The corner of getting rich: A company hung a $ 1 million prize for anyone who hacked WhatsApp and iMessage

If you are a hacker or a security researcher, have a profound knowledge about the iPhone, what are you waiting for without trying, maybe a warm new year!

If you are a hacker or a security researcher, have a profound knowledge about the iPhone, what are you waiting for without trying, maybe a warm new year!

On Monday, January 7, Zerodium, a start-up in the field of buying and selling hacking tools for agencies and organizations around the world, announced an increase in buying prices for most companies. tools they are looking for, such as remotely unlocking iOS and exploiting vulnerabilities in Windows.Zerodium representative said the company would be willing to pay $ 1 million security researchers if they could exploit the vulnerability in popular messaging / chat applications such as WhatsApp, iMessage and SMS / MMS. on all mobile operating systems.

'Messaging applications in general and WhatsApp in particular are sometimes the only communication channels used by the goals our customers target, and end-to-end encryption makes them difficult to block. or exploit those contacts.Therefore, tools to exploit these applications remotely directly without compromising the device's performance are much more efficient and effective strategies, 'said Chaouki Bekrar, founder of Zerodium shared in an online talk.

1. Quora's question and answer page was attacked, causing 100 million users to leak personal information

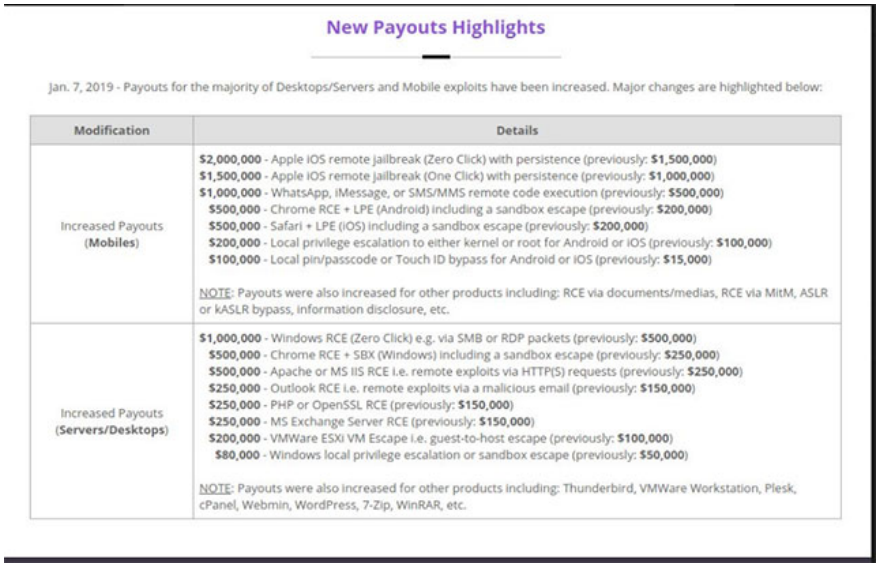
Hacking an iPhone, sometimes called a literal way of remote cracking, exploiting the iOS or root vulnerability, can be paid up to more than $ 2 million and often involves a series of errors and Vulnerabilities can be exploited.

'The main goal is to attract more resources, and we have the financial ability to buy many different iPhone hacks.We are supported by a lot of big customers as well as an abundance of potential customers, the funds to pay for such hacks can be called endless. '

Increasing the price of acquiring hacking tools suggests that mobile devices in general become more and more secure and therefore more difficult to hack.This means hackers will have to put more effort into finding tools to unlock or exploit vulnerabilities on iOS and Android devices.And of course, when the difficulty increases, the remuneration will be more plentiful.Organizations and agencies that need it will naturally have to accept more money.However, money is one thing, supply does not meet demand is the problem, and this is where companies like Zerodium, Azimuth and Crowdfense work.They are intermediaries between security researchers and agencies looking for tools that are often called zero-days.Zerodium is responsible for brokering, buying zero-days tools, and selling them to those in need.

