Symantec™
Security Response

Ransomware: A Growing Menace

Gavin O'Gorman
Geoff McDonald

Contents

Overview

Ransomware that locks a computer and uses law enforcement imagery to intimidate victims has spread from Eastern Europe to Western Europe, the United States, and Canada over the past year. The scam has been copied and professionalized from initial early attacks, with established online criminal gangs now branching out into the scheme. Each gang has separately developed, or bought, their own different version of the ransomware. This malware is highly profitable, with as many as 2.9 percent of compromised users paying out. An investigation into one of the smaller players in this scam identified 68,000 compromised computers in just one month, which could have resulted in victims being defrauded of up to $400,000 USD. A larger gang, using malware called Reveton (aka Trojan.Ransomlock.G), was detected attempting to infect 500,000 computers over a period of 18 days. Given the number of different gangs operating ransomware scams, a conservative estimate is that over $5 million dollars a year is being extorted from victims. The real number is, however, likely much higher.

Introduction

Ransomware is a category of malicious software which, when run, disables the functionality of a computer in some way. The ransomware program displays a message that demands payment to restore functionality. The malware, in effect, holds the computer ransom. In other words, ransomware is an extortion racket.

Figure 1

Example of a typical ransomware message

The scam has evolved over time, using various techniques to disable a computer. The most recent evolution locks the computer display and does not allow the user to access any programs. The computer then displays a message that claims to be from a branch of local law enforcement. Messages are usually something along the lines of "You have browsed illicit materials and must pay a fine" (as in the preceding Figure 1 example). Law enforcement logos are used to give the message an air of authenticity. A lot of individuals do pay up, either because they believe the messages or because they realize it is a scam but still want to restore access to their computer. Unfortunately, even if a person does pay up, the fraudsters often do not restore functionality. The only reliable way to restore functionality is to remove the malware.

Initially confined to one or two countries in Eastern Europe, the malware has spread throughout Europe and across the Atlantic to the United States and Canada. Criminals will go wherever the money is. From just a few small groups experimenting with this fraud, several organized gangs are now taking this scheme to a professional level and the number of compromised computers has increased. Symantec has identified at least 16

different versions of ransomware. Multiple gangs have retained programmers to develop these different versions independently. In fact, there is not just one single family of ransomware composed of multiple variants, but rather multiple families each with their own unique behavior.

This paper documents an investigation into these different families, describing how multiple gangs are branching out from previous frauds, such as fake antivirus or financial Trojans, and moving into ransomware. It discusses how the criminals launder their money, how much money the scheme may be worth, and how ransomware has become a serious threat.

