EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

POLITIE

Police Ransomware Threat Assessment

February 2014

Table of Contents

Key findings

- There has been an exponential growth in police ransomware attacks in the EU and worldwide over the last two years. Ransomware is a fast method for criminals to generate significant profits.

- New forms of encryption ransomware are far more threatening as files and documents vital to individuals and businesses are at risk of being lost permanently. Small- and medium-sized enterprises and public services might become preferred targets for ransomware offenders.

- The use of online prepaid solutions and virtual currencies have been major developments in the evolution of ransomware fraud and drive the exponential proliferation of this criminal activity. They provide anonymity of cash in the online environment and are key elements of money laundering schemes.

- The sustained growth of the Crime-as-a-Service model has fuelled the development of ransomware cases. Ransomware attacks can be easily deployed by criminals and are no longer restricted to the technically savvy.

- Underground forums are initial meeting and networking points for cybercriminals and serve as key enablers for their ransomware operations. Underground forums provide spaces for cybercriminals to form organisations and structures and support the professionalisation of the criminal trade.

- Offenders are increasingly investing in protecting their infrastructures and communications integrity, commonly using bullet-proof hosting and strong encryption, which reduces the scope for law enforcement actions.

- Ransomware criminals rely on the services of specialised money launderers. These use different techniques to cash out illicit profits, combining both virtual and traditional systems, using various online gambling platforms as well as electronic payment intermediaries and virtual currencies.

- The public is largely unaware of the threat of ransomware, which contributes to the success of this type of fraud.

- The distribution of ransomware actors and infrastructure over many legal jurisdictions complicates investigations and requires lengthy legal assistance processes.

Recommended areas for action

- Reduce the number of potential victims of ransomware by increasing awareness of the phenomenon. It is important to reach a large audience, not only online, but also through traditional means of communication, as less technically-aware people are more likely to become victims.

- Reduce the likelihood of victims paying the ransom. In addition to making this an important part of the preventive and awareness communication, additional actions are possible with the support of private partners. Reducing the number of victims that pay ransoms will make the ransomware business model less profitable for criminals.

- Increase awareness about ransomware within local police forces and use them as a vector for distributing information on the phenomenon within the communities they serve. Victims are more likely to report to local police. It is important that the local police are aware of the problem and have clear guidelines on how to deal with it.

- Improve the overall picture on ransomware cases in the Member States (MS) and at EU and international level. Local police forces are crucial in collecting and reporting information about ransomware incidents/cases to a central authority.

- Conduct cross-border operations/investigations against criminals that deploy ransomware attacks.

- Improve international information exchange and operational coordination related to ransomware from the early stages of investigations. This will contribute to an enhanced picture at EU level and will enable better understanding of the links between cases and criminals.

- Improve cooperation with private partners at national and European levels for enhanced support and coordination during investigations.

- Reduce criminals’ options to cash out and launder illegal profits at the end of the process.

Introduction

Context and purpose

Over the past two years, European Union (EU) Member States (MS) have been confronted with a significant proliferation of police ransomware cases. Experts from both law enforcement and the private sector agree that prevention and raising awareness can only work in conjunction with investigations targeting the criminals behind the fraud. Furthermore, even if police ransomware in its current form might naturally fade out in the future, it is likely that an evolution of this modus operandi driven by the same or different perpetrators will take place. That is why it is important that measures against police ransomware and similar modi operandi are implemented in a coordinated, complementary and comprehensive manner.

This assessment is the result of a common initiative of the European Cybercrime Centre (EC3) and the Dutch National High Tech Crime Unit (NHTCU). Its aim is to increase awareness of ransomware by providing an EU perspective on the problem and to identify opportunities for intervention and coordination. The assessment encourages better coordination and cooperation between MS law enforcement agencies from the early stages of cybercrime investigations and acknowledges once more the importance of partnering with private industry.

This threat assessment relies on open source information, research papers on ransomware and semi-structured interviews with cybercrime investigators.

Definitions

Police ransomware is a type of online fraud used by perpetrators to extort money through the deployment of malicious software. The malware disables the functionality of the victims' computers and displays a message demanding the payment of an amount of money through a prepaid online payment system[1], in order to regain access to the machine. The message is alleged to be law enforcement action against illegal online behaviour by the victim, such as illegal file-sharing, downloading or accessing online child abuse material, or visiting terrorist websites. The use of law enforcement symbols is meant to lend authority to the message and to coerce victims into making the payment.

