Executive Summary

In stark contrast to many other cybercrime models that infiltrate systems with the aim of stealthily manoeuvring to locate and quietly siphon data to be monetized at a later stage, crypto-ransomware surreptitiously encrypts files then employs an abrupt, confrontational extortion demand; with a timeline ensuring resolution for the victim in one way or another within hours. Ransomware epitomises the nexus between the modern criminal cyber marketplace and effective use of age-old psychological intimidation.

The infection vector criminals use to propagate ransomware varies, and is often symbiotic with prior malware infections; during 2014 it would often be a result of the Gameover Zeus botnet, and 2015 has seen an increase in ransomware as part of a malware lifecycle encompassing 'click fraud' and 'malvertising'. Abusing the most effective means to protect data and privacy, ransomware uses the asymmetric encryption technique to create a public-private key pair in order to encrypt files. The key used to encrypt the files is often itself encrypted again using a combination of RSA and AES cryptography, and ultimately without access to the attacker's private key it is next to impossible to decrypt the data. The number of file types vulnerable has grown exponentially over the past several years in a trend that suggests the increased targeting of enterprise.

The price point of the ransom demand has been tested by criminals and is now commonly around $400 (€360) to be paid in Bitcoin, which appears to be close to the price ceiling at which untargeted ransomware balances likelihood of payment with the maximum ransom demand. While ransom demands are displayed in a multitude of languages, the geographic spread is currently weighted towards English speaking countries; in June 2015 the FBI stated the CryptoWall variant that had demanded ransoms of $200-$10,000 had caused $18 million in damages within the U.S alone.

Ransomware is low-risk and low-maintenance for criminals to deploy, yet can be a high-yielding and quick way to monetize a malware infection; the modern criminal marketplace has lowered barriers to entry and done away with a complicated logistic chain. Ransomware is a growth area, and would appear to scale well to technologies like mobile, cloud and IoT, alongside potential of a far more targeted enterprise threat by the more advanced groups.

The only contingency should infection occur is to have sufficient backups; ideally three copies, in two different formats, with one stored offline. Coding errors and seizures by law enforcement relating to specific variants may offer a chance of decryption in a small percentage of cases, but a 'cure' should be regarded as non-existent. The criminals may never even intend to provide decryption, but the trajectory of ransomware is testament to the number of unprepared victims who felt they had no other choice.

Contents

Introduction: The History of Ransomware

Extortion can be defined as the act of obtaining property or money by threatening almost any kind of force, the leverage used may refer to violence, property destruction, damage to brand or reputation, or some kind of unfavourable action. One of the earliest incidents relating to data theft in the modern era occurred in the 1970's, when physical data tapes belonging to the Bank of America were stolen and held to ransom, and although criminals have moved with the times this remains the premise of crypto-ransomware.

Widely regarded as the earliest case of crypto-ransomware, floppy disks containing malware that hid folders, encrypted file names, and stated that a licence has expired requiring a $189 payment to a PO Box based in Panama were distributed at an AIDS conference in 1989. Due to difficulties in spreading the malware and subsequently anonymising payments at this time, cyber-criminals were not able to widely employ this model for another 10 years. In the interim, fake Anti-Virus began to evolve, using spam, blackhat SEO, malvertising, and drive by downloads.

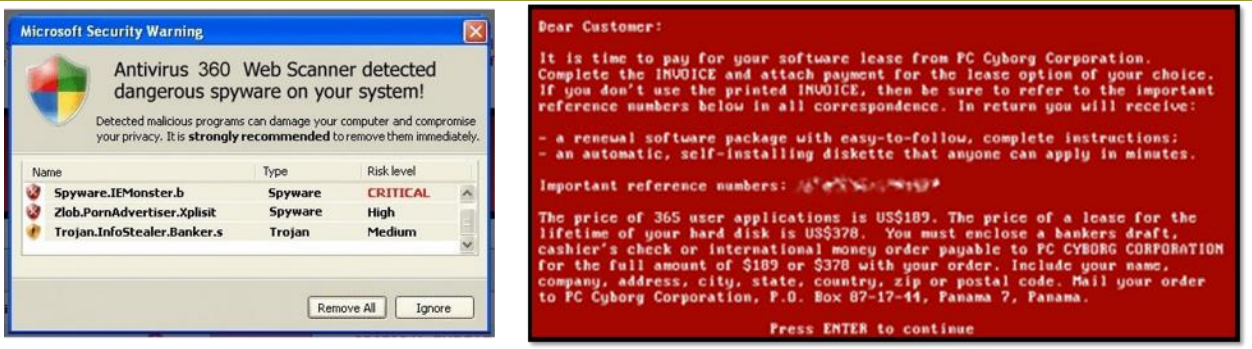

Figure 1. Fake Anti-virus pop-up and the 1989 AIDS Trojan ransom demand.

As computer users became more accustomed to ignoring scareware and pop-ups suggesting users needed anti-virus, the evolution of ransomware continued as cyber criminals began locking the computer, using the narrative that the user had broken the law and was required to pay a fine. However, the target audience was beginning to be made captive around 2006 when files began to be encrypted alongside the warning. The launch of Bitcoin in 2009 and the uptake of crypto-currencies, provided criminals with the means to reinvigorate the ransomware model, and by 2011 it was becoming increasingly professional [1]. High-res and localised law enforcement agency iconography was used, and the spelling mistakes from non-native speakers began to diminish. According to analysis conducted by Trend Micro [2], until Q1 2015, ransomware actually encrypting files had remained a minority as a percentage of overall cases, however the proportion of infections employing encryption is now at an all-time high (see Figure 2).

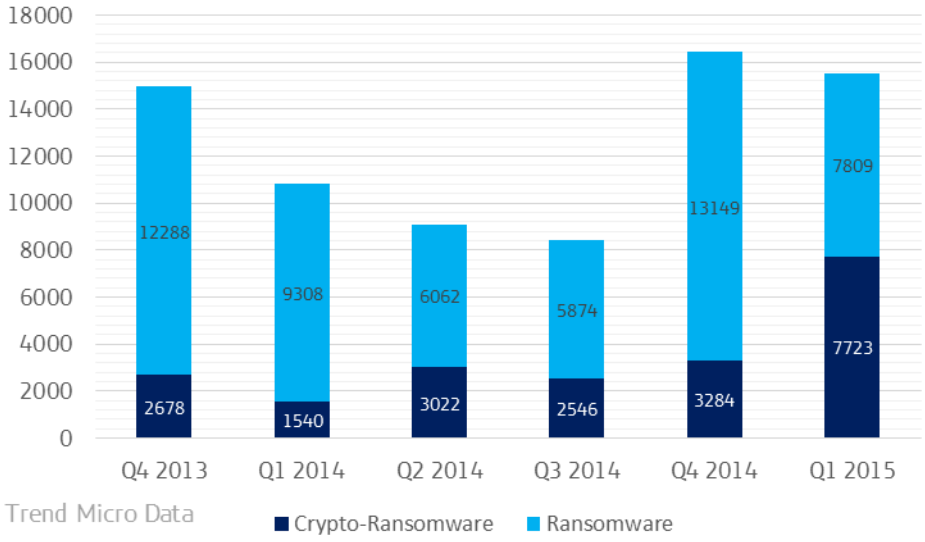

Figure 2. Variation in locking and encrypting ransomware variants.

