

# HACKERS LOUNGE

## Memory Forensics Analysis Report

Report Date: 1/10/2023

Analyst: Manthan Modi

Analyst: Meghraj Patil

### 1. Project Overview

The objective of this project was to conduct a memory forensics analysis to identify evidence of harmful activity in volatile memory. The analysis aimed to detect and document any suspicious or malicious activities that may have occurred within the memory of the target system.

### 2. Target System Information

- System Name: Jackcr's
- Operating System: Windows XP x86
- Memory Type: bin 523,760 Kb
- Acquisition Date and Time: 31/11/2023

### 3. Memory Acquisition

The volatile memory of the target system was acquired using [Insert Memory Acquisition Tool and Version]. The acquisition process was performed [Insert Information on Acquisition Process, e.g., as part of an incident response investigation].

#### 4. Analysis Findings

During the memory forensics analysis, several key findings and indicators of potentially harmful activities were identified:

```
(windows@windows11)-[~/Downloads/ENG-USTXHOU-148]
$ volatility -f memdump.bin imageinfo

Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
      AS Layer1 : IA32PagedMemory (Kernel AS)
      AS Layer2 : FileAddressSpace (/home/windows/Downloads/ENG-USTXHOU-148/memdump.bin)
      PAE type : No PAE
      DTB : 0x39000L
      KDBG : 0x8054cde0L
      Number of Processors : 1
      Image Type (Service Pack) : 3
      KPCR for CPU 0 : 0xffdf000L
      KUSER_SHARED_DATA : 0xffdf000L
      Image date and time : 2012-11-27 01:57:28 UTC+0000
      Image local date and time : 2012-11-26 19:57:28 -0600
```

#### A. Running Processes:

- A number of running processes were identified, some of which raised suspicions. Notable processes included

```
(windows@windows11)-[~/Downloads/ENG-USTXHOU-148]
$ volatility -f memdump.bin --profile=WinXPSP3x86 pstree

Volatility Foundation Volatility Framework 2.6
Name                               Pid  PPid  Thds  Hnds Time
-----
0x823c8830:System                   4      0    51   271 1970-01-01 00:00:00 UTC+0000
. 0x821841c8:smss.exe               356     4     3    19 2012-11-26 22:03:28 UTC+0000
.. 0x82189da0:winlogon.exe          628   356    18   653 2012-11-26 22:03:29 UTC+0000
... 0x82194650:services.exe         680   628    15   243 2012-11-26 22:03:30 UTC+0000
.... 0x820b3da0:svchost.exe         1024   680    76  1645 2012-11-26 22:03:32 UTC+0000
..... 0x82045da0:wuaucflt.exe       1628  1024     3   142 2012-11-26 22:04:43 UTC+0000
..... 0x82049690:wc.exe             364   1024     1    27 2012-11-27 01:30:00 UTC+0000
..... 0x8203c020:alg.exe            1888   680     6   105 2012-11-26 22:03:35 UTC+0000
..... 0x821a62e0:svchost.exe        1068   680     5    81 2012-11-26 22:03:32 UTC+0000
..... 0x822e9700:spoolsv.exe        1348   680    10   105 2012-11-26 22:03:34 UTC+0000
..... 0x82192b10:svchost.exe        940   680     9   258 2012-11-26 22:03:31 UTC+0000
..... 0x821a3c10:svchost.exe       1116   680    14   248 2012-11-26 22:03:33 UTC+0000
..... 0x8219e2c8:svchost.exe        852   680    14   187 2012-11-26 22:03:31 UTC+0000
... 0x82244020:lsass.exe            692   628    22   407 2012-11-26 22:03:30 UTC+0000
.. 0x821b0020:csrss.exe             604   356    12   351 2012-11-26 22:03:29 UTC+0000
. 0x8204f020:explorer.exe           284   244     9   372 2012-11-26 22:03:58 UTC+0000
. 0x82226650:msmsgs.exe             548   284     3   204 2012-11-26 22:04:03 UTC+0000
. 0x822d0828:cmd.exe                1796   284     1    33 2012-11-27 01:56:21 UTC+0000
.. 0x820b13b8:mdd.exe              244  1796     1    24 2012-11-27 01:57:28 UTC+0000
. 0x821feda0:msimn.exe             1984   284     7   359 2012-11-26 22:06:33 UTC+0000
. 0x822408d0:ctfmon.exe            556   284     1    75 2012-11-26 22:04:03 UTC+0000
```

