REMOTE ACCESS TOOLS

Remote Access Tools and the Hybrid Attack

The Fusion of Remote Access Tools and Hacker Automation

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

EXECUTIVE SUMMARY

The modern cybersecurity threat landscape is defined by its speed and autonomy. While ransomware has traditionally been the headline-grabbing threat, a more insidious and sophisticated form of attack is emerging: the fusion of remote access tools (RATs) with hacker automation. This white paper will explore how attackers are leveraging pre-built surveillance and theft capabilities within remote access tools to conduct completely autonomous operations. It will contrast the network dependencies of these attacks with the more self-sufficient nature of ransomware and detail the new hybrid methodologies attackers are employing to achieve both rapid and long-term data theft.

01 The Evolution of Remote Access as an Attack Vector

Remote access tools (RATs) were originally designed for legitimate purposes, such as IT administration and remote support. However, hackers have long exploited these tools to gain unauthorized control over a victim's system. The latest evolution of this threat is the integration of full automation into these tools.

Hackers are now deploying RATs that, upon installation, behave entirely autonomously. They no longer require a hacker to manually navigate the victim's environment, search for data, and exfiltrate it. Instead, the tools are pre-configured to automatically conduct surveillance and theft activities, operating much like a self-guided missile.

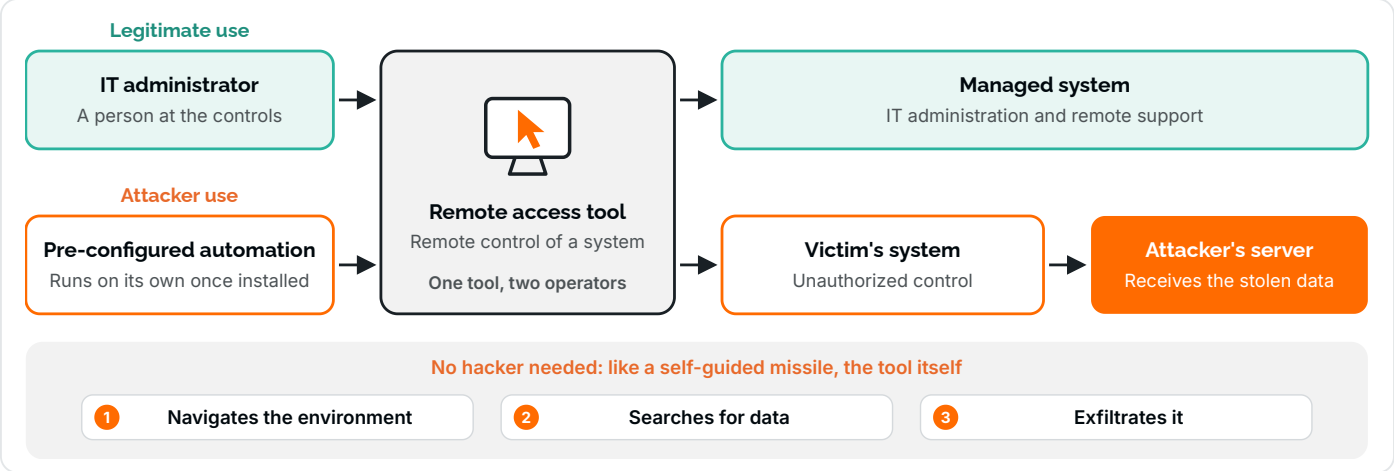

Figure 1. The same remote access tool: built for IT administration, turned into an autonomous intruder

- **Ransomware: The Self-Sufficient Threat:** Ransomware is designed for a high-impact, immediate result. Its primary goal is to encrypt data and hold it hostage, which can be accomplished with or without network access. Many ransomware variants are engineered to operate even if a machine is completely offline, ensuring the attack's success and preventing a victim from simply disconnecting from the internet to stop the encryption process. This makes ransomware a resilient, low-dependency threat.
- **Data Theft Tools: The Network-Dependent Intruder:** In contrast, data theft tools, by their very nature, require network access to succeed. The stolen data must be transmitted to a server controlled by the attacker. This dependency on a stable network connection creates a potential vulnerability for the attacker, as a disrupted connection can halt the data exfiltration process and potentially alert security teams.

A specialized subset of data theft tools, known as **infostealers**, are designed to mitigate this risk. Infostealers operate on very small, very targeted pieces of information, such as identity keys, session tokens, and passwords. Because the data packets are so small and the targets are so specific, these tools can be more easily specialized to work with minimal attacker interaction,

allowing them to perform their "smash and grab" activities and exfiltrate their small payload quickly and stealthily.