Mechanics of a Ransomware Attack

Infection Vector

Historically a large part of scareware and ransomware campaigns has relied on manipulating human behaviour and this remains a strong theme to this day with regard to the initial infection vector. Like much of the malware deployed by criminals, phishing emails with malicious attachments such as fax reports or zip files are commonly reported [3] [4]; however exploit kits hosted on web pages that leverage Flash, IE, Adobe, Silverlight, and Java vulnerabilities are increasingly common. A variety of methods are used to entice victims to the webpage hosted or taken over by the criminal. Targeting top search engine results for certain potentially illicit or embarrassing search terms, such as those of a pornographic nature is an example of the psychology employed by criminals.

More disturbing is the increasing manner in which ransomware campaigns are being commercialised by cyber-criminals, often linked to criminals commanding botnets utilising the already compromised machines. The takedown of the Gameover Zeus botnet impacted the distribution of certain variants of ransomware, however the evolving business model now indicates cyber criminals are increasingly using an affiliate program as part of the business model [5].

Command & Control and Cryptography

The communication channels ransomware uses to communicate back to the criminal command and control (C&C) servers has evolved in order to avoid detection [6] [7]. Previously, prior to any encryption, a domain name generating algorithm would cause the malware to try and connect with over 1,000 unique domains every day in order to find a criminal server from which to download the encryption key; however most variants discovered in Q1 2015 now use heavily obfuscated hardcoded URLs within the malware itself [8] [9]. Communication commonly takes place via Tor, or HTTPS encrypted channels. While attempting Tor communication may trigger alerts in enterprise networks, HTTPS traffic would likely be indistinguishable from legitimate outbound communication. Highlighting the constant evolution, the latest CryptoWall 3.0 variant utilises a peer-to-peer anonymity network based on the I2P protocol. Such methods prevent the sink-holing of domains, and subsequently the insight into the true extent of infection rates.

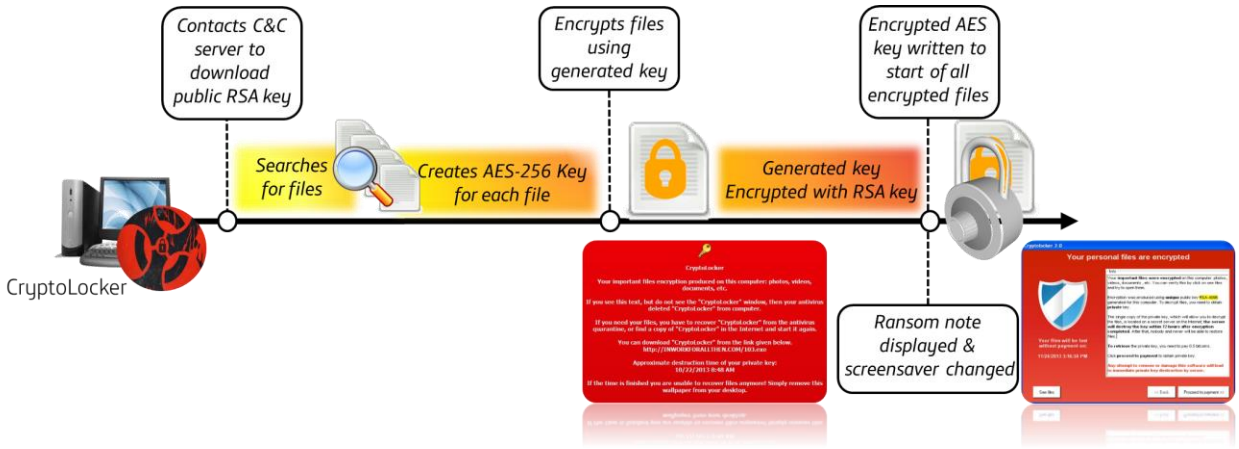

Figure 3. Mechanics of encryption used by the CryptoLocker variant.

Crypto-ransomware utilises the same asymmetric encryption as users do in order to protect their own data; whereby a pair of keys are used to encrypt and decrypt a file. The public-private key pair is generated by the criminal and is unique for each user. The key used to encrypt the file may itself be encrypted, the 2015 Poshcoder variant using a combination of AES and 4096-bit RSA encryption. Over time encryption strength has increased and cryptographic flaws are increasingly rare, poor implementation by malware authors had occasionally left the private key available to be recovered from the malware residing on the victim device, however now they are nearly always stored on the criminals' server [10]. The adoption of the Microsoft cryptographic API or elliptical curve cryptography utilised in current variants ensures that the only means of file recovery is with the private key held by the criminal. Even if the malware is removed the files remain encrypted and the malware must be downloaded again in order to access the ransom payment screen.

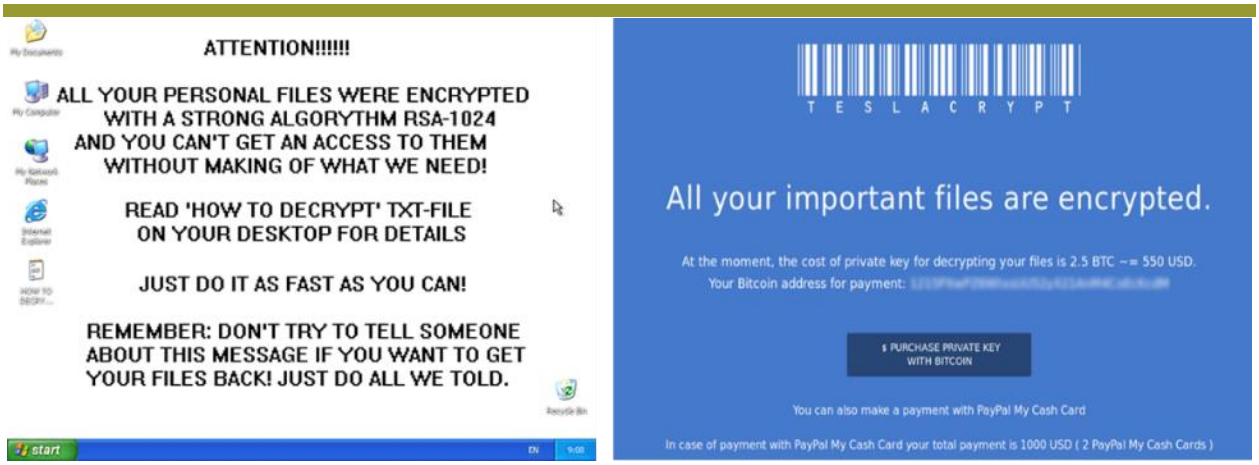

Figure 4. Increasing professionalism of ransomware authors.

The variety of file types has significantly increased in the past several years, as criminals have widened their scope. For example during a 2013 campaign, the CryptoLocker variant was configured to encrypt 67 file types, whereas in 2015, TorrentLocker was able to encrypt 236 [11]. The file types selected do not suggest a dragnet approach however, and specialised CAD formats and image extensions are targeted, suggesting a targeting of enterprise as well as the likely sentimental value of photo albums.

Q1 2015 also witnessed the Telsacrypt variant conduct a targeted campaign against online gamers [12] [13]. The popular games Minecraft, StarCraft II, Assassin's Creed, Call of Duty, World of Warcraft, and League of Legends were the most affected as criminals continue to seek out pressure points in their victims that provides the greatest returns, with this particular campaign assessed to have extorted $75,000 in ransom payments within 3 months. Variants such as CryptoFortress will also look for all network shares with write access at the time of infection as well as the local files, and if afflicting a server this could encrypt files used by multiple users.

