

Emotet Returns With New Methods of Evasion

blogs.blackberry.com/en/2023/01/emotet-returns-with-new-methods-of-evasion

The BlackBerry Research & Intelligence Team



Summary

Emotet, a Trojan that is primarily spread through spam emails, has been a prevalent issue since its first appearance in 2014. With a network made up of multiple botnets, denoted as “epochs” by security research team [Cryptolaemus](#), Emotet has continuously sent out spam emails in campaigns designed to infect users via [phishing](#) attacks. Once it is successfully running on an endpoint, Emotet drops other malicious programs such as [Qakbot](#), Cobalt Strike, or in some cases, even the notorious [Ryuk](#) ransomware. However, as of July 2022, the heavily distributed Malware-as-a-Service (MaaS) seemingly went dark, and no longer appeared to be running these spam campaigns.

For the next four months, Emotet remained silent. Then, on November 2, the Cryptolaemus group found that its botnets, particularly those known as Epoch4 and Epoch5, had begun sending out spam emails once again. These phishing emails used various methods to lure

victims into first opening them, and then downloading and executing .xls files, with macros used to download the Emotet dropper. With as little fanfare as when it went dark, it seems that Emotet has returned, appearing to be as malicious as ever.

Emotet's Growing Toolbox of Modules

Since its inception, Emotet has continued to steadily evolve, adding new techniques for evasion and increasing its likelihood of successful infections. It is also able to host an array of modules, each used for different aspects of information theft that report back to their command-and-control (C2) servers. From process monitoring to grabbing Microsoft® Outlook® email addresses, Emotet has been observed to inject both proprietary modules and readily available freeware tools, adding and tweaking them over the years with alarming effectiveness. More recently, Emotet has added a new Server Message Block (SMB) spreader module, used as an effective method for lateral movement once placed on a target machine.

The SMB spreader starts this process by gaining the same security privileges as the initial target account. Once loaded onto a victim's system, this module begins impersonating that user by duplicating their account token via the SecurityImpersonation level. This gives a process the same privileges as the current user on that system. With these duplicated privileges, the spreader calls a function "ImpersonateLoggedOnUser" to perform actions in the same security context of the account that is currently logged in. Pseudocode for the use of this function can be seen in Figure 1.

```
114 |         active_console_session_id = fn_WTSGetActiveConsoleSessionId();
115 |         if ( fn_WTSQueryUserToken(&token, active_console_session_id) )
116 |         {
117 |             fn_DuplicateToken(&int_struct.user_duplicated_token, token);
118 |             fn_CloseHandle(token);
119 |         }
120 |         state = 0x9AD2;
121 |         break;

91 |         fn_ImpersonateLoggedOnUser(*&int_struct.user_duplicated_token);
92 |         state = 0x45AA3;
93 |     }
```

Figure 1 – Pseudocode for SMB Spreader impersonating user (Source: Bitsight)

From here, the module begins enumerating network resources using the WinAPIs WnetOpenEnumW and WnetEnumResourceW. Of these resources, it saves any potential remote servers to a list. Then, using two additional hardcoded lists (one of common usernames, another of common passwords), the spreader will iterate over this list of server names and begin bruteforcing the IPC\$ share with the WinAPI WNetAddConnection2W in hopes of a successful connection.

