The Business of Rogueware

Analysis of the New Style of Online Fraud

PandaLabs
Sean-Paul Correll - Luis Corrons
# Executive Summary

# Background: The History of Malware Growth

## Rogueware
- The Effects of Fake Antivirus Programs
- Evolution of Rogue AV from 2008 to Q2 2009, and Predictions for the Future
- Rogue infections in H1 2009
- The Financial Ramifications
- A Look Inside of the Rogueware Business
- The Affiliate System
- Where is it all coming from?
- Rogueware Distribution
- Top 5 Attacks in Social Media

# Conclusion

# The authors
Executive Summary

In recent years, the proliferation of malware has been widespread and the threats have reached staggering proportions. Cybercrime has unfortunately become a part of a hidden framework of our society and behind this growing trend lies a type of malware called rogueware; a breed that is more pervasive and dangerous than threats previously seen by security researchers. Rogueware consists of any kind of fake software solution that attempts to steal money from PC users by luring them into paying to remove nonexistent threats.

At the end of 2008, PandaLabs detected almost 55,000 rogueware samples. This study seeks to investigate the growing rogueware economy, its astounding growth and the effects it has had thus far.

The study revealed staggering results:

- We predict that we will record more than 637,000 new rogueware samples by the end of Q3 2009, a tenfold increase in less than a year
- Approximately 35 million computers are newly infected with rogueware each month (approximately 3.50 percent of all computers)
- Cybercriminals are earning approximately $34 million per month through rogueware attacks
Background: The History of Malware Growth

Malware has rapidly increased in volume and sophistication over in the past several years. The graph below illustrates the malware landscape from 2003 to 2006 over which the total number of malware samples doubled every year:

Barely five years ago, just 92,000 total malware strains existed; by the end of 2008, there were approximately 15 million. At the conclusion of this study in July 2009, PandaLabs detected more than 30 million malware samples in existence.

The reason behind this vast increase in malware is clear: money. In 2003, banking Trojans quietly emerged on the scene. These malicious codes, designed to steal online banking credentials, now rank among the most common forms of malware. Every day, we see new variants that have evolved technologically in order to evade the security measures banks have implemented. Organizations such as the Anti-Phishing Working Group (www.antiphishing.org) have brought industry players together to thwart the efforts of cybercriminals. Still, it's been an upward battle and it remains unclear if it's a battle that can ever be won.
Overall, more Trojans, keyloggers and bots are created than any other type of malicious code because they are the most useful in committing identity theft. Looking back to 2005, almost half the new malicious codes that emerged were Trojans:

Now, in the second quarter of 2009, the situation is far worse and 71 percent of malware are Trojans:

As with any business, cyber-criminals look to operate as efficiently as possible. When developing a Trojan, they must decide what platform it will support and the potential number of individuals they will be to victimize. Windows is consequently targeted in more than 99 percent of cyber-criminal cases, with it being the most widely used platform to date.
The ultimate goal of cyber-criminals is to profit from the malware. While Trojans are adept at stealing information, this stolen information still must be turned into hard cash and cyber-criminals must find innovative methods to accomplish this.

Enter fake antivirus programs. These applications pass themselves off as antivirus products, and claim to detect hundreds of threats on their victims’ computers. When users try to eliminate the threats with the application, they are then asked to purchase a corresponding license. Users, naturally worried about the supposed infection, will often buy the license. Once they have handed over the money, they will no longer hear from the ‘vendors’ and the fake antivirus will remain on their computers.

These applications have been in circulation for several years, but it wasn’t until early 2008 that cybercriminals adopted fake antivirus on a massive scale.
Rogueware

The Effects of Fake Antivirus Programs: Warning Signs of Rogueware

In addition to taking money from consumers and delivering the antithesis of security protection, many fake antivirus programs share a number of commonalities:

- They display fake pop-up warnings, launch messages in the task bar and make changes to the screensaver and desktop
- Their design is similar to that of a real antivirus
- They complete scanning of the entire system very quickly
- The ‘infections’ detected often refer to different files on each scan

Fake antivirus programs also make a series of alterations to the operating system in order to prevent their fake warnings from being removed. This includes hiding the Desktop and Screensaver tabs from the Display properties section. This way, users cannot restore the desktop theme or the screensaver. The purpose of these techniques is to exhaust the users’ patience so that they finally register the product and pay the corresponding fee.