Ransom Demand

After initially asking for credit card payment, the voucher system was quickly adopted, using formats such as Ukash or MoneyPak [14]. This system was relatively well established before being superseded by the use of Bitcoin. While Bitcoin payment is likely unfamiliar to many victims, the level to which it lowers the risk when combined with Tor means that it is likely to remain the method of choice, particularly as awareness of digital currencies is growing. The time period given to pay the ransom is typically 72-96 hours, and the ransom often rises exponentially if not paid within this period [15]. Recent variants have adapted this to offering a free decryption service for a small number of the files as a proof of concept in order to gain trust.

Based on the variants cited in this report, the price point of the ransom demand of crypto-ransomware is around $400 on average, with screen locking variants slightly less. FBI statements indicate enterprise ransoms as high as $10,000, although unsurprisingly no companies have publically announced it [16].

Malware authors have tested and adjusted to the marketplace, balancing the likelihood of getting a victim to pay and extorting the maximum amount possible, hence this figure is likely to remain the same in the short term. Conversely, it should be noted estimates of criminal profits from ransomware were estimated to have been greatest from WinLock during a 2010 campaign [17] as shown in Figure 5. This merely locked a user out, threatening law enforcement investigation into the device if payment was not made using a $10 premium SMS. Profits for this campaign were thought to be around $16 million, far higher than the estimated $3 million from the significantly more advanced CryptoLocker which had a ransom demand of around $300.

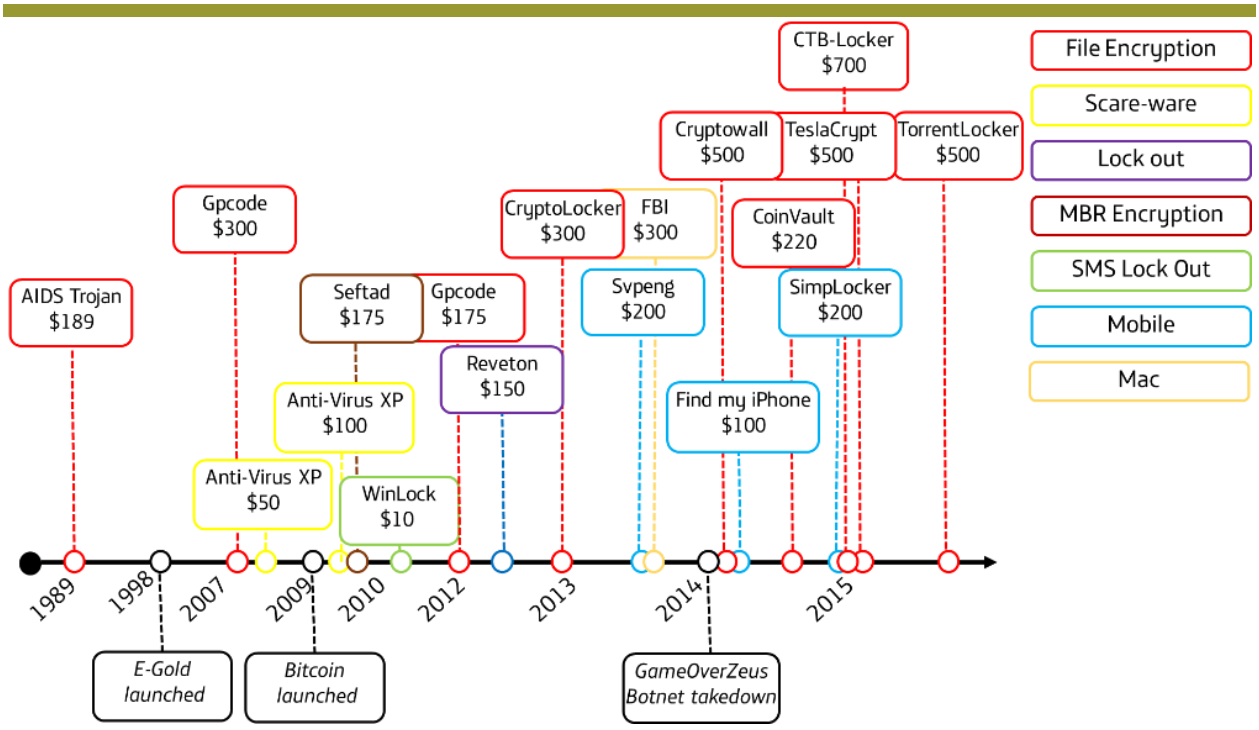

Figure 5. Ransom demand variation over time.

In 2014 U.S CERT highlighted Symantec research that some cyber criminals could extort up to $394,400 per month in ransoms from a single C&C server [18] [19]. Over time, analysis of Bitcoin wallet activity, criminal forums and crime statistics has placed the estimated percentage of victims that pay the ransom across differing variants between 0.2% and 13% [20] [21].

Current Situation

While still maintaining a mass delivery approach, ransomware has evolved to become more complex, and features such as secure communications, covert launching techniques and awareness of sandbox environments are now found more frequently. Individual variants are often tailored to the locale, however the most consistently targeted countries for criminals appear to be the English-speaking countries of the United States, Canada, United Kingdom, and Australia, followed by the other major European economies. Technical advancement makes it likely that criminals will continue to target countries with higher per capita income such as those that have historically provided lucrative returns on criminal investment

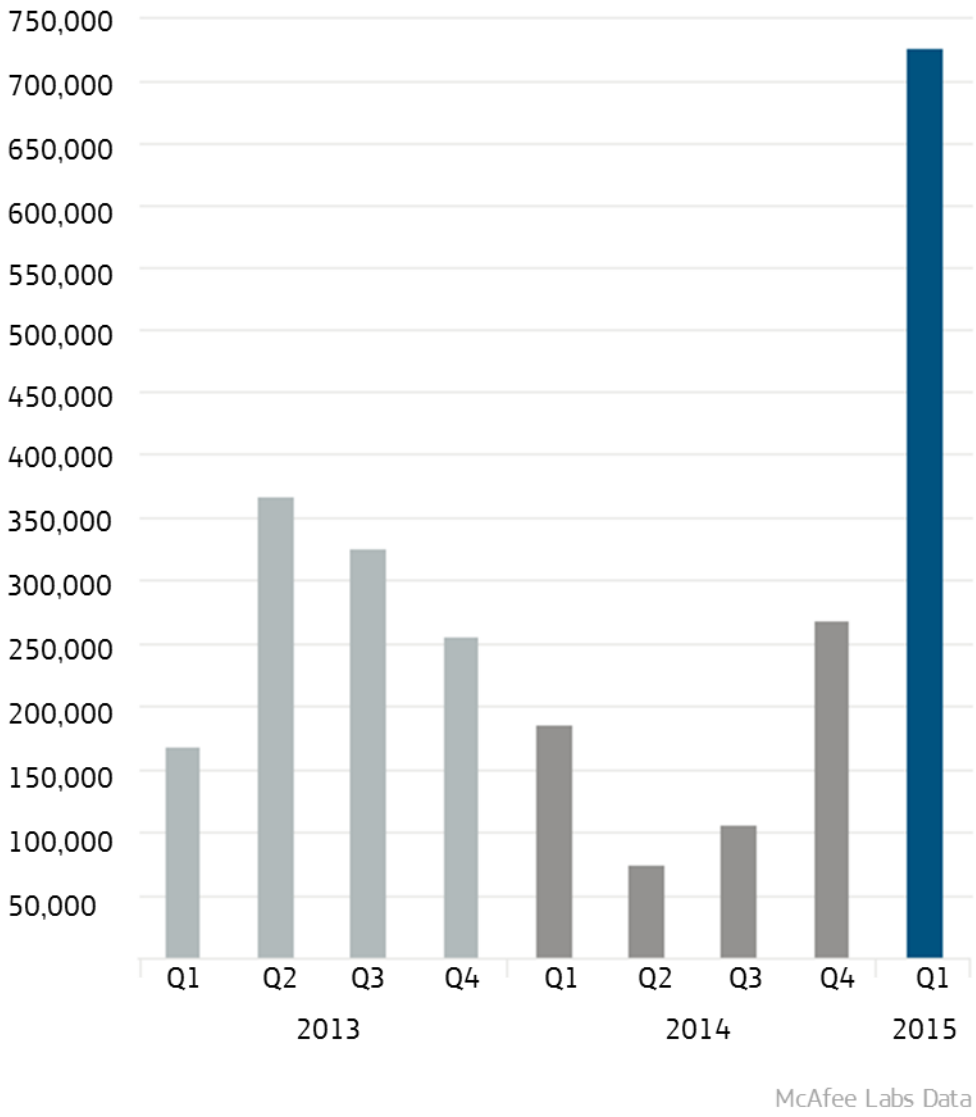

Figure 6. Crypto-Ransomware infections 2013-2015.

