Catching Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits

Brian Kondracki, Babak Amin Azad, Nick Nikiforakis
PragSec Lab

Stony Brook University
Computer Science

MITM Phishing Toolkits

Man-in-the-middle (MITM) phishing toolkits function as reverse proxy servers, brokering communications between victims and one or more targeted web servers.

Credentials, 2FA tokens, authentication cookies, and webpage content are proxied between the victim and web server, in full view of the attacker.

MITM phishing toolkits mirror live content from targeted websites, thwarting content-based phishing detection.

The three most popular MITM phishing toolkits in use today are: Evilginx, Muraena, and Modlishka.

Key Findings

> We create a machine learning classifier utilizing network-level features to detect MITM phishing websites with **98.9%** accuracy.

> We discover **348** phishing webpages hosted by MITM phishing toolkits.

> MITM phishing toolkits target popular trademarks such as **Google, Facebook, Twitter, and Yahoo.**

> Only **4.6%** of phishing domains and **8.03%** of phishing IP addresses are present on anti-phishing blocklists.

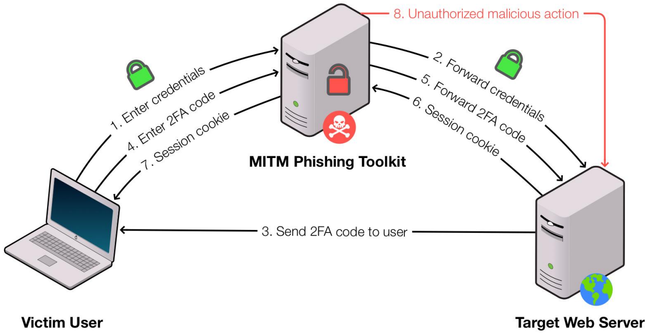
MITM Phishing Toolkit Detection

MITM phishing toolkits exhibit unique properties on the network-level which can be used to detect them from the client-side. These properties include:

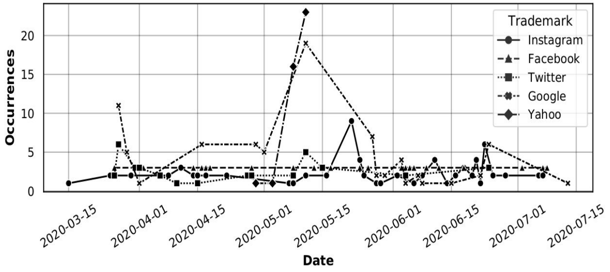
- Large network packet RTTs
- Unusual TLS library usage
- Support for outdated and vulnerable TLS versions

Using these features, we created a machine learning classifier capable of detecting these toolkits with **98.9% accuracy**.

Due to their usage of unique TLS libraries, requests from these toolkits can also be detected by targeted web servers, allowing for the flagging of suspicious authentication requests.



Architecture of MITM Phishing Toolkits



MITM phishing toolkits detected during our observation period.

Phishing Website Discovery

Using our classifier, we analyzed domains from popular anti-phishing lists and Certificate Transparency logs to search for MITM phishing toolkits in the wild over the course of 114 days.

In total, **we discovered 348 MITM phishing toolkits** targeting popular brands such as: Yahoo, Google, Twitter, and Facebook.

We find that **MITM phishing toolkits occupy a blindspot of the anti-phishing ecosystem,** as only 4.6% of domains and 8.03% of IP addresses associated with these toolkits are listed by such services.