Formbook Coronavirus Campaigns

Overview

From 24 March through 2 April, Infoblox observed several malicious spam (malspam) campaigns delivering Formbook malware. The campaigns are loosely connected by a Coronavirus or COVID-19-related theme in their subject lines or file attachment names.

As with our previous reports, the Appendix will include indicators for these campaigns as well as others we have observed over the last week.

Customer Impact

Formbook is an information stealer (infostealer) that is sold as a service to threat actors. Its capabilities include process hollowing, clipboard monitoring, keylogging, webform hijacking, screenshotting, downloading additional payloads, and communicating with a command and control (C2) server.

Campaign Analysis

All of the campaigns we observed used a Coronavirus theme, or were related to a campaign that did. One of the campaigns spoofed a message from the World Health Organization (WHO), alleging to provide a safety instruction manual. A second urged the recipient to provide a price quote on surgical masks for COVID-19. The final set of campaigns had shipping themes, some related to vessel delays due to the Coronavirus crisis.

The message sender names and file attachment names reflected the theme of the email: the WHO, a requested price quote, and maritime or shipping companies. The campaigns delivered Formbook via email attachments that were ZIP, DOCX, and RAR files.

Attack Chain

Once the recipient opens (and if necessary, decompresses) the attached file, the malware performs process hollowing and injects itself into the Microsoft File Explorer process. Next, a portable executable (either doc.exe or RFQ-QUOTAION-31-03-2020.exe) launches the Formbook payload (nbtstat.exe or mstsc.exe). The malware then proceeds to steal victim credentials and information, and uses firefox.exe to create new files with the stolen information.

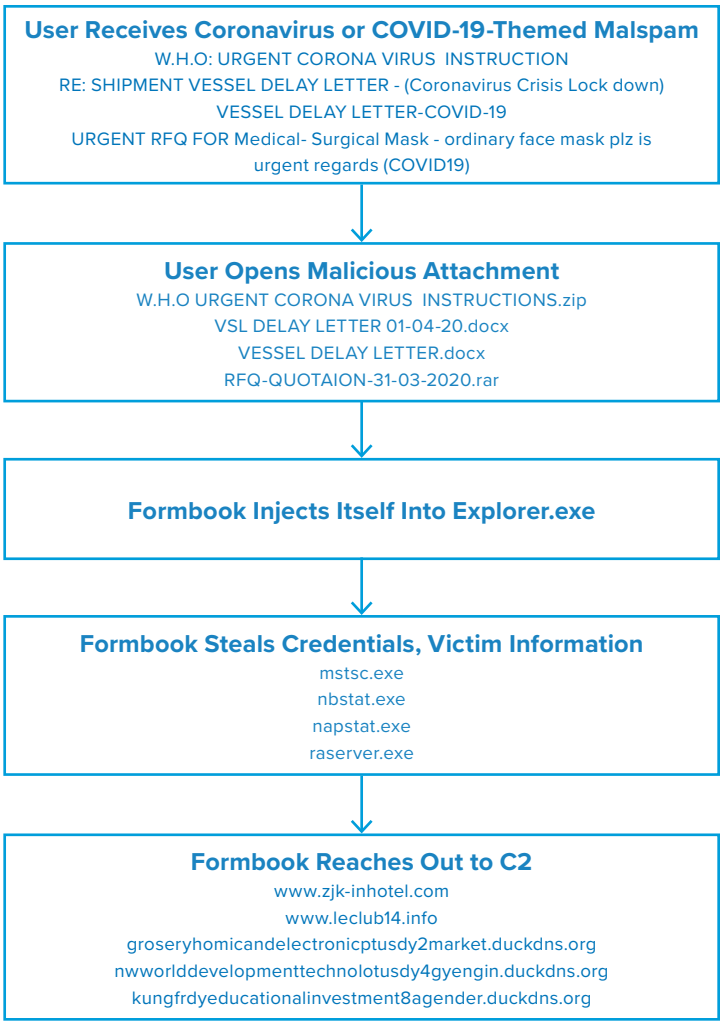
In some of our samples, opening the attachment launched the Microsoft Equation Editor to exploit CVE-2017-11882, a vulnerability in Microsoft Word. The CVE enabled eqnedt32.exe to download and run a file named vbc.exe (not the actual Visual Basic Compiler). It then used dllhost.exe to launch the Formbook payload (napstat.exe, mstsc.exe, help.exe or raserver.exe).

