BEWARE: Cyber Criminals are Having a “Field Day” with Software Vulnerabilities by Heimdal Security Company

Heimdal Security just completed a widespread intelligence analysis of system software vulnerabilities. Our data clearly shows that the problem of software vulnerabilities is actually growing and you may think that companies already got better at closing security gaps faster.

The Bad News

The main problem here is that time periods between patches don’t follow and fix the great amount of vulnerabilities that continue to appear.
Some vendors are improving though.
Security holes in software is arguably one of the most used attack vectormalicious hackers employ in a modern IT environment, with exploits accounting for 60 – 90% of the attack , depending on which data you look at.
This is precisely one of the reasons why you would think that software companies should be very quick at closing their security gaps, but the actual situation indicates quite the opposite.
If we take a quick look at the most vulnerable 3rd party software in the market, the list narrows in on some of the most used software components in the world.

The Numbers Speak for Themselves

The top 4 pieces of most commonly used vulnerable 3rd party software in 2012 / 2013 / 2014 are:

1. Oracle Java Runtime environment
2. Adobe Acrobat Reader
3. Adobe Flash Player / Plugin
4. Apple Quicktime

Of these 4, Adobe Flash Player accounts for 314 registered vulnerabilities alone in 2015. That comes to 26 vulnerabilities PER MONTH! The next piece of software on the list is Acrobat Reader with 130 vulnerabilities or 10,8 per month, still quite high, but not as extreme.

All this data is more than scary. Intelligence shows that usage of Java, Acrobat Reader and Adobe Flash Player is very common on business computers and has been for a while. The good news is that Flash usage has dropped significantly, mainly because HTML 5 replaced the need for having it installed, but also because Flash was a preferred attack vector in 2015. Meanwhile, the widespread usage of software is most likely linked to the fact that we consume more and more data on the computer, and that we access a broader variety of software to do so.

Most likely, your private computer system is not much different from a standard business computer, therefore consumers, as well as companies, should be very aware there is a crucial risk here.

Corporate Security Risks are High

We now know 4 key facts which should have your full attention, since they put you or your corporate data at risk:

1. The top 4 pieces of vulnerable 3rd party software is and has always been vulnerable to attacks
2. Vulnerabilities are severe and there is a high number of them!
3. Most computer systems actually use a minimum of 3 top vulnerable software presented here
4. Cyber criminals commonly exploit and develop attack vectors for these vulnerabilities

Knowing all this, you may think that manufacturers keep us safe by quickly fixing these problems for their users and customers. Well, our analysis indicates that is not the case.

So what can you do to protect yourself or your company?

• Make sure your 3rd party software is as up to date as possible, at all times. You can use an external tool to keep your software patched for you.
• Protect yourself using a Traffic checking service, such as Heimdal Pro/Corp, because most exploit attacks have a vector originating from the Internet. Corporations should potentially add a Bluecoat, CSIS Secure DNS, Palo Alto or Fireeye solution for an extra layer of centralized scanning.
• Use a corporate spam filter to remove phishing or exploits focused on malicious emails. This way, you have 2 layers of protection against malicious URLs, which may be heading for your computer. Consumers can use a client based filter and businesses can used a centralized solution.