ThreatExpert

## Submission Summary:

- Submission details:
  - Submission received: 26 July 2014, 04:10:02 AM
  - Processing time: 6 min 32 sec
  - Submitted sample:
    - File MD5: 0xA29C95105D15906EDC7439085EB91149
    - Filesize: 226,304 bytes
    - Packer info: *packed with* UPX [Kaspersky Lab]
- Summary of the findings:

| What's been found | Severity Level |
|---|---|
| Capability to steal information such personal financial data (credit card numbers, online banking login details), user profiles, software registration keys, passwords. | 🟥🟥🟥🟥🟥🟥🟥🟥🟥🟥 |
| Downloads/requests other files from Internet. | 🟨 |
| Contains characteristics of an identified security risk. | 🟥🟥🟥🟥🟥🟥🟥🟥🟥🟥 |

## Technical Details:

### Possible Security Risk

- **Attention!** The following threat category was identified:

| Threat Category | Description |
|---|---|
|  | A keylogger program that can capture all user keystrokes (including confidential details such username, password, credit card number, etc.) |

### Memory Modifications

- There were new processes created in the system:

| Process Name | Process Filename | Main Module Size |
|---|---|---|
| lsass.exe | %Programs%\startup\lsass.exe | 1,306,624 bytes |
| [filename of the sample #1] | [file and pathname of the sample #1] | 102,400 bytes |

- Note:

    - %Programs% is a variable that refers to the file system directory that contains the user's program groups. A typical path is C:\Documents and Settings\[UserName]\Start Menu\Programs.

## Registry Modifications

- The following Registry Key was created:
    - HKEY_CURRENT_USER\Software\WinRAR
- The newly created Registry Value is:
    - [HKEY_CURRENT_USER\Software\WinRAR]
        - HWID = 7B 45 44 38 38 44 38 36 39 2D 36 33 31 34 2D 34 42 39 41 2D 42 43 38 44 2D 42 42 30 44 33 46 43 44 43 39 42 35 7D

## Other details

- The following Host Name was requested from a host database:
    - walex2.ddob.us
- The following Internet Connection was established:

| Server Name | Server Port | Connect as User | Connection Password |
|---|---|---|---|
| walex2.ddob.us | 80 | (null) | (null) |

All content ("Information") contained in this report is the copyrighted work of Threat Expert Ltd and its associated companies ("ThreatExpert") and may not be copied without the express permission of ThreatExpert.

The Information is provided on an "as is" basis. ThreatExpert disclaims all warranties, whether express or implied, to the maximum extent permitted by law, including the implied warranties that the Information is merchantable, of satisfactory quality, accurate, fit for a particular purpose or need, or non-infringing, unless such implied warranties are legally incapable of exclusion. Further, ThreatExpert does not warrant or make any representations regarding the use or the results of the use of the Information in terms of their correctness, accuracy, reliability, or otherwise.

Copyright © 2014 ThreatExpert. All rights reserved.