Below is a series of rogueware examples and the respective pay-platforms to which users are directed when they try to ‘disinfect’ their systems:
Cyber-criminals no longer need to steal users’ information in order to make their money; instead, they simply need to find ways to get users to part with their cash voluntarily. As shown above, rogue antivirus programs’ interfaces are carefully crafted and extremely convincing, indicating that cyber-criminals are spending enormous amounts of time and effort developing and distributing these programs. They also employ aggressive techniques, aiming to frighten users into buying the license.
Evolution of Rogue AV from 2008 to Q2 2009, and Predictions for the Future

Fake antivirus is experiencing an exponential growth. In the second quarter of 2008, PandaLabs created a specialized team to detect and eliminate this type of malware. The following graph illustrates the growth of fake antivirus programs over the course of 2008:

The number of samples grew exponentially, and the progression through 2009, as evidenced below demonstrates an even greater growth curve:
In the first quarter of 2009 alone, more new strains were created than in all of 2008. The second quarter painted an even bleaker picture, with the emergence of four times as many samples as in all of 2008. In the third quarter, PandaLabs estimates a malware total greater than the previous eighteen months combined.

The primary reason for the creation of so many variants is to avoid signature-based detection by (legitimate) antivirus programs. The use of behavioral analysis, which works well with worms and Trojans, is of limited use in this type of malware because the programs themselves do not act maliciously on computers, other than displaying false information.

Several methods are being used to create the many variants. One of the most widespread techniques is known as server-side polymorphism, which means every time the fake antivirus is downloaded it is a different binary file.

Although there are approximately 200 different families of rogueware, extrapolating the data from Q2 2009 found that 10 of these families are responsible for 77.47 percent of the variants:
Taking a look at the Top 20 families in the past six months, the number amounts to approximately 90 percent of all malware samples:

<table>
<thead>
<tr>
<th>Fake Antivirus</th>
<th>Number of samples</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>SystemSecurity</td>
<td>70883</td>
<td>18.94%</td>
</tr>
<tr>
<td>SystemGuard2009</td>
<td>38927</td>
<td>10.40%</td>
</tr>
<tr>
<td>Xpantivirus2008</td>
<td>33233</td>
<td>8.88%</td>
</tr>
<tr>
<td>WinPcDefender</td>
<td>32749</td>
<td>8.75%</td>
</tr>
<tr>
<td>Antivirus2009</td>
<td>29666</td>
<td>7.93%</td>
</tr>
<tr>
<td>SpywareGuard2008</td>
<td>24323</td>
<td>6.50%</td>
</tr>
<tr>
<td>XPPolice</td>
<td>20151</td>
<td>5.39%</td>
</tr>
<tr>
<td>AntivirusXPPro</td>
<td>19536</td>
<td>5.22%</td>
</tr>
<tr>
<td>SystemSecurity2009</td>
<td>10265</td>
<td>2.74%</td>
</tr>
<tr>
<td>MSAntiSpyware2009</td>
<td>10191</td>
<td>2.72%</td>
</tr>
<tr>
<td>SecuritySystem</td>
<td>9512</td>
<td>2.54%</td>
</tr>
<tr>
<td>ProAntispysware2009</td>
<td>8628</td>
<td>2.31%</td>
</tr>
<tr>
<td>RogueAntimalware2009</td>
<td>7382</td>
<td>1.97%</td>
</tr>
<tr>
<td>MalwareDefender2009</td>
<td>6120</td>
<td>1.64%</td>
</tr>
<tr>
<td>PCProtectionCenter2008</td>
<td>4949</td>
<td>1.32%</td>
</tr>
<tr>
<td>VirusResponseLab2009</td>
<td>4409</td>
<td>1.18%</td>
</tr>
<tr>
<td>VirusShield2009</td>
<td>4218</td>
<td>1.13%</td>
</tr>
<tr>
<td>WinDefender2009</td>
<td>4038</td>
<td>1.08%</td>
</tr>
<tr>
<td>VirusRemover2008</td>
<td>3242</td>
<td>0.87%</td>
</tr>
<tr>
<td>AdvancedVirusRemover</td>
<td>2931</td>
<td>0.78%</td>
</tr>
</tbody>
</table>
Rogue infections in H1 2009

The number of variants does not necessarily correspond to the proportion of computers infected by fake antivirus programs. To verify exactly how widespread they are, PandaLabs generated infection ratios from its statistics servers and found that from the global infection data for 2009 approximately 98 percent of all computers scanned were infected.

