TECHNION
Israel Institute
of Technology

Resilient C&C Infrastructure Based on Reddit

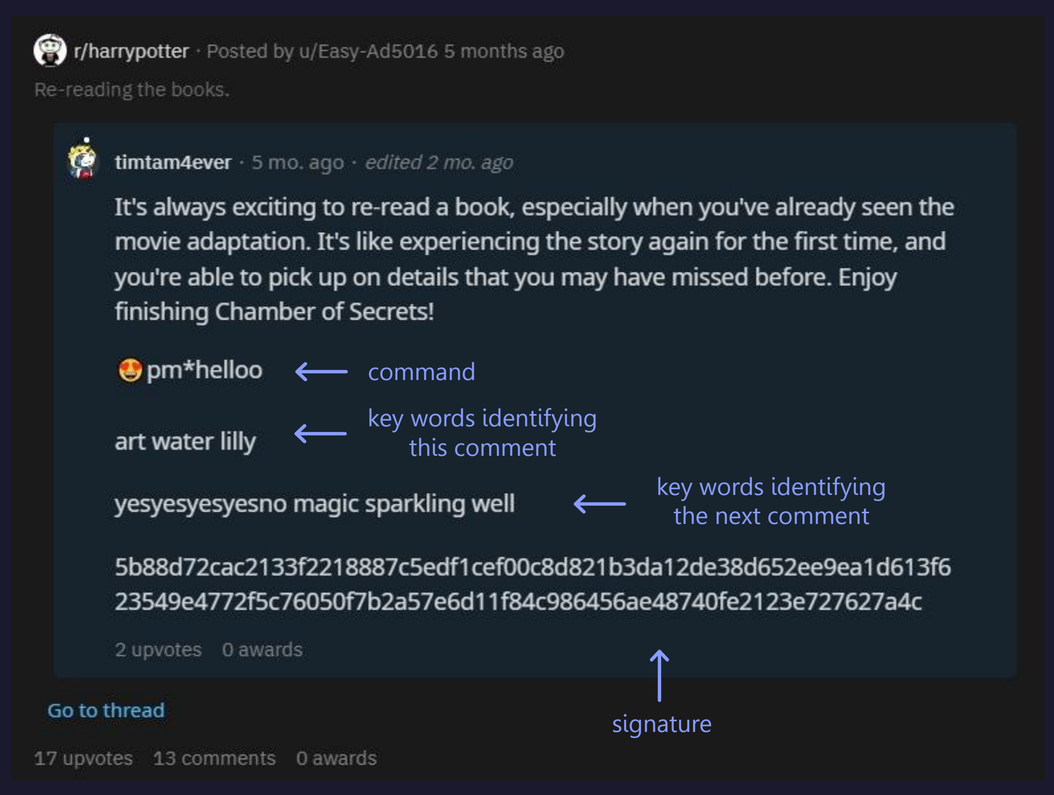
Anna Novin and Barak Sofir supervised by Amichai Shulman

MOTIVATION

Command and Control (C&C) infrastructure is a critical component of any modern cyber attack campaign.
Presently, most of the C&C infrastructures rely on server-based systems, which are expensive to maintain and require complicated technical skills to operate them in a stealthy and resilient way.
The disruption and dismantling of these servers consequently incapacitate the attack communication, effectively bringing the campaign to a standstill.

GOALS

The goal of our project is to create a highly resilient, virtually undetectable C&C infrastructure based on a public platform. The infrastructure should be cost-effective to implement and maintain. Also, it must recover swiftly after disruptions attempts.



OUR SOLUTION

We have developed a sophisticated C&C infrastructure that seamlessly integrates into the existing infrastructure of Reddit, by concealing the command messages in comments on existing content. This innovative approach effectively hides communication in plain sight.

Leveraging the search functionality of Reddit, we established a link between the controller and the bot. This is accomplished by using everyday keywords embedded within the command message.

Intriguingly, commands are identified only by these keywords and not by the user that posted the comment, making it harder to detect or dismantle the infrastructure.

Each control message serves as a breadcrumb to the next - by incorporating the keywords for the subsequent command into the current one, creating a continuous and hard-to-detect chain of commands.

We have made a significant finding that it is possible to create a Reddit account using a false email address, combined with breaking through the reCAPTCHA security measure. This revelation allowed us to establish an under-the-radar reverse communication channel from the bot back to the controller, based on comments as well.

Interestingly, not only do our comments comply with Reddit's policy, but they also prompt positive interactions from legitimate users. This unexpected engagement stands as compelling evidence that our covert infrastructure effectively remains undetectable.