02 The Hybrid Attack: A New Frontier in Hacker Automation

Given the limitations of network-dependent data theft, attackers have developed hybrid solutions that combine the best of both automated "smash and grab" techniques with the historically effective, yet more manual, long-term data theft attack. This new methodology provides the attacker with both immediate value and future persistence.

The hybrid attack can be broken down into a two-stage, automated process:

- **Stage 1: The Automated Infostealer "Smash and Grab":** Immediately upon installation, the remote access tool's automated infostealer module executes its pre-built surveillance and theft activities. It doesn't waste time with a comprehensive search. Instead, it targets known locations of digital identity information, such as browser credential stores, email client files, and standard VPN key locations. This crucial payload is exfiltrated quickly, often in seconds. The attacker now possesses the "keys to the kingdom"—session tokens and passwords—that can be used to re-access the network at will. The tool can begin its automated sequence immediately after making first contact with the hacker's command and control server.
- **Stage 2: The Longer-Term, Exfiltration-Oriented Data Theft:** After the initial smash and grab, the attacker can use the stolen credentials to return to the network in a more methodical, less detectable manner. This allows them to conduct a more traditional data theft operation, focusing on larger volumes of data. The initial smash and grab provides a quick return on investment and a persistent backdoor, while the second stage allows for a more comprehensive and lucrative data theft operation.

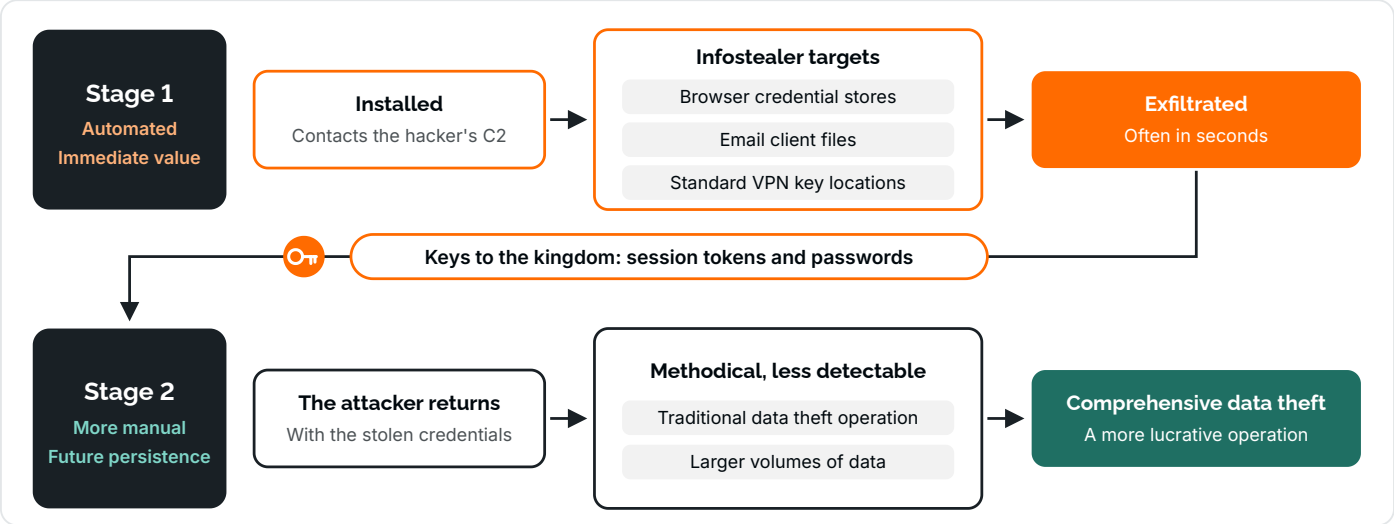

Figure 2. The hybrid attack: an automated smash and grab in seconds, then longer-term data theft with the stolen credentials

Related papers

- **Part 2 of 2:** Burned and Dormant: Why Sandbox Testing Misses Remote-Access Malware www.cybercrucible.com/intelligence-hub/burned-and-dormant-sandbox-testing-remote-access-malware
- **Hacker Automation:** How Hacker Automation Changed the Attack www.cybercrucible.com/intelligence-hub/how-hacker-automation-changed-the-attack
- **Identity Protection:** The New Digital Identity: Tokens, Keys and Wallets on the Endpoint www.cybercrucible.com/intelligence-hub/new-digital-identity-tokens-keys-wallets
- **Identity Protection:** Stealing Browser-Protected Credentials: Defeating App-Bound Encryption www.cybercrucible.com/intelligence-hub/stealing-browser-credentials-app-bound-encryption

Read online (six languages): www.cybercrucible.com/intelligence-hub/remote-access-tools-and-the-hybrid-attack
Book a live technical demo: www.cybercrucible.com/demo