\$ Volatility -f memdump.bin --profile=WinXPSP3x86 dlllist -p 1024

```

0x72240000 0x37000 0x2 C:\WINDOWS\System32\rasppp.dll
0x724b0000 0x6000 0x2 C:\WINDOWS\System32\ntlsapi.dll
0x71cf0000 0x4c000 0x1 C:\WINDOWS\system32\kerberos.dll
0x76790000 0xc000 0x1 C:\WINDOWS\System32\cryptdll.dll
0x72ae0000 0x13000 0x2 C:\WINDOWS\System32\RASQEC.DLL
0x768d0000 0xa4000 0x1 C:\WINDOWS\System32\RASDLG.dll
0x77b40000 0x22000 0x1 C:\WINDOWS\system32\Apphelp.dll
0x50640000 0xc000 0x1 C:\WINDOWS\system32\wups.dll
0x5f740000 0xe000 0x1 C:\WINDOWS\System32\wbem\ncprov.dll
0x10000000 0x1c000 0x1 c:\windows\system32\6to4ex.dll
0x73b80000 0x12000 0x1 c:\windows\system32\AVICAP32.dll
0x75a70000 0x21000 0x2 c:\windows\system32\MSVFW32.dll
0x74ed0000 0xe000 0x1 C:\WINDOWS\System32\wbem\wbemsvc.dll
0x71b20000 0x12000 0x1 C:\WINDOWS\system32\MPR.dll
0x75f60000 0x7000 0x1 C:\WINDOWS\System32\drprov.dll
0x71c10000 0xe000 0x1 C:\WINDOWS\System32\ntlanman.dll
0x71cd0000 0x17000 0x2 C:\WINDOWS\System32\NETUI0.dll
0x71c90000 0x40000 0x1 C:\WINDOWS\System32\NETUI1.dll
0x75f70000 0xa000 0x1 C:\WINDOWS\System32\davclnt.dll
0x73d30000 0x17000 0x1 C:\WINDOWS\System32\wbem\wbemcons.dll

```

## B. Open Network Connections:

- The memory dump revealed active network connections, including [Insert Notable IP Addresses and Ports], which may be indicative of network communication related to malicious activities.

```

(windows@ windows11)-[~/Downloads/ENG-USTXHOU-148]
$ volatility -f memdump.bin --profile=WinXPSP3x86 connscan

Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address          Remote Address          Pid
-----
0x01f60850 0.0.0.0:0              1.0.0.0:0              36569092
0x01ffa850 172.16.150.20:1291     58.64.132.141:80       1024
0x0201f850 172.16.150.20:1292     172.16.150.10:445      4
0x02084e68 172.16.150.20:1281     172.16.150.10:389      628
0x020f8988 172.16.150.20:2862     172.16.150.10:135      696
0x02201008 172.16.150.20:1280     172.16.150.10:389      628
0x18615850 172.16.150.20:1292     172.16.150.10:445      4
0x189e8850 172.16.150.20:1291     58.64.132.141:80       1024
0x18a97008 172.16.150.20:1280     172.16.150.10:389      628
0x18b8e850 0.0.0.0:0              1.0.0.0:0              36569092
0x18dce988 172.16.150.20:2862     172.16.150.10:135      696

```

### C. Memory Artifacts:

- Evidence of volatile artifacts, such as open files, sockets, and registry keys, indicated potential system and application manipulation.

```
(windows@windows11)-[~/Downloads/ENG-USTXHOU-148]
$ volatility -f memdump.bin --profile=WinXPSP3x86 dlldump -p 1024 --dump-dir ./dumpout -r 6to4ex
Volatility Foundation Volatility Framework 2.6
Process(V) Name      Module Base Module Name      Result
-----
0x820b3da0 svchost.exe      0x01000000 6to4ex.dll          OK: module.1024.20b3da0.10000000.dll

(windows@windows11)-[~/Downloads/ENG-USTXHOU-148/dumpout]
$ md5sum module.1024.20b3da0.10000000.dll
156f2c6a65a1eab1c03e1dc7f215a044 module.1024.20b3da0.10000000.dll
```

### D. Malware Indicators:

- Several memory areas exhibited signs of code injection, which is a common tactic used by malware to maintain persistence.