If no connection is made with the credentials at hand, the SMB spreader can also attempt to seek additional usernames from the server being targeted with the NetUserEnum WinAPI. Any potential new usernames found will also be bruteforced with the hardcoded list of passwords to login to the IPC\$ share.

```
usernames:
user,owner,operator,HP_Owner,HP_Administrator,administrator,admin

passwords:
letmein,tigger,jennifer,999999,lovely,qazwsxedc,hunter>Password,147258369,q1w2e3r4t5,222222,an
drew,123456789a,joshua,secret,samsung,starwars,11111111,nicole,1111,123abc,michelle,lo1123,tho
mas,liverpool,jordan,soccer,Status,jessica,naruto,a123456,qwer1234,charlie,123654,0123456789,b
aseball,asd123,asdfgh,555555,aaaaaa,fuckyou,computer,1234561,abcd1234,1q2w3e,sunshine,7777777,
master,azerty,qwe123,123456a,superman,1234qwer,qazwsx,asdasd,daniel,121212,shadow,michael,kill
er,football,112233,pokemon,asdfghjkl,123123123,q1w2e3r4,monkey,zxcvbnm,159753,123qwe,987654321
,princess,ashley,dragon,666666,1qaz2wsx,password1,1qaz2wsx3edc,qwerty123,654321,qwertyuiop,1q2
w3e4r,123321,000000,123,iloveyou,q1w2e3r4t5y6,1q2w3e4r5t,abc123,1234567,1234567890,111111,1234
,123123,12345,12345678,qwerty,password,123456789,123456
```

Figure 2 – Hardcoded usernames and passwords used in bruteforce attack

If a connection succeeds, the spreader finally attempts to connect to either the ADMIN\$ and C\$ shares. From there, it finally copies the Emotet loader to said share and launches it as a service. The service executes with regsvr32.exe, and lateral movement is achieved.

Along with the SMB spreader, another recently added module is used to target a victim’s Google Chrome™ browser in the hopes of stealing stored credit card information. While Emotet has used other modules for digging out financial information in the past (such as NirSoft’s WebBrowser PassView module), Proofpoint found the following decrypted strings in early June 2022 that appear to be looking at Chrome™ specifically.

```
[info] decrypted string      [__main__] decrypted_str=ECDH_P256
[info] decrypted string      [__main__] decrypted_str=Cookie: %s-%s
[info] decrypted string      [__main__] decrypted_str=wtsapi32.dll
[info] decrypted string      [__main__] decrypted_str=advapi32.dll
[info] decrypted string      [__main__] decrypted_str=userenv.dll
[info] decrypted string      [__main__] decrypted_str=POST
[info] decrypted string      [__main__] decrypted_str="encrypted_key":
[info] decrypted string      [__main__] decrypted_str--%S--
[info] decrypted string      [__main__] decrypted_str=%s\Google\Chrome\User Data\Default\Web Data
[info] decrypted string      [__main__] decrypted_str=SELECT name_on_card, expiration_month, expiration_year, HEX(card_number_encrypted) FROM credit_cards
```

Figure 3 – Evidence of credit card exfiltration from Chrome (Source: ProofPoint)

A Demon at Heaven’s Gate

To load some of its previously used modules, Emotet has been observed to use an injection technique known as Heaven’s Gate. Made popular in the mid-2000s, Heaven’s Gate is an infamous method used by malware to bypass Windows® on Windows64 (WoW64) API hooks, by taking malicious 32-bit processes to inject into 64-bit processes. This technique works because while many security products monitor file activity by hooking 32-bit APIs (CreateFile, WriteFile, OpenFile), when running 64-bit code, an opportunity is presented to completely bypass many system calls which would render the malicious code segments far too noisy.

In the interests of backwards compatibility, WoW64 actually allows 32-bit applications to be run on 64-bit systems too. When a 32-bit application is run, both the 32-bit and 64-bit version of ntdll.dll is loaded. While a 32-bit process would normally pass through the 32-bit API hooks, malicious processes can perform a jump instruction past these hooks in order to execute 64-bit code. This allows the injection of any malicious code to be run without setting off immediate alerts via system calls. Windows initially developed this on the assumption that the 64-bit ntdll.dll could not be accessed by a 32-bit process, but Heaven's Gate takes advantage of this by running x64 instructions which will be completely missed by any application expecting x86 instructions. Heaven's Gate was therefore an early exploit on 64-bit systems that is still used to this day.

Once through Heaven's Gate, Emotet loaders will use a technique known as process hollowing to suspend a legitimate process, then remap its image with malicious code. The malicious code will then be able to run from the now hollowed out process in order to load modules at will.