McAfee data from Q1 2015 found a 165% increase in ransomware detections from the previous quarter (See Figure 6), and the most prevalent variants that were responsible for this explosion in propagation are listed below; although more information on these and other notable variants can be found at Appendix A.

- **Cryptolocker** – The most prolific crypto-ransomware variant, Cryptolocker rose to prominence during 2013 when commonly spread by the "Gameover Zeus" botnet. Testament to how well it is regarded in the criminal marketplace as a brand, it has spawned numerous copycat variants, albeit of varying quality. During 2015 the top languages used by Cryptolocker Tor pages indicate the variant was likely targeted at English speaking countries and Europe (See Figure 7) [22].

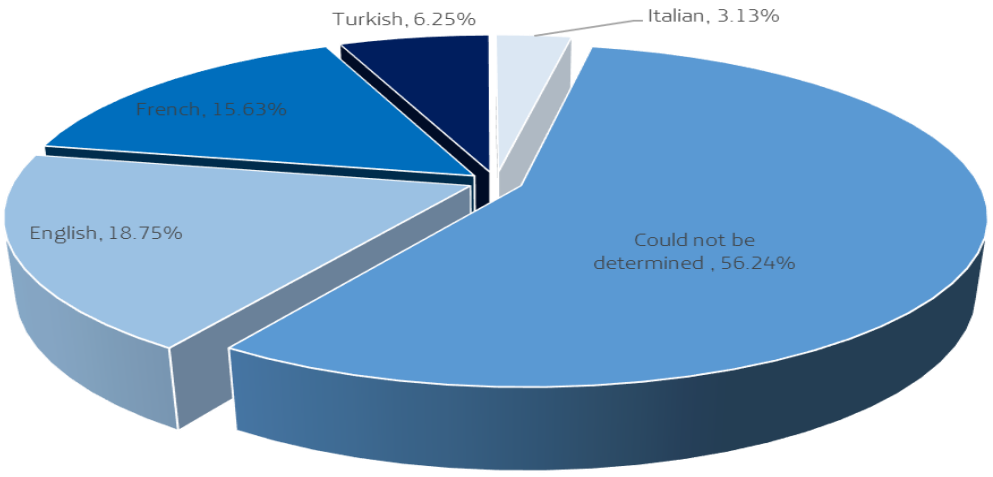

Figure 7. Top languages used by CryptoLocker Tor pages.

- **Cryptowall** – Cryptowall emerged as one such variant mimicking Cryptolocker. The perpetrators are estimated to have extorted over $1 million in a six-month period in 2014 [23], and Cryptowall 2.0 variant was highlighted in a June 2015 warning by the FBI [24].

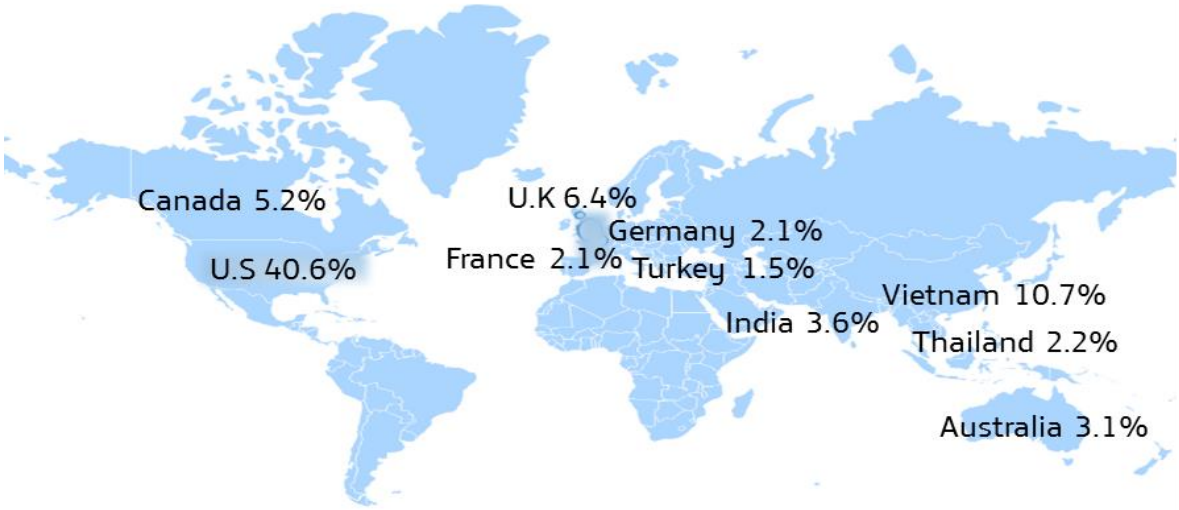

Figure 8. Top 10 countries infected by CryptoWall in 2014.

- **CTB-Locker** –CTB-Locker pioneered the use of the Tor anonymity network and elliptic curve cryptography in ransomware. Its authors epitomise the increasingly business-like approach in the manner they established an affiliate programme in underground marketplaces.

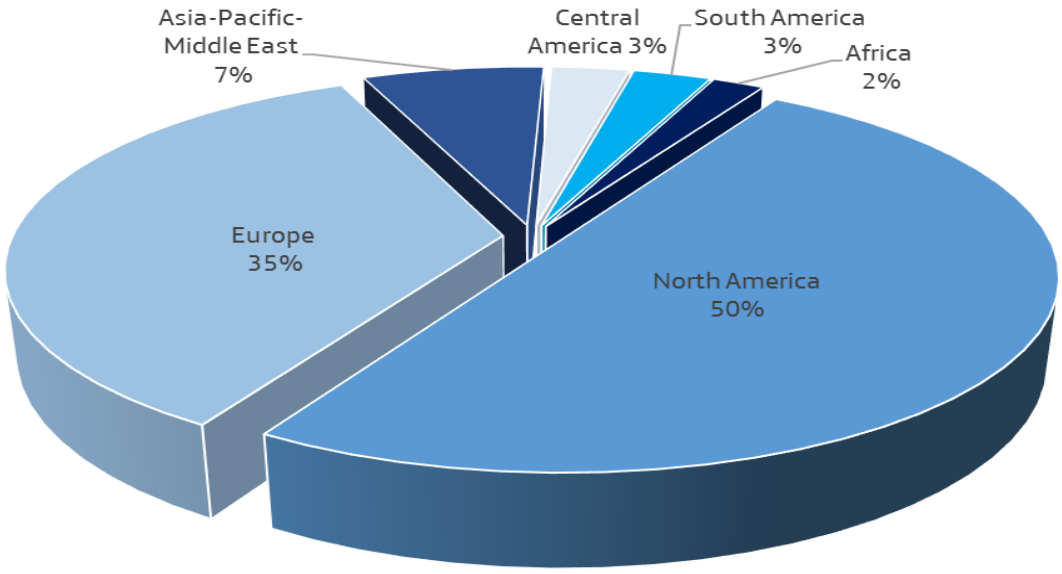

Figure 9. CTB-Locker infections during Q1 2015.