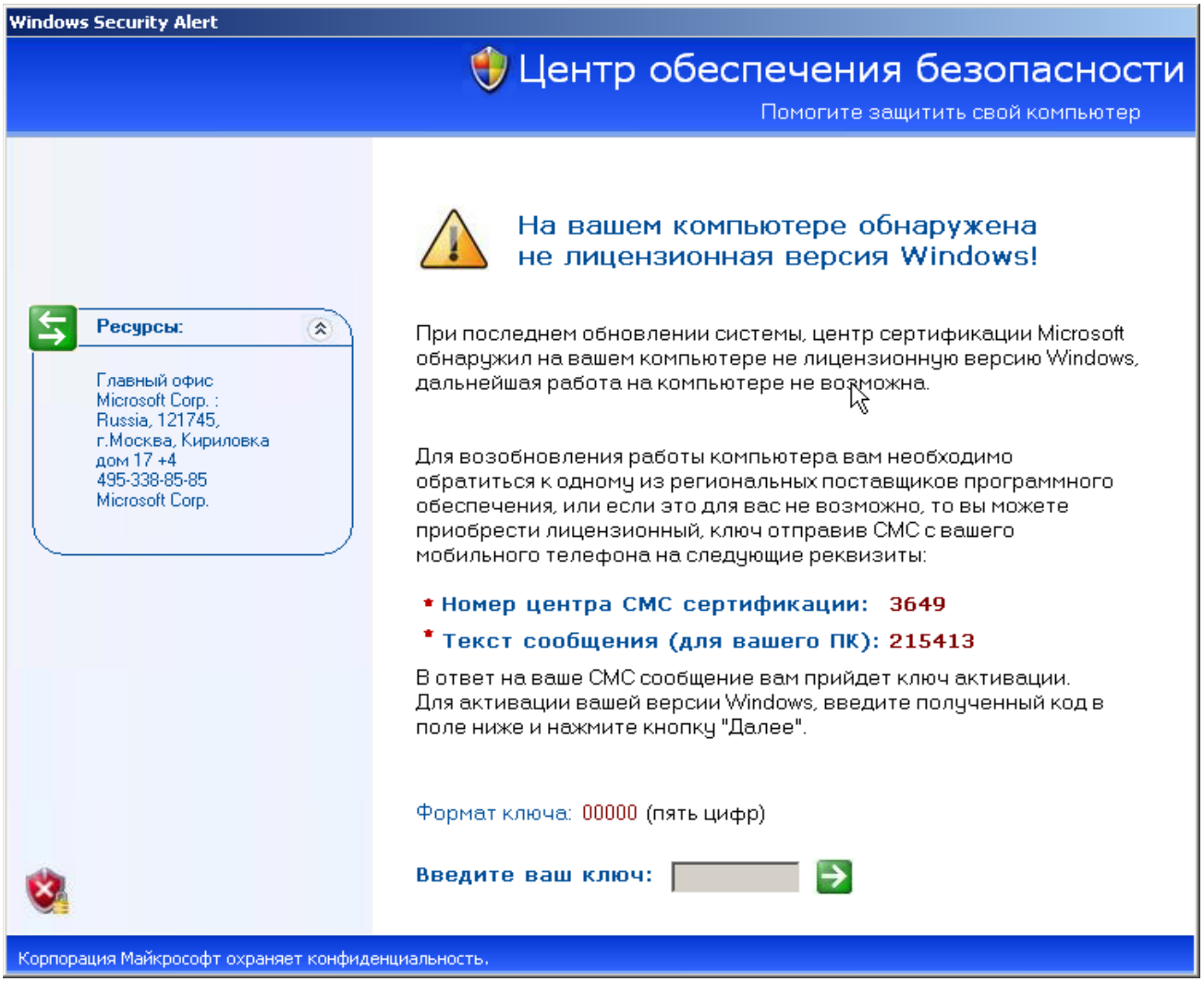
Background

Ransomware which locked a screen and demanded payment was first seen in Russia/Russian speaking countries in 2009. Prior to that, ransomware was encrypting files and demanding payment for the decryption key.

Figure 2 is an example of the message displayed by one of these early variants.

Figure 2

Example of an early Russian based ransomware



In figure 2 the message, which claims to be from Microsoft, states that your computer must be activated before use. To activate, a specific number must be entered. This number is obtained by sending an SMS message to a premium rate number. The circumstance is completely false, however, and has nothing to do with Microsoft.

The next ransomware variant used a different tactic. Instead of claiming to be from Microsoft, the Trojan displayed a pornographic image and demanded payment to have this image removed. Payment could be made through either an SMS text message or regular call to a premium rate number. The idea of shaming victims into payment seems to have been an effective one, as all subsequent ransomware variants used this idea. Again, the messages were written in Russian and the premium rate numbers were Russian numbers. The charge to remove the ransomware could be as high as $460 USD. Throughout 2009 and 2010 there were several variations of this pornographic ransomlock. It was not until early 2011 that a substantial shift occurred in the operation of these Trojans.

In 2011 several major changes occurred. First, instead of using a pornographic image the new image purported to be from law enforcement. The text in the image would claim the computer was locked because a crime was committed and a fine was therefore necessary. The second major change was the language. The ransomware was now targeting German speakers instead of Russian. The scam was moving out of Russia into Europe. Finally, the last major change was the method of payment. No longer was an SMS or phone-based payment required. Abuse of prepaid electronic payment systems began.

Prepaid electronic payment systems allow people to purchase products or services online, without using a credit card. To use them, one purchases a special PIN. That PIN can be bought from local bricks-and-mortar businesses. For example, local convenience stores or corner shops may offer purchase of these payment options. The PINs are sold in fixed denominations such as 10, 20, or 50 currency values. When buying something online a customer can enter a valid PIN as payment if the seller accepts that payment method. A number of different prepaid electronic payment systems are being abused by the fraudsters behind ransomware, but the top three are Paysafecard, Ukash, and Moneypak. These three are the most widely available to consumers. Both Paysafecard and Ukash are predominantly used in Europe, whereas Moneypak is predominantly used in the United States.

The scam

Fake police ransomware can be installed on a computer in a few ways but the most common to date has been through Web exploits and drive-by downloads. Drive-by download is a term used to describe how a piece of malware is installed on a user's computer without their knowledge when that user browses to a compromised website. The download occurs in the background and is invisible to the user.