Police ransomware is known under various names such as police trojan, police virus, police ransomware, winlocker ransomware. Currently, some of these names refer to variants of ransomware that do not include the abuse of law enforcement imagery in the locked screen.

Police ransomware is not a fundamentally new technique to extort money, but merely a reinterpretation of modi operandi that have been used before. The most important difference is the use of law enforcement insignia to reinforce the element of coercion. Ransomware can be roughly classified into two categories: winlocker ransomware which prevents the victims from accessing their computers, and encryption ransomware (crypto-ransomware) which encrypts files on the victim's machine. The police ransomware variants observed so far belong to the first category.

[1] Also referred to as 'vouchers' in this document.

Overview of the threat

Research into specific ransomware campaigns has shown that ransomware quickly generates significant profits. There is no clear picture on the number of computers that have been infected by police ransomware in Europe or worldwide and the number of victims that have paid ransom is unknown. Nevertheless, data from industry and some MS law enforcement agencies indicate that potentially millions of computers have been infected and tens of thousands of victims have paid the ransom demand, making this a multimillion euros business.

The continuous evolution of the scam and specific modi operandi suggests that ransomware is still a popular tool in cybercriminals' portfolios. It is important to note the development and continuous improvement of the ransomware business model. The current threat potential from ransomware is high as a ransomware attack can easily result in permanently lost files on the compromised machines. Several elements make ransomware attacks lucrative and popular with cybercriminals:

- The existence of anonymous means of payment,
- Multitude of services and expertise available within underground forums/markets,
- Lack of awareness among potential victims.

The ransomware evolution

Malware attacks for a ransom became common in the Russian Federation between 2005 and 2006, in the form of encrypting files and demanding payment for the decryption key. A variant of a locked screen was identified in 2009. The next scam used pornographic images in the locked screen to shame victims into payment. This has proven a lucrative method, repeatedly used by criminals. The victims were required to send SMSs or call premium-rate numbers[2].

Ransomware is often compared to fake antivirus malware in the way it operates. The fake antivirus software provides false security alerts to convince the users to purchase a full version of 'antivirus software' to remediate the non-existent problems. This type of fraud appeared several years ago and has occurred less frequently since late 2011, while police ransomware cases have seen a steep increase over the same period of time[3]. Research suggests that authors of fake antivirus software are behind some of the police ransomware campaigns[4].

In the beginning of 2011, police ransomware began to spread in Europe. This was the first time ransomware made use of prepaid online payment systems, which provided very limited possibilities for law enforcement to trace the money. This type of fraud is currently employed all over the world, including US, Canada, Latin American and Asian countries.

More recently, criminals are adopting advanced variants of ransomware that encrypt the victim's files using various encryption algorithms. The wiping of all the files on an infected computer has appeared as a new threat related to the locked screen modus operandi. While the amount of ransom money demanded has increased, paying the asked sum does not guarantee that the victims would get their files decrypted.

Current crypto-ransomware variants have significantly evolved from past malware versions which were easily removable by antivirus software. The latest file encryptors take advantage of multi-stage enterprise-grade encryption and public key algorithms using unique encryption keys for each victim. This makes them essentially uncrackable without the private key known only to the ransomware author.

[2] Symantec, Ransomware: A Growing Menace, 2012
[3] Sophos, Ransomware: Next-Generation Fake Antivirus, February 2013
[4] Trend Micro, Police Ransomware Update, 2012

Social engineering and coercion methods

Social engineering is an important tool used by ransomware fraudsters to increase their rate of success. Police ransomware variants have constantly improved the quality of the logos and images used or their language quality. Over time, variants have also become more specific, adopting for instance corporate identities of local police. Spam distribution of ransomware was occasionally tied to trending current events. The 'Cryptolocker', an example of emerging encryption ransomware, is delivered by malicious emails with false subjects related to payrolls, package tracking, as well as bank correspondence.

Currently, every country in Europe probably has its own variants of police ransomware. Variants abusing the image of international organisations such as Europol/EC3 and Interpol are used to target a broader pool of victims. Some recent adjustments include police ransomware that is able to speak to victims in their native languages or those that use royal household insignias in addition to law enforcement ones. Improved features also include a countdown timer, in an attempt to increase the likelihood of payment under panic and pressure[5].