- **Kryptovor** – Unlike the others in this list, Kryptovor primarily targets businesses in Russia. Its modular nature was first identified stealing crypto-currency wallets from victims before a ransomware component was added.

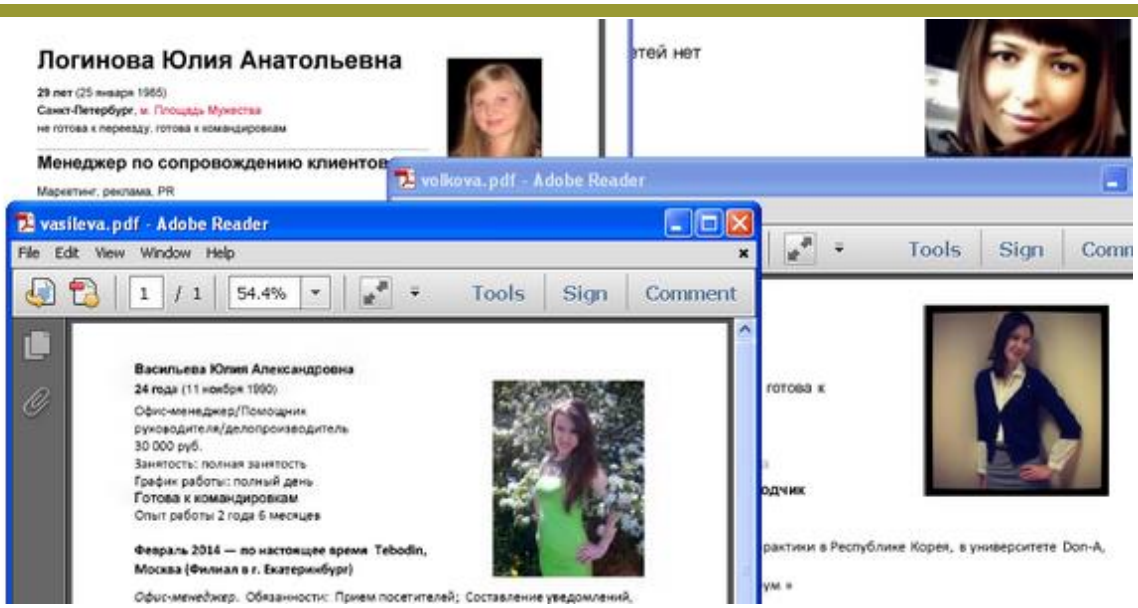

Figure 10. Malicious attachments from phishing emails used as the infection vector for Kryptovor.

Mutually Supportive Malware Infrastructure

Ransomware has retained a symbiotic relationship with botnet infections and phishing attacks, however the resurgence of the criminal abuse of third party advertising infrastructure as a means of distributing malware saw 'malvertising' a key distribution channel during Q1 2015. Distributing malware via legitimately bought advertising impressions teamed with exploit kits can easily infect even a security conscious user. Reflecting the professionalization of the criminal marketplace in using this technique, criminals are to effectively distribute ransomware with precision and stealth, and also set an investment ceiling with which they assess will provide the maximum return on investment. The technique is often funded by 'click fraud' malware, and, while comparatively less harmful, an infection may also act as a harbinger of more damaging infections to come.

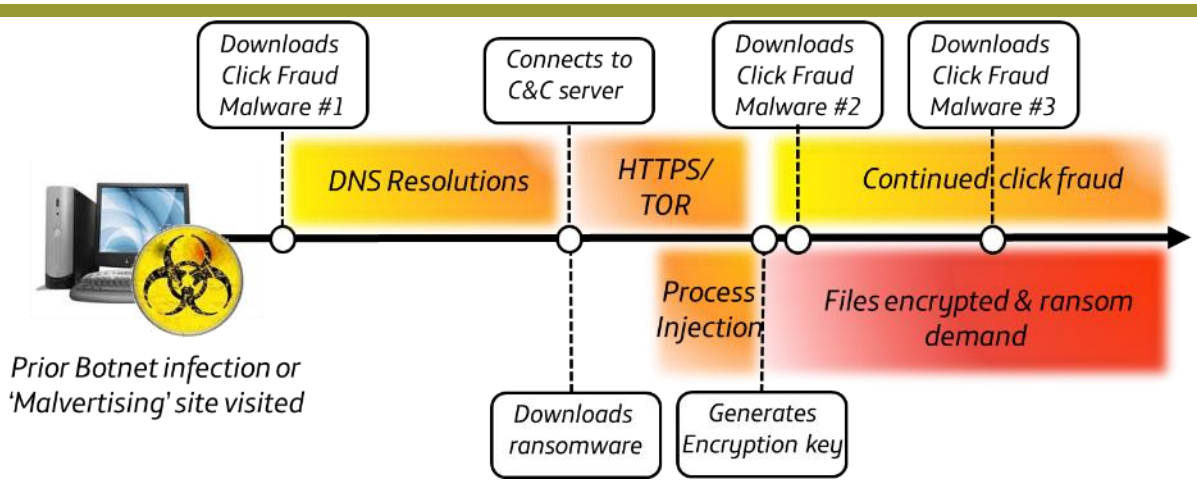

Figure 11. Illustrative malware lifecycle encompassing 'click fraud' and ransomware.

Rather than renting out infected devices in a botnet, or trying to steal banking credentials, criminals are able to use the ransomware model to immediately monetise the infection. In keeping with the flexible business model of ransomware distributors, exploit kits can be rented or licenced out and when paired with zero-day vulnerabilities can see propagation rates soar, and is likely to be a theme during the remainder of 2015. This underground marketplace opens ransomware up to criminals with few, or no technical skills; and with some estimates suggesting that a criminal investing in ransomware and exploit kits can achieve a 1,425% return on investment, there is sure to be significant interest in the criminal community [25].

Future Development

RansomWeb

Early cases of criminals adapting the brazen ransomware methodology to the enterprise environment by maliciously encrypting the backend database of a website could be an indicator of a future trend. The RansomWeb technique was publicised in early 2015 when the database of a financial services firm was held to ransom for $50,000, a figure stated to rise by 10% with every passing week [26]. The operation had gradually taken place over a period of 6 months, with encryption and decryption silently taking place until the attackers withdrew access to the private key, subsequently taking the website offline. Despite this, due to mistakes made by the criminals the key was recoverable by the company ensuring to ransom was paid.

The City of Detroit faced a similar attack, although the demand of $800,000 was nullified by the obsolescence of the database encrypted [27]. Similar attackers targeting SME's for lesser ransoms of around $1,000 have however been more successful, and have also involved encryption of backups.

Ransomware-as-a-Service

While the distribution of various types of Crimeware-as-a-Service is not new, ransomware distributors are proving particularly innovative with their criminal business strategy. Variants of Cryptowall have been found to be bundled with information stealing Trojans, if not a direct result of a previous botnet infection. The CTB-Locker infrastructure is available to affiliates using their botnets to send spam to potential victims. As the infrastructure is hosted by a third party, combined with the use of Bitcoin and Tor, this is a low-risk addition to existing criminal operations.

