Indicators of Compromise

SHA256	Icon Filename	C2 URL Extracted
210c9882eba94198274ebc787fe8c88311af24932832a7fe1f1ca0261f815c3d	icon0.ico	
a541e5fc421c358e0a2b07bf4771e897fb5a617998aa4876e0e1baa5fbb8e25c	icon1.ico	https[:]//msstorageazure[.]com/window
2c9957ea04d033d68b769f333a48e228c32bcf26bd98e51310efd48e80c1789f	icon2.ico	https[:]//officestoragebox[.]com/api/session
268d4e399dbbb42ee1cd64d0da72c57214ac987efbb509c46cc57ea6b214beca	icon3.ico	https[:]//visualstudiofactory[.]com/workload
c62dce8a77d777774e059cf1720d77c47b97d97c3b0cf43ade5d96bf724639bd	icon4.ico	https[:]//azuredeploystore[.]com/cloud/services
c13d49ed325dec9551906bafb6de9ec947e5ff936e7e40877feb2ba4bb176396	icon5.ico	https[:]//msstorageboxes[.]com/office
f1bf4078141d7ccb4f82e3f4f1c3571ee6dd79b5335eb0e0464f877e6e6e3182	icon6.ico	https[:]//officeaddons[.]com/technologies
2487b4e3c950d56fb15316245b3c51fbd70717838f6f82f32db2efcc4d9da6de	icon7.ico	https[:]//sourceslabs[.]com/downloads
e059c8c8b01d6f3af32257fc2b6fe188d5f4359c308b3684b1e0db2071c3425c	icon8.ico	https[:]//zacharryblogs[.]com/feed
d0f1984b4fe896d0024535510ce22d71e05b20bad74d53fae158dc752a65782e	icon9.ico	https[:]//pbxcloudeservices[.]com/phonesystem
d459aa0a63140ccc647e9026bfd1fccd4c310c262a88896c57bbe3b6456bd090	icon10.ico and icon11.ico	https[:]//akamaitechcloudservices[.]com/v2/storage
d51a790d187439ce030cf763237e992e9196e9aa41797a94956681b6279d1b9a	icon12.ico	https[:]//azureonlinestorage[.]com/azure/storage
4e08e4ffc699e0a1de4a5225a0b4920933fbb9cf123cde33e1674fde6d61444f	icon13.ico	https[:]//msedgepackageinfo[.]com/microsoft-edge
8c0b7d90f14c55d4f1d0f17e0242efd78fd4ed0c344ac6469611ec72defa6b2d	icon14.ico	https[:]//glcloudservice[.]com/v1/console
f47c883f59a4802514c57680de3f41f690871e26f250c6e890651ba71027e4d3	icon15.ico	https[:]//pbxsources[.]com/exchange