**RAT.Unknown.exe**

**File Hash and Analysis**

**VT Analysis:**

**Basic Static Analysis (Floss Output)**

|  |  |
| --- | --- |
| Floss Output | @SSL support is not available. Cannot connect over SSL. Compile with -d:ssl to enable.  @https  @No uri scheme supplied.  InternetOpenW  InternetOpenUrlW  @wininet  @wininet  MultiByteToWideChar  @kernel32  @kernel32  MessageBoxW  @user32  @user32  @[+] what command can I run for you  @[+] online  @NO SOUP FOR YOU  @\mscordll.exe  @Nim httpclient/1.0.6  @/msdcorelib.exe  @AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup  @intrt explr  @http://serv1.ec2-102-95-13-2-ubuntu.local |

**Initial Detonation:**

A screenshot of a computer error message

Description automatically generated

**Network Signatures**

Wireshark Packet Analysis

A screenshot of a computer

Description automatically generated

|  |  |
| --- | --- |
| **Potential file download** | msdcorelib.exe |

**Host Base Indicator**

A screenshot of a computer

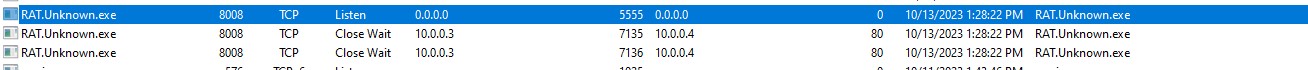
Description automatically generated

**Persistent Binary**

A screenshot of a computer

Description automatically generated

**TCP Socked in listening state.**



|  |  |
| --- | --- |
| Base64 encoded data from socket on TCP 5555 | A black and orange sign  Description automatically generated with medium confidence |
| Command injection capability | A computer screen with a white background  Description automatically generated |

|  |
| --- |
| **Program Execution Flow:**   * **If URL exists:**   + **Download favicon.ico**   + **Write to disk (CR433101.dat.exe)**   + **Run favicon.ico (CR433101.dat.exe)** * **If URL does not exist:**   + **Delete from disk**   + **Do not run** |