We also observed the malware in at least one sample establishing persistence by using schtasks.exe to set up a scheduled task to run a file in C:\Users\admin\AppData\Local\Temp.

Vulnerabilities & Mitigation

This campaign relies on both a software vulnerability and social engineering tactics to infect users with Formbook. As such, Infoblox recommends taking the following actions to reduce the likelihood of infection:

- Keep computers and all endpoints up-to-date with the latest security patches to block known vulnerabilities that threat actors could target.
- Be cautious of emails from unfamiliar senders and inspect unexpected attachments before opening them.
- Always be suspicious of vague or empty emails, especially if there is a prompt to open an attachment or click on a link.
- Implement attachment filtering to reduce the likelihood of malicious content reaching a user's workstation.



Appendix

Representative Indicators of Compromise	Description
W.H.O: URGENT CORONA VIRUS INSTRUCTION -- URGENT RFQ FOR Medical- Surgical Mask - ordinary face mask plz is urgent regards (COVID19) -- VESSEL DELAY LETTER-COVID-19 RE: SHIPMENT VESSEL DELAY LETTER - (Coronavirus Crisis Lock down) -- M/T SUN SHINE / V-G2006 / DUE CHINA OR TANGJUNG PELEPAS, MALAYSIA FOR LOADING - AGENT APPOINTMENT -- -- RE: M/T ITHA BHUM / V.309S / DUE KOREA OR TANGJUNG PELEPAS, INDONESIA FOR LOADING - AGENT APPOINTMENT -- MT RADIANT PRIDE - REQ. NO. RAPRI-V20-200669 M/V A RACER // REQ, ARC 052/20 MV.SEA PALACE V.05/2020 ^.+Singapore_Cigading.+$ re:ship doc R21 CUTUP FACTORY COST SHEET - QPS	Formbook malspam subject lines (some subjects are multiple lines long, denoted with “--” at the beginning and end)
W.H.O URGENT CORONA VIRUS INSTRUCTIONS.zip RFQ-QUOTAION-31-03-2020.rar VESSEL DELAY LETTER.docx VSL DELAY LETTER 31-03-2020.docx VSL DELAY LETTER 01-04-20.docx ARC 052.20.docx MT SUN SHINE (V-G2006)-Q88.docx	Formbook malspam file names
04ba697e6593d3fa1610a56ef598cf2d6c3330f3936d5f4d1b62dad6ec63f711 493816ead0973451a440aea16a1713affefe51a3bd3aeef1422d412b42bafd8c d88753eaf17fac2ac9331d87866a6c7c6c41b5de89dd5ff8a250846fec90ac17 4d4114a5a4cb80256fac19e5fcbf07374a7598a586eab864b6c52a753e3b8ea9 c7d100343439e0b7dd8eafed2d787fdb52a8db0fbce2118b2f90eba6d907516f c5c43b340957830f5d7484ce06f9de0ef593d88f3d48c09cd2150e670661f672 273704d103f3d31b5bb42fb9bd040301ea21509b4ede30736bcad2da037374b7 67b268f1e4ec8cd13940eff3a442445dca813ca706993211ff32e9eda1db35b4 d969f416ec716d26f307dd6f24a081875485b464086ad307da51b51bb8af43b1	Formbook attachment file SHA256s
(see below the table)	Formbook downloaders