New Trap, New Bait

With the newest wave of Emotet spam emails, the attached .xls files have a new method for tricking users into allowing macros to download the dropper. In addition to this, new Emotet variants have now moved from 32bit to 64bit, as another method for evading detection. It seems that Emotet has utilized its time offline to refine/retool itself and come back with stronger attacks and more intricate methods of spreading than ever before. We'll go into more detail on this below.

Operating System

Windows	MacOS	Linux	Android
Yes	No	No	No

Risk and Impact

Impact	High
Risk	High

Technical Analysis

Studying Emotet’s most recent campaign, it’s clear that a variety of different emails have been generated to lure victims into downloading the malicious attachment. While this method of infection is certainly nothing new, there appears to be one clever twist in the threat actor’s attempts to convince users to compromise their own machines.

When a user downloads an .xls attachment from one of these phishing emails, the infection vector is entirely dependent on the user enabling macros to download the Emotet dropper. Now, all files downloaded from the Internet, including email attachments such as Excel® files, are given a special flag from Microsoft by default. Known as a Mark-of-the-Web (MOTW) flag, this is a security feature originally introduced by Internet Explorer® to force saved web pages to run in the same security zone that the page was saved from. What this does is it basically forces programs to treat certain types of files more cautiously. For instance, an Excel file bearing a MotW flag will be opened in Protected View, which automatically disables macros; this is very bad news for Emotet.

In order to bypass this built-in security functionality, Emotet infections rely instead on good old-fashioned social engineering to manually override these protections. Users are finally getting more savvy when it comes to identifying suspicious attachments, but this new variant does something particularly sneaky. In an .xls attachment (ef2ce641a4e9f270eea626e8e4800b0b97b4a436c40e7af30aeb6f02566b809c) sent in this new spam campaign conducted by the Epoch4 botnet, users are instructed to move the newly-downloaded file into Excel’s ‘Templates’ folder, as shown below in Figure 4.

Seeing as this folder is automatically trusted by Microsoft, any file executed from here is ignored by the Protected View functionality, allowing any macros to run without hinderance.

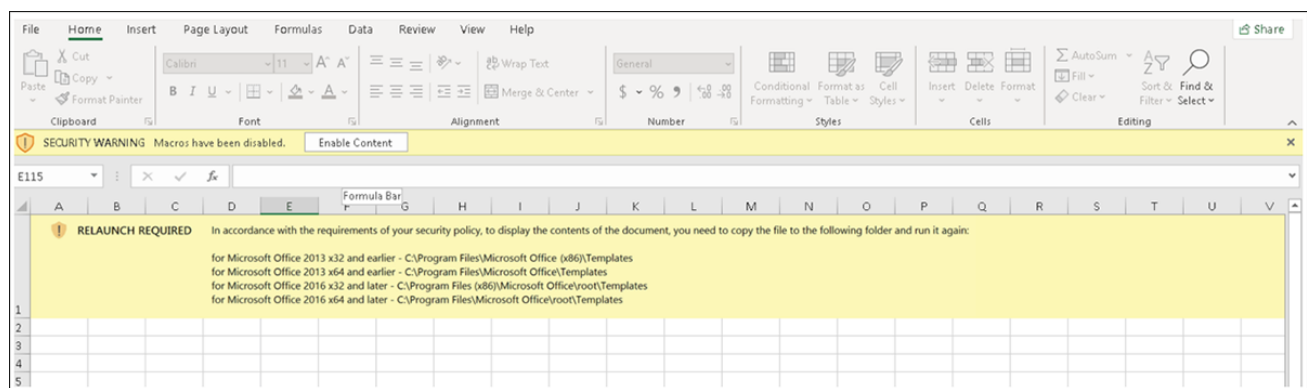


Figure 4 – Message displayed to convince users to bypass Protected View

Once the macros are run, they reach out to the Internet to download and execute the Emotet malware. Looking at Figures 5 and 6, you can see the macros used by the .xls file, as well as the malicious URLs used to download Emotet. In Figure 7, you can see the macros from a different variant of this .xls file (199a2e0e1bb46a5dd8eb3a58aa55de157f6005c65b70245e71cecec4905cc2c0) reaching out to alternate web URLs.