PandaLabs then proceeded to take details from all computers infected by fake antivirus programs and found that 3.50 percent of all the computers scanned each month were infected with this rogueware. As explained earlier, the massive creation of new variants is made to avoid antivirus detection, so the most infectious families do not necessarily have to be the more prolific.

The following chart represents the Top 20 fake antivirus families in the last six months that comprised 81.67 percent of all rogueware related infections detected by PandaLabs. Those highlighted in red are also in the Top 20 with the most samples:

<table>
<thead>
<tr>
<th>Rank</th>
<th>Family Name</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Antivirus2009</td>
<td>15.89%</td>
</tr>
<tr>
<td>2</td>
<td>VirusRemover2008</td>
<td>9.90%</td>
</tr>
<tr>
<td>3</td>
<td>Xpantivirus2008</td>
<td>8.52%</td>
</tr>
<tr>
<td>4</td>
<td>XPAntiSpyware2009</td>
<td>6.13%</td>
</tr>
<tr>
<td>5</td>
<td>SystemGuard2009</td>
<td>5.26%</td>
</tr>
<tr>
<td>6</td>
<td>SpywareRemover2009</td>
<td>4.34%</td>
</tr>
<tr>
<td>7</td>
<td>Antivirus360</td>
<td>3.88%</td>
</tr>
<tr>
<td>8</td>
<td>RealAntivirus</td>
<td>3.57%</td>
</tr>
<tr>
<td>9</td>
<td>RogueAntimalware2008</td>
<td>3.45%</td>
</tr>
<tr>
<td>10</td>
<td>SystemSecurity</td>
<td>3.42%</td>
</tr>
<tr>
<td>11</td>
<td>SpywareGuard2008</td>
<td>2.67%</td>
</tr>
<tr>
<td>12</td>
<td>AntivirusPro2009</td>
<td>2.39%</td>
</tr>
<tr>
<td>13</td>
<td>AntivirusXP2008</td>
<td>2.04%</td>
</tr>
<tr>
<td>14</td>
<td>MSAntiSpyware2009</td>
<td>1.87%</td>
</tr>
<tr>
<td>15</td>
<td>RogueAntimalware2009</td>
<td>1.69%</td>
</tr>
<tr>
<td>16</td>
<td>AntivirusXPPro</td>
<td>1.67%</td>
</tr>
<tr>
<td>17</td>
<td>ProAntispyware2009</td>
<td>1.57%</td>
</tr>
<tr>
<td>18</td>
<td>SecurityCenter</td>
<td>1.38%</td>
</tr>
<tr>
<td>19</td>
<td>AntiMalwareSuite</td>
<td>1.02%</td>
</tr>
<tr>
<td>20</td>
<td>Antispy2008</td>
<td>1.00%</td>
</tr>
</tbody>
</table>
The Financial Ramifications

Given the rapid growth of rogueware and its sole purpose of financial gain, PandaLabs sought to quantify the economic effect of this type of malware on the global economy. Using existing industry estimates, PandaLabs extrapolated information and estimated the following figures to demonstrate the financial consequences of rogueware. According to analyst firm, Forrester Research, there are approximately 1 billion computers worldwide. Based on this figure, PandaLabs estimates that approximately 35 million, or 3.5 percent of all computers, are infected with rogueware each month. We shouldn’t translate this into 35 million people being infected, since there are people that manage a different computer at home and at work. Given this variable, let’s assume half of this amount are actual users: 17,500,000.

Another industry research analyst firm, Gartner Group, has projected that 3.30 percent of people are losing money due to phishing, where victims are sending their banking information to phishers. Rogueware is much more aggressive and deceptive than phishing, and there have been no studies to date that investigate how many people are being fooled into purchasing fake antivirus "software" to eliminate infections that do not actually exist. Since there is no hard evidence available, PandaLabs estimated that based on the Gartner figure of 3.30 percent of users paying for phishing, 557,500 users are buying rogueware each month. It is important to note that the techniques used by rogueware are much more aggressive, so it is likely that Gartner’s forecast is higher.