Representative Indicators of Compromise (Continued)	Description
www[.]zjk-inhotel[.]com added www[.]allixanes[.]com added www[.]sysnl[.]com added www[.]briled[.]com added www[.]monavocatonline-altoavocats[.]com added www[.]labtextileschool[.]com added www[.]ourhabitk[.]com added www[.]elmalikurabiye[.]net added www[.]pruftechnikrental[.]com added www[.]o0ay4k[.]info added www[.]hominemprint[.]com added www[.]oecali[.]com added www[.]cws-incentive-events[.]com added 23[.]20[.]239[.]12 added 156[.]238[.]103[.]49 http://www[.]leclub14[.]info/g9g/ nwworlddevelopmenttechnolotusdy4gyengin[.]duckdns[.]org www[.]lotto-winner[.]info www[.]accommodationavon[.]info www[.]leclub14[.]info 103[.]133[.]108[.]118 192[.]64[.]116[.]61 www[.]wizardmadness[.]com www[.]stjameseutawville[.]com tuodqka[.]com www[.]crisngrt[.]com meinnatura[.]com www[.]qdbfqfphjidqgtbttnq[.]com yangzhie288[.]com www[.]lewesdelawarerealestate[.]com www[.]markcici[.]com www[.]standardpitbullpups[.]com septsix[.]com flycoz[.]com kiranabharati[.]com 207[.]148[.]248[.]143 202[.]172[.]28[.]51 34[.]251[.]91[.]168 23[.]227[.]38[.]64 63[.]250[.]42[.]84 groseryhomicandelectronicptusdy2market[.]duckdns[.]org www[.]theworldcuppa[.]com www[.]gununminikdetaylari[.]com westernslopewellness[.]com www[.]richardklu[.]com yzw169[.]com	Formbook C2s

Representative Indicators of Compromise (Continued)	Description
jdmoji[.]com www[.]zhonglianrong[.]com lygsxgt[.]com iwroteathing[.]today www[.]abbottworlds[.]com www[.]fascinatinginteriors[.]com 103[.]133[.]106[.]81 184[.]168[.]221[.]92 192[.]0[.]78[.]24 109[.]68[.]33[.]18 50[.]63[.]202[.]32 154[.]218[.]107[.]177 156[.]244[.]145[.]202 grosery2frdyhomicandelectronicspmarket[.]duckdns[.]org www[.]alexandajay[.]net www[.]blackswanutopia[.]com www[.]canproduccionesmexico[.]com www[.]taylormacroibeaird[.]com www[.]bestgreenhouseplan[.]com www[.]sh-changce[.]com kungglobalinvestmenteductgpmstdy8addres[.]duckdns[.]org investmenteducationkungykmtsdy8agender[.]duckdns[.]org	Formbook C2s
corona virus	Agent Tesla malspam subject line
e-dekont.rar	Agent Tesla attachment file name
8cd04fd84098759c54e3ec0b85374c7231a2c580b237b915a4b5b64546b96314	Agent Tesla attachment file SHA256
mail.mkkarakosemobilya.com	Agent Tesla downloader
COVID-19 UPDATE !!!	Lokibot malspam subject line
Covid-19_UPDATE_PDF.7z	Lokibot attachment file name
f6f5f839aa7edf51468ad3ccc16f1e6e20314f2b5f4b5a765d2aa66f19c32009	Lokibot attachment file SHA256
brokenme.xyz	Lokibot downloader

Formbook downloaders:

http://www[.]zjk-inhotel[.]com/p02/?Lv14=5IlSiK2+ZOn1TfaBdHH0prZKcDyCRdv+yNeW+4L50LN5uTS-b5eLnt1ZFLTV6AHe4Ksb0pA==&VRp4=GfGTFTbpsl
http://www[.]allixanes[.]com/p02/?Lv14=ftU6cliT5JyVW8VDI130VKkRGzoWYL9tp9t7L8AegC82sOKZXoRuKa67aLF8oT-sIoYAQxQ==&VRp4=GfGTFTbpsl
http://www[.]briled[.]com/p02/?Lv14=m3m3FgmXnSNIzK9wWR/VafZSEfTvC4Fzd8bTKQV2sfHnxMWUrHL/t7yWvMB/Dp-tUaEtu2g==&VRp4=GfGTFTbpsl
http://www[.]labtextileschool[.]com/p02/?Lv14=eg079kpwseyX76OFZeiskxD4wlPmnwGRqlGE1gt92tn-WKy7l2dYWESgav+ow5ZONIjQSqw==&VRp4=GfGTFTbpsl
http://www[.]pruftechnikrental[.]com/p02/?Lv14=UZWluzLj+jKTtHOnsmuPJ8III90mUG0q2jZvp5DgzD5uXGou-rIDKpZ7XsNxlL6cv2CNBuA==&VRp4=GfGTFTbpsl
http://www[.]hominemprint[.]com/p02/?Lv14=BQ3El6kjN4RByuNj2sZoB2lm738lC/rrQXdKNsu6gCaAewyVGoXi/OHIjnU2s-rPJ9dXgpg==&VRp4=GfGTFTbpsl
http://www[.]cws-incentive-events[.]com/p02/?Lv14=ovmXMqiLQLODEp9OIkAs+jAPWnegFvobLFudkbxAQ37w-fKHw0951sLaHWjOhqfokwzDbzw==&VRp4=GfGTFTbpsl
http://nwworlddevelopmenttechnolotusdy4gyengin[.]duckdns[.]org/office
http://nwworlddevelopmenttechnolotusdy4gyengin[.]duckdns[.]org/office/
http://nwworlddevelopmenttechnolotusdy4gyengin[.]duckdns[.]org/dashboard
http://nwworlddevelopmenttechnolotusdy4gyengin[.]duckdns[.]org/
http://www[.]leclub14[.]info/g9g/?Lh54A=vuM5nChz6b+FzZiyKdeXMuZ0lyrpln7rVMQN7ytsSjb9QHHonopS0ollbmWrrp-N+RJfOwQ==&URpX=D8TpFTbpXv5&sql=1
http://www[.]nercox[.]com/g9g/?Lh54A=Z/4wndMorAVLFgcAJqK1PhoqetsiI3OYq3nSBmX9RYUXewvkM2g0xP609iQpB-10kE1kolA==&URpX=D8TpFTbpXv5http://nwworlddevelopmenttechnolotusdy4gyengin[.]duckdns[.]org/office/in-voice_12449[.]doc
http://nwworlddevelopmenttechnolotusdy4gyengin[.]duckdns[.]org/engindoc/winlog[.]exe
http://kungfrdyeducationalinvestment8agender[.]duckdns[.]org/
http://kungfrdyeducationalinvestment8agender[.]duckdns[.]org/office
http://kungfrdyeducationalinvestment8agender[.]duckdns[.]org/office/
http://kungfrdyeducationalinvestment8agender[.]duckdns[.]org/office/invoice_11154[.]doc
http://kungfrdyeducationalinvestment8agender[.]duckdns[.]org/kungdoc/winlog[.]exe
http://kungfrdyeducationalinvestment8agender[.]duckdns[.]org/dashboard/
103[.]140[.]250[.]215
207[.]148[.]248[.]143
202[.]172[.]28[.]51
34[.]251[.]91[.]168
23[.]227[.]38[.]64
63[.]250[.]42[.]84
http://www[.]wizardmadness[.]com/te/?00A=+koc0RPnQ+bEvTQ5Fo6e9vRARDXz9hlo8Ga0+ePh5eFzrElu/Cf0rvHengK3gP6Uq9QFiA==&-ZX4A=LhLhEPPpzB78R
http://www[.]stjameseutawville[.]com/te/?00A=aZVEg7qSwpXDhs0ZmD3YjCwaf0p169ZROgz49nAHoJ3qMK24Q8FS8bd-NTj/VEDaSpJBGGQ==&-ZX4A=LhLhEPPpzB78R&sql=1
http://www[.]stjameseutawville[.]com/te/
http://www[.]markcici[.]com/te/?00A=TnShM28uj8RXSt75y+Tz2w8xkjwma+iT0stV2RJtgTkpwJS0c-NadH6KZrTiLzoVTWMsWJQ==&-ZX4A=LhLhEPPpzB78R&sql=1
http://www[.]markcici[.]com/te/
http://www[.]crisngrt[.]com/te/
http://www[.]crisngrt[.]com/te/?00A=9yWE2ENoe+bIaYrOACXdu7jgvU3L2FmzjtlHdxzMiTbsSbAA/e8z0faFeNa/xiZTVmPy/Q==&-ZX4A=LhLhEPPpzB78R&sql=1
http://www[.]flycoz[.]com/te/
http://www[.]flycoz[.]com/te/?00A=M2ouDOfOiUiNyX3uUObsisyNcixzNrb8Di1ovfXvoI92pKmGeIAPwhtYtLua+qBsa-3ZEVw==&-ZX4A=LhLhEPPpzB78R
77[.]88[.]21[.]158