In another development, during May 2015 McAfee discovered the 'Tox' ransomware kit available for free on the dark web, with the distributor taking a 30% share of the Bitcoin ransom [28]. A 2MB executable is produced after creation via a dashboard, using the Tor anonymous browser for communication, and Bitcoin for whatever ransom payment the criminal configures.

Despite the standard of anti-malware evasion being quite high at the time of discovery, the Tox codebase lacked the complexity of other crypto-ransomware variants and was found to have been created by a lone student before he dissociated with the malware. However it is likely that this model will develop to offering more advanced malware to less technical criminals during 2015.

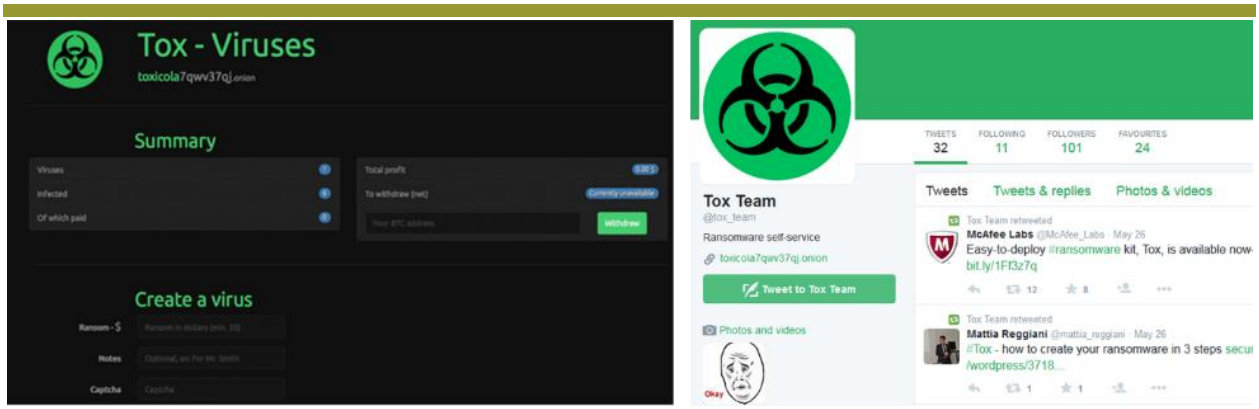

Figure 12. The 'Tox' malware creation dashboard available through the Tor browser and Twitter account.

Mobile Ransomware

The level of sophistication employed by mobile ransomware lags behind that of Desktop variants. They only relatively recently have begun actually encrypting files as opposed to merely claiming to have done so, and the chance for recovery without a ransom is greater. This gap is narrowing however, and notable features include propagation over SMS and use of AES encryption. Further development is likely, with Kaspersky Lab reporting a 65% increase in mobile ransomware samples during Q1 2015, the majority targeting Android devices [29]. The only attack to date targeting iOS was a June 2014 campaign that locked the iPhone after compromising the victims' iCloud account as opposed to a malware encryption.

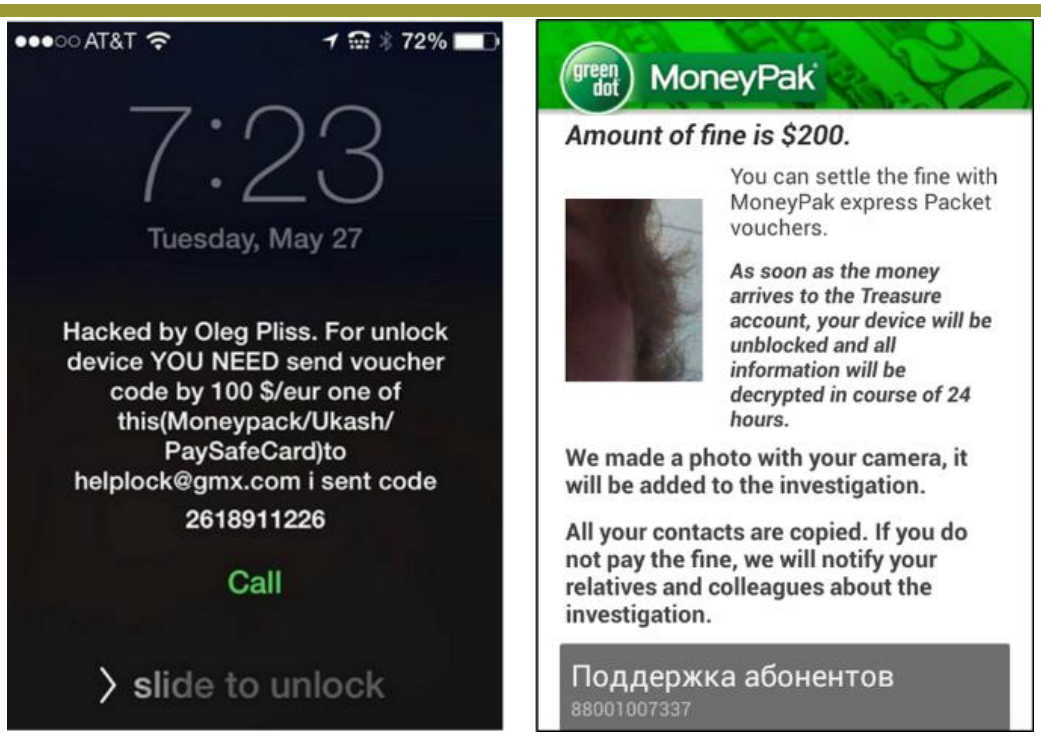

Figure 13. Mobile ransomware affecting iOS and Android smartphones.

Cloud, Point of Sale and Internet of Things

Looking to the future of smart devices and increasing use of the cloud, ransomware would appear to scale well, it is possibly the easiest way to monetize a malware infection of device that does not even have to have any personal or financial data present, and comes with direct payment into a criminal's bank account. Even if not financially motivated, ransomware is capable of turning a device into a 'brick' for any malicious or activist goal. Further refinement is also possible into point of sale (POS) terminals as faster alternative to exfiltrating card data particularly if launched in peak sales periods.

Mitigation measures

The strategies that should be employed regarding ransomware are prevention and contingency planning. The chance of a cure is minimal and is closing further as the variants evolve. Similar to countering many malware threats distributed via phishing, a comprehensive employee security education programme can go a long way.

In the case of ransomware this is particularly pertinent as threats shift toward the enterprise, and with it have become more professional and grounded in human psychology to achieve infection. Although when paired with delivery vectors like malvertising, technical controls must also be optimal. Anti-virus and HIPS have two windows of opportunity to prevent the malware encrypting the device; at the stage of the 'drive-by' exploit, and then the stage of process injection.

Backups

Ensuring redundancy against ransomware should ideally entail regularly restored backups to insure integrity, conducted as per the 3-2-1 methodology; three copies, two different formats and one copy offsite. Merely synced copies are not sufficient as they may be duplicating the infection, however some cloud storage providers, such as Dropbox [30] allow restoration from a previous version for a limited period.

System Hardening

Software restriction policies to prevent ransomware executing in common directories like %AppData% or %LocalAppData%, restricting permissions on Registry keys like HKCU\SOFTWARE\, and restricting *write* privileges on file servers alongside regular patching can be effective controls. Withdrawing the use of non-essential software, such as Adobe Flash will restrict the effectiveness of exploit kits and the resurgence of 'malvertising' which looks set to continue throughout 2015.

