Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

EVEN GOVERNMENTS ARE NOT IMMUNE TO HACKTIVISM

Governments—both online and offline—should represent a sense of authority and security. What would happen then if these so-called bodies of power fall prey to cybercriminals and their malicious activities? In the previous month alone, the websites of high-profile political figures and organizations from around the world were hacked, which raised an important question, "If government websites are not spared from such attacks, who then is safe from hacktivism or cybervandalism?"

A Hacker's Favorite Target

Over the years, news about website defacement and hacking of varying degrees of notoriety have consistently been cropping up. Despite variations in the techniques cybercriminals use and in the messages they leave behind, one thing remains constant—that government websites are always among their top targets.

Hacktivism or cybervandalism refers to the various malicious techniques cybercriminals use to infiltrate sites or to gain access to the classified information they contain.

Hacktivism or cybervandalism has been around for over a decade now and yet old tricks still continue to create disruptions online. Utilizing cross site scripting (XSS) or Structured Query Language (SQL) injection, among other techniques, cybercriminals successfully infiltrate websites and, in some cases, even gain access to classified information. To date, these hacking methods have led to thousands of security breaches worldwide.

Hacktivism in History

In recent years, Trend Micro has encountered a number of noteworthy hacktivism-related incidents, one of the most notable of which was when the Supreme Court of Nepal's website was compromised. Cybercriminals turned its home page into a pornographic video host with 157 embedded links to more adult sites. The supposed distributed denial-of-service (DDoS) attacks were executed in conjunction with the street protests that occurred after the Iran presidential elections. The event rendered several Iranian websites inaccessible for a certain period of time. We have since seen similar occurrences. And if January is any indication of what 2010 has in store for us, then this year may be no different.

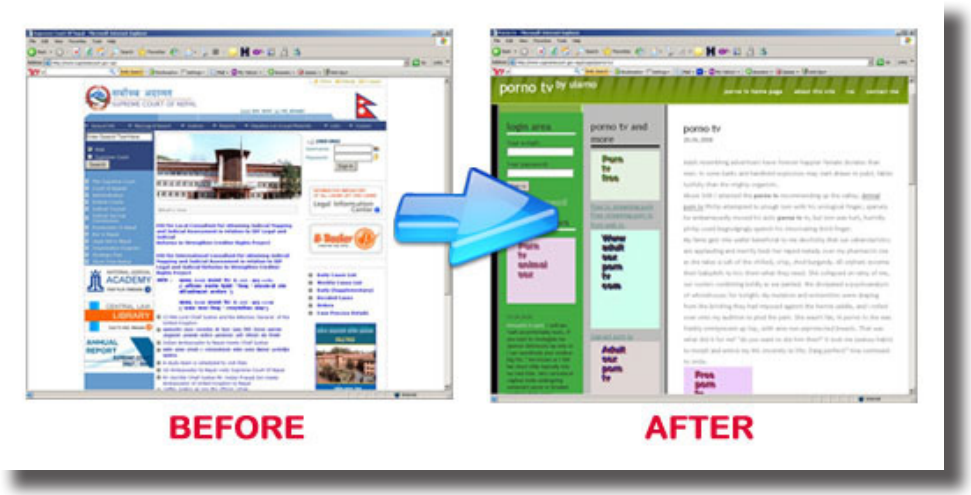


Figure 1. *Supreme Court of Nepal's site before and after the hactivism attack*

TREND MICRO

Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

Last month, we witnessed several hacktivism-related incidents, including attacks targeting the Spanish government, the Pakistani National Response Centre for Cyber Crimes, the U.S. Army, and, more recently, 49 U.S. Congressional Members and Committees. It is thus quite alarming that instead of learning from past experience, government websites remain vulnerable to malicious attacks. Even worse, the number of similar attacks continue to rise.

Need for Tighter Security

A recent *Network World* article states that 80 percent of U.S. federal agencies failed to meet the December 31, 2009 deadline designed to improve their current security efforts. The plan to deploy DNS Security Extensions (DNSSEC) in several federal agencies would have been a significant move toward tightening the U.S. government's online security. Unfortunately, however, the missed deadline only supports the findings of the "Database State Report," which claims that a quarter of all U.S. public-sector database projects have privacy flaws. While the numbers were met with criticism, it cannot be denied that the study highlights a critical truth—that there is a huge need to improve government websites' security. As *BusinessWeek* asked, why is the government vulnerable to a simple cyber attack? The answer could perhaps be found within the websites themselves.

While it cannot be denied that government sites are among the top cybervandalism targets, this does not mean that there is no way for them to avoid being hacked or defaced. On the contrary, knowing that government websites are especially vulnerable should trigger the use of better-protected servers, regular patching, and the implementation of more stringent security measures. Unfortunately, this is not always the case, as shown by the continuous proliferation of politically motivated online attacks.

Hacktivism in Today's Threat Landscape

Despite the messages cybercriminals leave on compromised websites that often explain their political stands or to stake their claim, one can only guess their true motives. Trying to understand their reasons may be helpful but it will be more efficient to spend more time trying to better understand the technologies behind these mishaps.

