THREAT BRIEF

Gartner
COOL VENDOR 2020™

TwoFace

Beating an ASPX Shell Game • Spring 2019

TwoFace is a malicious ASPX web shell originally exposed in 2017. Its two “faces” are HighShell and HyperShell, which were tools leaked in 2019 and used by the Iranian hacker group APT34. A TwoFace attack is delivered in two stages and, if successful, can easily grant attackers access to the compromised webserver. The first stage is a lightweight loader that infects vulnerable webservers running the Microsoft ASP.NET framework, hiding the more dangerous second-stage payload encrypted within. Attackers can later instruct the loader to decrypt and activate the second-stage shell.

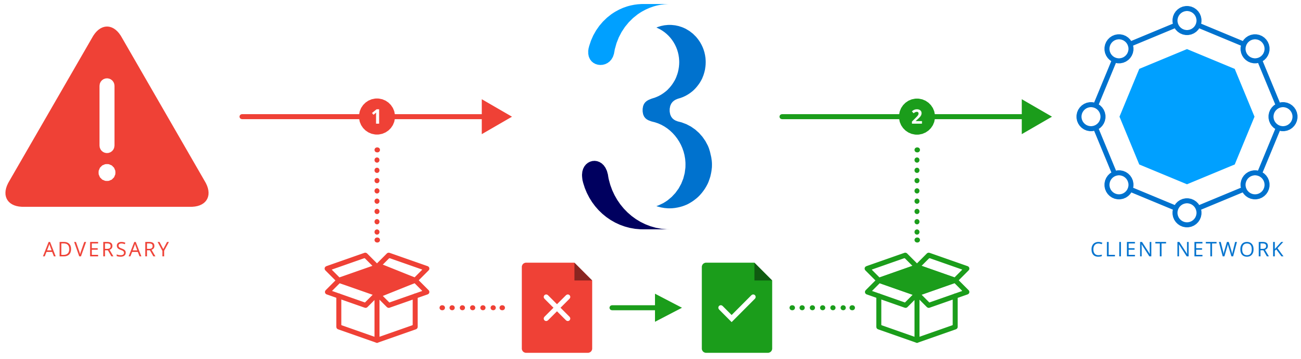
The first stage of TwoFace, HighShell, is relatively small and, once it has been placed on an ASP.NET webserver, masquerades as a legitimate login page. The second stage, HyperShell, remains dormant and undetectable until remotely activated. Once activated, TwoFace allows an attacker to control the compromised server, harvest user credentials, upload malicious files, or extract sensitive data. Attackers can also pivot from infected webservers to move laterally, compromising other assets on the network.

Hijacking the Attacker’s Disguised Web Shells

Trinity Cyber detects TwoFace by analyzing HTTP traffic at the session level, allowing us to identify multiple characteristics of TwoFace web shells in real time, even when they are heavily disguised. This ensures we detect the upload of either HyperShell or HighShell, as well as the subsequent command-and-control (C2) traffic used to activate the second-stage payload.

When we detect TwoFace, we enact one of several imperceptible measures to neutralize the threat without revealing our tactics to the attacker. This may include removing the TwoFace content, altering its cryptographic properties, or forcing all of the attacker’s attempts at authentication to fail. Based on a client’s preference, we can even fool the attacker into believing they have successfully uploaded the first-stage web shell. Lastly, when we encounter attempts to authenticate or C2 traffic to or from a TwoFace web shell, we can invisibly alter that traffic, disrupting the attack in flight.

Trinity Cyber’s unique position between the Internet and the network, cutting-edge technology, and unique actions protect our clients by preventing both deployment and interaction with TwoFace.



sales@trinitycyber.com • (240) 842-9900 • trinitycyber.com

Trinity Cyber was named a Cool Vendor in Gartner’s Cool Vendors in Network and Endpoint Security, Mark Harris, Rob Smith, et al., 30 September 2020.

Trinity Cyber