HACKER AUTOMATION

How Hacker Automation Changed the Attack

Hackers now leverage sophisticated tools, including AI and Robotic Process Automation (RPA), to automate every stage of an attack.

Dennis Underwood, Founder & CEO, Cyber Crucible · November 2026

EXECUTIVE SUMMARY

The cybersecurity landscape is in a state of continuous evolution, but perhaps no trend is as transformative and dangerous as the rise of **hacker automation**. Once a domain of manual, human-driven attacks, cybercrime has shifted into a hyper-efficient, machine-speed operation. This two-part series explores the evolution of hacker automation, from its early roots in simple scripts to today's sophisticated, AI-powered "smash and grab" attacks. It will detail the specific tactics that make these automated attacks so effective, the critical vulnerabilities they exploit, and the necessary paradigm shift in defense strategies required to combat them.

01 The Evolution of Cyberattacks: From Manual to Automated

In the early days of hacking, attacks were a laborious, manual process. A hacker would spend days or weeks on reconnaissance, manually scanning networks, and crafting a unique payload. This "human-in-the-loop" model meant that attacks were slower, less scalable, and more detectable. Today, this model is a relic. Hackers now leverage sophisticated tools, including AI and Robotic Process Automation (RPA), to automate every stage of an attack:

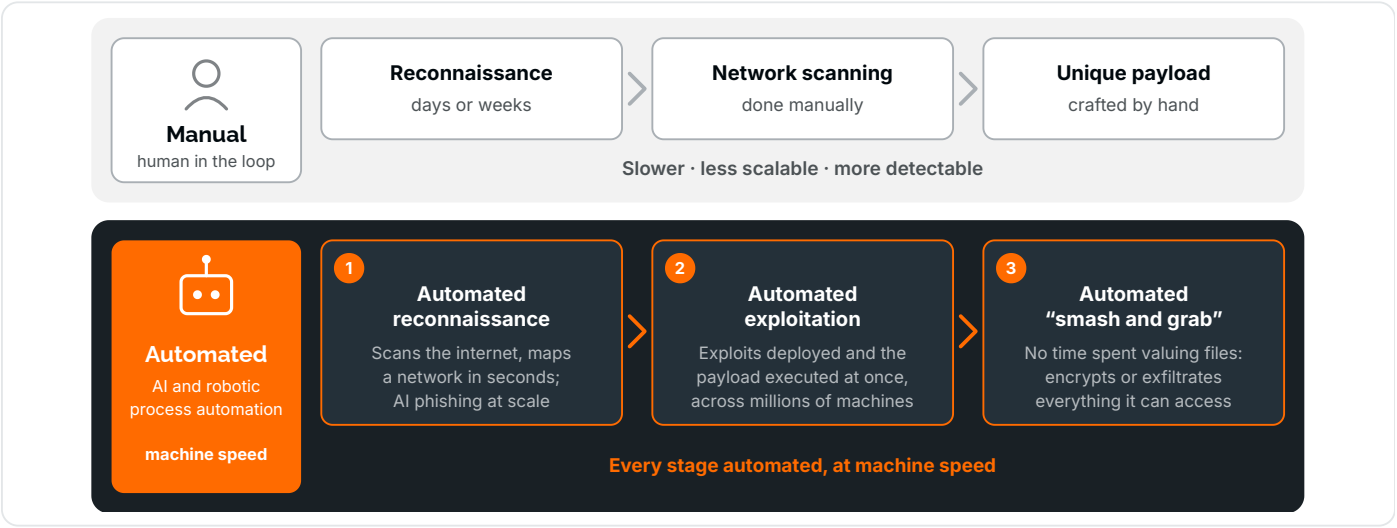

Figure 1. The manual, human-in-the-loop attack chain and the automated one that replaced it

- **Automated Reconnaissance:** Tools can now automatically scan the internet for vulnerable systems and map a target's network in seconds. They can also use AI to craft highly convincing phishing emails at a massive scale.
- **Automated Exploitation:** Once a vulnerability is found, automated frameworks can immediately deploy exploits and execute a malicious payload. The speed of this process is critical; a hacker can exploit a zero-day vulnerability across millions of machines before a human could even register the alert.
- **Automated "Smash and Grab" Attacks:** The most dangerous evolution is the move away from targeted, data-inspection attacks. Modern ransomware and data theft are now fully automated. The malware doesn't waste time trying to determine the value of a file; it encrypts or exfiltrates everything it can access at machine speed.

02 Automated Surveillance and Attack Patterns: Relying on Known Data Points

One of the most critical aspects of hacker automation is its reliance on **predictable, known data points** across all operating systems. Since hackers do not have specific knowledge of a

victim's unique environment, their automated tools must be programmed to operate based on universal assumptions about how computers are structured. This creates a predictable pattern of surveillance and attack that, while efficient for the attacker, also reveals a critical vulnerability in their methodology.

