Dazzle-attack: Anti-Forensic Server-side Attack via Fail-free Dynamic State Machine

Kyungchan Lim, University of Tennessee
Bora Lee, University of Virginia
JiHo Lee, University of Virginia
Chijung Jung, University of Virginia
Doowon Kim, University of Tennessee
Kyu Hyung Lee, University of Georgia
Haehyun Cho, Soongsil University
Yonghwi Kwon, University of Virginia

Abstract

Dazzle-attack retrieves contents from benign and uncompromised websites to avoid detection and mislead the investigation to erroneously associate the attacks with benign websites.

Dazzle-Attack

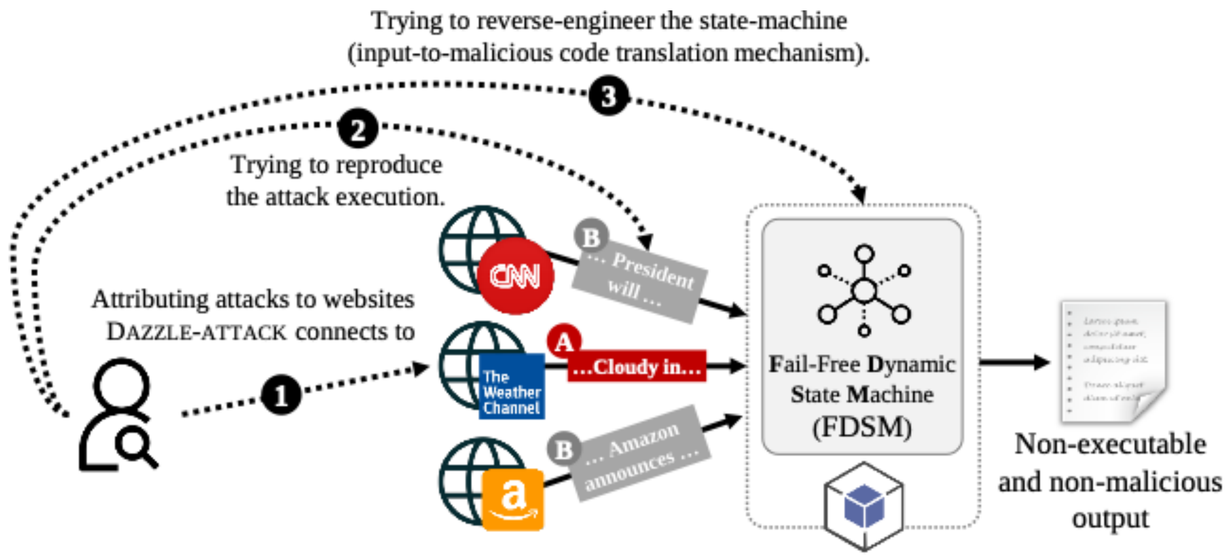
Demonstrate its resilience to forensic analyses.
Dazzle-attack takes input from webpages that are not under control of the attacker, meaning that the reliability of Dazzle- attack's attack is probabilistic.

Evaluation

Table 1 shows that all existing malware detection tools are unable to detect Dazzle-Attack.

Conclusion

Dazzle-Attack is a new type of attack that secretly delivers malicious payloads while imposing fundamental challenges to post-mortem forensic analysis.
We leverage FDSM that effectively thwarts various forensic analysis attempts. Dazzle-Attack is highly effective in preventing forensic analysis.



Input	Output
"**Airlines say**", "**Cloudy in**", "**Amazon recommends**", ...	@fopen("tmp");@fwrite(...);...
"President will", "**Cloudy in**", "Amazon announces", ...	Invested @amazonnews more information ...

(d) Input Translation by FDSM

A Content that will deliver the attack B Content that will ***not*** deliver the attack

Table 1. Detection results on malicious and benign samples.

Obfuscator	PHP Mal. Finder		Linux Mal. Detect		Shellray		MalMax	
	Mal.	Benign	Mal.	Benign	Mal.	Benign	Mal.	Benign
PHP Obfuscator [39]	399/413	161/573	98/185	0/573	479/524	0/573	573/573	0/573
YAK Pro [52]	264/413	139/573	16/185	0/573	239/524	1/573	573/573	0/573
Best PHP Obfuscator [6]	412/413	573/573	25/185	0/573	505/524	557/573	573/573	0/573
Simple PHP Obfuscator [56]	413/413	573/573	0/185	0/573	524/524	573/573	573/573	0/573
Dazzle-attack	0/413	0/573	0/185	0/573	0/524	0/573	0/573	0/573

THE UNIVERSITY OF TENNESSEE KNOXVILLE