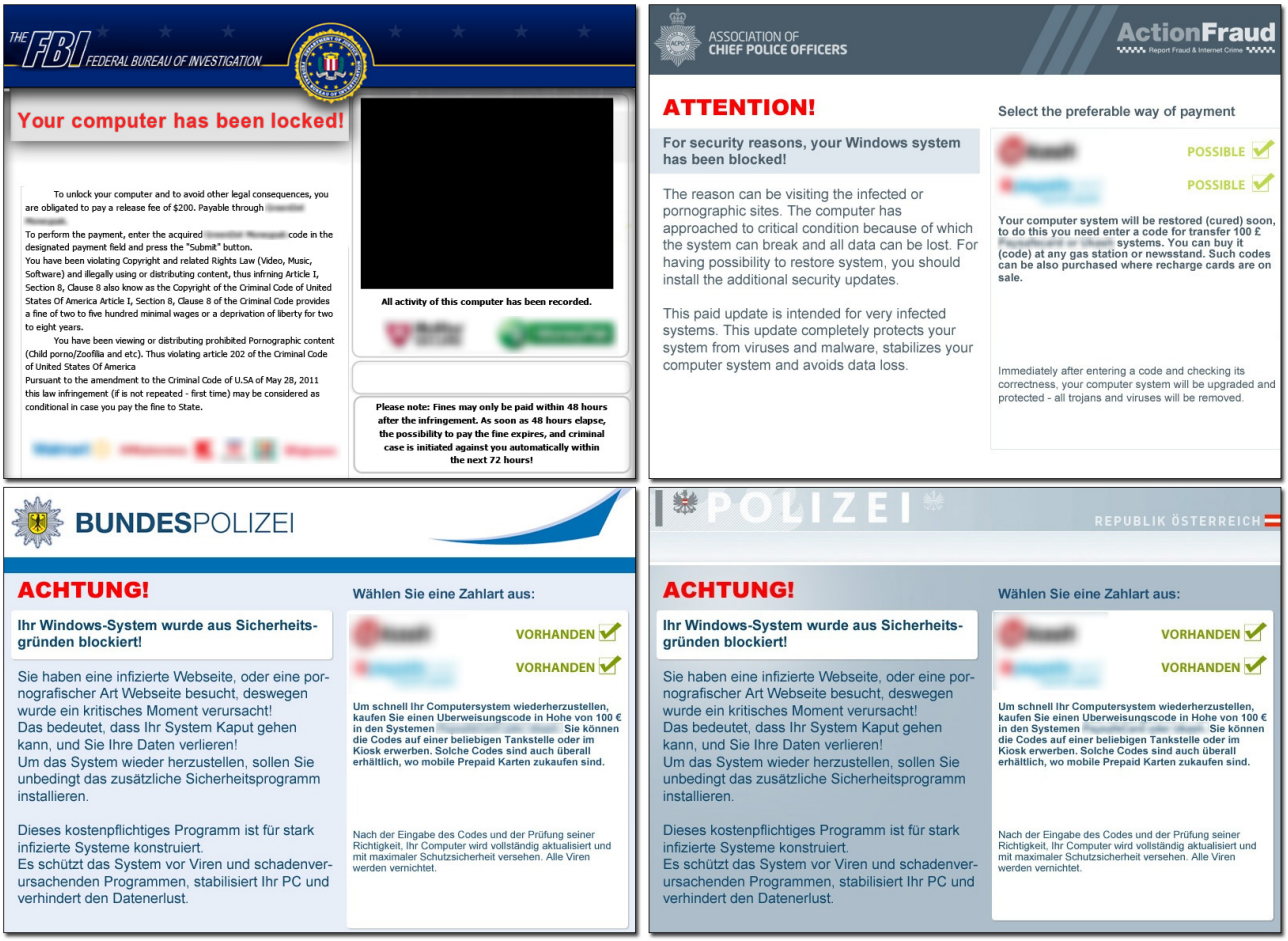
In a typical drive-by download, the user browses to a website (in the case of ransomware, the websites tend to be pornographic in nature). The attacker has inserted a hidden iFrame—a special redirect—into this website. This redirection causes the user's browser to actually connect to a second website containing an exploit pack. Exploit packs contain multiple different exploits, which, if the computer is not fully patched, causes the browser to download a file (the malware).

Injecting an iFrame into the first website is a difficult process. To gain access to the website, the attacker must find a vulnerability in the website. An alternative approach, which the ransomware attackers have been using, is to buy advertising, which is then displayed on the website. The attackers approach an advertising company, which specializes in advertising on pornographic websites, and provide them with a URL to be advertised on its ad network. When clicked, that URL leads to the second website containing the exploit pack. The attackers have to pay for the advertising, but the return on their investment is more than enough to cover the cost. An alternative source for the malware could be through spam email or it may be downloaded by other malware already compromising the user's computer.

After the file has been downloaded, it is executed. The ransomware then proceeds to disable the computer by disallowing execution of various programs. A ransom is then demanded in an appropriate language and using local police images. Localization of content is performed by geo-locating the user's IP address using an online service, which tells the ransomware where the compromised computer is located. Geo-location services are usually not associated with the attackers, but are freely available. Figure 3 shows an example of a single Trojan with several different localized ransomware messages.

Figure 3

Location-specific images for USA, UK, Germany, and Austria (clockwise from top left)



Once the ransomware has determined what country it is in, it sends that data to its command-and-control (C&C) server. This server then responds with the appropriate ransom message written in the local language and with police images from that country.

The message shown in Figure 3 shows demands for payment of either $200 USD or 100 euros within 72 hours, otherwise arrest is threatened. The reason cited for payment is "viewing or distributing prohibited pornographic content".

Because the compromised individual may have indeed been browsing a pornographic website prior to infection, the message carries some more weight. In addition, the nature of the message may be embarrassing to some, encouraging them to get rid of it at any cost. The victim purchases an electronic payment PIN and then enters that number into the box provided.

This payment PIN will then be sent by the ransomware to a C&C server where the attackers can retrieve it. At this point, the attackers should honor their promise and send a command to the ransomware telling it to uninstall itself. Unfortunately, this rarely happens. In actuality, many of the ransomware variants do not even contain the code to uninstall themselves. All the attackers care about is obtaining the payment PIN.

