Notes and Summary

Tel Aviv U (etc) Getting to the Root of Concurrent *BST Performance*

*Key words*;

phishing; web security; social engineering; Man-in-the-middle(MITM), TTL, TLS, Proxy Server

**Abstract**

Goal using analyzing and experimenting toolkits, identifying network-level properties can be used to find MITM

Machine learning classifier developed to identify with 99.9% accuracy

MITM toolkit has blind spot with only 43.7% of domain and 18.8% of IP address associated

**Introduction**

1|Almost every webpage have certain private credentials – phishers lure victims into disclosing them.

2| Before vs after of phishing website, hosted by themselves vs now they clone (everything and up-running

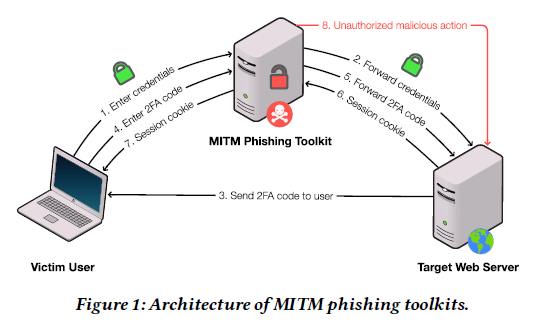
3| Static cloned content is not that applicable, hence phishers now act as invisible, to attack victim, 2FA adaptation has caused problem so phishing approach has changed.

4| Man-in-the-middle(MITM) phishing toolkit act a malicious reserve proxy (turns infected computer into proxy server -> attacker access unanimously) . Enables no need of phishing web page.

5| The research accuracy of 99.9%, (ML Classifier->robust). Fingerprinting method to uniquely find the MITM phishing toolkits by pinpointing malicious login request and flag them before authentication.

6| PHOCA automate discovery and analysis of MITM phishing which can be easily integrated.

7| 1-year -> Discovery MITM 1220 websites(focused on Big Companys FAMG). Unanimous nature creates blind spot only 44.7% o domain and 18.8% of IP associated have toolkit. Partnered with Palo Alto Network -> discovered 6403 request on 260 phishing sites.



**Summary**

The paper went into brief on how the attack happen, what toolkit they use, how to learn the possible attacks and how the product deals with the issue with maximum accuracy.

* Attack -> Uses session cookie of the user login until the TTL is expired.
* Toolkits -> Evilginx, Muraena, Modliska
* Classifier -> Random Forest
* PHOCA -> Learns, identifies either URL or domain-name, adds, trains new data

…to be contd.

**Scope**

…to be contd.

**Limitation**

Started with no data even of similar toolkits, dataset created by own -> Hence might be missing some important features as well. For eg MITM with extra layer redirection.

Unable to track all the brands that might have been targeted by MITM toolkit

Unable to detect traditional phishing website.

Can be used as additional tool.

**Conclusion**Tracing and learning is possible and can be done accurately. However traffic proxying is a weakness. The method can be used by targeted brand and do TLS fingerprinting.