QUAKBOT Malware cleanup manual using ClamAV

Introduction:

ClamAV is an open source (GPLv2) anti-virus toolkit, designed especially for e-mail scanning on mail gateways. It provides several utilities including a flexible and scalable multi-threaded daemon, a command line scanner and advanced tool for automatic database updates. The core of the package is an anti-virus engine available in a form of shared library.

Fixes for the following operating systems:

1. Linux
2. CentOS/RHEL
3. Fedora
4. Windows (WSL)

Installation:

- `Linux:   sudo apt-get install -y clamav clamav-daemon`
- `CentOS:  sudo yum install -y clamav clamav-update`
- `Fedora:  sudo dnf install -y clamav clamav-update`
- `Then update ClamAV database:  sudo freshclam`

Configuration: We shall configure ClamAV to scan for Quakbot signatures

- `sudo sed -i '/^#ScanArchive/s/^#//' /etc/clamav/clamd.conf   #Enable scanning inside archives`
- `sudo sed -i '/^#ScanPE/s/^#//' /etc/clamav/clamd.conf         #Enable scanning of PE files (Windows executables)`
- `sudo sed -i '/^#ScanMail/s/^#//' /etc/clamav/clamd.conf       #Enable scanning of mail files`
- `sudo sed -i '/^#PhishingSignatures/s/^#//' /etc/clamav/clamd.conf #Enable phishing signatures`
- `sudo sed -i '/^#HeuristicScanPrecedence/s/^#//' /etc/clamav/clamd.conf  #Enable heuristic scanning`
- `sudo sed -i '/^#PhishingScanURLs/s/^#//' /etc/clamav/clamd.conf  # nable phishing URL scanning`

and exclude unnecessary files and directories:

- `sudo sed -i '/^ExcludePath/s/^#//' /etc/clamav/clamd.conf`

We can then configure ClamAV to remove the detected files

- `sudo sed -i '/^#RemoveInfected/s/^#//' /etc/clamav/clamd.conf`

We can then restart ClamAV to apply changes and run

```
sudo systemctl restart clamav-daemon
clamscan -r
```

Since Quakbot is primarily spread through phishing emails some steps can be taken to prevent infection:

1. Email Filtering: Check your Office 365 email filtering settings to ensure you block spoofed emails, spam, and emails with malware.
2. Zero-hour Auto Purge (ZAP): Enable ZAP in Exchange Online, which is an email protection capability that retroactively detects and neutralizes malicious messages that have already been delivered in response to newly acquired threat intelligence.
3. Advanced Threat Protection for Email: As Qbot is typically delivered via phishing emails, the most effective way to protect against this malware is with Advanced Threat Protection for email.

Notes:

- Update ClamAV's database before performing cleanup for best results.
- Check ClamAV logs for troubleshooting: grep clamav /var/log/syslog
- Prevention is the best solution to Qbot thus avoid suspicious emails and apply the aforementioned preventative steps for best results against Qbot
- The provided bash scripts should be used with the appropriate operating systems to remove Qbot from infected systems.