Cybercriminals use a variety of techniques to carry out their malicious activities. XSS primarily involves attacking a website at the browser level. This is usually done by injecting code, often obfuscated JavaScript, into websites with XSS holes or vulnerabilities. In doing so, they are able to insert images and/or text into the compromised sites or to redirect users to malicious URLs.

An SQL injection is similar to an XSS attack in the sense that code injection occurs in both. The main difference is that an SQL injection attack directly targets the database. This practically gives cybercriminals full access to the website, enabling them to deface and even steal information from it.

In a DNS-hijacking attack, DNS records are altered to enable redirection to rogue DNS servers. These servers, in turn, substitute the IP addresses of malicious sites to legitimate domain names.

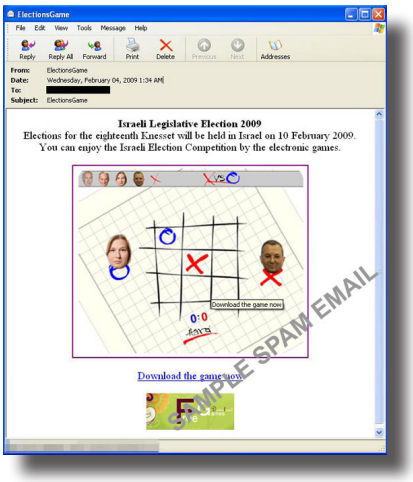
DDoS is another method cybercriminals use to render a website inaccessible. It uses remotely controlled bots to attack target sites. Infected machines are then set to connect to the targets at a specific time to overload their bandwidth capacities, rendering them inaccessible.

Cybercriminals use the following techniques to carry out their malicious activities:

- XSS involves attacking at a vulnerable site's browser level by injecting code.
- SQL injection involves code injection in a vulnerable site's database.
- DNS hijacking involves altering DNS records to redirect a vulnerable site's visitors to rogue DNS servers.
- DDoS uses remotely controlled bots to render vulnerable sites inaccessible for a certain period of time.

TREND MICRO

Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.



Looking Beyond the Surface

At the most basic level, hacktivism causes temporary site service disruption. Websites are rendered inaccessible for minutes or hours, depending on how fast their owners or administrators can counter the intrusion. Hacktivism creates confusion among site visitors until the sites they wish to gain access to return to their normal state. Of course, it is a different story altogether when malware are involved, as in certain mass compromises and spam runs targeting political websites. Hacktivism-related incidents that involve data breaches are even more dangerous, as these tread the fine line between hacking and stealing information.

Stop Hacktivism Even Before It Happens

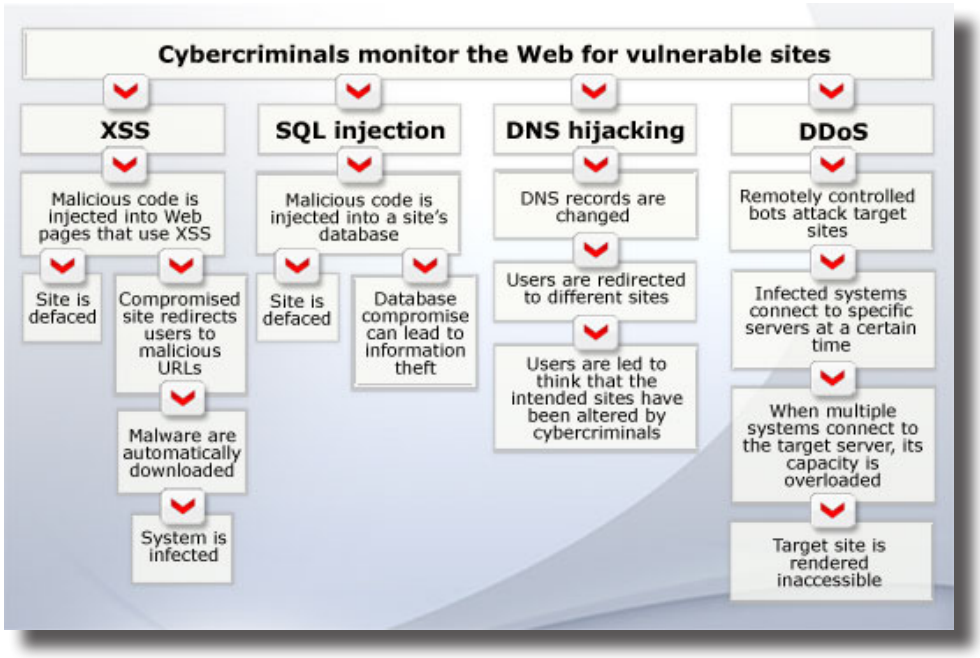


Figure 2. *Typical techniques cybercriminals use to compromise websites*

Since predicting exactly which websites will suffer from hacktivism-related attacks is quite a huge challenge, users are advised to constantly be on the lookout for suspicious-looking pages. It is also important to check a website's credibility before giving out personal information even if it seems legitimate. Finally, using a reputable security solution that provides overall smarter protection against all kinds of Web threats—malicious files, spammed messages, and malicious sites and domains—is critical.

