script kiddie

Ben Lutkevich, Technical Features Writer

What is a script kiddie?

Script kiddie is a derogative term that computer hackers coined to refer to immature, but often just as dangerous, exploiters of internet security weaknesses.

Not all novice hackers are script kiddies. Some inexperienced attackers do try to learn about and understand the tools they use. Script kiddies aren't interested in learning and understanding the exploits they use, instead using what is easy to find and available.

What are the characteristics of a script kiddie?

The typical script kiddie uses existing, well-known techniques, programs and scripts to find and exploit weaknesses in internet-connected computers. Their attacks are random and with little understanding of the tools they are using, how they work and the harm they cause.

Script kiddies are typically motivated by simple, personal reasons -- to have fun, create chaos, seek attention or take revenge.

Hackers view script kiddies with contempt because they do not advance the art of hacking or contribute to the development of hacking culture. Also, script kiddies can do major damage. As a result, they can unleash the wrath of security authorities on the entire hacker community. The media often portrays script kiddies as bored teenage loners seeking recognition from their peers.

What is the origin of script kiddie?

The term *script kiddie* first appeared in hacker zines, blogs, message boards and Internet Relay Chat in the mid-1990s. It was used to describe people who downloaded a tool without knowing or caring how it worked.

The exact origin of the term is unknown. Some early uses of script kiddie and related terms include the following:

- **1993.** Terms such as *k0deZ kiddies* appeared on an internet message board called Yabbs.
- **1996.** According to the hacker blog LiveOverflow, the term *script kiddie* appeared in the comments of a Unix exploit.
- **1998.** The hacking zine Phrack made reference to "script kiddie behavior" in one of its articles.

More recently, the term was used in several episodes of the television series *Mr. Robot*.

What is the difference between a hacker vs. a script kiddie?

Hackers and script kiddies differ in three areas:

1. **Level of experience.** Script kiddies are less experienced with cybersecurity exploits than real hackers. They generally cannot write exploits or scripts on their own, so they use programs written by other people and found on the internet.
2. **Skills.** Script kiddies have less developed hacking skills than more advanced, well-organized threat actors. As a result, they often use attacks that are easier to perform. They may prepare less for an attack, doing little research before launching it. They are also more likely to give up if their easy exploit doesn't work in the first few tries. Experienced hackers have the programming and computer networking knowledge to adapt their attacks to dynamic internet security defenses. They can interpret a situation and adapt to new scenarios.
3. **Intent.** Script kiddies are more likely to perform exploits for personal acclaim or to troll. They don't always understand the tools they use and pay less attention to the consequences of hacking. A hacker will take pride in the quality of an attack, such as leaving no trace of an intrusion, for example. Most experienced threat attackers understand the consequences and ethics of what they do. By comparison, a script kiddie often focuses on quantity, seeing the number of attacks that can be mounted to get attention and notoriety.

There's an added level of complexity to what hackers do compared to script kiddies. Because of that, there are many different types of hackers, and they are categorized based on intent.

For example, ethical hackers seek vulnerabilities and perform exploits where they know it is legal to do so. They often work as penetration testers, who are information security professionals paid to test an organization's network and computer systems for vulnerabilities.

Script kiddies don't fit in hacker categories because they lack the skills, experience and general competence.

Examples of script kiddies

Script kiddies are not talented hackers, but they are still capable of performing exploits with powerful consequences. Some examples of low-skill but potentially detrimental exploits that script kiddies might pull off include the following:

- **Denial of service (DoS)** attacks overwhelm the target server, network or website with traffic so that the target cannot provide service to its users. Off-the-shelf hacking programs that enable users to perform DoS attacks are easy to find on the internet.
- **Social engineering**, such as the various types of phishing attacks, deal less with manipulating code and more with manipulating people. A social engineering attack may be as simple as sending emails with malicious links that contain free malware, which the script kiddie can use to steal the victim's personal data.
- **Website defacement** is attractive to script kiddies because the skills needed -- web development and Hypertext Markup Language -- are simple to learn. Defacing a website can get the attention script kiddies crave, while damaging the website owner's image.

Real-world script kiddie attacks include the following:

- **2015 U.K. distributed DoS (DDoS) attacks.** Police in the U.K. arrested six teenagers for allegedly using a DDoS tool to attack corporate websites and other entities. The tool used was hacker group Lizard Squad's Lizard Stresser.
- **2016 Mirai DDoS attacks.** The Mirai botnet DDoS attacks relied heavily on DDoS-for-hire services, such as the website Webstresser.org. With these services, anyone can buy DDoS attacks and launch them with little or no technical skill.

The bottom line: Script kiddies are unskilled but dangerous

A script kiddie is considered a bad thing to be in the hacker community. They are often less skilled, experienced and knowledgeable than true hackers.

Hackers view them with contempt because they use powerful hacking tools with little understanding of how they work and of the consequences. Many of these tools are open source and free to use for script kiddies and more experienced hackers alike.

Learn how cybercriminals can take advantage of open source tools to attack vulnerable enterprise systems and what security professionals can do to prepare.

This was last updated in October 2021