ANATOMY OF A SHELLSHOCK ATTACK

"Shellshock" is the name of a serious bug in Bash, a shell commonly used in computers running Linux, UNIX and OS X. Shellshock could allow an attacker to execute malicious commands across the Internet on remote computers, notably web servers.

THE BUG

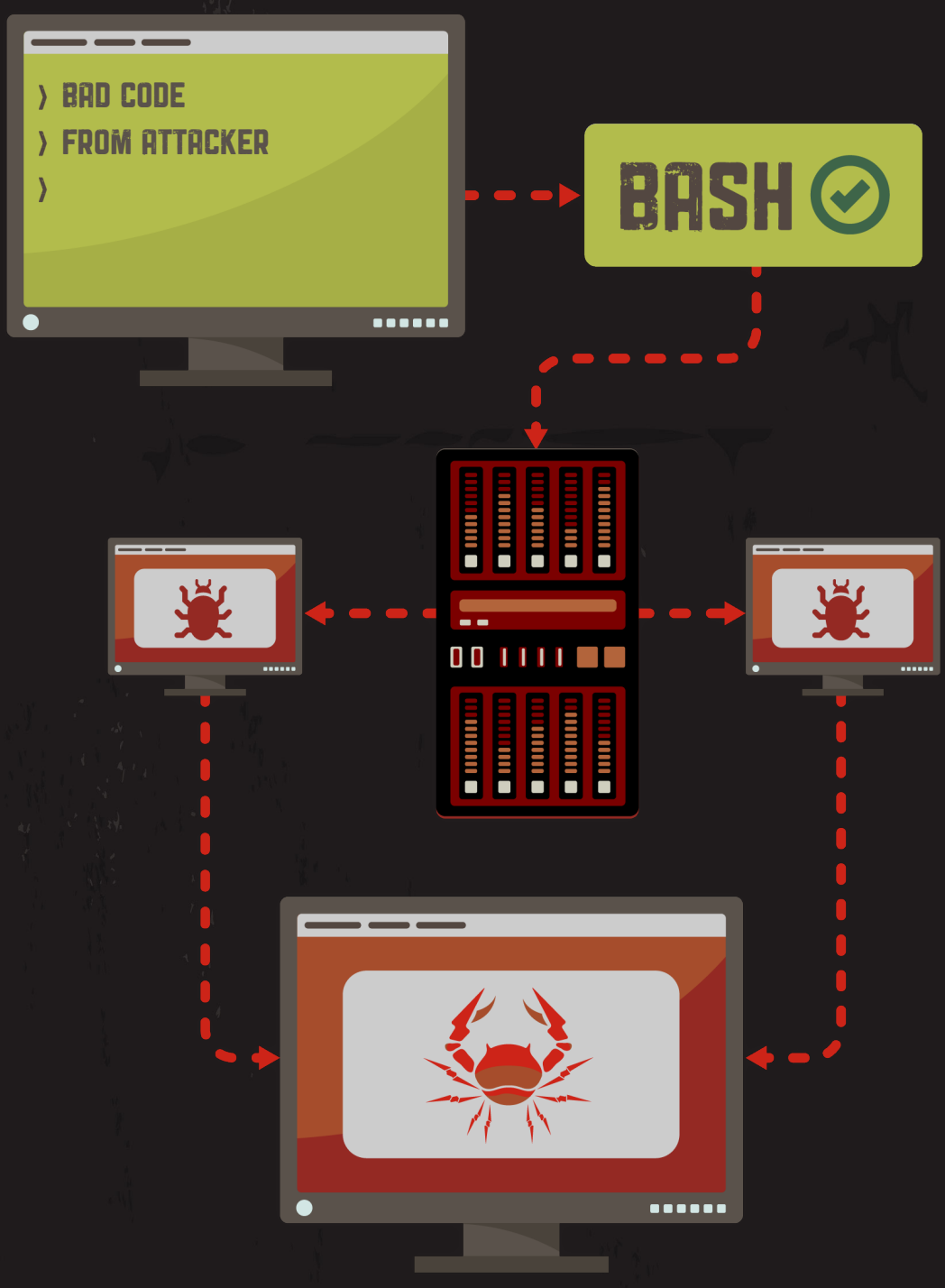
Because of a flaw in the way Bash handles data requests, it can be tricked into executing unexpected commands, what is known as command injection.

```
~ User$ F="() { echo Expected; }; echo NOT Expected"
NOT Expected
Expected
```

THE THREAT

An attacker can exploit Shellshock by injecting malicious commands into a website to compromise a server.

Once the server is under the cybercriminals' control, they can drop malware on the server to steal data, compromise other computers, or launch Distributed Denial of Service (DDoS) attacks.



THE PROTECTION

Sophos products protect against Shellshock attacks in several ways:

- Sophos Antivirus blocks malware-related payloads exploiting Shellshock in Linux, UNIX and OS X.
- Web Application Firewall (WAF) and Intrusion Prevention System (IPS) rules in Sophos UTM stop Shellshock requests before they reach the server.
- Advanced Threat Protection (ATP) in Sophos UTM blocks malware call-home attempts, and creates a threat alert for malicious traffic.

SHAKE OFF SHELLSHOCK

To learn how, visit **sophos.com/shellshock**

SOPHOS