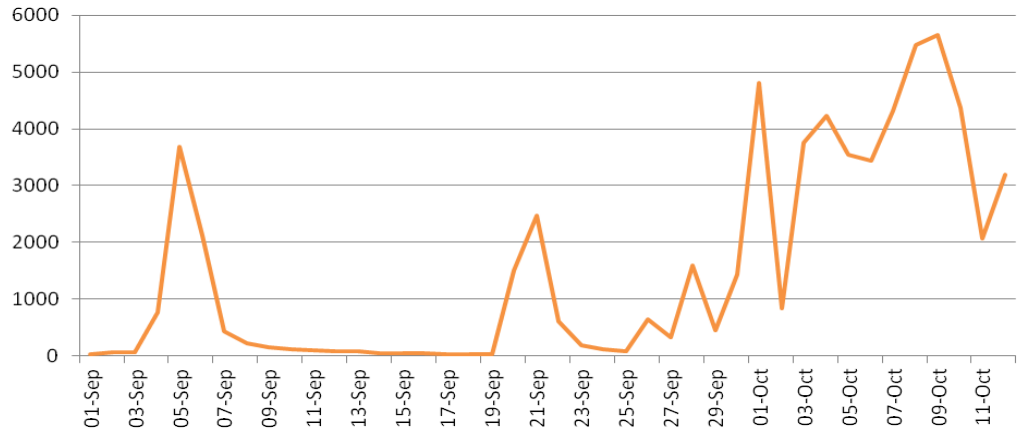
Having obtained the payment PIN, the attackers need to turn it into cash. Several techniques are used to do this including selling the PINs through online trading forums, using the PINs to gamble on websites, and also using the PINs as payment for illicit services such as exploit packs. The most common technique appears to be selling the PINs, at a reduced rate, in exchange for alternative electronic money. This electronic money can be then transferred directly to a standard bank account and withdrawn as cash, potentially anywhere in the world.

Profit

For professional criminals to expand into distribution of ransomware, it must be a profitable exercise. The so-called 'fines' that the fraudsters charge range from €50 to €100 in Europe or up to $200 USD in America. Analysis of the C&C server of a single ransomware family gives some insight into the potential earnings behind the scam.

Figure 4

Compromised computers for a single ransomware family



This particular variant charges $200. Over a period of approximately one month of activity, from September to early October, 68,000 unique infected IP addresses were identified connecting to the C&C server. Figure 4 graphs the total number of infections, as obtained from the C&C server, over time.

It is possible to perform some crude estimates of potential earnings from this scam by examining the data on the C&C server. In one day, 5,700 unique IP addresses were recorded connecting to the C&C servers. Out of those 5,700 connections, 168 people entered what appeared to be a valid PIN in an attempt to unlock their computer. The percentage of people who responded is roughly 2.9. On that day, the criminals may have obtained 33,600 dollars, although they will lose a percentage of that as they attempt to launder it.

Table 1

Estimation of earnings based on C&C server data

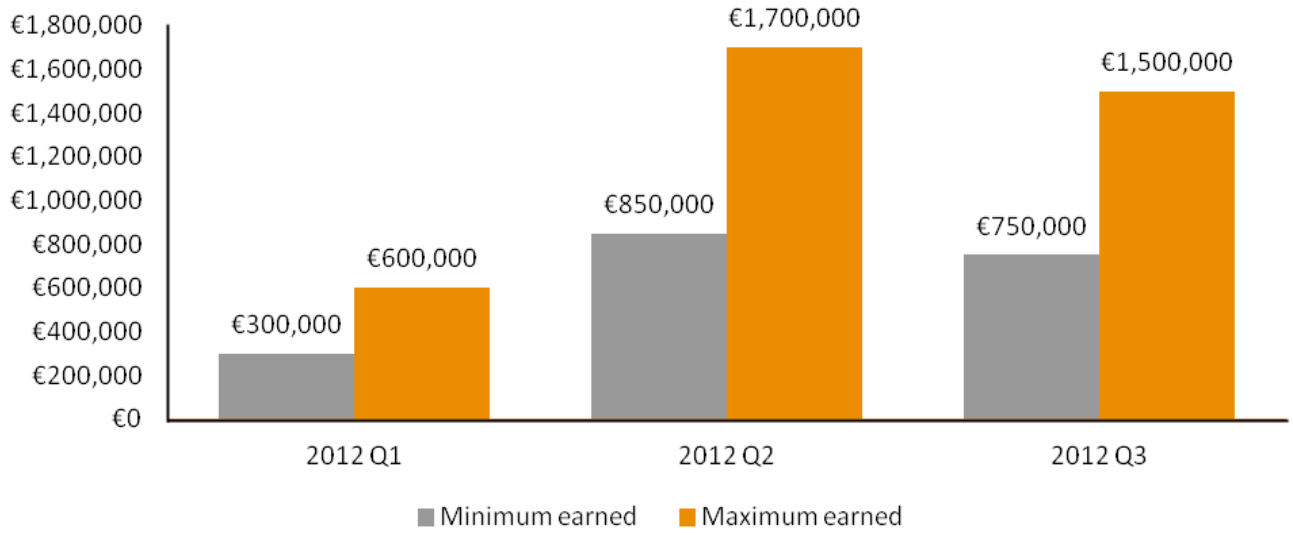
	Compromised computers	Paid up	Percentage	Ransom	Total
Day	5,700	168	2.90%	200	**33,600**
Month (estimated)	68,000	1972	2.90%	200	**394,400**

Extrapolating for 2.9 percent of 68,000 unique infections comes to approximately $394,000 over the one-month duration of this particular variant of the scam. Again, this is the maximum the criminals could earn and they will lose money as they seek to convert the payment PINs into cash.

