Emotet 2.0: Everything you need to know about the new Variant of the Banking Trojan - CloudSEK

By Co Authors

Published: 2021-12-22 · Archived: 2026-04-05 23:17:43 UTC

Since it was first identified in 2014, the Emotet banking trojan has been a persistent threat that has affected over 1.6 million computers and led to millions of dollars in loss. However, in January 2021 a collaborative effort between law enforcement in several countries, coordinated by Europol and Eurojust, dismantled the operations of Emotet, which was followed by several arrests in Ukraine.

Despite the disruptions in their operations, within 9 months, in November 2021, new Emotet samples were discovered in the wild. Though the new variant of Emotet is very similar to the previous bot code, it differs in the encryption scheme used for command and control communications.

In this article, we delve into the technical aspects of the re-emerged Emotet malware dubbed Emotet 2.0.

After almost a year-long hiatus, the Emotet malware has returned to the threat landscape through spamming campaigns. Adversaries are using weaponized Microsoft Word document files to spread the infection.

As shown in the image below, users are tricked into clicking “Enable Content” to execute the malicious Macros that downloads Emotet malware hosted on various WordPress websites compromised by the attackers.

The images below illustrate the different Powershell payloads from multiple malicious documents:

When the payload is DLL, the campaign uses **Rundll32** to execute an exported function ***Control_RunDLL*** to deploy the Emotet payload.

When the payload is a .exe executable file, the Powershell payload fetches the .exe file from the attacker’s infrastructure and executes on the victim’s system.

As seen in the image below, the memory permissions for the region 0x10000000 to 0x00028000 have been set to **ERW** (Execute, Read, Write).

File Hash – SHA256	
fc0d549104f2c18619758a5ca56847c65e16981121dfebc50b9a8eebc886573b	f717350418d58d2ba6c0492794508bc7cd5d3cdfcb3c4334276dba940
f57b21a4d6338a3d3552216e1cd2a39cfdc58310bce524d8f63004ee71aa2938	f227c59532fa2aad62305a79cac5e13019a7d969765758a86218b85b00
f023bf21ed5a54f84d75aa8ec2c0f40628dca0443b0e07375b52a657af838e3c	ef4f5373736a876fbfa74f6e9904f6f23f9c052f3f474d3ba0638cafd5185
ef0ee0f3b035a9aff22171da5cb6ce2870aad3ff4482ff36dcc54e8ee9c9c4fe	edf90b6422680bf15e95c8ce3fea26162fca3cfdf8dbb6c04f253089c0f7
e383a83e1f5c3c207418d26d3bfd88fb176c4e83f54bc07b2c9c783e09e35a15	df68d5f7df57a1109b6a3a1c7b7295ef427a8a2542cee5bc8654eab0aad
dc13a72e1e5325435158cc9151c2dc85a21b9f3f3e3bedc3f23a16ca8228dbd2	d7ba34224a23a54ced6d118e44c2cdebc7365cae81e168aa6f3cb72b540
ccda6d2b252f30164eb8947e2ec403bf84f023988e678cb91892a95bfc051131	cc73ad809eeba4440454fce00ee8d2076a57c6a64761af465f8f34cdc38
cb5ac045795644ed2f7aeadc1526f438375248bb6cdedf300015a1978245a32a	c9aaf815abe2d627ea9ac3ee7fa9fa62971a3710acd33a438a4581ee95a
c436e7c76e37650fe6c6efb6ffb5836bbce8b192c2b750bfcb0f089b255a0e0f	c3235d8500c49161130b852defb4963e68e78bd149714e7f7c850e9587
c199e4c4607e53ad448227314fa7f31d7464e9d4138446d32ddf7e1390a3e794	bc1a988b403559ad5da8b393414bec3bbed8cc3016476d9dd63779947
ba3b47d0e52f983be9c585e9b30f4af080249836cd7c9e1b401d19b7db7cf939	b7bb028310c3e03f25ffb3955e2f9fd2018caaf2da268ed0eea2306981a5
b243bf0122828c99bf083af2f324b5f336aa46769fd94349eb2a9828bbdefc86	ad278f4cf2e1eaa01f4a77db435f66f15cd49e6a8e3af5f04998fbeff8277
9d4d9beaaeeac9fa7c3e6dcbcfa13da3619a28d20ec820de8ee9a6bfe952c148	9c2148eb0d49971908766b1c9c1875b7e8a627347ed19458ff2f8fa238
9af62bbd1381d9566f907d99a7cfc9f532936cddb04f359736aa4bd3231ad020	9721c3df9f18b63c21f81604cf7b0d1ae45e603eb9d6d85189298b7e39
918fb07d648cd5235b6361d30256c37c4bc07cd4c3312b713276d035e0004fa6	8d728385d57b0bcd128751ace9f7550c210e841a41ba366c09d8cbcd78
88e8fa38140a1a3f906fac5b9a526132e978cc9c2de05ee3b5a49ff8f312c03e	86a6f7971fae83e42ff5af58c1364a66a9f40f0fbe6f88f536e8746aed051
84e9eff680264b95cbc8fe0bb3850a9c0ac11a9d0e33d867744ec720fcef875f	83b01c1031a2f40d9d563363eded81373d19815ded57596bb467c0672
82f9d9279b752c4c7b6ca40c737a09b55e4be09d96093351bb6b0614f12d08ed	824a6047233e2ac4af1ec01470fa6c92aafeb4edbe50170ffcd8a71fbdaa