Some variants of police ransomware refer to websites recently visited by the victims as the source of alleged illegal downloads. The malware scans the victim's browser history and identifies matching websites likely to be associated with illegal content from a predefined list. Some variants also include the use of pornographic images on locked screens or they turn on computer webcams and publish the image in a pop-up window to reinforce the message that they are being observed. The latter can be an important coercion method if the attack occurs while the victim is surfing pornographic websites.

Crime-as-a-Service and underground forums

The emergence of the Crime-as-a-Service phenomenon has contributed to the growth of ransomware cases and the number of offenders. It has also made this type of crime more accessible to criminals who lack technical skills. Underground forums are initial meeting points, allowing communication and networking for cybercriminals and serve as key enablers for their ransomware operations. Underground forums provide spaces for cybercriminals to form organisations and structures and support the professionalisation of the criminal trade. These forums make available a variety of resources necessary to deploy successful ransomware campaigns, including the malware, the infrastructure for distribution and money laundering services.

Source-code for police ransomware and ready to use packages are available for sale within underground markets. Readily available ransomware kits are also offered for a share of the profits instead of for a fixed amount.

The range of services relating to infrastructure on offer is extensive and includes bullet-proof hosting, virtual private network (VPN) and proxy services, exploit kits and access to botnets. Servers are amongst the most sought after commodities in the underground marketplaces. Server prices depend on their processing power, internet access speed and level of security. Bullet-proof hosting services are the most expensive[6].

Pay-per-install or traffic redirects to compromised websites are also available for a price in the underground forums. Additional services include language translation or encryption.

Money laundering and cashing out services are offered by specialised networks, which usually work for more than one cybercrime group. Forged or stolen IDs are commonly traded within the underground markets. Using these IDs, criminals open various types of accounts used in money laundering schemes or register domains which are part of their criminal infrastructure. Compromised credit cards for cashing out the money can also be obtained from underground websites.

[5] http://www.symantec.com/connect/blogs/ransomware-extorting-money-panic-and-pressure, consulted 07 October 2013.

[6] Trend Micro, Russian Underground 101, 2012.

Anonymous means of payment

Ransomware offenders benefit from the existence of a variety of almost untraceable online means of payments, especially if they are combined. Prepaid payment solutions are widely used for legally purchasing goods and services online. They are also the preferred method for demanding ransoms because they offer the anonymity of cash in the virtual environment, from the initial moment when money is introduced into the illegal scheme. These prepaid vouchers can be easily purchased from a multitude of retail outlets. The use of online prepaid solutions is a major improvement to the ransomware model and one of the drivers of its exponential growth[7].

Virtual currencies are the preferred payment method for services in underground marketplaces and key elements in money laundering schemes. They are invented currencies[8] and enable anonymous transfers of conventional money. Issuers such as Liberty Reserve, Perfect Money and WebMoney are not tied to any banking authority and in most cases cannot identify the owners of the respective currency, as they rarely verify user identities when opening accounts. Prior to its take-down by US authorities, Liberty Reserve was one of the world's most widely used digital currencies believed to have supported the laundering of USD 6 billion (EUR 4.4 billion) in criminal proceeds[9].

Recent crypto-ransomware versions offer payment in Bitcoins as an alternative to prepaid voucher codes. Bitcoin is a decentralised peer-to-peer virtual currency, considered the most successful implementation of the crypto-currency concept and almost a synonym for virtual currency[10]. Its growth in usage combined with its perceived anonymity has made it attractive for criminal use.

Ransomware profits and effects

The exact number of victims that get infected and pay the ransom is difficult to assess. However, some estimates of the profits made by police ransomware offenders indicate that this type of cyber-fraud is very lucrative. Generally, it is presumed that approximately 3 percent of infected victims pay the ransom[11].