Separately, estimates provided by a European based financial institution investigating ransomware paint a similar picture of high potential earnings for the criminals (Figure 5).

Figure 5

Estimate of ransomware profits



Considering the number of detections for Trojan.Ransomlock.G (a.k.a. Reveton), this is one of the most serious variants of ransomware with approximately 500,000 detections observed in 18 days, such projected earnings are quite conservative. If the operators behind Trojan.Ransomlock.G are able to purchase an effective zero-day and increase the number of installs, the potential earnings would be far higher.

Increasing problem

Over the past two years, Symantec has identified at least 16 different ransomware variants. That is, 16 different families of malware, the majority of which are developed independently by competing criminal gangs. To be clear, each variant is not merely version 2.0, or 3.0 of the same malware, but completely separate, developed by different people and using different messages. The variants all operate in a similar manner, locking a computer screen and displaying a message purporting to be from a law enforcement agency. Figure 6 is a timeline of those different variants' activity over time.

The earliest variants identified appeared in early July 2011. The last few months have seen an increase in the number of Trojans, up to five in two months.

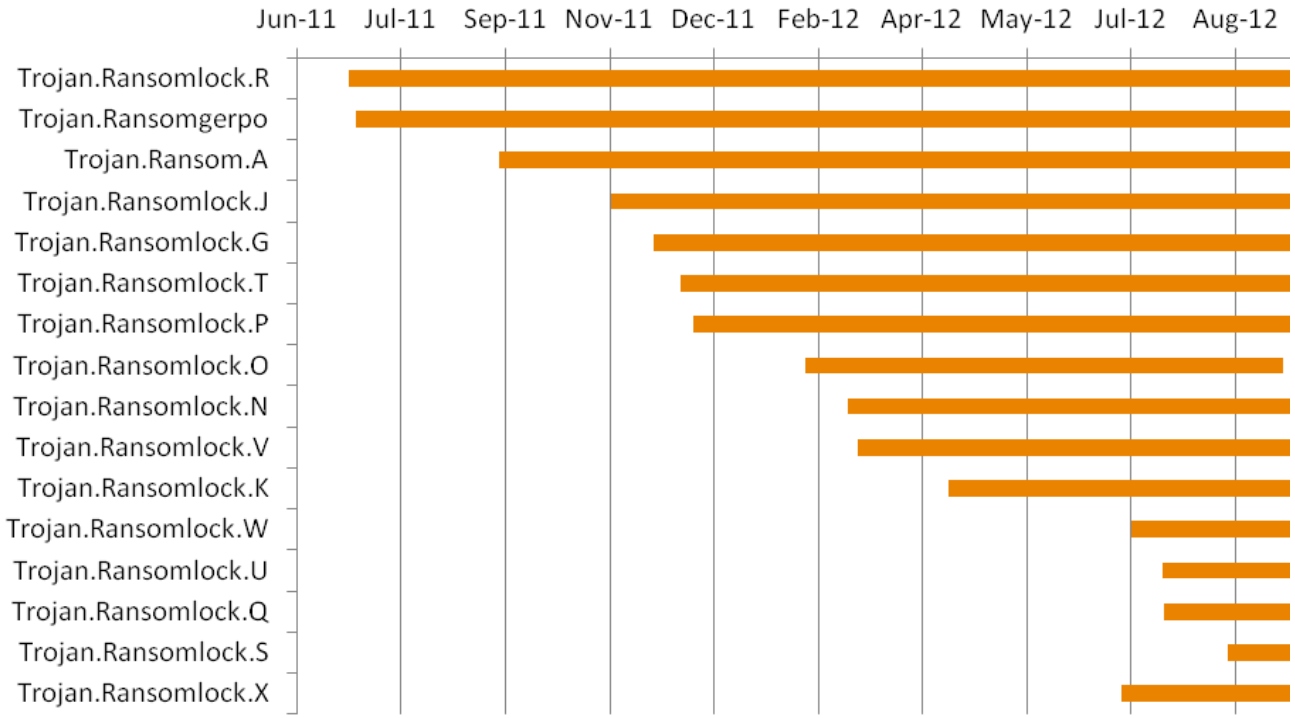
This recent increase in variants may be related to established online criminals branching out into ransomware from other scams. The variants active in early 2011 were quite small in terms of infection size. The fraudsters often distributed the ransomware executables from the same server they used for command-and-control. This server reuse indicates a lack of resources, a small-scale operation. A different model is in use for some of the more recent variants.

