# Inside a ‘Reveton’ Ransomware Operation

krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/

The **U.S Federal Bureau of Investigation** is warning about an uptick in online extortion scams that impersonate the FBI and frighten people into paying fines to avoid prosecution for supposedly downloading child pornography and pirated content. This post offers an inside look at one malware gang responsible for orchestrating such scams.

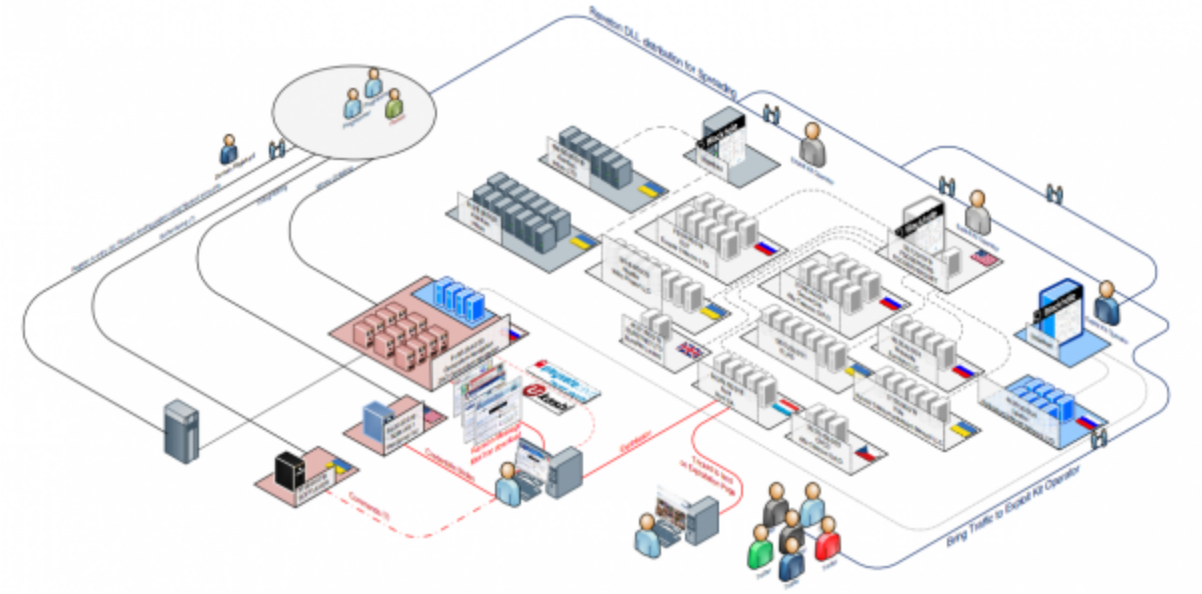
In an alert published last week, the FBI said that The Internet Crime Complaint Center — a partnership between the FBI and the National White Collar Crime Center — was “getting inundated with complaints” from consumers targeted or victimized by the scam, which uses drive-by downloads to hijack host machines. The downloaded malware displays a threatening message (see image to the right) and blocks the user from doing anything else unless he pays the fine or finds a way to remove the program.

Reveton ransomware scam page impersonating the FBI

The FBI alert said the attacks have surged with the help of a “new drive-by virus” called **Reveton**; in fact, Reveton and its ilk are hardly new. These types of attacks have been around for years, but traditionally have targeted European users. The scam pages used in the attacks mimic official notices from various national police or investigatory agencies, corresponding to the country in which the victim resides. For a breakdown of these Reveton-related ransomware scam pages by country, see this comprehensive gallery set up at botnets.fr.

Reveton.A is blamed in these most recent attacks, and the FBI said it appears Reveton is being distributed in conjunction with **Citadel**, an offshoot of the ZeuS Trojan that I have written about on several occasions. It is certainly possible that crooks are using Citadel to deploy Reveton, but as I’ll illustrate below, it seems more likely that the attackers in these cases are using exploit kits like **BlackHole** to plant both threats on victim PCs.

INSIDE A REVETON MALWARE GANG



Operations of one Reveton crime group. Source: 'Kafeine,' from botnets.fr.

At least that's the behavior that's been observed by a ragtag group of researchers that has been tracking Reveton activity for many months. Some of the researchers are associated with botnets.fr, but they've asked to remain nameless because of the sensitivity of their work. One of them, who goes by the screen name "Kafeine," said much of the Reveton activity traces back to a group that is controlling the operation using reverse proxies at dozens of servers scattered across data centers globally (see this PDF for a more detailed look at the image above).

Kafeine said the groups involved in spreading Reveton are constantly fine-tuning all aspects of their operations, from the scam pages to solidifying their back-end hosting infrastructure. The latest versions of Reveton, for example, serve the scam pages from an encrypted (https://) connection, and only cough up the pages when an infected machine visits and sends a special request.