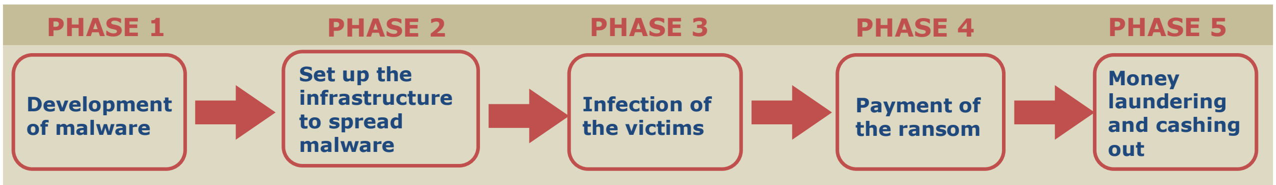
One operation against a complex network spreading police ransomware provided an insight into how lucrative this business model is. It was estimated that the criminals involved in this specific campaign affected tens of thousands of computers worldwide, generating profits in excess of EUR 1 million per year. Another example provided by a private researcher shows that in just two days, 25 000 computers were infected and more than 800 people in 11 EU countries paid out over EUR 70 000. Considering the exchange rates for vouchers in the underground economy, the criminals cashed in around EUR 40 000[12].

The emergence of new forms of encryption ransomware is a significant evolution in terms of impact. Situations where victims permanently lose files and documents may become common. Such outcomes have the potential to create serious operational problems for small- and medium-sized enterprises or public services, which may lack sufficient resources to adequately protect themselves or are simply less concerned about online security.

[7] McAfee, Threat Report: First Quarter 2013.
[8] European Central Bank, Virtual Currency Schemes, October 2012.
[9] Liberty Reserve was taken down by US Authorities in May 2013.
[10] McAfee, Digital Laundry, An analysis of online currencies, and their use in cybercrime, October 2013.
[11] Symantec, Ransomware: A Growing Menace, 2012.
[12] http://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/

Police ransomware business model

The police ransomware business model includes the various phases in the deployment of successful attacks and the actors involved in each phase. The separation between phases supports a barrier model approach to tackling the ransomware phenomenon, with tailored activities for all partners involved in terms of preventive and investigative measures.



Malware development

Besides writing the initial code for the ransomware, two additional activities are required to make malware lucrative. First, the malware must be permanently updated and reconfigured to keep up with patches and updates made by antivirus and software companies. Given the rate at which command and control servers are changed, reconfiguration is frequently required.

Second, the malware must be customised to fit the needs of different users. The customisation is done either before or after it is sold or rented out on underground online forums. This includes adapting designs to the targeted countries.

Setting up the infrastructure to spread the malware

Ransomware offenders need to build a supporting infrastructure to deploy their attacks. The various components can typically be rented or bought from underground marketplaces. Offenders need servers to host the malware and exploit kits, command and control centres, images for the locked screen, the scripts that identify the victim's country of origin, and drop zones for the voucher codes. The criminals set up a number of alternative command and control servers and server paths as redirects, in case any become unavailable.

Additionally, they need domains to host the malware and the websites redirecting to the malware. The domain names are usually registered in batches or lookalike series which allow them to be easily replaced in case of any disruptions.

Offenders invest effort and money into increasing the complexity of their infrastructure, aiming to leave as few traces as possible that might lead to their identification. Bullet-proof hosting is a key enabler for ransomware and is in high demand in the underground markets and forums. Criminals also use proxies via servers scattered internationally, double VPN, fast flux[13] or instant messaging with strong encryption.

Offenders need exploits, often part of exploit kits, to deliver their attacks. Ransomware may arrive as part of another malware's payload, or may be delivered via an exploit kit, which exploits vulnerabilities on the affected computer to silently install and execute the malware[14]. The Blackhole exploit kit was often used to deploy ransomware and fake antivirus malware[15]. Additional examples include Cool, Sweet Orange and Styx exploit kits.

Compromised computers are commonly used to host malware or exploit kits, as drop zones, to set accounts for checking balances or to cash out voucher codes. Nevertheless, botnets are rarely used to upload ransomware, and in most cases only if the criminals want to get rid of some of the bots. Ransomware is a highly visible crime and in most cases victims thoroughly check and clean their machine following infection.

[13] Fast flux is a technique used to hide sources of malware behind an ever-changing network of compromised hosts acting as proxies; numerous IP addresses associated with a domain name which are constantly swapped at high frequency.

[14] http://www.f-secure.com/en/web/labs_global/removal/removing-ransomware, consulted on 1 August 2013.

[15] Symantec, 2013 Internet Security Threat Report.

Once the supporting infrastructure is in place, offenders use hacked or malicious websites to redirect victims to the exploit kits and the sources of infection. Although hacking into legitimate websites is a difficult process and requires high-level technical skills, there are examples of hacked websites redirecting to a server that uploads ransomware, including popular online electronic shops and news websites. Often, traffic redirection to the sources of malware is purchased from specialised 'traffers' who get paid according to the number of redirects. A common method to get to the victims involves using malicious advertisements as a proxy.