Trojan.Ransomlock.P, which became active in December 2011, is closely associated with a banking Trojan called Trojan.Bebloh (a.k.a. URLZone). Both threats primarily target victims in Germany and share the same command-and-control infrastructure. That is, variants of Trojan.Ransomlock.P connect to the same servers as Trojan. Bebloh to retrieve commands. It is highly likely that a single gang, or individual, is responsible for both threats.

Trojan.Bebloh has been active for several years, since at least 2009. The individuals responsible for it are clearly professional criminals, and for them to have expanded into the distribution of ransomware is a sign of the profitability behind the scam.

Figure 6

Ransomware activity over time



There are other signs that ransomware is becoming increasingly professional. Several different ransomware families, sold to what appear to be separate gangs, have all been tracked back to a single individual. That individual, who we have been unable to identify, is seemingly working full-time on programming ransomware on request. This dedicated development of multiple different versions of the same type of malware is reminiscent of how fake antivirus was developed.

Another variant that appears to be using the same techniques associated with fake antivirus is called Trojan.Ransomlock.G (a.k.a. Reveton). This Trojan has been active since at least December 2011. The fraudsters responsible for Trojan.Ransomlock.G use adult advertising networks to distribute ads on pornographic websites that lead back to their exploit pack websites. Considerable investment is made into their infrastructure, with the attackers moving exploit pack websites to new addresses regularly. The amount of advertising is also substantial with at least 500,000 people clicking on their malicious ads over a period of 18 days.

Geographical distribution

Figure 7 and 8 map out ransomware infections in the first and third quarter of 2012, respectively. The primary infections in Q1 are clearly in Germany, France, and the UK. Fewer detections are in Brazil. Q3 shows the progress of the infection, with detections still high in Europe, but also very high in the US. Low detection numbers are also present in significantly more countries.

Figure 7

Ransomware geographical distribution, Jan–Mar 2012

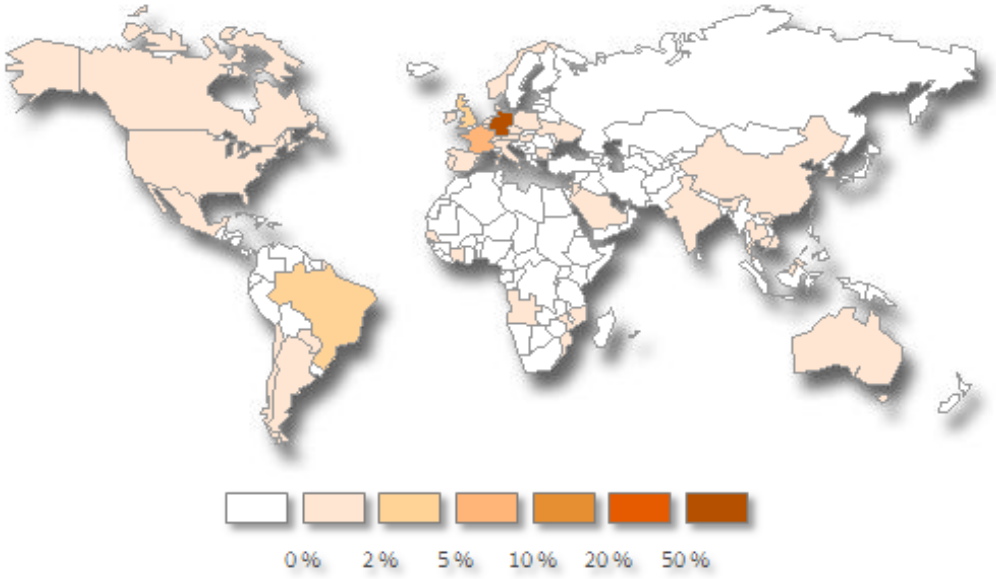
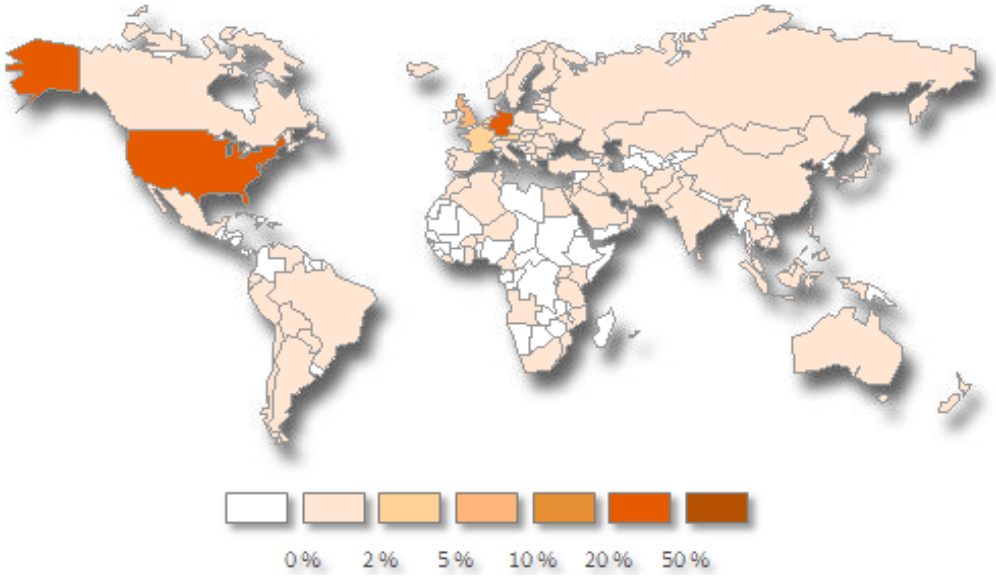


