Poster: A Website Protection Framework Against Targeted Attacks based on Cyber Deception

Jianbao Lin*, Chaoge Liu†, Xiang Cui*†‡, Zhaopeng Jia*
* Beijing University of Posts and Telecommunications, Beijing, China
† Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
‡ School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China
Email: liuchaoge@iie.ac.cn

***Abstract*—Web attacks have been a serious threat to cyber security for a long time. Conventionally, measures such as Web Application Firewall (WAF), Intrusion Detection System (IDS) have proved to be very successful in deterring non-targeted attack, but they are ineffective in combating targeted persistent attacks. Sophisticated and determined adversaries are always known to find their way around these. In this poster, we develop a novel hybrid leveraging multifarious cyber deception technology, named Web Shadow Service. On this basis, we creatively present forwarding-based defense mechanism which means that the malicious traffic will be forwarded to the shadow rather than blocked. And we propose a website protection framework that integrates the best advantages of the traditional perimeter-planted security mechanisms and cyber deception technology to enhance the security of the protected website.**

Keywords—website protection;targeted attack; cyber deception; shadow service; honey tokens

I. INTRODUCTION

Web attacks could be divided into non-targeted scanning attacks and targeted persistent attacks. We propose the web attack chain for these two attacks, as shown in Fig.1 and Fig.2

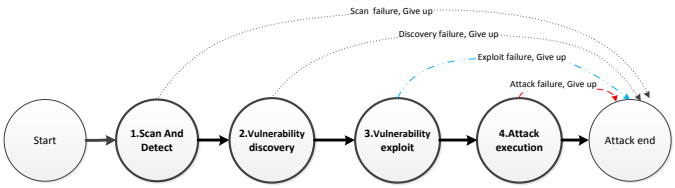

Fig.1 Non-targeted scanning web attacks chain model

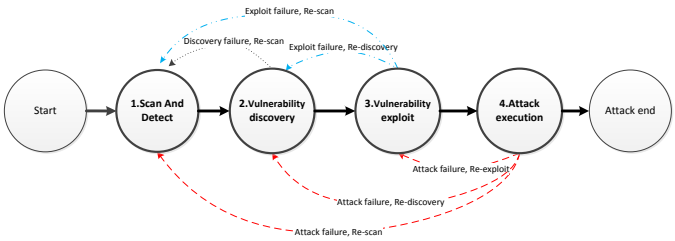

Fig.2 Targeted persistent web attacks chain model

The most obvious difference between non-targeted scanning attacks and targeted persistent attacks is that the former will give up the attack when a failure occurs at any stage of the attack chain as shown in Fig.1, while the latter will upgrade the attack method and re-attack until the attack is successful. Website defense has traditionally been provided using reactionary tools such as rules-based detectors, white/blacklisting, intrusion detection/protection systems, etc. often employing obstruction-based responses (e.g., blocking) to prevent the attack. These can guard against non-targeted scanning attacks effectively, but are ineffective in combating targeted persistent attacks.

For these targeted persistent attacks, a successful intercept means the beginning of the next attack. Because of the static, isomorphic, and similar nature of perimeter-planted defense equipment, sophisticated and determined adversaries are always known to find their way around these and are willing to spend large amounts of money, time and expertise until reaching their goals. The perimeter-planted security mechanisms and obstruction-based strategy is ineffective in combating these determined attacks.

In order to defend against such determined adversaries we need to redesign our defenses, developing technologies focused more on active confrontation than passive prevention. We recognize cyber deception [1] as an important strategy to make up for the weakness of perimeter-planted security mechanisms. We creatively employ forwarding-based deception strategy instead employing obstruction-based strategy to deceive and fight against targeted persistent attackers.

II. INNOVATIVE DEFENSE STRATEGY

We develop a novel hybrid leveraging multifarious cyber deception technology, named Web Shadow Service. The shadow is cloned from the protected website, preserving public data and confusing sensitive data, and is heavily instrumented with deception elements (e.g., honey tokens, honey files, honey accounts [2]) to detect and combat the sophisticated attacks.

On this basis, we propose a website protection framework that integrates the best advantages of the traditional perimeter-planted security mechanisms and cyber deception technology. Under the deception framework, we use the traffic identification and forwarding engine to inspect all traffic to the protected website. Malicious traffic and suspicious traffic sieved out based on intrusion detection module and blacklist are both processed by the web shadow service. Suspicious traffic is processed by the shadow to determine the accuracy of the intrusion prediction module. Legitimate traffic that was misclassified by the intrusion detection module will be validated by the web shadow service and will be transparently handled correctly by the protected website.

It is critical to emphasize that we propose and employ forwarding-based responses instead employing obstruction-based responses. That is to say, attack traffic will be forwarded to the shadow service instead being blocked. This is mainly according to two reasons. First, with the persistent attack attempt, attack tools and techniques are becoming more sophisticated, obstruction-based security mechanisms are unable to meet the needs of counteract advanced unknown attacks (especially 0day attacks). Second, attackers can use a proxy against IP address blocked.

Our forwarding-based mechanism based on the web shadow service provides a live, authentic target website to deceive, attract and misdirect the adversary.