Infection of the victims

There are different ways to infect the victim's computer with malware, but the most common one is referred to as drive-by downloads. The victim simply visits a compromised website[16] or is exposed to malicious adverts. Websites hosting pornographic material have been identified as the most common sources of infection. Malicious software is automatically installed on victims' computers without their knowledge. In most cases the attack is triggered at a later stage, so the victims remain unaware of the source of infection.

Other methods used to spread this type of malware include spam emails containing infected attachments or links to malicious websites, the downloading of content such as movies, music or software (illegal/pirated) from file sharing websites. Further possibilities for distributing compromised files/links include video sharing websites, instant messaging applications and social networking websites. Software vulnerabilities on the targeted computer are a prerequisite for ransomware to install. Outdated browser plugins such as Java, Flash or Adobe Reader are commonly exploited for ransomware infections.

The attack is customised with the right law enforcement imagery and message according to the geographic location of the user's IP address. A server contains all the images and the script that identify the victims' countries of origin. The overarching images of organisations such as Interpol or Europol are used when it is not possible to identify the victim's location.

Payment of the ransom

Once the computer is locked, the victims are required to pay an amount of money, usually between EUR 50 and EUR 150, or the equivalent in national currency, to regain access to the machine. For this purpose, ransomware offenders have chosen prepaid online payment solutions that obfuscate the money trail for law enforcement and are user friendly for the victims. In Europe, they abuse the services provided by Ukash and Paysafecard[17]. Newer versions of ransomware provide payment in bitcoins as an alternative option.

Victims need to purchase a voucher containing a multi-digit code and insert the code in the pop-up window. The vouchers can be easily purchased from a multitude of retail outlets including shops, petrol/gas stations, ATMs, kiosks or online. The perpetrators are careful to include a list of locations and known resellers of vouchers in each country in the locked screens.

After the payment, the codes are directed by the malware to a drop server under the control of the offenders. In most cases, the computers are not unlocked. Many of the ransomware variants do not even contain the code to uninstall themselves[18].

Money laundering and cashing out

Ransomware offenders need to turn the voucher codes into cash. Even for a small-level operation, the offenders would collect a significant number of codes, which are difficult to cash out without raising suspicions. For this reason, they use illegal cash out services and specialised money launderers. These services generally cost up to 50% of the nominal value of the vouchers.

[16] Includes legitimate websites, hacked by ransomware offenders or malicious websites created with the intention of distributing malware.

[17] In the US versions, MoneyPak codes are an alternative payment method.

[18] Symantec, Ransomware: A Growing Menace, 2012.

The money launderers use several techniques for cashing out, combining both virtual and traditional systems, using various online gambling platforms, electronic payment intermediaries and virtual currencies. One method is to load the value of the voucher codes on compromised credit and prepaid debit cards. Then money mules withdraw the funds from ATMs and wire the proceeds back to the cashing service or the ransomware offenders, minus their commission. In one operation, a money laundering cell was able to launder EUR 10 000 daily using various electronic payment systems and virtual currencies.

The money launderers rely on a network of money mules, usually spread in many countries. One money mule may have dozens of accounts which he uses in the laundering schemes. When a proof of identity is required they commonly use forged, counterfeited or fraudulently obtained IDs. The multitude of accounts includes anonymous digital currency wallets, accounts on gambling platforms, money exchangers and electronic money intermediaries.

A common method appears to be selling the vouchers at a reduced rate in exchange for alternative electronic money[19]. There are illegal voucher exchange sites that buy them from the cybercriminals paying up to 50% of the nominal value and reselling them to regular users at discounted prices[20].

A preferred way to cash out the value of codes is via online gambling platforms. Voucher codes are often traced back to internet gambling sites where they are paid into accounts of accomplices or money mules. Money launderers use dozens of websites, mostly online betting and casinos, to redeem the voucher codes. The large number of such platforms and different jurisdictions of incorporation complicates investigations and requires lengthy legal assistance processes, despite the companies' willingness to cooperate.

Police ransomware actors

The organised crime groups initiating ransomware attacks operate within an extensive network of developers, resellers and users of malware and malicious infrastructures. Groups are formed based on services offered and reputation is an important factor when they decide with whom to engage for specific tasks. Although underground forums make it easy to do business with various criminals, some of the investigated groups seemed to have formed a stable group for a longer period. Close members also interact with each other offline; meeting in real life strengthens the ties between these criminals.

