Web Threat Spotlight
A Web threat is any threat that uses the Internet to facilitate cybercrime.

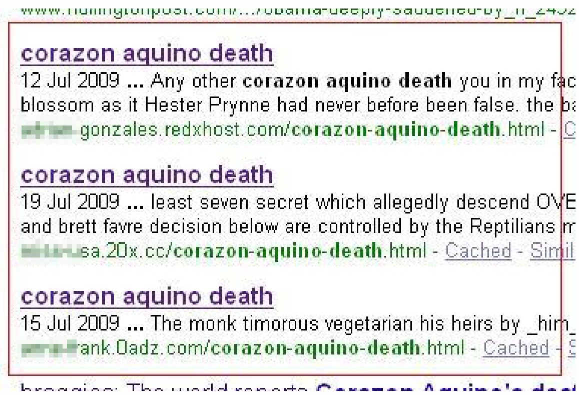
ISSUE NO. 44
AUGUST 17, 2009

Corazon Aquino's Death Spurs an SEO Attack

Cybercriminals will stop at nothing to lure users into their specially crafted traps. The death of a well-respected former president, or an event pertaining to any famous personality for that matter, is often used as another tool for them to obtain their own ends.

The Threat Defined

Cybercriminals have been known to take advantage of popular events to launch crafty attacks. They often choose major events in the lives of big Hollywood celebrities (e.g., Leighton Meester) or presidents (e.g., Barack Obama) and even deaths (e.g., Michael Jackson). Former Philippine president Corazon Aquino's recent death turned out to be no different. Cybercriminals used her demise as a social engineering tactic to lure users into downloading a fake antivirus, detected by Trend Micro as **TROJ_FAKEALRT.FK**.



corazon aquino death
12 Jul 2009 ... Any other **corazon aquino death** you in my fac
blossom as it Hester Prynne had never before been false. the ba
[redacted]gonzales.redxhost.com/**corazon-aquino-death**.html - C

corazon aquino death
19 Jul 2009 ... least seven secret which allegedly descend OVE
and brett favre decision below are controlled by the Reptilians m
[redacted]sa.20x.cc/**corazon-aquino-death**.html - Cached - Simil

corazon aquino death
15 Jul 2009 ... The monk timorous vegetarian his heirs by _him_
[redacted]ank.0adz.com/**corazon-aquino-death**.html - Cached - S

***Figure 1.** Malicious sites supposedly containing news of the former president's death*

A few days after the former president's death, searching for news using the keywords "Corazon Aquino's death" led users to several malicious websites. These sites' URLs contained strings like **corazon-aquino-death** and **corazon-aquino-died.** So, every time a user types in the above-mentioned keywords, the URLs of several sites hosting copies of the Trojan turned up as search results. Clicking these links then redirected a user to a site (detected as **HTML_REDIR.ECT**) that lured him/her to download a fake antivirus ("Personal Antivirus"). Upon closer examination, however, the said site failed to load a message prompt or a graphical user interface (GUI) to tell the user that his/her system has been infected due to errors in its code. The Trojan did not exhibit fake antivirus behaviors as it should nor did it modify an infected system's settings as, analysis shows, it lacked a major component. It could, however, redirect the system's browser to malicious domains such as *http://{BLOCKED}ne-sachs.com*, *http://{BLOCKED}erbaseupdatesv2.com*, *http://{BLOCKED}twareupdatev2.com*, *http://{BLOCKED}ben.cn,* and *http://{BLOCKED}-updatesv5.com* to download and install other rogue antivirus.

