer pathway for help and advice in the event of an attack.

6. References

Hadnagy, C. (2010). *Social Engineering: The Art of Human Hacking*. *The Art of Human Hacking*. Indianapolis, Indiana: Wiley Publishing Inc. http://doi.org/10.1093/cid/cir583

Liao, Q. (2008). RANSOMWARE : A GROWING THREAT TO SMEs. In *Conference Southwest Decision Institutes* (pp. 360–366).

Luo, X., & Liao, Q. (2007). Awareness Education as the Key to Ransomware Prevention. *Information Systems Security*, *16*(4), 195–202. http://doi.org/10.1080/10658980701576412

Sweller, J. (1988). Cognitive load during problem solving: Effects on learning. *Cognitive Science*, *12*, 257–285. Retrieved from papers3://publication/uuid/4D754756-5B9C-4178-8BB5-BD220FE1083E

Uebelacker, S., & Quiel, S. (2014). The Social Engineering Personality Framework. *2014 Workshop on Socio-Technical Aspects in Security and Trust*, 24–30. http://doi.org/10.1109/STAST.2014.12

Dr. Lee Hadlington, De Montfort University

Dr Lee Hadlington has been a Senior Lecturer at De Montfort University since 2006 after completing his PhD at Wolverhampton University. Originally coming from a background in applied cognitive psychology, he has developed a research profile in Cyberpsychology. His focus of interest is exploring the way in which humans use cognition in the online environment as well as the potential for digital technology to change the underlying processes that we use in daily life. Associated with his work in Cyberpsychology, he has a keen interest in exploring key aspects of technology-enabled crime. He has also worked extensively with a variety of external organisations in exploring aspects of insider threat, susceptibility to cybercrime and attitudes towards cybersecurity.

About SentinelOne

SentinelOne is shaping the future of endpoint security with an integrated platform that unifies the detection, prevention and remediation of threats initiated by nation states, terrorists, and organized crime. SentinelOne's unique approach is based on deep inspection of all system processes combined with innovative machine learning to quickly isolate malicious behaviors, protecting devices against advanced, targeted threats in real time. SentinelOne was formed by an elite team of cyber security and defense experts from IBM, Intel, Check Point Software Technologies, McAfee, and Palo Alto Networks. To learn more visit sentinelone.com or follow on Twitter at @SentinelSec.