National Conference on Research Challenges and Opportunities in Digital and Cyber Forensics
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 4 | Issue 11 | ISSN : 2456-3307 (www.ijsrcseit.com)

RACCOON ATTACK : A Timing Attack to Leak Secret Keys

Akansha
Information Science and Engineering, New Horizon College of Engineering Bangalore, India

ABSTRACT

In today's socio-economic atmosphere one of the firmest developing areas of technical infrastructure development is the Internet. The aggregate cyber-attacks over the past decade are posing a thoughtful threat to the digital world. The paper centers around the Raccoon: The Story of a Typical Information stealer. Raccoon stealer was found in April 2o19. Raccoon is a mainstream information stealer these days on account of its low value (USD$75 every week and $2oo every month) and its rich highlights. Otherwise called "Racealer, "Racoon is used to steal sensitive and personal data which includes login credentials, credit card data, cryptocurrency wallets and browser data (cookies, history, autofill) from very nearly 6o applications. "Raccoon," the attack has been described as complex and the vulnerability is "very hard to exploit." While most clients ought to presumably not be worried about Raccoon, a few significant programming merchants have delivered patches and mitigations to ensure customers. Raccoon can permit a man-in-the-middle (MitM) attacker to break encrypted communications that could contain delicate data. However, the attack is only successful if the targeted server reuses public Diffie- Hellman (DH) keys in the TLS handshake (i.e. the server uses static or ephemeral cipher suites such as TLS-DH or TLS-DHE), and if the attacker can conduct precise timing measurements.

Keywords : Fibre reinforced composite, mechanical properties, banana fibre, biodegradable, hand layup

I. INTRODUCTION

A team of researchers has uncovered a theoretical attack on the TLS cryptographic protocol, which can be used to decrypt HTTPS connections between users and servers and to read sensitive communications. As the name implies, Rachkon portrayed the attack as "really difficult for adventure" and its hidden circumstances as "rare". "The attacker needs specific conditions for the Raccoon attack to work," the specialists composed on a site committed to the Raccoon attack. "He needs to be close to the target server to achieve high precision timing measurements. He needs the victim connection to use DH(E) and the server to reuse ephemeral keys. And finally, the attacker needs to detect the original connection."

"For a real attacker, this is a lot to ask for. However, in comparison to what an attacker would need to do to break modern cryptographic primitives like AES, the attack does not look complex anymore. But still, a real-world attacker will probably use other attack vectors that are simpler and more reliable than this attack," as they described.

The hidden weakness has existed for more than 2o years, and it was fixed with the arrival of TLS 1.3.

As we know that it is a server-side vulnerability, there is nothing that clients can do to avoid attacks, apart from guaranteeing that their web browsers don't utilize the problematical cipher suites — the current internet browsers no longer use them. Then again, the researchers have brought up that the timing measurements may not be important to introduce an attack if there is a specific kind of bug in the focused on programming.

F5 Networks, which tracks the defect as CVE-2o2o-5929, has delivered a fix. Mozilla has relegated the vulnerability CVE-2o2o-12413 and incapacitated the DH and DHE ciphers in Firefox 78, however this move was arranged before the Raccoon attack was found. Microsoft has delivered an update for Windows to address the vulnerability, and openSSL, which has allocated the issue a low severity rating, has published an advisory depicting effect and alleviations. However, even if the timing requirements are avoided, a server still needs to reuse DH keys for the attack to work. An analysis conducted by the analysts indicated that over 3.3% of the servers facilitating the Alexa top 1oo,ooo websites reuse keys.

II. A TIMING ATTACK TO LEAK SECRET KEYS

Utilizing time measurements to compromise a cryptosystem and leak sensitive data has been the care of many timing attacks, and Raccoon employs the similar methodology to the Diffie-Hellman (DH) key exchange process during a TLS handshake, which is critical to exchange information over a public network securely.

This shared secret key produced during the exchange enables secure browsing on the Internet, permitting clients to securely visit websites by ensuring the communication against eavesdropping and man-in-the-middle (MitM) attacks.

To break this security wall, the noxious party records the handshake messages between a client and server, utilizing it to start new handshakes to the similar server, and thusly estimating the time it takes for the server to react to the tasks associated with inferring the shared key.

III. ATTACK OVERVIEW

Diffie-Hellman (DH) key exchange is a focused strategy for exchanging keys on a TLS connection. When using Diffie-Hellman, two TLS peers randomly create private keys (a and b) and create their own social buttons: ga mod p and gb mod p. These public buttons are sent to TLS KeyExchange messages. once two keys are found, the client and server can calculate the shared key of the mod mod p - called premaster secret - which is used to insert all of the TLS session keys with a specific access key function.

our Raccoon attack exploits a particular TLS channel; TLS

1.2 (with all one previous variance) recommends that all leading zero bytes leading to the premaster secret are subdivided before use in other calculations. Since pre- encryption is used as an input to the acquisition key function, which relies on hash functions with various time profiles, accurate time measurements can enable the attacker to create an oracle from the TLS server. This oracle tells the attacker whether the secret of the premaster used starts at zero or not. For example, an attacker could send a gavesdrop ga sent to a client, resubmit it to a server, and then decide whether the emerging praster secret starts at zero or not.

