2 February 2012 Last updated at 11:12 ET

redtape.msnbc.com

VeriSign, at Web's core, is hacked: What does it mean to you?

It should be clear by now that nothing online is sacred, and no security company is safe from hackers. VeriSign Inc., the firm at the center of so many critical systems on the Web, was infiltrated by hackers in 2010. Because details of the attack, first disclosed Thursday by Reuters, are so vague we are left to assume the worst -- and the worst is pretty bad.

It's possible that the VeriSign hackers could turn the Web upside down and create an Internet where nothing would be what it seems. A hacker website could look and act just like your bank's website. Your PC could easily be tricked into downloading automatic software updates that would appear authentic but actually contain viruses. And no matter what web address you typed into your browser, you could be redirected to a criminal's website half-way around the world.

But there's important context to this story which might ratchet down the "Oh My God!" factor considerably. For starters, there is reason to believe that VeriSign's revelation is nothing more than evidence companies are starting to comply with rules forcing them to disclose such incidents: In other words, similar successful hacks like this may have occurred in the past but simply went unreported. We'll discuss the evidence for that in a moment. First, let's look at the possibilities raised by the VeriSign attack.

VeriSign is involved in two distinct, fundamental Internet security structures that could be impacted by this attack. A successful attack on one would be serious, but a raid on the other could threaten the Internet itself. So let's start there.

VeriSign's most critical function is its role in the Domain Name System address book, which governs what happens when Web users type common name Web addresses into their browsers. There are 13 "root" DNS servers placed strategically around the planet for redundancy. VeriSign operates two of them. Should a hacker gain access to this part of VeriSign's business, he or she could theoretically poison the other 11 root DNS servers, and the bad data would eventually spread to the other DNS servers. The consequences could be dire: It could mean that everyone who typed "msnbc.com" into a Web browser would be sent to a computer controlled by criminals, instead of the real msnbc.com website. A computer criminal with destructive intensions could theoretically ruin the database that maps names with IP addresses and effectively shut down parts of the Internet. It has long been discussed that these root name servers are perhaps the most vulnerable point of the attack on the Internet

But it's more likely that the agencies controlling the other 11 root Domain Name Servers would be able to regain control of the DNS table and restore the system within a day or two, if not within hours. As you might imagine, root DNS servers do disagree from time to time and there is a process for handling that.

It's also important to note that VeriSign, in the SEC disclosure which started this incident, claims that its DNS servers were not attacked by hackers.

"Access was gained to information on a small portion of our computers and servers. We have investigated and do not believe these attacks breached the servers that support our Domain Name System ("DNS") network," the firm wrote in the filing.

VeriSign's other crucial function is issuing digital certificates through its VeriSign Authentication Services group. Certificates impact your computer use every day because they tell your PC that a company's website or software is really what is says it is. Certificates are a crucial part of the SSL system that ultimately displays a friendly looking lock when you visit your online bank. They also identify the legitimacy of software updates sent to your computer by software makers. Many modern PCs won't install software unless it is digitally signed.

A hacker who could influence the way VeriSign issues certificates would be a massive problem for both consumers and corporations.

"VeriSign is one of the most important enterprise trust authorities in the world, which delivers people safely to more than half the world's websites," wrote Catalin Cosoi, Chief Security Researcher at Bitdefender Labs. "A certificate issued by VeriSign will automatically be accepted by both browsers and operating systems. This kind of incident practically voids all the security provided by 64-bit operating systems,"

In other words, hackers would have an easy time loading viruses onto PCs around the world.

That's terrible, but it's not new. Virus writers have been compromising certificate issuers with abandon for the past 18 months. It's one of the reasons that Stuxnet computer virus managed to infect millions of PCs worldwide. That also means structures are in place to deal with fraudulent certificates.

"The worst case scenario would be several phishing attacks with valid certificates that browsers will render as legit," Cosoi said. "This would potentially yield a huge level of data that could be exploited for financial gain. However, it's important to remember that a strong anti-phishing solution will keep you protected."

Of course, it's not even clear from VeriSign's filing that its certificate business was compromised. Complicating matters further: Symantec Corp. purchased most of that business from VeriSign last year. For its part, Symantec said on Thursday that the assets it acquired in the sale were not compromised.

"We want to make it very clear that Symantec takes the security and proper functionality of its solutions very seriously. The Trust Services (SSL), User Authentication (VIP) and other production systems acquired by Symantec were not compromised by the corporate network security breach mentioned in the VeriSign, Inc. quarterly filing," said Symantec spokeswoman Nicole Kenyon in a statement to msnbnc.com.

Of course, it's possible that one of Verisign's other business unit – it provides extensive security consulting, for example – was the hackers' only target. That seems unlikely, however, given the target-rich environment the offers to computer criminals.

To be sure, many experts think the Verisign attack is serious business.

"The SEC filing says 'Information stored on the compromised corporate systems was exfiltrated.' That sounds like a targeted attack to me," said Mikko Hypponen, chief technology officer at F-Secure.com. "Like the one against Google. And RSA. And Lockheed-Martin."

But it's possible the VeriSign admission, buried in the SEC filing, is little more than paperwork which puts in print something that security professionals have long understood: No firm is safe from hackers. This might be at once comforting and disturbing: In October of last year, the SEC issued guidelines that called out public firms for under-disclosing security leaks and hinted

strongly that fines would come when firms failed to report successful hacker attacks. The VeriSign quarterly report was issued soon after, and it's easy to imagine the disclosure is more routine than anyone would like to admit. In fact, Stewart Baker, a lawyer at Steptoe & Johnson, predicted as much in a blog earlier this month.

"With enforcement so easy, and the harm from breaches so tangible, so serious and so likely to bring headlines, no one should expect the enforcers to go easy on companies that have been slow to disclose. Instead I expect a growing wave of cases based on companies' failure to make timely disclosure of ongoing breaches," he wrote.

Clearly, admission by VeriSign that executives at the firm were unaware of the breach shows a terrible lack of coordination inside the firm. And it's scary to read this admission, too: "Given the nature of such attacks, we cannot assure that our remedial actions will be sufficient to thwart future attacks or prevent the future loss of information."

Still, it’s important to note that we are talking about attacks that could be a year old, and whatever they were, criminals are already deep-in the process of exploiting them. Sad to say there’s nothing most consumers can do in response to this report.

In health news, there’s always the complicated issue of increased diagnosis vs. increased incidence. Is a new disease on the rise, or are we simply better at finding cases of it? The VeriSign incident raises the same question.

But the deeper truth here is probably something that professionals have known for some time: In the cat and mouse game between hackers and security firms, hackers are winning and, in some places, it's starting to look like a blowout.