TwoFace (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 14:31:04 UTC

TwoFace

aka: Minion, HighShell, HyperShell, SEASHARPEE

Actor(s): APT27, APT34, OilRig, Turla, UNC215

According to Unit42, TwoFace is a two-staged (loader+payload) webshell, written in C# and meant to run on webservers with ASP.NET. The author of the initial loader webshell included legitimate and expected content that will be displayed if a visitor accesses the shell in a browser, likely to remain undetected. The code in the loader webshell includes obfuscated variable names and the embedded payload is encoded and encrypted. To interact with the loader webshell, the threat actor uses HTTP POST requests to the compromised server.

The secondary webshell, which we call the payload, is embedded within the loader in encrypted form and contains additional functionality that we will discuss in further detail. When the threat actor wants to interact with the remote server, they provide data that the loader will use to modify a decryption key embedded within the loader that will be in turn used to decrypt the embedded TwoFace payload. Commands supported by the payload are execution of programs, up-, download and deletion of files and capability to manipulate MAC timestamps.

References

2022-07-18 · Palo Alto Networks Unit 42 ·
Evasive Serpens
TwoFace ISMAgent ISMDoor OopsIE RDAT OilRig

2021-12-14 · Recorded Future · Insikt Group®
Full Spectrum Detections for 5 Popular Web Shells: Alfa, SharPyShell, Krypton, ASPXSpy, and TWOFACE
TwoFace

2021-12-14 · Recorded Future · Insikt Group
Full Spectrum Detections for 5 Popular Web Shells: Alfa, SharPyShell, Krypton, ASPXSpy, and TWOFACE
TwoFace ASPXSpy SharPyShell

2020-11-27 · PTSecurity · Alexey Vishnyakov, Denis Goydenko
Investigation with a twist: an accidental APT attack and averted data destruction
TwoFace CHINACHOPPER HyperBro MegaCortex MimiKatz

2020-09-25 · Emanuele De Lucia
APT vs Internet Service Providers
TwoFace RGDoor

2020-06-18 · Australian Cyber Security Centre · Australian Cyber Security Centre (ACSC)
Advisory 2020-008: Copy-Paste Compromises –tactics, techniques and procedures used to target multiple Australian networks
TwoFace Cobalt Strike Empire Downloader

2020-03-12 · Recorded Future · Insikt Group
Swallowing the Snake's Tail: Tracking Turla Infrastructure
TwoFace Mosquito

2020-01-01 · Secureworks · SecureWorks
COBALT GYPSY
TwoFace MacDownloader BONDUPDATER pupy Helminth jason RGDoor TinyZbot OilRig

2020-01-01 · FireEye · Mandiant, Mitchell Clarke, Tom Hall
Mandiant IR Grab Bag of Attacker Activity
TwoFace CHINACHOPPER HyperBro HyperSSL

2019-08-22 · Cyware · Cyware
APT34: The Helix Kitten Cybercriminal Group Loves to Meow Middle Eastern and International Organizations
TwoFace BONDUPDATER POWRUNER QUADAGENT Helminth ISMAgent Karkoff LONGWATCH OopsIE PICKPOCKET RGDoor VALUEVAULT

2019-07-08 · SANS · Josh M. Bryant, Robert Falcone
Hunting Webshells: Tracking TwoFace
TwoFace

2019-04-17 · Malware Reversing Blog · F-Secure Global
The Dukes: 7 Years Of Russian Cyber-Espionage
TwoFace BONDUPDATER DNSpionage

2019-02-13 · Youtube (SANS Digital Forensics & Incident Response) · Josh Bryant, Robert Falcone
Hunting Webshells: Tracking TwoFace - SANS Threat Hunting Summit 2018
TwoFace

2018-07-07 · Youtube (SteelCon) · Dan Caban, Muks Hirani
You've Got Mail!
TwoFace

2017-12-11 · Palo Alto Networks Unit 42 · Robert Falcone
OilRig Performs Tests on the TwoFace Webshell
TwoFace

2017-07-31 · Palo Alto Networks Unit 42 · Bryan Lee, Robert Falcone
TwoFace Webshell: Persistent Access Point for Lateral Movement
TwoFace OilRig

Yara Rules

▶ [TLP:WHITE] asp_twoface_w0 (20190503 | No description)

Download all Yara Rules

Source: https://malpedia.caad.fkie.fraunhofer.de/details/asp.twoface