The price of each rogueware application varies, but in general there are two types of licenses:

- The least expensive is $49.95
- The most expensive is $79.95

Using these figures and assuming that 2/3 of the people will buy the $49.95 option, the average price is $59.95, PandaLabs estimated that cybercriminals are profiting more than $34 million per month from rogueware campaigns.

\[
$59.95 \times 557,000 = $34,621,125 \quad \text{PER MONTH}
\]

$34 million per month translates into more than $415 million in economic loss per year.
A Look Inside of the Rogueware Business

In September of 2008, a hacker going by the handle “NeoN” was able to infiltrate Bakasoftware (a major Rogueware manufacturer) by exploiting SQL injection vulnerabilities on their website. The hacker was able to reveal key information about the way Bakasoftware conducted its business, and for the first time, we were able to see the real damage the Rogueware business was causing.

A six-day sales capture of a top selling affiliate for Baka revealed an $81,388.61 USD earning period, which means that if the sales were sustained over several weeks, the earnings for this one individual would be close to $400,000 USD per month. That’s almost $5,000,000 per year and it’s an astronomical number considering that this projection is just for one of many affiliates in Baka’s roster, not to mention that the rogueware business has grown about four times the size it was in 2008 (in terms of sample volume).
The Business of Rogueware
Analysis of the New Style of Online Fraud

The Affiliate System

The Rogueware business model consists of two major parts: program creators and distributors. The creators are in charge of making the rogue applications, providing the distribution platforms, payment gateways, and other back office services. The affiliates are in charge of distributing the scareware to as many people and as quickly as possible.

The affiliates are mostly comprised of eastern Europeans recruited from underground hacking forums. They earn a variable amount per each install and between 50-90 percent commissions for completed sales. Webmoney seems to be the payment collection method of choice, but Epassporte is used as well. After recruitment, the affiliate provides their payment method of choice and contact details, such as e-mail and ICQ number to stay in contact. Once the affiliate is entered into the system, they are assigned a unique identifier to be appended to the end of each malware distribution domain, which allows for the sales to be tracked. (E.g. http://www.rogueware.com/index.php?aid=1200)

Additionally, PandaLabs was able to uncover sales logs which contained personal data of victims duped by rogueware. Details such as full names, financial data, e-mail addresses, and IP addresses were obtained from the payment gateway servers. It’s obvious that not only do the...
cyber criminals want to take the money generated from the sale, but also generate additional revenues by reselling the extracted data logs from the payments.

Ultimately, these affiliate programs work as a normal business. One of the most known affiliate system is run by KlikVIP, who are giving commissions to anyone installing their rogueware applications, and from time to time they organize parties with their “distributors”. These pictures are from the last party they had in Montenegro, back in March 2008:
Taking a look at the Alexa statistics from KlikVIP for the last three months, we were able to identify the distributors' origin:

Klikvip.com users come from these countries:

- 28.0% Belarus
- 24.9% Russia
- 18.2% Ukraine
- 5.9% United States
- 5.4% Armenia

These distributors usually use a pay-per-install system. Following is a price range from one of the affiliate sites:

<table>
<thead>
<tr>
<th>Region</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>$0.30</td>
</tr>
<tr>
<td>Canada &amp; United Kingdom</td>
<td>$0.10</td>
</tr>
<tr>
<td>Western Europe</td>
<td>$0.03</td>
</tr>
<tr>
<td>Other countries</td>
<td>$0.02</td>
</tr>
</tbody>
</table>
Where is it all coming from?

There is no doubt that the major Rogueware distributors are physically located in Eastern Europe, but another interesting point is the location of the domains, servers, and countries used to distribute the attacks:

**Top 10 Countries**

- Germany: 25%
- United States: 20%
- Canada: 20%
- Czech Republic: 9%
- France: 5%
- Rest of the world: 4%

**Top 10 Domain Registrars**

- Whois.affil.info: 25%
- Todaynic.com: 19%
- Register Ltd.: 17%
- Netdirect: 14%
- Pctisic.net: 7%
- Directi.com: 5%
- Publicdomarine: 5%
- Onlinenic. Inc.: 3%
- Netdirect: 3%

**Top 10 ASN**

- America (ThePlanet): 29%
- Netdirect: 15%
- Vipcom: 11%
- Nettelenet: 9%
- China Telecom: 7%
- China Netcom: 5%
- China Netcom: 4%
- China Netcom: 4%
- China Netcom: 4%
Rogueware Distribution

The highly lucrative nature of the rogueware business fuelled a firestorm of distribution efforts in the latter part of 2008 and throughout 2009. For the first time social media sites, such as Facebook, MySpace, Twitter, and Digg, became large targets for distributors. But despite the plunge into social media, the single largest distribution effort came in the form of a Blackhat SEO attack in April 2009 against the Ford Motor Company. Over three million search terms were hijacked, which turned almost any top search result for Ford cars, parts, or services into rogueware distribution sites. After Ford acknowledged the situation publically, the cyber criminals quickly moved the targeted search campaigns to Nissan and Volkswagen.
Top 5 Attacks in Social Media

Following are the top five rogueware attacks in social media.