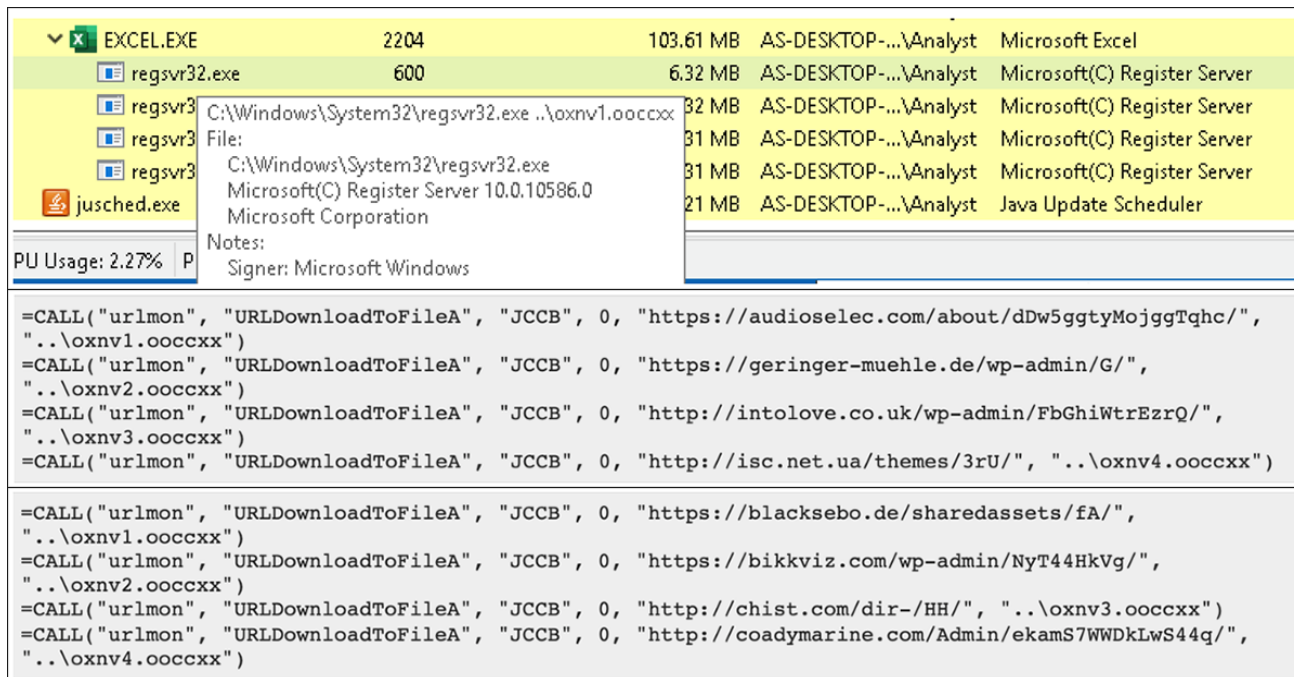


Figure 5, 6, and 7 – URLs used by macros to download Emotet droppers

From here, the Emotet dropper is downloaded to a randomly generated folder under %UserProfile%\AppData\Local as a .dll file. This .dll file is also given a randomly generated name. Once downloaded, macros use regsvr32.exe to execute Emotet, as shown in Figure 8.