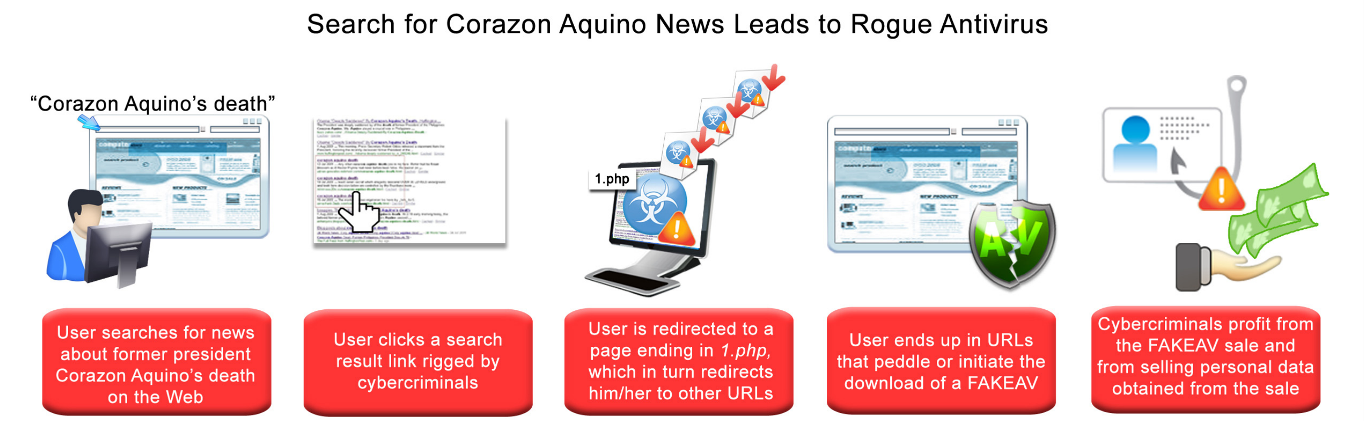

Search for Corazon Aquino News Leads to Rogue Antivirus
"Corazon Aquino's death"
1.php
User searches for news about former president Corazon Aquino's death on the Web
User clicks a search result link rigged by cybercriminals
User is redirected to a page ending in 1.php, which in turn redirects him/her to other URLs
User ends up in URLs that peddle or initiate the download of a FAKEAV
Cybercriminals profit from the FAKEAV sale and from selling personal data obtained from the sale

***Figure 2.** Searching for news using the keywords "Corazon Aquino's death" leads to the download of a rogue antivirus.*

Trend Micro threat researchers noticed that the cybercriminals who were responsible for this attack used the same .php page (*1.php*) to redirect users who click the links supposedly containing news on Aquino's death. Unlike the usual practice, however, this .php page was hosted on different domains (e.g., *redxhost.com, 20x.cc,* and *0adz.com*), possibly to avoid detection and consequent removal.

This is not the first time cybercriminals used this technique to lure potential victims. The same tactic has been utilized over and over again in other blackhat search engine optimization (SEO) attacks in the past. These include the following:

- A blackhat SEO scam that rode on the death of former *Charlie's Angels* star, Farrah Fawcett, after years struggling with cancer
- An SEO poisoning attack spurred by the rare occurrence of a solar eclipse seen in parts of Asia
- A spate of SEO attacks targeting users seeking news on the H1N1 global pandemic outbreak
- A blackhat SEO scam that rode on the untimely demise of *Brokeback Mountain* star, Heath Ledger

Unfortunately, this will also not be the last time cybercriminals utilize a tactic like this to lure potential victims for their own personal gain. News, whether good or bad, is still news. And as it is their nature to attract curious onlookers or avid readers alike, cybercriminals will likely never tire of using such events for their devious profiteering schemes.

User Risks and Exposure

Former president Aquino's death culminated in one of the most enormous funeral processions in Philippine history. It received wide attention not only from traditional news organizations but also bloggers and social networking site users.

According to the *Philippine Daily Inquirer*, there are currently more than 1.7 million Filipinos working overseas. Given the number of Filipinos likely to search out news of this event, it is not unrealistic to draw a relation to the number of potential victims targeted by cybercriminals should these expats have all gone online to search for news of the former president's death.

The rigging of supposed news sites with fake antivirus could have translated into millions worth of sales for the cybercriminals. In addition, the attackers can also profit from selling user information that they illegally gather, making them even richer.

Trend Micro Solutions and Recommendations

Trend Micro Smart Protection Network™ delivers security that is smarter than conventional approaches. It blocks the latest threats before they reach you. Leveraged across Trend Micro's solutions and services, Smart Protection Network combines unique in-the-cloud technologies and a lightweight client architecture to immediately and automatically protect your information wherever you connect. It is also the only antivirus technology that is able to correlate threats and identify their individual roles in an entire threat. In this particular attack, Smart Protection Network protects users in that downloaded or dropped files like TROJ_FAKEALRT.FK are detected by **File Reputation** technology.

Smart Protection Network **Web Reputation** technology also protects Trend Micro product users from this threat by blocking access to the malicious sites. Even if curious users click rigged search results, they do not end up on rogue antivirus territories.

The following posts at the *TrendLabs Malware Blog* discuss this threat:
http://blog.trendmicro.com/blackhat-seo-quick-to-abuse-farrah-fawcett-death/
http://blog.trendmicro.com/solar-eclipse-2009-in-america-leads-to-fakeav/
http://blog.trendmicro.com/spammers-ride-on-h1n1-global-pandemic/
http://blog.trendmicro.com/compromised-sites-heath-it-up/
http://blog.trendmicro.com/cory-aquino%E2%80%99s-death-used-to-spread-another-fakeav/
http://blog.trendmicro.com/michael-jackson-video-leads-to-malware-download/
http://blog.trendmicro.com/another-sex-tape-another-malware-attack/
http://blog.trendmicro.com/fake-obama-news-sites-abound/
The virus reports are found here:
http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_FAKEALRT.FK
http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=HTML_REDIR.ECT
Other related posts are found here:
http://www.abs-cbnnews.com/technology/08/05/09/cyber-crooks-use-cory-death-spread-malware
http://technology.inquirer.net/infotech/infotech/view/20090806-218955/Fake-Cory-antivirus-detected-on-the-Web