Figure 8

Ransomware geographical distribution, Jul–Sep 2012



Mitigating strategies

As the primary installation vector for ransomware is through advertisements on adult websites, avoid clicking on such advertisements. Ensure that the computer is fully patched with respect to Java, Adobe Flash, Acrobat Reader, Windows, and Internet browsers. If the computer is compromised, it is worth noting that e-commerce payments systems such as Paysafecard, Moneypak, and Ukash are never used by Government or law enforcement as a method of payment for fines. Do not attempt to use them as such.

Conclusion

During the past few years, end users were subjected to misleading applications claiming to be antivirus applications (fake antivirus). Estimates of fraudulent earnings amounted to tens of millions of dollars. While the fake antivirus problem seems to have faded, similar distribution and development techniques are being re-used by ransomware.

From early beginnings in Russian speaking counties, ransomware has evolved and spread into Western Europe, the United States, and Canada. It is likely that some of the gangs responsible for the original ransomware are part of this expansion, but other established criminal gangs are also becoming involved. Clearly, the fraud is profitable for criminals and is likely to increase in size.

It is also possible that ransomware gangs will come into conflict with more traditional malware distributors. Ransomware is a very obvious malware, it is not subtle, or discreet. The presence of ransomware on a computer will usually prompt the computer owner to clean the machine thoroughly, removing any malware from it. As the ransomware may have been installed by a separate piece of malware, that other malware will also be removed, cutting into the malware operator's business model. Malware distribution networks may refuse to distribute such obvious malware, forcing the ransomware gangs to develop their own distribution methods (as some, such as Trojan.Ransomlock.G and Trojan.Ransomlock.P have already done).

As awareness of these scams increases, the attackers and their malware are likely to evolve and use more sophisticated techniques to evade detection and prevent removal. The "ransom letter" will likely also evolve and the attackers will use different hooks to defraud innocent users.

Symantec protection

Many different Symantec protection technologies play a role in defending against this threat, including:

File-based protection (Traditional antivirus)

Traditional antivirus protection is designed to detect and block malicious files and is effective against files associated with this attack.

- Trojan.Ransomgerpo
- Trojan.Ransomlock
- Trojan.Ransomlock!g10
- Trojan.Ransomlock!g11
- Trojan.Ransomlock!g13
- Trojan.Ransomlock!g14
- Trojan.Ransomlock!g15
- Trojan.Ransomlock!g17
- Trojan.Ransomlock!g19
- Trojan.Ransomlock!g7
- Trojan.Ransomlock!g8
- Trojan.Ransomlock!g9
- Trojan.Ransomlock!gen2
- Trojan.Ransomlock!gen3
- Trojan.Ransomlock!gen4
- Trojan.Ransomlock.B
- Trojan.Ransomlock.C
- Trojan.Ransomlock.D
- Trojan.Ransomlock.E
- Trojan.Ransomlock.F
- Trojan.Ransomlock.G
- Trojan.Ransomlock.G!g1
- Trojan.Ransomlock.H
- Trojan.Ransomlock.I
- Trojan.Ransomlock.J
- Trojan.Ransomlock.K
- Trojan.Ransomlock.L
- Trojan.Ransomlock.N
- Trojan.Ransomlock.O
- Trojan.Ransomlock.P
- Trojan.Ransomlock.Q
- Trojan.Ransomlock.R
- Trojan.Ransomlock.S
- Trojan.Ransomlock.T
- Trojan.Ransomlock.U
- Trojan.Ransomlock.V
- Trojan.Ransomlock.W
- Trojan.Ransomlock.X
- Trojan.Ransomlock.Y
- Packed.Generic.388
- Packed.Generic.389

Network-based protection (IPS)

Network-based protection in Symantec Endpoint Protection can help protect against unauthorized network activities conducted by malware threats or intrusion attempts.