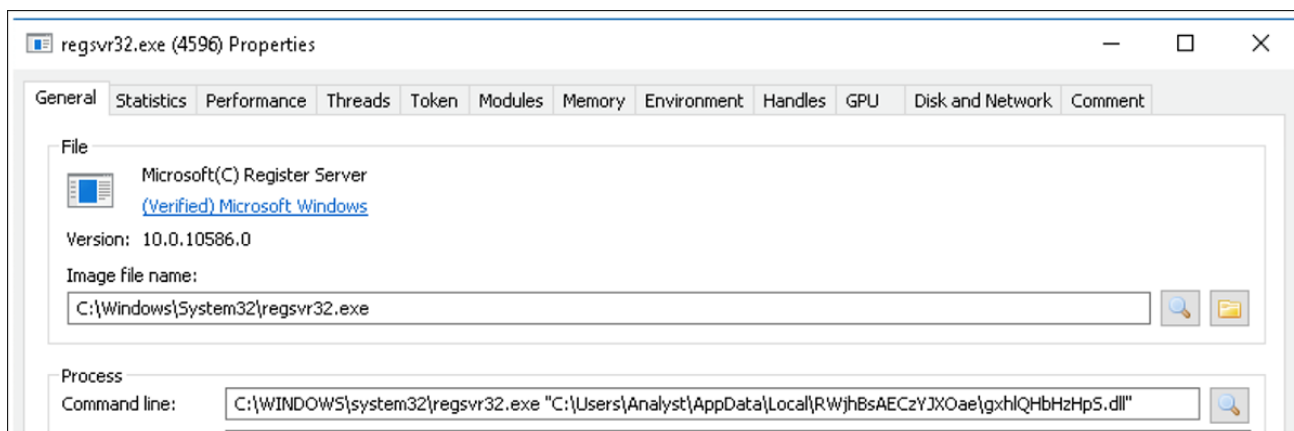


Figure 8 – Execution of Emotet dropper via regsvr32.exe

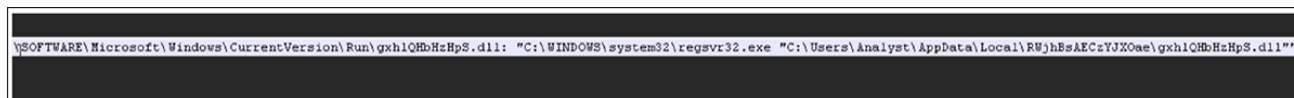
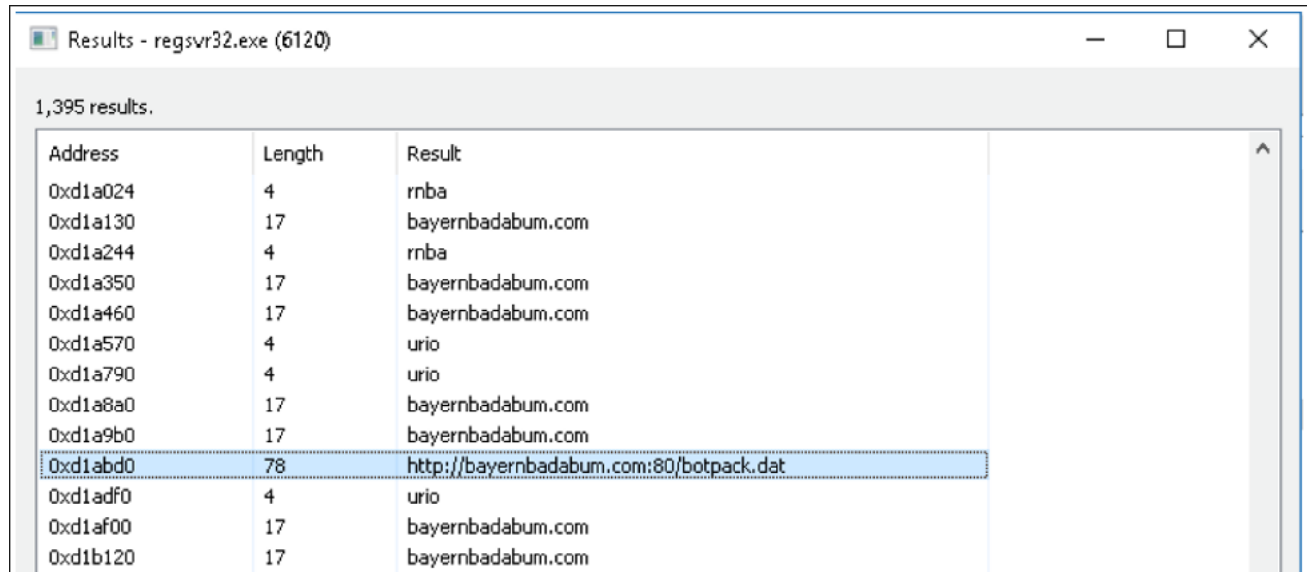


