

# HOW AN END-TO-END FILELESS ATTACK TAKES PLACE

**78%** OF ORGANIZATIONS ARE CONCERNED WITH FILELESS ATTACKS\*

**83%** OF SECURITY PROFESSIONALS WANT MORE INFORMATION ABOUT FILELESS ATTACKS\*\*

\*ESG TRENDS IN ENDPOINT SECURITY SURVEY 2017 \*\*CROWDSTRIKE FILELESS WEBCAST SURVEY

To explain how fileless attacks work, this infographic illustrates a real-world fileless intrusion uncovered by the CrowdStrike Services incident response (IR) team. See how a skillful adversary can avoid detection and conduct a successful attack without writing malicious executable files to disk.

FOR EACH STEP OF THE ATTACK, THE ADVERSARY HAS THREE ELEMENTS: A GOAL, A TOOL AND A TECHNIQUE

01

## GOAL: GAIN ACCESS

The attacker gains remote access to the victim's system, to establish a beachhead for his attack.

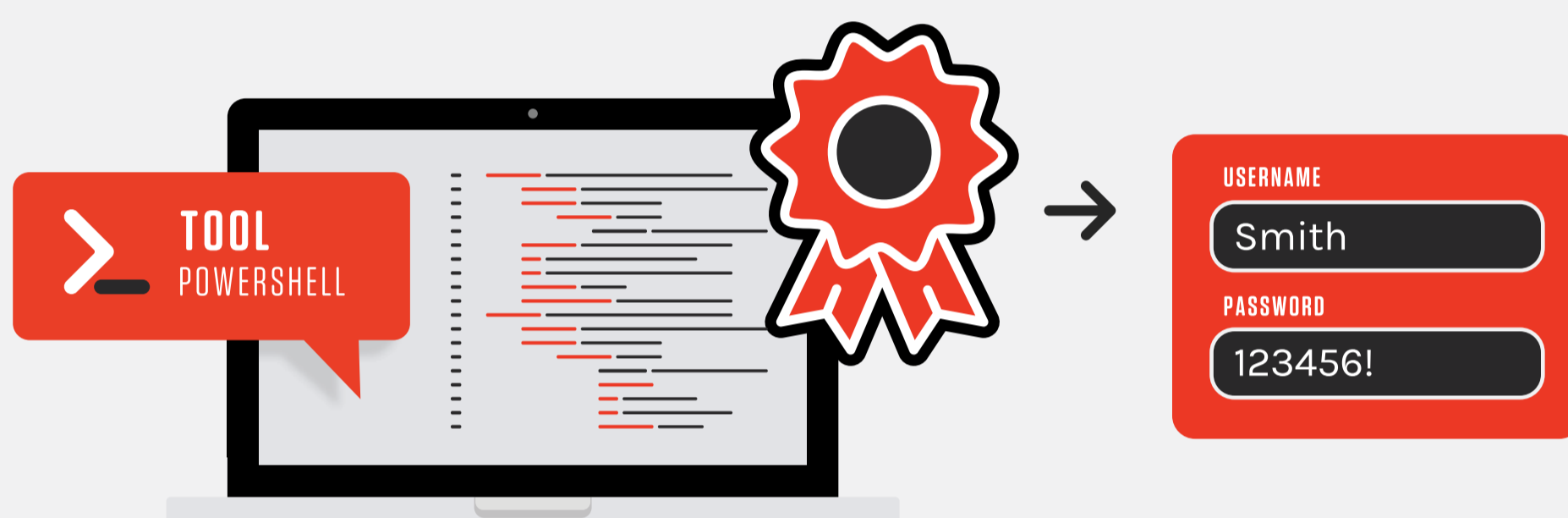


**TECHNIQUE:** REMOTELY EXPLOIT A VULNERABILITY AND USE WEB SCRIPTING FOR REMOTE ACCESS, E.G. CHINA CHOPPER.

02

## GOAL: STEAL CREDENTIALS

Using the access gained in the previous step, the attacker now tries to obtain credentials for the environment he has compromised, allowing him to easily move to other systems in that environment.