- Web Attack: Adobe Acrobat Suspicious Executable Download (23218)
- Web Attack: Malicious Toolkit Website 9 (24089)
- Web Attack: Malicious JAR File Download 6 (25431)
- System Infected: Trojan.Ransomlock.J (25685)
- System Infected: Trojan.Ransomlock.G 2 (25690)
- Web Attack: Malicious JAR Download 3 (25840)
- Web Attack: Blackhole Toolkit Website 20 (25845)
- System Infected: Trojan.Ransomlock.P 2 (25848)
- System Infected: Trojan.Ransomlock.Q 2 (25988)
- System Infected: Ransom Malware Activity 7 (26010)
- System Infected: Trojan.Ransomlock.T 2 (26012)
- System Infected: Trojan.Ransomlock.x (26018)
- System Infected: Trojan.Ransomlock.S (26022)
- System Infected: Trojan.Ransomlock.U (26032)
- System Infected: Trojan.Ransomlock.Q (26066)
- System Infected: Trojan.Ransomlock.Y (26069)
- System Infected: Trojan.Ransomlock.K 2 (26101)
- System Infected: Trojan.Ransomlock.K 4 (26103)
- System Infected: Trojan.Ransomlock.T (26011)
- System Infected: Trojan.Ransomlock.K 4 (26103)
-

Behavior-based protection

Behavior-based detection blocks suspicious processes using the Bloodhound.SONAR series of detections

Reputation-based protection (Insight)

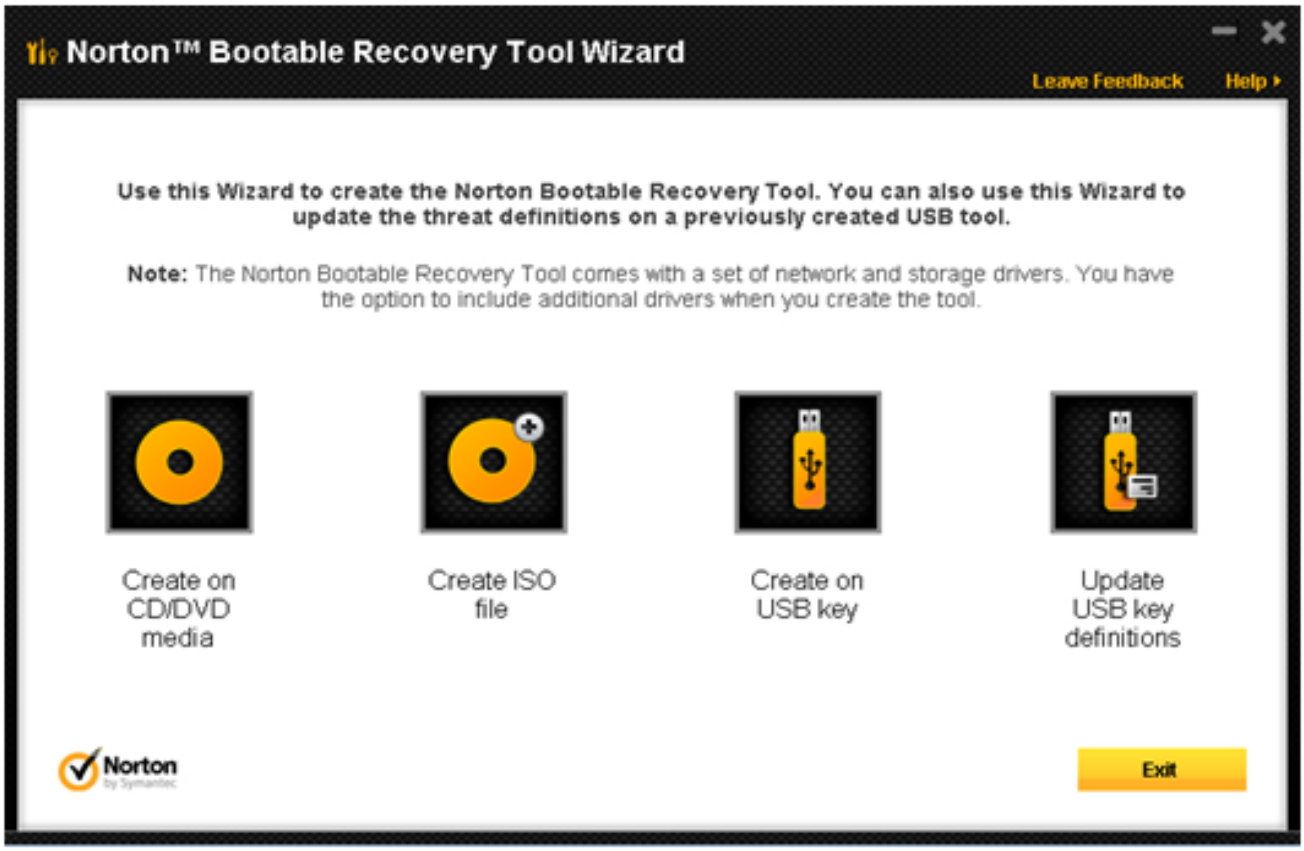
- Norton Safeweb blocks users from visiting infected websites.
- Download Insight detects and warns against suspicious files as WS.Reputation.1

Other protection

Browser Protection can protect against web based attacks which use exploits.

Recovery

Recovery is possible using Norton Power Eraser or Norton Boot Recovery tool.



See http://www.symantec.com/security_response/writeup.jsp?docid=2009-041513-1400-99&tabid=3 for detailed instructions.

Symantec
Security Response

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Mountain View, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

About the authors

Geoff McDonald - Threat Analysis Engineer
Gavin O'Gorman - Sr Threat Intelligence Analyst

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527-8000
www.symantec.com