Figure 9 – Registry key created for persistence

At this point, Emotet will run in the background, reaching out to its C2 server in order to download additional malware. It also achieves persistence on the system by creating the registry key shown in Figure 9 so that it may stay active on the local machine, awaiting further instruction.

The Endgame of Emotet

Emotet, as a MaaS, focuses on the spreading of other malware. Considered to be one of the most widely disseminated malware distributors, its resurgence has been met with great concern by the industry. With the introduction of more insidious variants designed to bypass automatic security checkpoints, it now appears that its dropper is being used to download banking Trojan IcedID. It achieves this by downloading an installer, which then downloads a separate binary file from the URL `hxxps[:]//bayernbadabum[.]com/botpack[.]dat` in order to drop the final payload onto the victim's machine.



Address	Length	Result
0xd1a024	4	rnba
0xd1a130	17	bayernbadabum.com
0xd1a244	4	rnba
0xd1a350	17	bayernbadabum.com
0xd1a460	17	bayernbadabum.com
0xd1a570	4	urio
0xd1a790	4	urio
0xd1a8a0	17	bayernbadabum.com
0xd1a9b0	17	bayernbadabum.com
0xd1abd0	78	http://bayernbadabum.com:80/botpack.dat
0xd1adf0	4	urio
0xd1af00	17	bayernbadabum.com
0xd1b120	17	bayernbadabum.com

Figure 10 – URL used to download IcedID banking Trojan

As if Emotet's inbuilt module for stealing credit card information isn't bad enough, its secondary payload IcedID is more sinister still. Otherwise known as BokBot, IcedID is a modular Trojan well-known for stealing financial information. While also establishing persistence through process hollowing, it in itself is fully capable of dropping additional malware. IcedID monitors and logs Internet browser activity in order to steal sensitive information such as login details for online banking sessions. In a recently found sample of IcedID dropped by new Emotet variants, a legitimate pdb path can even be seen within the file's strings. This may speak for how 'fresh' this variant is, or possibly even still in active development.

Address	Length	Result
0x25860a0	12	%016IX
0x2586140	5	RSD51
0x2586158	45	E:\source\anubis\Lite\bin\RELEASE\ghjfgfhf.pdb
0x258619c	4	GCTL
0x25861a8	8	.text\$mn
0x25861c8	8	.idata\$5
0x25861dc	6	.rdata
0x25861ec	13	.rdata\$voltmd
0x2586204	13	.rdata\$zzzdbg

Figure 11 – PDB path found in IcedID sample (05a3a84096bc2a5cf87d07ede96aff7fd5037679f9585fee9a227c0d9cbf51)

Bumblebee, a malware loader believed to be distributed by the Conti syndicate, has also been reported as a payload being dropped by the new Emotet variants. The dropper will download a PowerShell script that reaches out to a separate URL to download and execute the Bumblebee DLL using rundll32.exe.

Conclusion

With its steady evolution over the last eight-plus years, Emotet has continued to become more sophisticated in terms of evasion tactics; has added additional modules in an effort to further propagate itself, and is now spreading malware via phishing campaigns. While it may have been dormant for a few months, it has now returned with a vengeance, making it a threat to be reckoned with for business and individual users alike.

Mitigation Tips

- Anyone can be affected by Emotet. Always remain cautious when opening email attachments, regardless of file type.
- Be sure to carefully read all security popups when you're being asked to manually enable something on your machine, particularly macros.
- Monitor accounts for unusual and unauthorized access that falls outside of the baseline (MITRE D3FEND™ techniques D3-AZET, D3-LAM).