Awareness of Existing Malware Infection

Aside from backing up data and hardening systems as much as possible, being alert to existing malware infections that could be a harbinger of ransomware is also crucial. The malware infection lifecycle can often being with 'click fraud' malware, within the scope of overall threats, when viewed in isolation this may be considered a low-priority threat however it can lead to downstream ransomware infections. Research has shown this can take place in as little as two hours [31].

Hardware Security Modules

Secure storage of cryptographic keys such as that provided by hardware security modules (HSM) protects against RansomWeb type attacks. As the generated keys never leave the dedicated hardware it is easy to track who has used them, and ensures non-authorised personnel cannot get access. File integrity checks where possible can also ensure that a database or backups are not being slowly encrypted.

Decryption Tools and Services

Law enforcement cannot be relied on for resolution, however both law enforcement and private companies tracking malware authors have obtained criminal backups containing private keys for some variants. While eliminating any chance of decryption for those paying a ransom, this has previously resulted in security companies such as FireEye and Kaspersky [32] developing free online decryption tools for some variants of CryptoLocker [33] and CoinVault [34]. As of June 2015, some applications such as 'CryptoMonitor' claim to be able to kill an encryption infection and blacklist it from running again, and many variants of mobile ransomware can be decrypted without paying the ransom.

Paying the Ransom

The only way to nullify the criminal business model is if no-one paid a ransom; however such high-minded thinking is of no compensation to an individual or business who have been infected with ransomware, and have none of the contingency measures in place and decryption tools are not applicable to the variant. However those considering paying a ransom in this scenario should remember: there is no guarantee that the files will be decrypted. The criminals may have no intention of doing so, they may not be able to due to infrastructure takedowns, or the decryption could fail. Interacting with the ransomware distributors in a minority of cases has resulted in a reduced demand, but the psychology of someone who had perpetrated the crime in the first place must always be remembered.

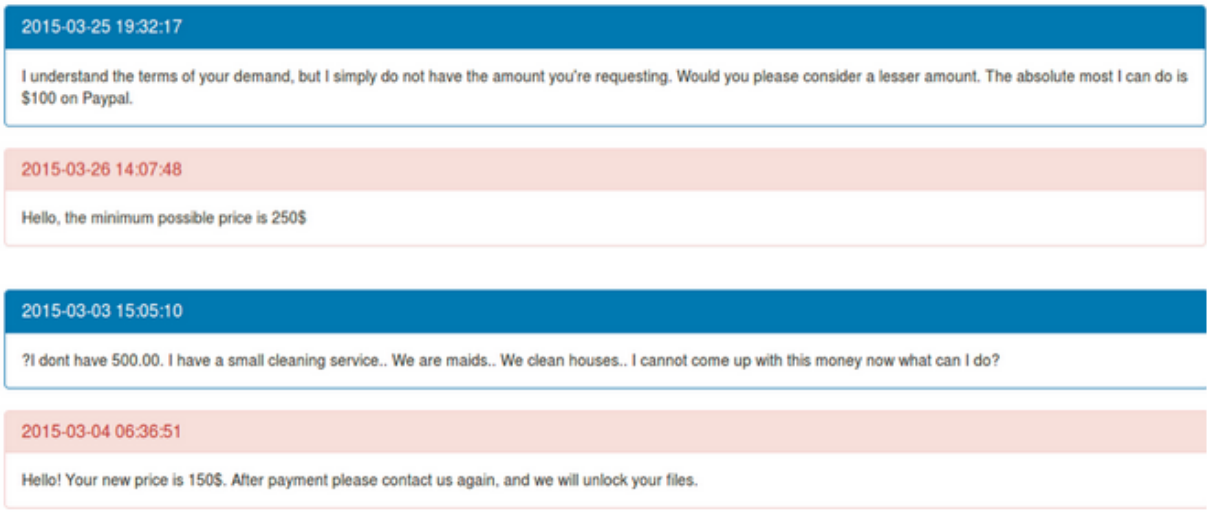

Figure 14. Varying interactions with the distributors of Teslacrypt ransomware.

In this final situation, ultimately a calculated business decision has to be made. Should this eventually result in decryption, because of symbiosis with other malware the computer and network it resides on must still be regarded as compromised.

ANNEX A – Common Ransomware Variants

TorrentLocker

Launched during 2014, and initially only in Australia, TorrentLocker was distributed via spam emails and used the branding of several well-known Australian businesses. The variant spread to over 13 countries and had affected approximately 39,000 systems by the end the year. Less than 2% of victims were thought to have paid the ransom, however the businesses suffering reputational damage incurred significant costs through increased monitoring, brand protection and takedown operations on malicious domains.

CryptoLocker

Using 2048-bit RSA encryption, CryptoLocker represented a noticeable increase in professionalism with regard to the cryptographic implementation. First appearing in September 2013, CryptoLocker was spread widely through peer-to-peer malware the 'Gameover Zeus' botnet, affecting an estimated 250,000 within the first 100 days. CryptoLocker was malware of some renown in the criminal underground and various copycats have been later released trading on the name.

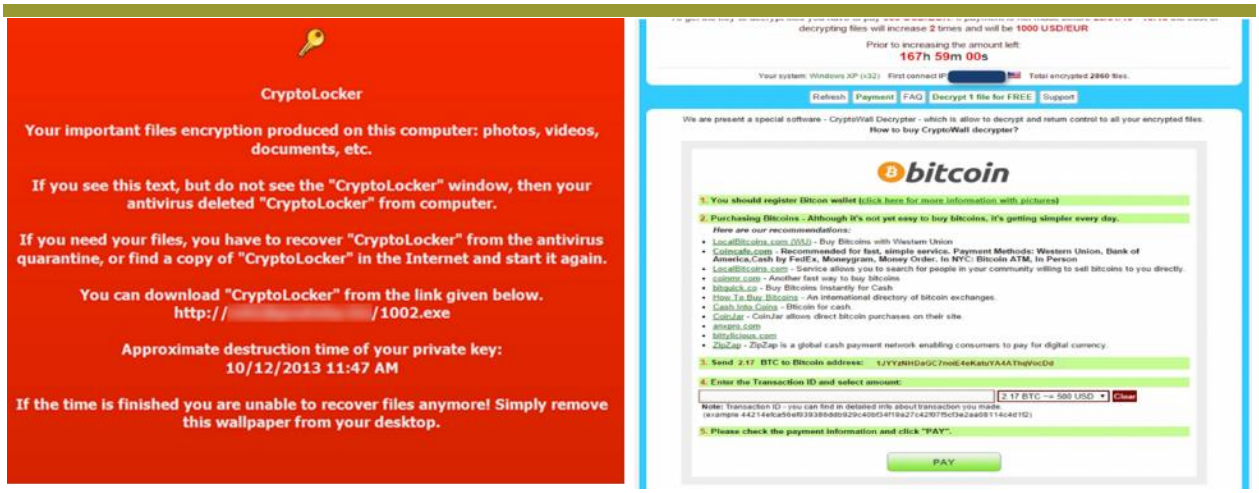

Figure 15. The sadly all too common CryptoLocker wallpaper & CryptoWall payment page.

CryptoWall

Currently active in the CryptoWall 3.0 variant, CryptoWall was originally a copycat of CryptoLocker, and was one of the most prevalent variants during Q1 2015. Using 2048-bit RSA encryption and additional features such as disabling and deleting the cache of the Volume Shadow Copy Service (VSS) that runs on all modern versions of Windows means this is a particularly effective variant. Primarily distributed via exploit kits, CryptoWall communicates over Tor and therefore requires the victim to install Tor browser in order to complete the ransom payment.

