Golden Chickens: Uncovering A Malware-as-a-Service (MaaS) Provider and Two New Threat Actors Using It

medium.com/@quoscient/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using-61cf0cb87648

QuoScient GmbH June 26, 2020

QuoScient GmbH

Nov 29, 2018

.

3 min read

This article was initially written by the QuoINT Team as part of QuoScient GmbH. Since the foundation of QuoIntelligence in March 2020, this article was transferred to the QuoIntelligence website on 21 April 2020.

Executive Summary

Over the last few years, QuoScient's Intelligence Operations Team (QuoINT) has tracked activities attributed to the Cobalt group, and observed their notable evolution and continuously improving Tactics, Techniques, and Procedures (TTPs).

Since September 2018, we have identified multiple attacks that share similar TTPs used by Cobalt during a specific timeframe but exhibit enough differences to attribute them to separate threat actors. This blog post provides an overview on a specific Malware-as-a-Service (MaaS) used within the e-Crime threat actor landscape. It also provides details on two different threat actors using the MaaS that fall under the umbrella of a family we dubbed *Golden Chickens*: GC01 and GC02. The success of GC operations heavily relies on a specific MaaS sold in underground forums, which provides customers with the malwares and the infrastructure they need for targeted attacks. The service owner provides the MaaS through the use of the following toolkits: Venom and Taurus building kits for crafting documents used to deliver the attack, and the more_eggs (aka Terra Loader, SpicyOmelette) backdoor for taking full control of the infected computer.

Between November 2017 and July 2018, we attributed to GC02 five spear phishing waves which indiscriminately targeted companies and organizations in at least India and the United States. As a result of using the same MaaS provider, GC02 and Cobalt group's TTPs and

infrastructure strongly overlapped in May 2018, making it hard at first glance to differentiate the two threat actors.

Between August and October 2018, we attributed to GC01 nine spear phishing waves targeting multiple companies and organizations operating in the financial industry. Throughout the campaign, we observed the installation of multiple Remote Access Tool (RAT) variations as the result of a successfully compromised victim machine.

By highlighting the multi-layer infrastructure adopted by Cobalt and Golden Chickens, as well as the multi-client business model of the MaaS behind it, we emphasize the difficulty of performing reliable attribution for cyberattacks, and the high uncertainty that analysts are confronted with during the process. To note, other researchers reported the same Indicators of Compromise (IoC) and C2 infrastructure covered in this blog post. We hope that our attribution will clarify the current threat landscape and make the covered threat actor profiles more accurate.

The following blog post is a preview of the Intelligence Assessment we will disseminate to our clients, partners, and vetted .

Introduction

Cyber attribution is becoming increasingly challenging as threat actors frequently use false flag techniques and shared infrastructure to increase the resiliency of their operations against takedowns and law enforcement investigations. Especially for e-Crime actors, it is a common practice to rent the same bulletproof infrastructure or botnet used by other e-Crime groups, resulting in the increased likelihood for an overlap of C2 servers. In the last years, we have noted a tendency of threat actors outsourcing even more parts of the kill-chain to third parties by using/offering MaaS solutions. Figure 1 shows an example of such a network where multiple stakeholders are involved.

, please visit the official QuoIntelligence Blog or access the article here: .