http://www.business-cloud.com/articles/news/security-researchers-exploiting-vulnerabilities
16 May 2014

Security researchers exploiting vulnerabilities

Written by Ian Murphy on 14 May 2014 in News

Security is a tough game on both sides of the fence. In its latest Security Intelligence Report, Microsoft says vulnerability disclosure is up.

Defending computer systems from those determined to get in is like trying to keep the sea at bay. There are reasonable defences that you can build, actions you can take to mitigate attacks but, eventually, the bad guys have more incentive and knowledge than your staff. The more defences you have, however, the more expensive you make it for those trying to get into your systems.

Zero day exploits declining

In the latest Microsoft Security Intelligence Report (SIR), Microsoft has said that zero day exploits, those where the exploit is already available before the software owner can patch is, are on the decline. However zero day exploits now make up the bulk of all exploits and Microsoft believes that given the cost of developing new exploits, some security researchers are resorting to selling access to exploits rather than report them to software vendors.

Microsoft stops short of naming individuals, companies or even exploits or what action it is taking to resolve this. Like many other software vendors, Microsoft offers a bounty for security exploits so it will interesting to see if it now increases what it is paying and indeed, if we see any increase across the vendor community.

Exploits kits are big money

The value of exploits and the growth in exploit kits is highlighted by Microsoft. In the report is says that the "criminal group behind the malware family Win32/Reveton was reportedly making $50,000 per day in 2012 through Reveton exploits deliverd by exploit kits". That equates to around $18,250,000 in a single year. Such numbers are increasingly attractive to criminals and this is likely to be just the tip of the iceberg in terms of revenue from an exploit.

Over the last few years exploit kits have moved from basic developer tools to simpler graphical user interfaces that mean virtually anyone can buy and use them. Microsoft points out that many now come with analytics showing detailed information about infected computers. These analytics are known to be used by Botnet owners when they set the rental rate for their Botnets.

It is not uncommon for exploit kits to come with user licenses, support agreements and regular updates to help avoid detection and to add new features. While Microsoft stops short of saying it, criminals gangs are now becoming a normalised part of the software industry in terms of process and product.

Vulnerability disclosure rising but overall are on the decline

Vulnerability disclosures rose 12.6% during 2013 to just over 2,500 but this is not a bad thing. It means that vendors were aware of problems and issuing security patches to their software. This is below the 2009 peak where over 3,500 disclosure per 6 months were being reported. Much of the drop off is

being attributed to better coding practices but the retirement of older software products and better patch management will have contributed substantially to this.

Looking at where the vulnerabilities occur shows that for operating system applications and web browsers, 2013 was a year of declining vulnerabilities. However the operating systems themselves and the end user applications both saw steady increases in reported vulnerabilities.

The severity of exploits saw a shift in 2013. Disclosure of high-severity exploits in H2-2013 are down although they are still above the level of H2-2012. Low-severity exploits are also down and continue to fall from their high point in 2012. However, medium-severity exploits now account for 59.3% of all disclosures in H2-2013 and increased by some 19/1%.

In terms of exploits by type, Microsoft reports these by percentage of computers running Microsoft operating systems. Of course, this means that a single tenth of a percent represents millions of computers .The majority of these top exploit vectors show a decline versus the same period in 2012:

- Java - 1% down from 1.25%
- HTML/JavaScript 0.55% down from 1.4%
- Operating Systems - 0.45% up from 0.4%
- Adobe Flash - 0.1% no change
- Documents - 0.05% down from 0.2%

Malware infection rates rising

Microsoft reports that malware infections continue to rise as a percentage of encounters with a surge in Q4 2013. However, the message around the need for software to always protect computers is getting through. 78% of computers tracked show they are always protected, 20% are intermittently protected but worryingly around 4% are completely unprotected.

The impact of malware Rotbrow caused all of Microsoft's desktop operating systems to show a significant hit in infection rates during Q4 2013. Windows XP showed an increase of 1.6x, Windows Vista 6x, Windows 7 5.1x and Windows 8 8x. Windows 8.1 appeared towards the end of the period and showed a minor infection rate although that may change when Q1 2014 numbers appear.

For the server operating systems, the impact of malware has been almost negated with the exception of Windows Server 2003.

As would be expected, the consumer segment has a higher infection that corporate but this is nothing for IT departments to relax over. Bring Your Own Device (BYOD) and the continued rise of home working means that these computers are entering the enterprise space and have the potential to cause chaos on the corporate network.

The types of malware show that Trojan downloaders are the biggest malware threat. This is because it allows infected machines to be used and infected multiple times.

Email

Email continues to be a problem more in terms of the unwanted volume rather than as a major infection point. Microsoft reports that more than 75% of emails are unwanted. Only 7.1% of these emails contain malware while 4.1% are targeted phishing emails. The rest are just noise and their impact is more about bandwidth and storage than anything else.

Websites

SmartScreen Filter now shows that for every 1,000 websites on the Internet, 5.5 are phishing sites and 18.4 host malware. Taken together, that means that just over 2% of the sites on the Internet are a problem. The number of sites increases every year and the main countries involved in hosting these sites are Ukraine, Russia, Romania, Indonesia and South Africa.

For corporate IT administrators, it is relatively easy to set up firewalls rules that prevent users from accessing sites in these countries unless they are known business partners. These rules could also be deployed to local machines to help improve security.

Education

One thing that makes it easy to infect computers is the willingness of people to follow a link in an email or through social media to a top news story. Disasters and wars are good for this and often emails will be couched in terms as to "what the press doesn't want to report" or "this is happening now". Users are then taken to sites where malware is downloaded onto their machine in the background.

The solution is to improve user education but as several security reports have shown in the last year, end user security education is on the decline with companies not willing to invest in training. The rationale often used is that they should know better. If they did, then infections would be going down and regular security reminders are always a good thing.

Overall, security is getting better

Despite some of the things in this report which show increases in some types of security issues, the picture is getting better. However, at Rotbrow demonstrated, it only takes one successful exploit and the number of infected computers increases substantially.