Hackers use automated tools to conduct surveillance and plan attacks based on these common locations:

- **User Profile and Desktop Locations:** Regardless of whether the victim uses Windows, macOS, or Linux, there is a known, predictable location for user profiles and the desktop. For example, on a Windows machine, the path is typically `C:\Users\[Username]`. An automated script can easily find all user directories on a compromised machine, bypassing the need for a human to manually inspect the file system. The script doesn't care what the user's name is; it simply follows the known path to find the data.
- **Drive Letters:** In Windows environments, attackers rely on the predictable nature of drive letters (e.g., `C:\`, `D:\`). Automated attacks can quickly scan all available drive letters to locate and encrypt network drives, external hard drives, or other storage partitions that are mounted to the system.
- **Common Application Data Folders:** All operating systems have known locations for application data, configuration files, and browser data. An automated tool can be programmed to immediately target these directories to steal credentials, cookies, and other sensitive information.

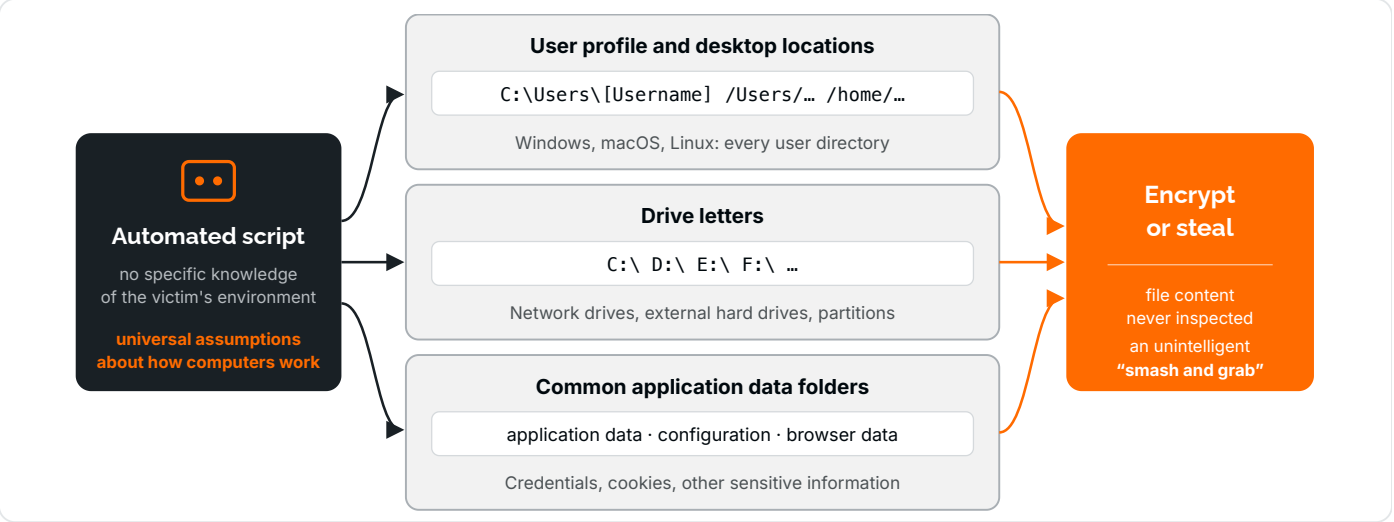

Figure 2. What automated surveillance keys on: the same known locations on every machine

The hacker's surveillance and attack pattern is not a meticulous, thoughtful process. It's an **unintelligent "smash and grab"** that exploits these known data points. The script doesn't care about the content of the files; it simply knows that by targeting `C:\Users`, it's highly likely to find valuable data to encrypt or steal. This automated, surveillance-based attack is a direct counter to any defense that relies on the attacker needing to manually navigate and understand a specific network environment.

03 The Shift to Identity Theft for Persistent Access

A key evolution in hacker automation is the strategic shift away from prolonged persistence within a victim's network. Instead of staying in the victim's environment after initial access, hackers prioritize **targeting known locations of digital identity information**, such as session tokens and passwords. This allows them to quickly exfiltrate this crucial data and then retreat from the network.

The purpose of this strategy is to:

1. **Reduce Risk:** Staying in a victim's network increases the risk of being detected by security teams or Endpoint Detection and Response (EDR) tools. By exfiltrating identity data and leaving, the hacker can analyze the stolen information at their leisure in a safe environment.
2. **Ensure Easy Return:** With a stolen session token, password, or VPN key, the hacker can return to the network at any time by simply logging in as an authorized user. This grants them a backdoor that is legitimate from the perspective of the network's authentication system.

Automated tools are specifically designed to find this identity information. For example, a script may navigate to the user's folder (`C:\Users\[Username]\`) and then follow a known path to an Edge browser's credential store or a standard location for VPN keys. These are predictable data points that the automated tool can target without any specific knowledge of the victim's unique network configuration. The script doesn't need to stay and surveil; it just needs to find the "keys to the kingdom," grab them, and run.

Related papers

- **Part 2 of 2:** Machine Speed vs Human Speed: Why Only Automated Prevention Keeps Up www.cybercrucible.com/intelligence-hub/machine-speed-vs-human-speed
- **Ransomware Defense:** The Technical and Business Failures of Ransomware Key Capture Defense www.cybercrucible.com/intelligence-hub/ransomware-key-capture-defense-failures

Read online (six languages): www.cybercrucible.com/intelligence-hub/how-hacker-automation-changed-the-attack
Book a live technical demo: www.cybercrucible.com/demo