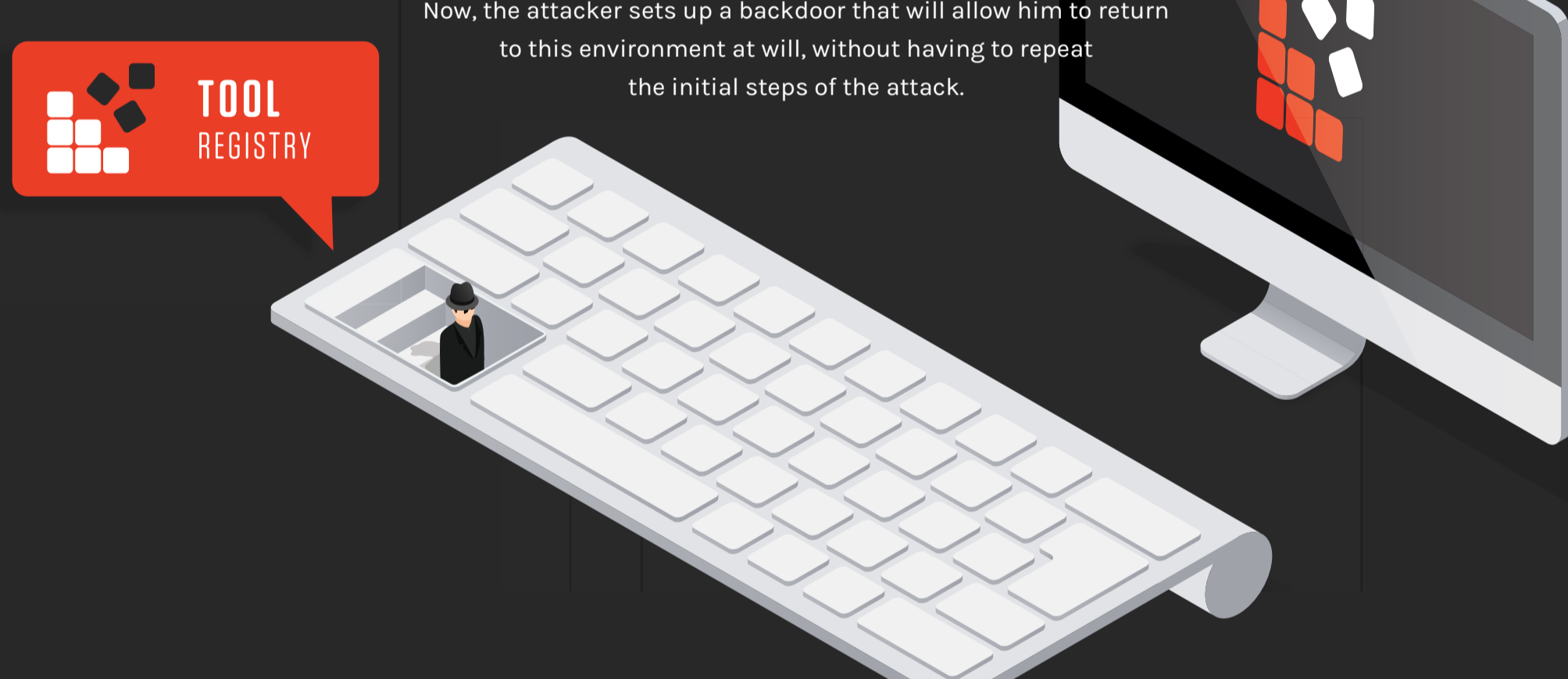


**TECHNIQUE:** RUN A POWERSHELL SCRIPT TO DUMP CREDENTIALS, E.G. MIMIKATZ.

03

## GOAL: MAINTAIN PERSISTENCE

Now, the attacker sets up a backdoor that will allow him to return to this environment at will, without having to repeat the initial steps of the attack.

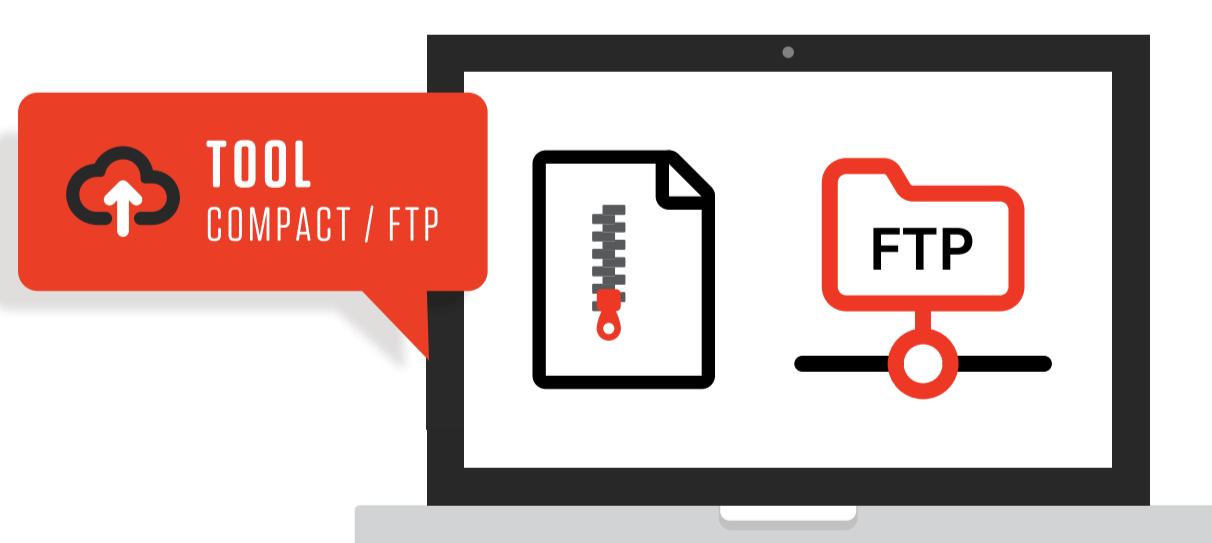


**TECHNIQUE:** MODIFIES REGISTRY TO CREATE A BACKDOOR E.G. STICKY KEYS BYPASS.

04

## GOAL: EXFILTRATE DATA

In the final step, the attacker gathers the data he wants and prepares it for exfiltration, copying it in one location and then compressing it using readily available system tools such as Compact. The attacker then removes the data from the victim's environment by uploading it via FTP.



**TECHNIQUE:** USES FILE SYSTEM AND BUILT-IN COMPRESSION UTILITY TO GATHER DATA, THEN USES FTP TO UPLOAD THE DATA.

### 3 KEY TAKEAWAYS

- 1-THE THREAT OF FILELESS ATTACKS IS REAL
- 2-TRADITIONAL DEFENSES CANNOT STOP FILELESS ATTACKS
- 3-SECURITY TEAMS NEED TO THINK BEYOND MALWARE AND FOCUS ON STOPPING THE BREACH

### LEARN MORE:

**WATCH AN ON-DEMAND VIDEO:** Understanding Fileless Attacks and How to Stop Them

**READ THE WHITE PAPER:** Who Needs Malware? How Adversaries Use Fileless Attacks to Evade Your Security

**VISIT OUR WEBSITE** to learn how the CrowdStrike Falcon Platform® prevents and detects fileless attacks with a single lightweight agent