FBI Ransomware

Only notable due to affecting OS X, the so called FBI ransomware provides the user with a warning that they have broken the law and the device will be locked until a fee of $300 is paid. No encryption actually takes place and the malware simply leverages the browser 'restore from crash' feature using JavaScript code, and therefore can be simply removed by restarting Safari and selecting to reset all options.

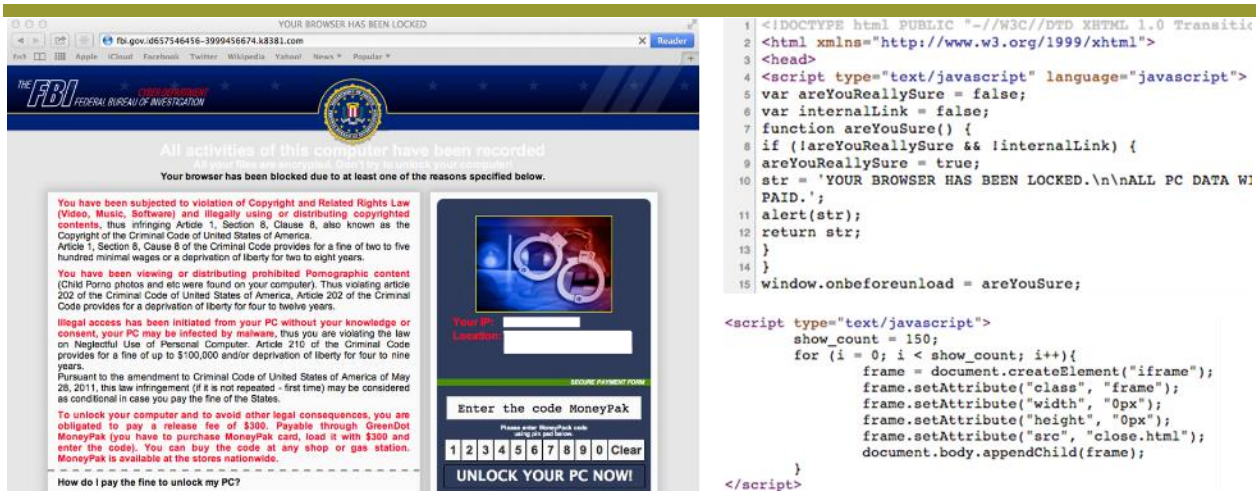

Figure 16. FBI Ransomware affecting Mac OS X and the Javascript code.

CTB-Locker

CTB-Locker is so named due to combined use of elliptic-curve cryptography, Tor, and Bitcoin, and typifies the advancement in ransomware that is becoming ever more prevalent. Phishing emails used to spread CTB-Locker are noticeably of a high-standard, and are tailored specifically to the locale in which they target, commonly using a .zip file attachment. It also allows a 'free' decryption service of five files to attempt to appear to the victim that there is more chance of the files being decrypted if they pay the ransom. CTB-Locker has been named in a number of advisories during 2015 and now affects many European countries.

References

[1] Symantec, 2012. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf.

[2] Trend Micro, 2015. [Online]. Available: http://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup.

[3] Phish Me, 2014. [Online]. Available: http://phishme.com/top-10-phishing-attacks-2014/.

[4] Imperva, 2015. [Online]. Available: http://blog.imperva.com/2015/06/spear-phishing-using-a-net-.html.

[5] McAfee, 2015. [Online]. Available: https://blogs.mcafee.com/executive-perspectives/franchising-ransomware.

[6] J. G. d. I. P. I. S. D. B. P. G. B. Félix Brezo, *International Joint Conference CISIS'12-ICEUTE´12-SOCO´12 Special Sessions*, vol. 189, pp. 97-108, 2013.

[7] Sophos, 2015. [Online]. Available: https://secure2.sophos.com/en-us/security-news-trends/whitepapers/gated-wp/cryptolocker-cryptowall-remove-ransomware.aspx?cmp=701j0000000LOhOAAW.

[8] Trend Micro, 2015. [Online]. Available: http://blog.trendmicro.com/trendlabs-security-intelligence/cryptowall-3-0-ransomware-partners-with-fareit-spyware/.

[9] Cisco, 2015. [Online]. Available: https://blogs.cisco.com/security/talos/cryptowall-2.

[10] McAfee, 2015. [Online]. Available: https://blogs.mcafee.com/business/advice-unfastening-cryptolocker-ransomware.

[11] Bromium, 2015. [Online]. Available: http://www.bromium.com/sites/default/files/bromium-report-ransomware.pdf.

[12] FireEye, 2015. [Online]. Available: https://www.fireeye.com/blog/threat-research/2015/05/teslacrypt_followin.html.

[13] McAfee, 2015. [Online]. Available: https://blogs.mcafee.com/mcafee-labs/teslacrypt-joins-ransomware-field.

[14] Action Fraud, 2012. [Online]. Available: http://www.actionfraud.police.uk/alert-public-to-be-on-guard-against-new-ransomware-scam-may12.

[15] Bromium, 2015. [Online]. Available: http://www.bromium.com/sites/default/files/bromium-report-ransomware.pdf.

[16] IC3, 2015. [Online]. Available: http://www.ic3.gov/media/2015/150623.aspx.

[17] Kaspersky Labs, 2010. [Online]. Available: https://securelist.com/blog/opinions/29623/the-winlock-case-im-taking-bets/.

[18] U.S CERT, 2014. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA14-295A.

[19] Symantec, 2012. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf.

[20] Dell SecureWorks, 2014. [Online]. Available: http://www.secureworks.com/cyber-threat-intelligence/threats/cryptowall-ransomware/.

[21] FireEye, 2015. [Online]. Available: https://www.fireeye.com/blog/threat-research/2015/05/teslacrypt_followin.html.

[22] Trend Micro, 2015. [Online]. Available: http://www.trendmicro.co.uk/media/wp/exploring-the-deep-web-whitepaper-en.pdf.

[23] Dell SecureWorks, 2014. [Online]. Available: http://www.secureworks.com/cyber-threat-intelligence/threats/cryptowall-ransomware/.

[24] IC3, 2015. [Online]. Available: http://www.ic3.gov/media/2015/150623.aspx.

[25] TrustWave, 2015. [Online]. Available: https://www2.trustwave.com/rs/815-RFM-693/images/2015_TrustwaveGlobalSecurityReport.pdf.

[26] High Tech Bridge, 2015. [Online]. Available: https://www.htbridge.com/blog/ransomweb_emerging_website_threat.html.

[27] Detroit News, 2014. [Online]. Available: ww.detroitnews.com/story/news/politics/michigan/2014/11/17/north-american-international-cyber-summit/19162001/.

[28] McAfee, 2015. [Online]. Available: https://blogs.mcafee.com/mcafee-labs/meet-tox-ransomware-for-the-rest-of-us.

[29] Kaspersky Labs, 2015. [Online]. Available: https://securelist.com/analysis/quarterly-malware-reports/69872/it-threat-evolution-in-q1-2015/.

[30] Dropbox, 2015. [Online]. Available: https://www.dropbox.com/help/8408.

[31] Damballa, 2015. [Online]. Available: https://www.damballa.com/state-infections-report-1h-2015/.

[32] Kaspersky Labs, 2015. [Online]. Available: https://noransom.kaspersky.com/?utm_source=securelist&utm_medium=text&utm_campaign=com-securelist .

[33] FireEye, 2014. [Online]. Available: https://decryptcryptolocker.com/ .

[34] Kaspersky Labs, 2015. [Online]. Available: https://noransom.kaspersky.com/static/convault-decrypt-manual.pdf.