On the one hand, using real website cloning, the shadow is difficult to be detected and identified by the attacker and can effectively reveal the attacker's strategies and keep protected website safe. On the other hand, even if the assailant has been successful, it has not any impact on the protected website. Moreover, the attacker mistakenly believe that the attack had been successful, thus giving up the attack. This is also another deceptive strategy to protect the real website.

III. Framework Overview

As we mentioned above, the overall design of the website protection framework is illustrated in Fig.3.

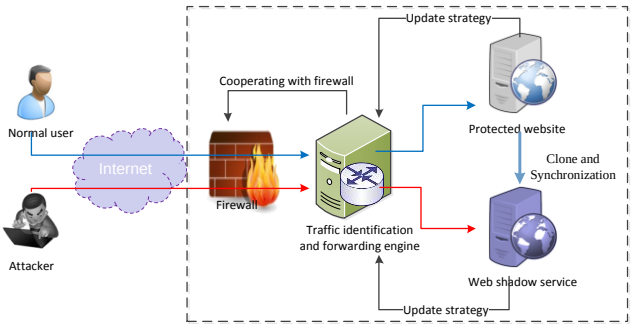

Fig.3 Website protection framework

A. *Web shadow service*

Shadow service is completely cloned from the protected website, including the server system, the web container, the web scripts and public data. The only difference is that the shadow need to perform data desensitization which means attempting to recognize sensitive data and substituting random, but validly formatted, values for the data [3] to prevent attackers from stealing and abusing. In order to improve the authenticity of the shadow service, regular data synchronization is required between the protected website and the shadow.

The shadow is instrumented to detect and combat the potential attackers. Attacks against the shadow service are caught and any incurred state changes are discarded. Logging tools and analyzer in the shadow recognize an attack and create a complete attack profile. Based on the attack profile, we can effectively reveal attacker's strategies and fix the vulnerabilities of the protected website to enhance its robustness.

Moreover, we deploy a variety of deception elements in the shadow and protected website to discover, trace and deter sophisticated attackers. Such as, honey tokens, which share similar characteristics with honey files, to attract and detect unknown attacks.

We employ a novel detect strategy based on web honey tokens. Both in the protected server and web shadow server, we insert some forged sensitive directories (e.g. "/admin" or "/login") into the robot.txt file, deploy fake accounts in HTML comments. Legitimate users have no need to review the robot.txt file or the source code of a web page; however, attackers frequently do in trying to identify vulnerabilities. So, the detected traffic containing these web honey tokens will be treated as malicious traffic and processed by web shadow service. Another example, we deploy some tracking script using fingerprint technology (e.g. WebRTC, Canvas) into some sensitive vulnerable (interesting from the attacker's perspective) page to trace the sophisticated attacker.

In addition, the outcome or status of processing a request by the shadow or the protected website could be used to update the strategy of the traffic identification and forwarding engine, which will be used to identify future attack instances more effectively.

B. *Traffic identification and forwarding engine*

Traffic is identified as legitimate, malicious and suspicious by the traffic identification module. The legitimate traffic will be forwarded to the protected website to process, while the other will be processed by the web shadow service.

Our innovative forwarding-based deception mechanism will not block the malicious traffic, but record its source IP address and forward it to the shadow. Then, traffic from this IP address will be recognized as suspicious traffic and forwarded to the shadow to determine. A sophisticated attacker would exploit more and more advanced vulnerabilities when the attacker has experienced many failures. So, when the adversary implements an unknown advanced attack or 0day attack, the deception mechanism will also be effective against the sophisticated attack. So, we can combat unknown attack from some point of view.

In addition to the above, suspicious traffic is also sieved out based on other two criteria: either the intrusion detection module detects an attack pattern in the traffic flow or the traffic originates from gray address space which is the set of IP address that may often be used as a springboard (e.g. tor exit node address, some already identified botnet addresses). This is taken into account that advanced attackers often use proxy or springboard networks (e.g. Tor network) to increase anonymity while normal users will not do.

IV. Discussion and Conclusion

In this paper, we identified deception as an important tool of defense, and we focus on designing a novel framework and an innovative forwarding-based defense strategy to effectively combat the targeted web attack. The major challenge is the availability and reliability of data desensitization, which need to achieve a compromise in the security of the data and attractiveness to attackers. We have implemented a prototype of this framework. In future, we plan to combine machine learning to address the challenge and work towards evaluating the prototype in a real business environment.

Acknowledgments

The authors would like to thank the anonymous reviewers for their helpful comments for improving this paper. This work is supported by the Key Laboratory of Network Assessment Technology, Chinese Academy of Sciences and Beijing Key Laboratory of Network security and Protection Technology.

References

[1] Pingree L. Emerging Technology Analysis: Deception Techniques and Technologies Create Security Technology Business Opportunities[J]. Gartner, Inc, 2015.

[2] Virvilis N, Serrano O S, Vanautgaerden B. Changing the game: The art of deceiving sophisticated attackers[C]// International Conference on Cyber Conflict. IEEE, 2014:87-97.

[3] Castellanos M, Zhang B, Jimenez I, et al. Data desensitization of customer data for use in optimizer performance experiments[J]. 2010, 41(3):1081-1092.