Lizar, Software S0681 | MITRE ATT&CK®

Archived: 2026-04-02 12:14:27 UTC

Enterprise T1087 .003 Account Discovery: Email Account

Lizar can collect email accounts from Microsoft Outlook and Mozilla Thunderbird.[1]

Enterprise T1560 Archive Collected Data

Lizar has encrypted data before sending it to the server.[1]

Enterprise T1217 Browser Information Discovery

Lizar can retrieve browser history and database files.[2][1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Lizar has used PowerShell scripts.[1]

.003 Command and Scripting Interpreter: Windows Command Shell

Lizar has a command to open the command-line on the infected system.[2][1]

.006 Command and Scripting Interpreter: Python

Lizar has used Python scripts (ps2x.py script and ps2p.py) to execute files on remote hosts using the Impacket library.[1]

Enterprise T1555 .003 Credentials from Password Stores: Credentials from Web Browsers

Lizar has a module to collect usernames and passwords stored in browsers.[1]

.004 Credentials from Password Stores: Windows Credential Manager

Lizar has a plugin that can retrieve credentials from Internet Explorer and Microsoft Edge using `vaultcmd.exe` and another that can collect RDP access credentials using the `CredEnumerateW` function.[1]

Enterprise T1132 .002 Data Encoding: Non-Standard Encoding

Lizar has used a complex XOR operation to obfuscate C2 communications.[5]

Enterprise T1140 Deobfuscate/Decode Files or Information

Lizar has decrypted its configuration data, such as the C2 IP address, ports and other network communication.[1][5]

Enterprise T1573 Encrypted Channel

Lizar can support encrypted communications between the client and server.[2][1][4]

Enterprise T1105 Ingress Tool Transfer

Lizar can download additional plugins, files, and tools.[1][5][4]

Enterprise T1106 Native API

Lizar has used various Windows API functions on a victim's machine.[1]

Enterprise T1095 Non-Application Layer Protocol

Lizar has used a raw TCP connection to communicate with the C2 server.[5]

Enterprise T1027 Obfuscated Files or Information

Lizar has obfuscated the fingerprint of the victim system, the local IP address, and the Fowler-Noll-V 1 (FNV-1) hash of the local IP address using an XOR operation. The data is then sent to the C2 server.[5]

Enterprise T1588 .002 Obtain Capabilities: Tool

FIN7 has obtained and used tools such as Impacket, Mimikatz, and PsExec.[1]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

Lizar can run Mimikatz to harvest credentials.[2][1]

Enterprise T1057 Process Discovery

Lizar has a plugin designed to obtain a list of processes.[2][1]

Enterprise T1055 Process Injection

Lizar can migrate the loader into another process.[1]

.001 Dynamic-link Library Injection

Lizar has used the PowerKatz plugin that can be loaded into the address space of a PowerShell process through reflective DLL loading.[1]

.002 Portable Executable Injection

Lizar can execute PE files in the address space of the specified process.[1]

Enterprise T1620 Reflective Code Loading

Lizar has used the Reflective DLL injection module from Github to inject itself into a process’s memory.[5]

Enterprise T1113 Screen Capture

Lizar can take JPEG screenshots of an infected system.[2][1] Lizar has also used a plugin to take a screenshot of the infected system.[1]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

Lizar can search for processes associated with an anti-virus product from list.[1]

Enterprise T1082 System Information Discovery

Lizar can collect the computer name from the machine.[1][5]

Enterprise T1016 System Network Configuration Discovery

Lizar has retrieved network information from a compromised host, such as the MAC address.[1][5]

Enterprise T1049 System Network Connections Discovery

Lizar has a plugin to retrieve information about all active network sessions on the infected server.[1]

Enterprise T1033 System Owner/User Discovery

Lizar can collect the username from the system.[1][5]
