ShellClient RAT

Overview

Security researchers recently unveiled a long-standing campaign that was being carried out by a new Iranian threat actor known as MalKamak. The campaign, dubbed Operation Ghostshell, leveraged a previously unknown remote access trojan (RAT) called ShellClient with the end goal of stealing sensitive information about critical assets, organizations' infrastructure, and technology.

A key part of how ShellClient can avoid detection by traditional security solutions is that it uses legitimate cloud services, such as Dropbox, for command-and-control (C2) communications. In doing so, the attacker can blend in with normal web traffic moving in and out of the targeted organization's infrastructure. Within Dropbox, the attacker stores three folders that contain information about the infected machines, what commands are to be executed by the RAT itself, and the results of these commands.

Lookout Analysis

SaaS apps and cloud services are common attack targets with huge risk surfaces. Not only is the cloud a target, but it's also leveraged by attackers as a threat vector used to carry out reconnaissance and exfiltrate sensitive data as exemplified by this campaign. Since using legitimate cloud services as a C2 host enables attackers to fly under the radar, there's been significant growth in this tactic.

This incident exemplifies why most cloud exposures and leaks are due to misuse of the cloud services, user errors, and poor governance on the customer side. As people access these services from more places, there also needs to be a way to ensure that mobile users and devices are included in the dynamic access and data handling policies in place. Doing so enables you to continuously monitor all traffic to your cloud and apply user behavior analytics to identify malicious activities.

Recommendation for Lookout Admins

This incident exemplifies how critical it is to be able to monitor traffic into and out of your cloud-based apps and infrastructure. With Lookout CASB, admins can distinguish between corporate and personal accounts accessing their cloud infrastructure. Using this as a signal for cloud access and data loss prevention policies helps mitigate the risk of attackers using legitimate cloud services as C2 hosts. Lookout admins can set policies that only allow corporate accounts for services such as Dropbox to access the organization's infrastructure and data.

Lookout Cloud Access Security Broker (CASB)

Lookout Cloud Access Security Broker (CASB) provides full visibility into the interactions between users, endpoints, cloud apps and your data. It also enables you to dynamically dial in Zero Trust access controls. With continuous monitoring of user and entity behavior analytics (UEBA), you can detect and respond to insider threats and advanced cyberattacks. We provide advanced data loss prevention that can classify, encrypt and restrict sharing of your data on the fly so that only authorized users have access.

Click here to learn more about Lookout CASB