http://groseryhomicandelectronicptusdy2market[.]duckdns[.]org/
http://groseryhomicandelectronicptusdy2market[.]duckdns[.]org/dashboard/
http://www[.]gununminikdetaylari[.]com/f1k/?Rv=t2OrhxoRJF961sPFyFiD+K/+xm27wib0divYN0Sqy1kiLFGfa99QGUY-iz7lzM/yRxxMwtA==&E6UDU=GdTpfja0JbvXUzwp
http://www[.]theworldcuppa[.]com/f1k/?Rv=ISL2XDXi3S0cf44RW1xulzza1c/ZVh3b3Deby1ef9oeXIei/EJnpak0AB3jpy-IJlq+mcsQ==&E6UDU=GdTpfja0JbvXUzwp&sql=1
http://www[.]theworldcuppa[.]com/f1k/
http://www[.]richardklu[.]com/f1k/?Rv=r5rrnU3Vr2g7Vd6tFiU+AnL4Q7AvjbII+T+IfPC7uBC4T+ysGJORv2H3iN2XPqA8Y-So2Nw==&E6UDU=GdTpfja0JbvXUzwp&sql=1
http://www[.]richardklu[.]com/f1k/
http://www[.]westernslopewellness[.]com/f1k/?Rv=WZHEBrYfeolc2gf+7iQwwgR8ZNTwwxTV39tr4xjJifw5vqbgO-vdsAbwrX42EBoFoQn9ssA==&E6UDU=GdTpfja0JbvXUzwp&sql=1
http://www[.]westernslopewellness[.]com/f1k/
http://www[.]lygsxgt[.]com/f1k/?Rv=7HCnF7zcUOh6RApuM74+7Q3s8ceW50hHxqwQ5/RUdbOQFRD9r3TinwxX7a87s-FIuur/YIw==&E6UDU=GdTpfja0JbvXUzwp&sql=1
http://www[.]lygsxgt[.]com/f1k/
http://www[.]fascinatinginteriors[.]com/f1k/
http://www[.]fascinatinginteriors[.]com/f1k/?Rv=WO4kHba5m0v82vn7BpdCoiFI0d3pRN99R/aBjtOkKRPgROOq54WU+rz-EGYq6W49+RRuu+g==&E6UDU=GdTpfja0JbvXUzwp&sql=1
http://www[.]zhonglianrong[.]com/f1k/
http://www[.]zhonglianrong[.]com/f1k/?Rv=NIF+kHRWeFIoauQuBOkR/bLRRUsdcVpx893ZwmlHdRatsfoY6cGap3iWbAX-HWfJ3frHpUA==&E6UDU=GdTpfja0JbvXUzwp&sql=1
http://groseryhomicandelectronicptusdy2market[.]duckdns[.]org/chnsfrnd2/regasm[.]exe
http://groseryhomicandelectronicptusdy2market[.]duckdns[.]org/office/invoice_22119[.]doc
http://grosery2frdyhomicandelectronicspmarket[.]duckdns[.]org/
http://grosery2frdyhomicandelectronicspmarket[.]duckdns[.]org/dashboard/
http://grosery2frdyhomicandelectronicspmarket[.]duckdns[.]org/office/invoice_22118[.]doc
http://grosery2frdyhomicandelectronicspmarket[.]duckdns[.]org/office/
http://grosery2frdyhomicandelectronicspmarket[.]duckdns[.]org/chnsfrnd2/regasm[.]exe
192[.]169[.]69[.]25
http://kungglobalinvestmenteductgpmstdy8addres[.]duckdns[.]org/office
http://kungglobalinvestmenteductgpmstdy8addres[.]duckdns[.]org/office/
http://kungglobalinvestmenteductgpmstdy8addres[.]duckdns[.]org/office/invoice_11151[.]doc
http://investmenteducationkungykmtsdy8agender[.]duckdns[.]org/office
http://investmenteducationkungykmtsdy8agender[.]duckdns[.]org/office/
http://investmenteducationkungykmtsdy8agender[.]duckdns[.]org/office/invoice_11152[.]doc
http://investmenteducationkungykmtsdy8agender[.]duckdns[.]org/kungdoc/winlog[.]exe