Indicators of Compromise (IoCs)

EF2CE641A4E9F270EEA626E8E4800B0B97B4A436C40E7AF30AEB6F02566B809C –
xls Bait File

199A2E0E1BB46A5DD8EB3A58AA55DE157F6005C65B70245E71CECEC4905CC2C0
– **xls Bait File**

BB444759E8D9A1A91A3B94E55DA2AA489BB181348805185F9B26F4287A55DF36 –
Emotet Dropper

F6485AEF4BE4CB0EC50317B7F87694FB775F81733AF64C9BC6050F6806504207 –
Emotet Dropper

3D8F8F406A04A740B8ABB1D92490AFEF2A9ADCD9BEECB13AECF91F53AAC736B4
– **SMB Spreader Module**

05A3A84096BCDC2A5CF87D07EDE96AFF7FD5037679F9585FEE9A227C0D9CBF51
– **IcedID Trojan**

Malicious URLs used for downloading Emotet:

hxxp://audioselec[.]com/about/dDw5ggtyMojggTqhc/

hxxp://geringer-muehle[.]de/wp-admin/G/

hxxp://intolove[.]co[.]uk/wp-admin/FbGhiWtrEzrQ/

hxxp://isc[.]net.ua/themes/3rU/

hxxps://blacksebo[.]de/sharedassets/fA/

hxxps://bikkviz[.]com/wp-admin/NyT44HkVg/

hxxp://chist[.]com/dir-/HH/

hxxp://coadymarine[.]com/Admin/ekamS7WWDkLwS44q/

Malicious URLs used for downloading IcedID:

hxxps[:]//bayernbadabum[.]com/botpack[.]dat

References

<https://blog.cyble.com/2022/11/09/emotet-returns-targeting-users-worldwide/>

<https://www.bleepingcomputer.com/news/security/emotet-botnet-starts-blasting-malware-again-after-4-month-break/>

<https://news.vmware.com/security/vmware-report-exposes-emotet-malware>

https://twitter.com/Unit42_Intel/status/1590002190298804225

https://twitter.com/threatinsight/status/1534298451076431873?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1534298451076431873%7Ctwgr%5Ebe2909305dc964b5628509afc88bf08c38800f12%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fsecurityaffairs.com%2F132090%2Fcyber-crime%2Femotet-google-chrome-info-stealer.html

<https://www.proofpoint.com/us/blog/threat-insight/comprehensive-look-emotets-fall-2022-return>

<https://www.bitsight.com/blog/emotet-smb-spreader-back>

https://unit42.paloaltonetworks.com/banking-trojan-techniques/#post-125550-_3dy6vkm

BlackBerry Assistance

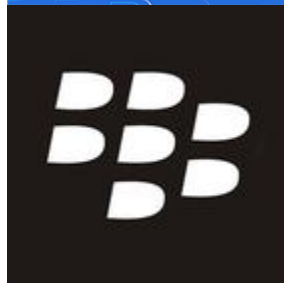
If you're battling this malware or a similar threat, you've come to the right place, regardless of your existing BlackBerry relationship.

The BlackBerry Incident Response team is made up of world-class consultants dedicated to handling response and containment services for a wide range of incidents, including ransomware and Advanced Persistent Threat (APT) cases.

We have a global consulting team standing by to assist you, providing around-the-clock support where required, as well as local assistance. Please contact us here: <https://www.blackberry.com/us/en/forms/cylance/handraiser/emergency-incident-response-containment>

Related Reading

The banner features the BlackBerry logo and tagline "Intelligent Security. Everywhere." on the left. The central text reads "THE BEST DEFENSE IS ABOUT TO BE A BEST SELLER." followed by the URL "BlackBerry.com/beacon". On the right, there is an image of the book cover for "FINDING BEACONS". The background is blue with faint binary code.



About The BlackBerry Research & Intelligence Team

The BlackBerry Research & Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.

[Back](#)