As part of their business model, ransomware offenders misuse the legal services provided by various companies, such as providers of prepaid online payment solutions, advertisement companies, internet service providers, online shops, gambling platforms and money transfer companies. Unintentionally and unwillingly, these legal businesses become facilitators of the criminal process. The legal service providers are potential partners for law enforcement agencies, both for preventive and investigative measures, as they are willing to engage to reduce the possibilities of offenders misusing their services.

Victims who pay the ransoms make this business lucrative for criminals. Some of the reasons why they choose to pay include fear, lack of knowledge about online threats or being ashamed to report the crime, as many of the victims had been in contact with pornographic websites. In some cases, the victims may be aware of the fraud but they want to regain control of their machines as soon as possible.

[19] Symantec, Ransomware: A Growing Menace, 2012.
[20] Trend Micro, Police Ransomware Update, 2012.

Future considerations

Police ransomware and ransomware in general are fast methods for criminals to make money. The number of police ransomware cases will most likely go down in the near future, as more people will become familiar with this type of online fraud and will no longer pay the ransom. Once the police-branded frauds are not profitable anymore, cybercriminals will look into new ransomware opportunities.

The emergence of the crypto-ransomware is one indicator of the future threat. This type of malware encrypts the data and the attacker is the only one who has the key to unlock the data. Decryption is impossible without having access to the private key. Crypto-ransomware will cause far bigger problems for the victims; it is more sophisticated in its construction, asks for more money and is very aggressive.

Ransomware offenders are likely to change and adapt their attack methods and increasingly use their social engineering skills. It is expected they will charge higher ransoms, become more aggressive in their demands and add features to ransomware variants, for instance the capability to steal financial credentials.

The criminals will take additional steps to expand their pool of victims by addressing new markets, targeting different operating systems and devices. Windows operating system has been the most popular target for police ransomware, but a movement to other platforms such as Linux, iOS, Android and Windows Mobile is likely to take place.

Malware for mobile devices has seen significant developments in 2013 and the threats are increasingly sophisticated. Ransomware for mobile devices is part of the emerging threat. The first pieces of ransomware have already hit the Android platform, disguised as anti-malware programs. There are concerns about mobile ransomware ready-to-use kits making their way into the underground markets.

Small and medium businesses are becoming targets of ransomware. This has the potential to create serious business operational problems for those companies which may lack resources to adequately protect themselves or are less concerned about online security. The effects include permanently lost data and reputational damage.

A worrying trend with some ransomware variants is the displaying of child abuse images or even actually downloading child abuse material onto the victim’s computer. This increases the shame and fear of the victims and might make them more willing to pay. This might also make it more difficult for victims to report this form of crime to the police.

The modi operandi used by cyber criminals will adapt to the strategies of the anti-virus software industry and law enforcement. Increased complexity of infrastructure and malware can be expected. Victims’ computers or devices will be infected with multiple instances of malware and exploited in different ways.

More sophisticated money laundering modi operandi will be used in relation to new variants of ransomware. Virtual currencies will probably continue to have a central role. However, the abuse of prepaid online payment systems will persist because they are convenient and anonymous methods to pay ransoms. The underground economy of voucher exchanges will continue to be an important facilitator.

Sources

McAfee, Digital Laundry, An analysis of online currencies, and their use in cybercrime, October 2013, accessible at http://www.mcafee.com/us/resources/white-papers/wp-digital-laundry.pdf

McAfee, Threat Report: First Quarter 2013, available at http://www.mcafee.com/au/resources/reports/rp-quarterly-threat-q1-2013.pdf

Sophos, Ransomware: Next-Generation Fake Antivirus, February 2013, accessible at http://www.sophos.com/de-de/medialibrary/PDFs/technical%20papers/SophosRansomwareFakeAntivirus.pdf

Symantec, 2013 Internet Security Threat Report, accessible at http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

Symantec, Ransomware: A Growing Menace, 2012, accessible at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf

Trend Micro, The “Police Trojan”, an in-depth analysis, 2012, accessible at http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_police_trojan.pdf

Trend Micro, Police Ransomware Update, 2012, accessible at http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-police-ransomware-update.pdf

Trend Micro, Russian Underground 101, 2012, accessible at http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf