

Forum:[Hack Forums](#)

Thread: [\[Explain\] What's Zero - Day 0Day Exploit Vulnerability](#)

UnKnOwN333 - August 4, 2015, 12:34 pm

Hey HackForum :)

- What is the Zero-Day Attack ? attack is a Zero-Day is any attack or threat is the exploitation of gaps or new vulnerabilities newly discovered was not known in advance in any application, program, or even a website or operating system or other. As the developers of these systems that have been discovered these gaps where they do not have time to fix this loophole, and so called the Zero-Day . When the company responsible for the system, which was discovered gaps by issuing a repair these gaps, these gaps are no longer gaps Zero-Day because it has been repaired.

[img]<http://www.trendmicro.com/vinfo/resources/images/tex/blogicons/badsite.jpg>[img]

- How to take advantage of such loopholes ? Since these gaps is a serious and threatening to all users of these systems infected by, so these gaps will be very useful for hackers and their discoverers in many ways in order to make money. Where can discoverers of these gaps that they reap outrageous profits from these gaps in many different ways and this is what Snodha now. So let us recognize the ways in which they can to the discoverers of these gaps make money from which the first method : the sale of these gaps for developers of these systems or their owners. For many companies that issue systems and programs and even large sites there have systems and programs equivalents of hackers security researchers who discover security holes in their products. So that after the security researcher or finder gap heading off a producing company which owns the program, the system or the site with details of the gap so they can review them and rewarded them. rely equivalent value provided by these gaps on the strength of the gap and severity, some gaps in the Facebook site got Mki_voha the amounts exceeded tens of thousands of dollars. Also, operating systems such as Windows and browsers such as Google Chrome browser discoverers gaps where one received an amount in excess of 120 thousand dollars to meet with his discovery of gaps in it. There are other companies from big companies do not have such programs Balmkaviat. Can of penetrating the gap that keeps the details to be used by and reported in a timely manner and that the company may be announced rewards programs and a tribute to the hackers. Or can that he uses in other Astglalat and this is what we will talk about in the rest of the roads. The second way : the sale of these gaps across sites Black Markets . There are many sites used to sell gaps and called the black market, where the discoverers of these gaps present details on the followers of these sites and then sell it to the person who pays the largest amount or sold to several people. So can the people who have purchased these gaps to use them in campaigns to control and penetrating the largest number of devices in order to steal information from them, or blackmail the owners as it happens in ransom programs (ransomware), or even to use this piercing devices to build a network botnet for use in different penetration operations and launch attacks denial of service and others. Most of these sites are Russian sites, and you can not sell such gaps, but if you talk of the Russian language and can be selling the gap process, but their value will be quite a few very, very. The third way : the sale of these gaps companies espionage and governments. Many of the companies that are designing and programming spyware to sell to governments are buying these types of gaps of their discoverers, to develop spyware and then you are selling to governments and private governments in third world countries so that governments monitor and spy on dissidents her through these programs. Also, governments and armies in the major countries is also seeking to buy such gaps and get them so as to not developed and exploited in espionage operations, electronic warfare, which is launching on other countries to steal ideas and military schemes and others. is a company Vupen in France of the biggest companies in the world that you are buying gaps Zero-Day and so you develop and sell them to governments. Where he some reports recently revealed that the company has signed a contract of agency NSA to sell Astglalat

gaps Zero-Day . method fourth : exploited by the hacker. If these gaps discovered by a team either follow the government or followed for a mail struggle groups, This could be the team to develop the exploitation of this loophole to be used in an attack on the State and Government, which is targeting this team.

[img]http://4.bp.blogspot.com/-ZBFH3sJLy1k/U134Mxz2JVII/AAAAAAAAAjjg/o-ym_o6MC50/s1600/z
eroDay.png[/img]

- how to protect them ?

Since this type of gaps and types of attack was discovered recently and since it is, even if it was launched Astglalat it can not be detected and repaired, so it should be anyone know how to protect against such This type of loopholes to reduce their impact, both manufacturers of software or operating systems or even developers of Web applications. Of course let's not deny that there can be and there is no way to protect you is 100% of such type of attacks and be objective is to protect yourself as much as and it is possible to take precautions due to it. It is these precautions that should be the people of the following: - companies must follow security measures and recommendations by setting policies on firewalls in their networks and make sure they match the business requirements of the company, in addition to giving less powers on hardware firewalls workflow . - it must be done to make sure that the struggles of viruses updated systems and are working well and that he could deal with the malicious files that are sent through e-mail and more. - You must make sure that all existing systems up to date fully and that existing programs it updated too, and do not where there are no gaps. - not to rely on firewalls and the struggles of viruses on the staff devices only, but must be with the company more than one layer of screening and protection layers across the network and across devices and others. - security awareness among the staff and users and do not download files via e cold from unknown destinations and others. - Working with detect and block intruders in corporate systems as well as dealing with its own applications Web firewalls and to monitor and analyze and detect new vulnerabilities. - put particular any security incidents may be incurred plans so as to minimize of the impact of such resulting from this type of attack incidents.

Thanks ????

UnKnOwnN333 - August 17, 2015, 1:36 pm

up thread !!!!! again up

Sennheiser - August 17, 2015, 1:39 pm

tl:dr

An exploit that hasn't been detected yet which poses a massive security risk

UnKnOwnN333 - August 17, 2015, 1:51 pm

(Aug 17, 2015 01:39 PM)Sennheiser Wrote: [\[CITE\]](#) tl:dr

An exploit that hasn't been detected yet which poses a massive security risk
hacker everytime exploiting !!!! and exploit has level : Low / Risk !!!

Driverfury - August 18, 2015, 2:06 am

Hmm, interesting thread. I will study more on how to defend from Zero-Day attacks. Good thread.

UnKnOwnN333 - August 18, 2015, 5:51 am

(Aug 18, 2015 02:06 AM)Driverfury Wrote: [\[CITE\]](#) Hmm, interesting thread. I will study more on how to defend from Zero-Day attacks. Good thread.

Thanks Bro :)

Famous Exploit Zero Day Is Drive By Download You Need Install

MalwareByte Anti-Exploit

And ADD NoScript For Your Browser for blocking script!!!

and Update Your java and your browse

then dont worry :D ????

KnockSteadys - *August 18, 2015, 9:32 pm*

nice info you got here thanks

UnKnOwn333 - *August 19, 2015, 3:42 pm*

(Aug 18, 2015 09:32 PM)KnockSteadys Wrote: [\[CITE\]](#) nice info you got here thanks
thanks my brother !!!! :)????

thiefhearts - *September 28, 2015, 1:49 am*

Hello possible ergonomics program to penetrate Facebook