1. There is a new zero-day vulnerability in Windows

Earlier, Zerodium announced it was willing to pay $ 500,000 immediately to anyone who could exploit the vulnerabilities in WhatsApp and iMessage, but it was clear that this amount was no longer commensurate with the current difficult situation. So the Zerodium price doubled is also understandable.



New Payouts Highlights

Jan. 7, 2019 - Payouts for the majority of Desktops/Servers and Mobile exploits have been increased. Major changes are highlighted below:

Modification	Details
Increased Payouts (**Mobiles**)	**$2,000,000** - Apple iOS remote jailbreak (Zero Click) with persistence (previously: **$1,500,000**) **$1,500,000** - Apple iOS remote jailbreak (One Click) with persistence (previously: **$1,000,000**) **$1,000,000** - WhatsApp, iMessage, or SMS/MMS remote code execution (previously: **$500,000**) **$500,000** - Chrome RCE + LPE (Android) including a sandbox escape (previously: **$200,000**) **$500,000** - Safari + LPE (iOS) including a sandbox escape (previously: **$200,000**) **$200,000** - Local privilege escalation to either kernel or root for Android or iOS (previously: **$100,000**) **$100,000** - Local pin/passcode or Touch ID bypass for Android or iOS (previously: **$15,000**) NOTE: Payouts were also increased for other products including: RCE via documents/medias, RCE via MitM, ASLR or kASLR bypass, information disclosure, etc.
Increased Payouts (**Servers/Desktops**)	**$1,000,000** - Windows RCE (Zero Click) e.g. via SMB or RDP packets (previously: **$500,000**) **$500,000** - Chrome RCE + SBX (Windows) including a sandbox escape (previously: **$250,000**) **$500,000** - Apache or MS IIS RCE i.e. remote exploits via HTTP(S) requests (previously: **$250,000**) **$250,000** - Outlook RCE i.e. remote exploits via a malicious email (previously: **$150,000**) **$250,000** - PHP or OpenSSL RCE (previously: **$150,000**) **$250,000** - MS Exchange Server RCE (previously: **$150,000**) **$200,000** - VMWare ESXi VM Escape i.e. guest-to-host escape (previously: **$100,000**) **$80,000** - Windows local privilege escalation or sandbox escape (previously: **$50,000**) NOTE: Payouts were also increased for other products including: Thunderbird, VMWare Workstation, Plesk, cPanel, Webmin, WordPress, 7-Zip, WinRAR, etc.

In an interview last December, an expert in security analysis said that to exploit messaging applications such as WhatsApp and Signal, hackers would have to drill through the advanced end-to-end encryption layer. of developers, so this will not be an easy task and it can be said that the amount of 1 million dollars (or maybe even 4 million dollars) is not 'easy' Come on.

1. Hacker purged two-factor security just by automated phishing attacks

'There are a number of tools that exploit vulnerabilities that companies are willing to buy in large amounts, amounting to more than $ 1 million.Usually it is related to remote code execution for iMessage, WhatsApp, Signal, Telegram, and other chat applications.Once you have your hands on how to exploit this kind of vulnerability, it means that you are a millionaire! 'Said security expert Maor Shwartz.

Bekrar warns that although exploiting and hacking some operating systems and applications is becoming increasingly difficult, it is not impossible.In addition, there will be fewer errors on today's applications, but these will often be very serious vulnerabilities if exploited.'Exploiting vulnerabilities in applications and operating systems is becoming more and more difficult, taking longer, but many security researchers have enough talent to do that, and the strategy of We are raising prices and further raising prices to encourage researchers to continue hunting and exploiting potential security vulnerabilities'.

In fact, 2018 is a booming year of market trading tools that exploit vulnerabilities.Although there are no specific forecasts from leading experts, it is likely that in 2019, the situation will still be maintained.

See more:

1. The provisions of the Criminal Code relate to the field of information technology and telecommunications networks
2. Warning: New extortion code GandCrab is attacking Vietnamese Internet users
3. China has at least 10 PoP presence points to hijack the network architecture
4. Facebook was attacked, more than 50 million user accounts are at risk of being leaked