Some readers may have a hard time understanding how such schemes could be successful. To those folks, I say consider the lucrative operations of the once-mighty scareware industry, which similarly hijacks infected machines with warnings about malware until the victim relents and pays for some worthless and fake cleaner program.

Kafeine shared a couple of screen shots of two similar and recent ransomware scams (not Reveton-related) targeting European users that shows just how successful these scams can be. Both of these images were obtained when security researchers stumbled upon statistics pages maintained by the criminal groups running the scheme.

The one on the right, for instance, shows that the attackers managed to get their malware installed on 2,116 PCs in France, and of those, only 3.7 percent — 79 victims — opted to pay to rid their machines of the ransomware. But those 79 victims each paid $100, earning the miscreants 7,800 Euros.

That's the haul from just one country; bear in mind that this stats page shows the total take from a single day (May 17, 2012). According to these stats, at least 322 people from all countries they ran the scam in opted to pay the ransom that day, earning the attackers more than €28,000 (~$34,500)! The next day (the screen shot below left), the miscreants earned €43,750 (~$54,000).

| # | COUNTRY | INSTALLS | PINS | AMOUNT | CONVERSION |
|---|---|---|---|---|---|
| 1 | Unknown Country (-1) | | | | 0% |
| 2 | Austria (14) | 375 | 11 | 900 | 2.4% |
| 3 | Sweden (221) | 735 | 45 | 2650 | 3.61% |
| 4 | France (84) | 2116 | 79 | 7880 | 3.69% |
| 5 | Italy (118) | 263 | 1 | 100 | 0.38% |
| 6 | Portugal (193) | 151 | 1 | 100 | 0.66% |
| 7 | Spain (217) | 655 | 11 | 1050 | 1.6% |
| 8 | Poland (191) | 187 | 4 | 400 | 2.14% |
| 9 | Netherlands (176) | 1021 | 45 | 4300 | 4.21% |
| 10 | Finland (77) | 1 | | | 0% |
| 11 | Belgium (21) | 400 | 6 | 600 | 1.5% |
| 12 | Germany (94) | 3797 | 119 | 10200 | 2.69% |
| Total | | 9701 | 322 | 28100 | 2.9% |

Ransomware earnings on 5/17/2012

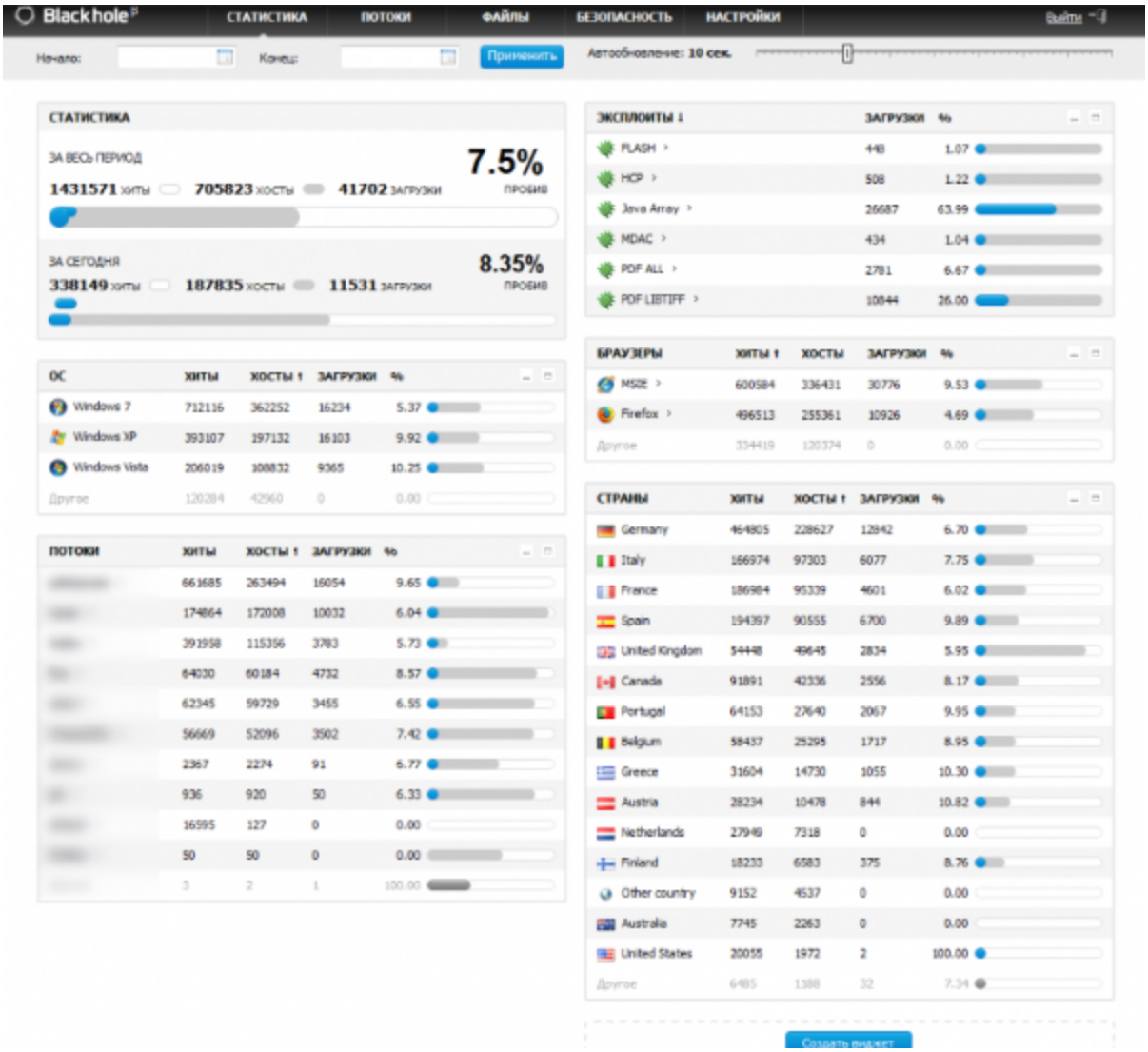
| # | COUNTRY | INSTALLS | PINS | AMOUNT | CONVERSION |
|---|---|---|---|---|---|
| 1 | Austria (34) | 529 | 13 | 1100 | 2.08% |
| 2 | Sweden (221) | 1066 | 87 | 5400 | 5.07% |
| 3 | France (84) | 2998 | 113 | 11200 | 3.74% |
| 4 | Italy (118) | 272 | 1 | 100 | 0.37% |
| 5 | Portugal (193) | 283 | 1 | 100 | 0.35% |
| 6 | Spain (217) | 1684 | 26 | 2450 | 1.53% |
| 7 | Poland (191) | 1462 | 16 | 1600 | 1.09% |
| 8 | Netherlands (176) | 1427 | 72 | 6650 | 4.66% |
| 9 | Finland (77) | 1 | | | 0% |
| 10 | Belgium (21) | 401 | 7 | 700 | 1.75% |
| 11 | Germany (94) | 5376 | 167 | 14450 | 2.69% |
| Total | | 15419 | 503 | 43750 | 2.84% |