Reading a single byte in a pre-existing secret would not help the attacker much. However, here the attack is interesting. Imagine an attacker capturing a ClientKeyExchange message that contains ga value. The attacker will now be able to create ga-related values and send them to the server with a different TLS handshake. Specifically, the attacker builds gri * ga values, leading to earlier secrets gri * b * gab. Depending on the behavior of the server, the attacker may receive values leading to

premature secrets starting with zero. Ultimately, this helps the attacker to develop a statistics collection

and use the Hidden Numbers (HNP) solution to register a pre-existing secret created between the client and the server.

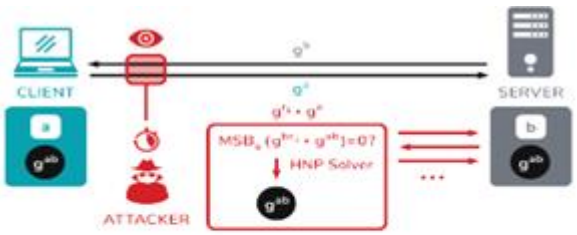

Figure 1: Raccoon attack overview. The attacker passively observes the public DH shares of a client-server connection and uses an oracle in the TLS key derivation to calculate the shared DH secret using a solver for the Hidden Number Problem.

IV. OPERATIONAL METHODS OF "RACCOON"

Let's find out how the infostealer's typical malware works as 'Raccoon'.

Raccoon is widely distributed using one of two methods:

Exploit Kits - A malicious site that displays targeted applications in any browser-based applications and directs the user to a malicious landing page. The landing page contains a code of abuse that takes advantage of the vulnerability and uses it to install malware.

Criminal data theft campaigns (Phishing Attacks) - A type of social engineering, the user is influenced by content that seems innocent to create a vicious payment burden. Usually, the victim receives an email with a Microsoft office document attachment, which contains a malicious macro. Automatically macros are disabled, so the attacker will try to persuade the user to enable macros and after that the malicious code will be applied.

A. Getting started

Most malware and especially MaaS have a C&C server to be able to retrieve data about malware options / features enabled by the attacker and send all the stolen information from the user.

The C&C server for malware is a requirement for malware operation, which is why, in order to keep it secret, malware authors retain the C&C server address in some way to keep it out of reach.

B. Stealer configuration

Like many authentication hackers, a client (e.g. invader) can customize his or her operating system suspension, which can be stored in a binary created by a malware or a C&C server, and then returned to the malware when it

uninstalled. In Raccoon, after a client chooses to be suspended, a malware builder generates a client configuration ID and writes this ID to the integrated malware. In this case, the suspension ID is encrypted, Raccoon has another 64-coded encrypted cord. Encryption The configuration ID, using the first key and, after the encryption process, receives the suspension .To obtain complete suspension, the thief must query C&C. The C&C server returns the JSoN containing the required suspension. it's a duck to work

V. CAPABILITIES

Raccoon monitors the scope of applications and uses well- known techniques to extract sensitive information from those applications.

Raccoon uses the same process for each targeted application:

1. Locate the application file containing sensitive information.
2. Copy the file to its operating folder (% Temp%).
3. Create specific application routes to extract and encrypt related information.
4. Write the text file in its operating folder with the stolen dates.

To uninstall and delete data in applications, Raccoon downloads certain DLLs for applications. Config JSoN contains a URL where malware will download those libraries. Raccoon aims at 29 chromium-based programs that include Google Chrome, opera, etc. (complete list below) that have the same folder structure and share the same codebase, leading to the same way to manage sensitive data. Sensitive data in those browsers is stored in the same format as the

"Data Data" application folder containing SQLite data. Most hackers, such as Raccoon, make inquiries about SQL using sqlite3.dll to retrieve user autologin passwords, credit card data, cookies and browser history.

More thieves are relying on the same process for Mozilla- based apps. Since these programs have the same strategy as the folder structure, the strategies for stealing applications are the same. The big difference is the names. The thief is looking at four Mozilla-created browsers including Firefox and SeaMonkey, (full list below) and one Mozilla-based email client, ThunderBird. In those applications, the hijacker removes and writes sensitive information such as username and password, cookies and history. It is worth noting that Raccoon also supports an

older version of Mozilla-based apps - it supports Firefox <32 versions, for example. To do so, Raccoon downloads a compressed file containing multiple DLLs for secure access. By using functions from nss3.dll, malware is able to encrypt and extract data from SQLite information and a JSoN log file. While searching for digital wallets, Racoon focuses on popular apps like Exodus, Jaxx and more. Like many hackers, Raccoon searches for those wallet files in the default location of the app, but it also has a wallet scan feature that allows you to find any wallet.dat file.

