Keylogger: kỹ thuật mà malware thu thập thông tin được nhập vào từ bàn phím, xác định các phím được nhập vào từ bàn phím để thu thập các thông tin nhạy cảm cần nhập xuất như mật khẩu, ID, …

RAT (Remote Access Tool): là loại phần mềm cho phép local user kết nối và truy cập được vào một máy tính remote, máy chủ hoặc network. Nó kích hoạt đường kết nối giữa 2 máy tính/ điểm kết nối được phân chia mạng và/hoặc trong các địa chỉ địa lý khác nhau. Thông thường, RAT được cài đặt trên máy tính cục bộ hoặc được triển khai qua network/Internet thông qua máy chủ remote. RATs hoạt động bằng cách tạo một kết nối giữa cục bộ và remote host qua network hoặc kết nối internet.

Credential dumping: kỹ thuật được sử dụng để thu thập thông tin xác thực – chẳng hạn như tên người dùng và mật khẩu – từ hệ thống. Nó liên quan tới việc truy cập và giải nén mật khẩu, hashes, hoặc token từ địa chỉ chẳng hạn như Windows Security Account Manager (SAM), Local Security Authority Subsystem Service (LSASS), hoặc web browsers. Kẻ tấn công sử dụng các tools như Mimikatz, ProcDump hoặc samdump2 để thực hiện kỹ thuật này.