Upload md5 hash to <https://www.virustotal.com/>

29f63761610079940e43abd1d7c9c50ab678fef1da43c4c961069bbb8f7d0628

64 / 71

64 security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

Size: 98.50 KB | Last Analysis Date: 1 year ago | DLL

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.dialer.pcclient2 | Threat categories: trojan | Family labels: dialer pcclient2 farfi

Security vendors' analysis

Vendor	Detection	Vendor	Detection
Acronis (Static ML)	Suspicious	Ad-Aware	Generic.PcClient2.OC4AE0CD
AhnLab-V3	Win-Trojan/Onlinegamehack9.Gen	Alibaba	Malware/Win32/km_2c4cd.None
ALYac	Generic.PcClient2.OC4AE0CD	Antiy-AVL	Trojan/Generic.ASMalwS.1CB
Arcabit	Generic.PcClient2.OC4AE0CD	Avast	Win32:Agent-AAMP [Trj]
AVG	Win32:Agent-AAMP [Trj]	Avira (no cloud)	TR/Rootkit.Gen

Do you want to automate checks?

## E. Credential Artifacts:

- Credentials, both in plaintext and hashed forms, were discovered in the memory dump, suggesting a potential breach of security.

```
(windows@windows11)-[~/Downloads/ENG-USTXHOU-148]
$ strings memdump.bin | grep -C 30 58.64.132.141

+OK 3217 octets
Received: from ubuntu-router ([172.16.150.8]) by dc-ustxhou.petro-market.org with Microsoft SMTPSVC(6.0.3790.0);
    Mon, 26 Nov 2012 14:00:08 -0600
Received: from d0793h (d0793h.petro-markets.info [58.64.132.141])
    by ubuntu-router (8.14.3/8.14.3/Debian-9.2ubuntu1) with SMTP id qAQK06Co005842;
    Mon, 26 Nov 2012 15:00:07 -0500
Message-ID: <FC1C36C7B8C46AFB7C2A251EA868B8B@d0793h>
From: "Security Department" <isd@petro-markets.info>
To: <amirs@petro-market.org>, <callb@petro-market.org>,
    <wrightd@petro-market.org>
Subject: Immediate Action
Date: Mon, 26 Nov 2012 14:59:38 -0500
MIME-Version: 1.0
Content-Type: multipart/alternative;
    boundary="-----_NextPart_000_0015_01CDCBE6.A7B92DE0"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.5512
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.5512
Return-Path: isd@petro-markets.info
X-OriginalArrivalTime: 26 Nov 2012 20:00:08.0432 (UTC) FILETIME=[A2ABBF00:01CDC10]
This is a multi-part message in MIME format.
-----_NextPart_000_0015_01CDCBE6.A7B92DE0
Content-Type: text/plain;
    charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
Attn: Immediate Action is Required!!
The IS department is requiring that all associates update to the new =
version of anti-virus. This is critical and must be done ASAP! Failure =
to update anti-virus may result in negative actions.
Please download the new anti-virus and follow the instructions. Failure =
to install this anti-virus may result in losing your job!
Please download at http://58.64.132.8/download/Symantec-1.43-1.exe
Regards,
--
IoCreateSymbolicLink
IoCreateDevice
```

## 6. Conclusions

What you see above is the phishing email that the users callb, amirs, and wright received. The sender address, isd@petro-markets.info, is designed to look familiar to the end users. At the end of the email we see the trojan, Symantec-1.43-1.exe.

We were also given a timeline file and we can see both the execution of the trojan and creation of 6to4ex.dll

A little further on, we see the same activity that we saw in the pcap file.

Based on the findings, it is highly likely that the target system has been compromised. The presence of suspicious processes, network connections, memory artifacts, and potential malware indicators strongly suggests harmful activity.

The results of this analysis should prompt immediate incident response and mitigation efforts to address the security breach. Further analysis and detailed forensic investigation may be required to fully understand the scope of the incident and identify the specific threat actors and their motives.

## 7. Recommendations

In light of the identified malicious activity, the following recommendations are provided:

- Isolate the compromised system to prevent further damage.
- Engage the incident response team to investigate and remediate the security breach.
- Preserve and secure the acquired memory dump for further analysis and potential legal proceedings.
- Review and enhance security measures to prevent similar incidents in the future.

## 8. Reporting and Documentation

This report is prepared for internal use only and should be treated as sensitive and confidential information. Proper documentation and chain of custody must be maintained for the acquired memory dump.

For more information contact

<https://hackerslounge.in/>



Please note that this is a sample report for a simulated project. In real-world scenarios, memory forensics would require more in-depth analysis, collaboration with incident response teams, and adherence to legal and ethical standards.