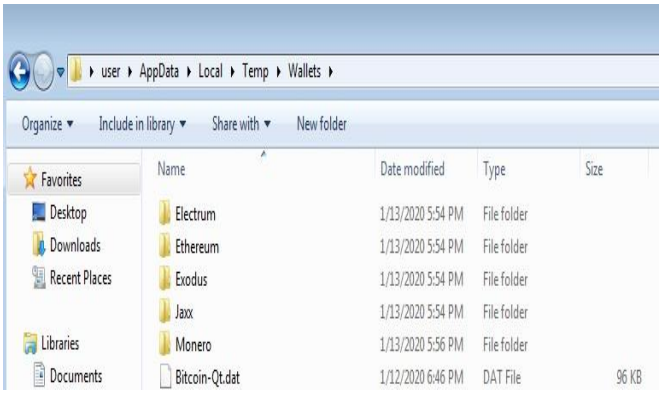

Figure 1 : Stolen Wallets Folder.

Malware collects data about the machine such as oS build and version, programming language, hardware details and installed applications. Additionally, it can take screenshots on the user's machine if that is enabled by the attacker's configuration. After satisfying all its theft skills, Raccoon collects all the files and writes them into a temporary folder into a single zip file called Log.zip. Now it has to restore the zip file to the C&C server and delete all traces itself.

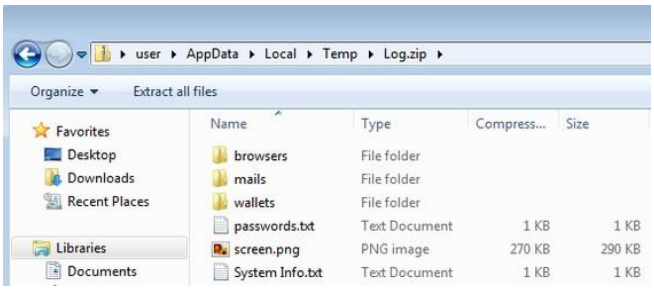

Figure 6: Zip File Content.

Raccoon does not use sophisticated methods to send a file back to C&C. It simply finds the C&C manager's URL (from config JSON) and Log.zip file path and sends Log.zip as it is, without encryption, using HTTP POST application.

Raccoon also has functionality to be used as a dropper, a feature that focuses on loading second-class malware download into the victim system. It downloads bad files and uses them. This is most commonly used to use other malware. In this case, the download feature is disabled by JSoN config, but when enabled, Raccoon takes the URLs from the loader_urls key, downloads the file to the temp folder and uses it at ShellExecuteA's call via file path.

VI. POTENTIAL DAMAGE & MITIGATION

This type of data theft can be very damaging to organizations and to an individuals. The attackers generally try to find out impressive details in so that they can find a rise in the right and the can perform their next movement. What is often saved by pure attackers can now be considered in any event, for beginner players who can buy thieves like Raccoon and use them to get sensitive organizational information. In addition, this goes beyond the names and passwords of users who can get instant financial

benefits such as credit card data and cryptographic (cryptocurrency) wallets.

Apart from the fact that Raccoon is not the most complex and typical tool present but it is still popular among criminals and it may last to be. To prevent malicious malware theft, organizations can use the solution, including basic understanding techniques such as updating systems and applications, avoiding suspicious attachment or clicking on anonymous URLs. Ensuring that the conclusions are weak is essential to improving the overall security action of the organization.

VII. CONCLUSION

Despite the fact that the Raccoon stealer may not be the most imaginative infostealer available, it is as yet increasing noteworthy foothold in the underground network. In view of tributes from the underground network, The Raccoon group gives solid client support to give cybercriminals a speedy and-simple approach to perpetrate cybercrime without a tremendous individual venture. This has not come without difficulty. The group

has confronted a few open questions in underground discussions, and has gotten some analysis from contenders. Regardless of this, Raccoon has immediately gotten one of the main ten referenced malware in the underground network, notwithstanding being dispatched in mid 2o19. In general, feeling around Raccoon is good, with some considering it the best swap accessible for the now ancient Azorult infostealer. Raccoon's notoriety joined with its restricted list of capabilities yet high selection addresses a developing pattern of the commoditization of malware, as malware creators shoot to make stages for wrongdoing as opposed to carrying out the violations legitimately. As malware creators decide to create MaaS, they should participate in a large number of similar exercises as a real SaaS business: advertising endeavors, depending on sure surveys, responsive client care, and consistently improving highlights in their item. We just anticipate that this pattern should proceed into 2o2o and push the development of MaaS forward.

VIII. REFERENCES

[1]. https://raccoon-attack.com

[2]. Raccoon Attack: Finding and Exploiting Most- Significant-Bit-oracles in TLS-DH(E). Robert Merget, Marcus Brinkmann, Nimrod Aviram, Juraj Somorovsky, Johannes Mittmann, and Jörg Schwenk.

[3]. https://www.zdnet.com/article/raccoon-attack-allows- hackers-to-break-tls-encryption-under-certain-conditions/

[4]. https://www.thesslstore.com/blog/raccoon-attack- researchers-find-a-vulnerability-in-tls-1-2/

[5]. https://thehackernews.com/2o2o/o9/raccoon-ssl-tls- encryption.html

[6]. https://www.securityweek.com/new-raccoon-attack- can-allow-decryption-tls-connections