1. **SEO attack against Ford Motor Company**

   ![SEO attack against Ford Motor Company](image)

   **The Attack:**
   - 1,000,000 malicious links indexed by Google
   - 3,000,000 legitimate search terms hijacked
   - Targeted users looking for instructions (E.g. How to loosen a tension belt)
   - Served 100 new MSAntiSpyware2009 binaries in 24 hours
2. **Comments on Digg.com leading to Rogueware**

- 500,000+ comments leading to Rogueware
- Comments targeted news submission title and content

3. **Twitter trending topics lead to Rogueware**

- Messages (tweets) targeting trending topics on Twitter.com
- 27,000 tweets per 24 hours
- 60 unique samples detected over 72 hour period
4. **Rogueware exploits Wordpress vulnerability to facilitate Blackhat SEO attack**

The Attack:

- Affected Ned.org and TheWorkBuzz.com
- Targeted a security vulnerability in an old version of Wordpress
- Redirected all links to point to Rogueware servers
- Facilitated a Blackhat SEO attack against 13,000 search terms
5. **Koobface moves to Twitter**

The Attack:

- Messages (tweets) pointing to 20 Rogueware sites.
- The worm further propagated on Twitter upon infection
- Malicious site presented a realistic looking Flash update popup
Conclusion

As we have demonstrated throughout this report, the rogueware situation is very serious and growing as cybercriminals continue to create new methods for developing and distributing malware. It is a very lucrative business for the cybercriminals, so the name of the game is to infect as many people as possible. As a result, social networks have proven to be an effective channel to infect users. Based on PandaLabs’ extensive research, the situation is most likely to escalate even further.

Furthermore, cybercriminals know how to avoid antivirus detection; on one hand, most of them don’t show suspicious behaviors, so antivirus companies have to focus on signatures (specific or generic) to deal with those programs. This is the main reason why cyber criminals are creating so many new samples. On the other hand, PandaLabs has started to identify more advanced malware variants that are using typical Trojan features, as well as Rootkits and other techniques to subvert virus protection technologies.

For many years consumers and businesses alike have been faced with new threats, ranging from viruses and spam to phishing. In order to fight the war against cybercrime, grassroots awareness, advocacy and individual user education will continue to be important. Antivirus companies must play a fundamental role in exposing the problem in near real-time and presenting solutions along the way.

Finally, antivirus companies must admit that the industry is not even close to winning this battle. This is precisely why Panda started to develop Cloud based technologies in 2006. The company needed to be able to quickly analyze every new sample against its 20 years of accumulated malware data in real time to deliver protection in minutes instead of days. Fortunately, other vendors are now following this trend, but cybercriminals will soon look to new channels for malware monetization.
Authors

Sean-Paul Correll
Sean-Paul started at Panda Security back in 2005 in our technical support area. Since that time, he has worn many hats throughout the organization all while staying true to his true passion--Security. He specializes in threat surveillance with an emphasis on emerging threats. He is an active member of the security community and frequently volunteers his time to helping individuals with malware infections.

Luis Corrons
Luis has been working for Panda Security since 1999. He started in the technical support department, helping home and corporate users with virus incidents. A year later, he joined the international technical support team assisting Panda's technical support belonging to their partners distributed over 50 countries around the world. In 2002, he became PandaLabs' director as well as malware alerts coordinator in worldwide infection situations, dealing with worm such as Klez, SQLSlammer, Sobig, Blaster, Sasser, Mydoom, etc. During this time, he has coordinated several automated projects related with malware, such as the automatic analysis and response system, and the malware automatic information system.

His first contact with computers was at the age of 4, with a Sharp MZ-80K, which he started Basic language programming with. His main hobbies are his wife Nerea, his dog Robin and his work as well as chess and videogames.