Website owners or administrators should also put a solid security system in place to ensure that their sites' visitors will have a safe computing experience. For starters, using strong passwords serve as a good first line of defense against the aforementioned attacks. It is also advisable to regularly check for malicious scripts to avoid XSS and SQL injection infections. When it comes to hacktivism and cybervandalism, an ounce of prevention is always better than a pound of cure.

How to protect your site from hacktivism or cybervandalism

- Constantly look out for suspicious-looking Web pages.
- Check a site's credibility before giving out personal information even if it seems legitimate.
- Use a security solution that provides smarter protection against all kinds of Web threats.
- If you own or manage a site, put a solid security system in place to ensure that your visitors will have a safe computing experience.
- Use strong passwords.
- Regularly check for malicious scripts on your site to avoid XSS and SQL infections.

TREND MICRO

References:

- Aivee Cortez. (August 5, 2008). *TrendLabs Malware Blog.* "Nepal's Supreme Court Website Compromised." http://blog.trendmicro.com/nepals-supreme-court-website-compromised/ (Retrieved February 2010).
- Carolyn Duffy Marsan. (September 22, 2008). *Network World.* "Feds Tighten Security on .gov." http://www.networkworld.com/news/2008/092208-government-web-security.html (Retrieved February 2010).
- Carolyn Duffy Marsan. (December 31, 2009). *Network World.* "80% of Government Websites Miss DNS Security Deadline." http://www.networkworld.com/news/2010/012010-dns-security-deadline-missed.html (Retrieved February 2010).
- Dan Raywood. (March 24, 2009). *SC Magazine.* "Industry Hits Out at Claims of Government Websites and Databases Being Unsecured." http://www.scmagazineuk.com/industry-hits-out-at-claims-of-government-websites-and-databases-being-unsecured/article/129319/ (Retrieved February 2010).
- Florabel Baetiong. (February 10, 2009). *TrendLabs Malware Blog.* "Political Issues Bleed Through the Web." http://blog.trendmicro.com/political-issues-bleed-through-the-web/ (Retrieved February 2010).
- J.D. Meier, Alex Mackman, Blaine Wastell, Prashant Bansode, and Andy Wigley. (May 2005). *msdn.* "How to Prevent Cross Site Scripting in ASP.NET." http://msdn.microsoft.com/en-us/library/ms998274.aspx (Retrieved February 2010).
- JM Hipolito. (June 16, 2009). *TrendLabs Malware Blog.* "Iran: Street Protests Paralleled by DDoS Attacks." http://blog.trendmicro.com/iran-street-protests-paralleled-by-ddos-attacks/ (Retrieved February 2010).
- Joseph Pacamarra. (May 31, 2008). *TrendLabs Malware Blog.* "XSS Methods Also Seen Being Used in Mass Compromises." http://blog.trendmicro.com/xss-methods-also-seen-being-used-in-mass-compromises/#ixzz0eMrBFMIP (Retrieved February 2010).
- Paul Litwin. (September 2004). *msdn Magazine.* "Stop SQL Injection Attacks Before They Stop You." http://msdn.microsoft.com/en-us/magazine/cc163917.aspx (Retrieved February 2010).
- Prefect. (January 28, 2010). *Praetorian Prefect.* "Congressional Website Defacements Follow the State of the Union." http://praetorianprefect.com/archives/2010/01/congressional-web-site-defacements-follow-the-state-of-the-union/ (Retrieved February 2010).
- Rik Ferguson. (January 5, 2010). *CounterMeasures Blog.* "Mr. Bean Comes Out of Retirement, Takes over Spain." http://countermeasures.trendmicro.eu/mr-bean-comes-out-of-retirement-takes-over-spain/ (Retrieved February 2010).
- Rik Ferguson. (January 8, 2010). *CounterMeasures Blog.* "Pakistani National Response Centre for Cyber Crimes... Hacked!" http://countermeasures.trendmicro.eu/pakistani-national-response-center-for-cyber-crimes-hacked/ (Retrieved February 2010).
- Softpedia News. (January 9, 2010). *CyberInsecure.com.* "U.S. Army Website Compromised Through SQL Injection." http://cyberinsecure.com/us-army-website-compromised-through-sql-injection/ (Retrieved February 2010).

TREND MICRO

- Stephen Wildstrom. (July 2009). *BusinessWeek.* "Why Is the Government Vulnerable to a Simple Cyber Attack?" http://www.businessweek.com/the_thread/techbeat/archives/2009/07/why_is_the_gove.html (Retrieved February 2010).
- Steven Whitney. (October 22, 2009). *25 Years of Programming.* "Best Practices for Website Passwords." http://25yearsofprogramming.com/blog/2008/20080315.htm (Retrieved February 2010).
- *TrendLabs Malware Blog.* "Search Results for Hacktivism." http://blog.trendmicro.com/?s=hacktivism (Retrieved February 2010).
- *Wikipedia.* (February 4, 2010). "Hacktivism." http://en.wikipedia.org/wiki/Hacktivism (Retrieved February 2010).