CANARYTOKENS: AN OLD CONCEPT FOR A NEW WORLD

Gionathan Armando Reale, Benjamin Zinc Loft
Hovmark Data ApS, Cyber Security Department

ABSTRACT. Cyber attacks are becoming more common, and the evolving nature of these attacks call for novel solutions to detect and prevent intrusion that costs businesses dearly each year. This article explores the concepts and limitations of Canarytokens, a honeytoken based software abstracted from coal miners' use of birds as early warning systems to detect toxic gas, a practice established over a hundred years ago.

KEYWORDS: cyber, security, intrusion, detection, theft, protection, attacks

The word *honeytoken* was stated first by Augusto Paes de Barros in February 2003 [1], but the core concept is as old as security itself. From map-making [2] to ancient military campaigns, deception based intrusion detection has been successfully used to detect risk and attackers. Canarytokens [3] offer a new perspective on honeytokens, modeling the software after mining canaries and turning what is an old basic concept into a novel detection system.

Concept

The Canarytokens software distributes tokens that consist of a unique randomly generated identifier (which can be placed in either HTTP URLs or in hostnames). When the HTTP URL is requested, or the hostname is resolved, it alerts the owner (signifying that the token has been triggered) and provides a summary of information regarding the circumstances of the event [4]. This is the core concept of Canarytokens. The information given can be as vague as the DNS which has been used to resolve an embedded hostname, to as informative and specific as the IP address or computer name of the entity who triggered the token.

Canarytokens can be implemented in many different ways. Document based tokens can be placed within Microsoft Word documents and Acrobat Reader PDF documents [4] triggering an alert when opened with their native document viewers. Document based tokens offer the advantage (compared to other deployments of Canarytokens) that they can easily and effectively be placed within a corporate environment. Another possibility with Canarytokens is the ability to create a Javascript based token [4] which can detect if the owner's website has been cloned or is being hosted in another domain. This feature of Canarytokens can be vital in protecting websites from phishing campaigns and fraud.

Canarytokens also offers an interesting way to protect databases by creating a VIEW that starts a DNS query when a SELECT is run against the VIEW [4]. Due to the simple, effective and customizable nature of Canarytokens, tokens can be used in executables, DLLs, Windows folders and much more. Regardless of the exact implementation, the core concept of Canarytokens does not change.

Limitations

Canarytokens has several limitations affecting the document based tokens. Currently, IP/DNS detection [5] can be easily obfuscated by submitting any potentially "infected" document to a public online scanning service before opening the document. By doing so, the token will be triggered repeatedly by various IP addresses all over the world, thus masking the virtual identity of the attacker. Executable based tokens are also affected by this vulnerability [5].

Another issue plaguing document based tokens is their reliance on the use of certain document readers and conditions to trigger the token [6,7]. If an attacker decides to use a document reader outside of those mentioned in the software documentation, or has enabled special security measures, the attacker can in some cases, successfully open an “infected” document without triggering the token [6,7].

Another important limitation has been brought to attention in CVE-2019-9768 [8]: Microsoft Word documents containing tokens have minimal variation in size, metadata, and timestamp, allowing attackers to – with create accuracy – detect which documents may be “infected”, making it an easy task to avoid triggering an alert. Proof of concept code exists for this issue [9] and there is evidence to suggest this is being actively exploited [10].

Other limitations may exist that have yet to be discovered.

Conclusion

Canarytokens is a powerful tool which has the potential to improve the security stance of organizations that choose to use it. However, the limitations we found suggest that at its current state, document based tokens are easily detectable and can be bypassed by a well informed attacker. This is concerning as document based tokens can be a popular option for businesses wishing to detect attackers or malicious employees. Nevertheless Canarytokens offers an interesting and useful solution to detect attackers and protect assets.

REFERENCES

[1]. Tarek Sobh. Innovations and Advances in Computer Sciences and Engineering: Springer Netherlands; 2010.

[2]. A. Shabtai, M. Bercovitch, L. Rokach, Y. Gal, Y. Elovici, E. Shmueli, "Behavioral study of users when interacting with active honeytokens", *ACM Trans. Inf. Syst. Secur.*, vol. 18, no. 3, Feb. 2016, [online] Available: https://doi.org/10.1145/F2854152.

[3]. Canarytokens. 2019. [online] Available:

[4]. [http://canarytokens.org]

[5]. Thinkst Applied Research Blog. Canarytokens.org - Quick, Free, Detection for the Masses . Sept 2015. [online] Available:

[6]. [https://blog.thinkst.com/p/canarytokensorg-quick-free-detection.html]

[7]. Github. Thinkst/canarytokens issue 37. March 2019. [online] Available:

[8]. [https://github.com/thinkst/canarytokens/issues/37]

[9]. Github. Thinkst/canarytokens issue 36. March 2019. [online] Available:

[10]. [https://github.com/thinkst/canarytokens/issues/36]

[11]. Github. Thinkst/canarytokens issue 35. March 2019. [online] Available: [https://github.com/thinkst/canarytokens/issues/35]

[12]. National Institute of Standards and Technology. CVE-2019-9768. March 2019. [online] Available:

[13]. [https://nvd.nist.gov/vuln/detail/CVE-2019-9768]

[14]. Exploit-DB. 46589. March 2019. [online] Available:

[15]. [https://www.exploit-db.com/exploits/46589]

[16]. YouTube. Canarytokens Detection Bypass. March 2019. [online] Available:

[17]. [https://www.youtube.com/watch?v=dHHsmswYzmw]