7b428765408589b1783d877924b1904c74036346a6d6561e064a50e68d25f9f3	7a36f90f9decaa862fad06b462cfe9756778e786345f84585fe0ce66e2a5
77bfee9cb826154ed07a2d8aef0b58e434984185751a0c0b35d080f3d816bf0a	77bdae696540c67e4c9fa5243667723191f2c7724280c4a566f0bdafa29
6d679474a78796803d07ce6fe31a215ac9f5de7e6cc4e29ccfff6cd809af2360	65b0db343f74c2d2df9af530ce27b7b4e80a9a4b644d6f422b139cbf787
62bcc4f1d51e92b4bf4797acd41bd9bcb0d66750e5c90555f6cc5d0bfa105581	62792a0de7959a7e4352fecea08adc050e22c965f6bd100a246bde5fd8f
5fef57576da8bcbb07d5858148f1fe0b70adddeed7394a4fa112ef9871b6b76d	5fc0e6c51016ae8e1e9fc0d6d96a28833947ce0872b333ef39f42e218c4
59f5ce0c5422c95f739c094cd177f1149d4f8d0d3091f32c959d0dad34e3da98	54533a4f2c942c589c93b8f494a28804b42a8ee049d292faff2a247172b
5246f80dc9da8cc6f40241f0846b0ba301604348005fe397704ec39b711c2fda	51ed1a79f300dd22a2fd558296df74cd0ca182d5301d1b22a31189d200
4dedc2bfa4657a52c66b190bcf4ff3b35d492bf13f1c8a6705078932e6a4883c	4da56959d4d126c44efbb99be3da0edc21d2e530c91035f7e04d63184d
47db58b63bcaa028cd345209a11e93334c0c9aad2b895e8a9a72b0c20be8adb6	45aecf95b1011751b81a88542fac64c2a747c445cef48b90b24f6303ea0
3dc904b04fb0178bed08752004daf9fe3023ba01f5c6a5466b3cf657deb2b1bd	3d605a6edf9007ce53e65c78c62070afc7da2cd1658546fd2e119a4bc03
3b940b1a3d79aeb998d24c750b1d8dd7b2813c0612ffaec14aff9c9761290483	3b51f9935edabda771bd7c33eba789c0552bff3240488e3daa4a1e7b39f
3710b6a12451de36d8743766a129677c0e6f3a95996fdb16819c4fc1503ce0ec	36fcc3252115a11533c543d81f8acb92da975aebbf6593a75a5826765ab
369e3867e57f226e567138dcafaf920c71bfb5ab959c6415f36fc16df1a56a0e	35347dd43af88f9adbbaff8dee84da9c6187bc3583246baa366c9dd6d25
2c3812c81ed37982aff0b5a0becf00dffa537da56acca8792c96740ea42b7df3	2b9ad1e926df4c7a6af565fff49e4f1b7c9fad97672de67aad273d8142d2
2717ddf8dc06e896ac9301202571353e2fa23acb4c9ba5978196e74c62c46909	20e25627fab8de69bac4e94599fab2767df36438697cccfc48e8539649b
1ea47a5d3f11650fc755a28fe54e8ab6557b635145925c23e42fc5eda85e4b8a	1e9345ee7d442805a04bf6bd5eefea8e5de05fde2b60f1362f5d0239d76
124449bd0b9097b454c35fa258bda625ff6ecf5bf6f1316d7abb46fad459a273	118aeefa04fb5338c15d7fa9fffa137fd3c1b6c86fb3b32fddf637b50aaa1
100cc1e3bcc4f5ad7ee601ca99ecaf17bbcf4fbf3878d0375c87cee00dd24756	0e662c5e7cc88a55c15b44685eb78ba249e9164513baa865800e4e1e83
073e41ee489ae16d60361a9abff708d92df0d3a2a5f7a4d1b05ecfa3880cbead	040760ffb0fb37f80a9654390879a12f036c614b5117f6fded7513db63d
023549c2246838ebf7bbd91c2414de4950c3c0eaabb875e66e24baf410438aa6	

Source: https://web.archive.org/web/20211223100528/https://cloudsek.com/emotet-2-0-everything-you-need-to-know-about-the-new-variant-of-thbanking-trojan/