Ransomware earnings 5/18/2012

Unlike scareware scams, ransomware schemes do not rely on credit card payments from victims — a key pressure point for squashing affiliate programs that help spread this crud. Most previous ransomware schemes have used alternative payment systems such as Ukash and Paysafe. The Reveton attacks that spoof the FBI instruct victims to pay their "fines" via MoneyPak, which allows people who don't have bank accounts to send money and pay bills at participating businesses. MoneyPak cards are available for purchase at Wal-Mart, CVS and other retailers, and can be reloaded with cash, and can be used to send money to **PayPal** accounts, prepaid credit cards, and to pay bills for some cell phone companies and **DirectTV**.

I mentioned earlier that most of these Reveton attacks that have been tracked so far used versions of the BlackHole exploit kit to deploy the malware. These are kits that are stitched into hacked or malicious Web sites, so that all visiting browsers are checked for a variety of insecure, outdated plugins, from **Flash** to **Java** to **Adobe Reader**. Browsers that are found vulnerable will be handed a Trojan downloader that fetches Reveton and most likely a copy of the password-stealing Citadel/ZeuS Trojan.

Kafeine and his fellow researchers recently gained access to one of the three main BlackHole exploit panels used by a Reveton malware gang. The screen shot below shows the BlackHole administration page; in the upper left portion of the image, we get a sense of how much traffic these crooks see on any given day. It shows that in just one day, the exploit kit was sent more than 187,000 potential victims, and that more than 11,000 of those were successfully seeded with Reveton. The "exploits" stats in the upper right portion of the image show that, once again, insecure and outdated installations of **Java** remain by far the most popular vehicle for exploiting PCs.




A recent screenshot of a BlackHole exploit kit panel used by a group spreading Reveton. Source: Kafeine from botnets.fr

A number of Web sites include instructions for removing the Reveton malware without having to pay the ransom (here's one example). But it's important for readers to understand that if you have been hit by a ransomware attack, the ransomware component is almost certainly just the most visible of the threats that reside on your system. For one thing, Kafeine said, the latest Reveton versions will steal all passwords stored on the victim's PC. What's more, the FBI's report indicates Reveton is being bundled with Citadel, which is an extremely powerful and advanced family of malware that can be quite difficult to remove.

Attacks such as Reveton illustrate the need to have a solid plan for backing up your data, because the surest way to clean a machine infected with the likes of Reveton is to completely reinstall Windows (from the Master Boot Record on up). The most advanced ransomware threats (the subject of a future post) will steal your passwords and then encrypt all of your important files before demanding a ransom payment.