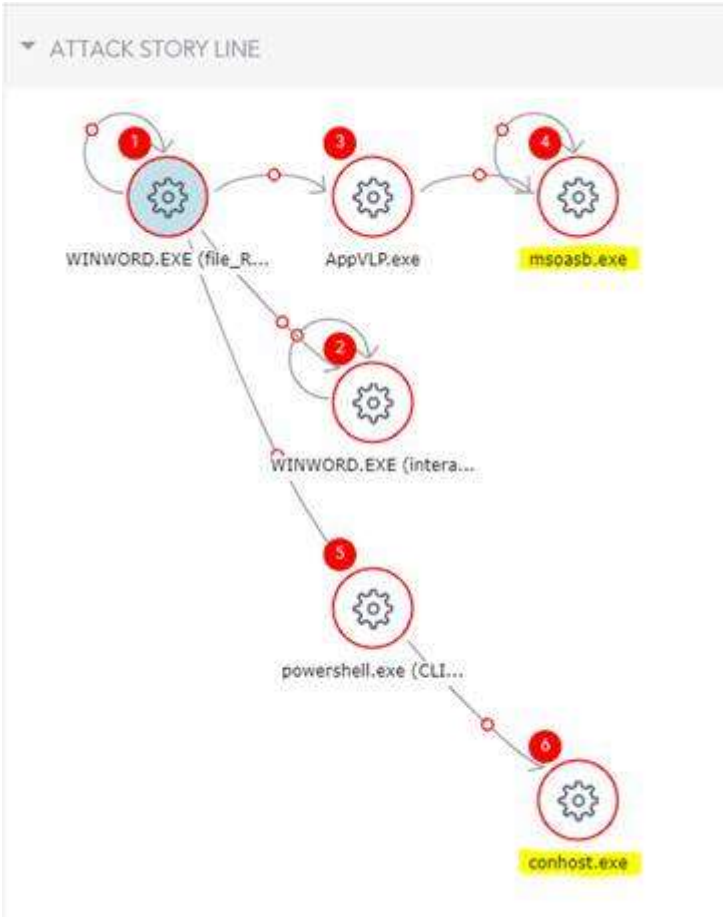
Sentry Defender detects new UNKNOWN Botnet version

Without boring you with techie details, this is a report so you understand the threats targeting you, and how **Sentry Defender** will keep you safe. When detected this was an UNKNOWN threat – there was no record of it on **Virus Total**, which is where all new threats are registered and shared to the cyber security community. It took 2 days to show up as the new version of the **Emotet Botnet** – a PC takeover malware which is so nasty and well known it has its own Wikipedia page: https://en.wikipedia.org/wiki/Emotet

Imagine how many devices were infected in the two days before the Anti-virus software vendors caught up with this new threat…

Our story starts when the user downloaded a Word document (an email attachment pretending to be an order) and the file had some malicious code in it. When the doc was opened the code ran and started up applications in the background:

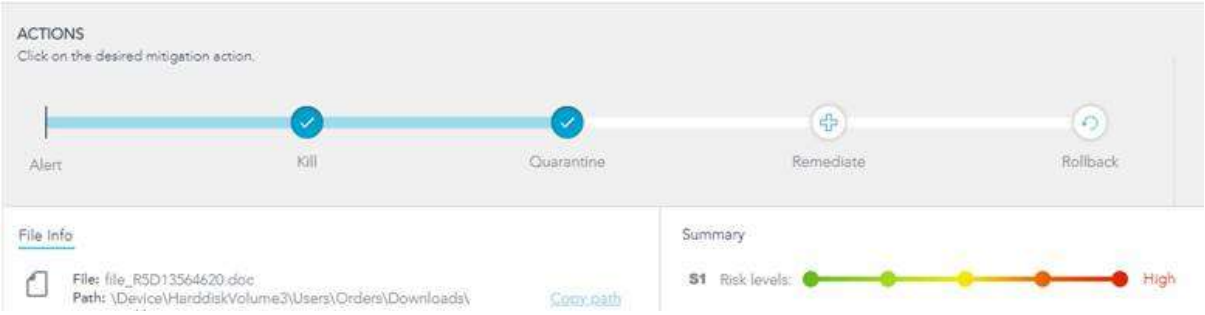


msoasb.exe shown above installed a key logger to track all user input (usernames, passwords, etc.)

conhost.exe (connection host application) tried to connect to various servers around the world – 9 in Finland, 2 in the Netherlands, 1 in Austria, and 28 in the US:

Sentry Defender detected the unusual behaviour and killed the threat before any data could be captured or exfiltrated to the cyber criminal's servers!

The file was then quarantined it so it cannot be activated again:



This user has an international customer base, so they receive orders in various formats, with varying degrees of English language ability, making it much harder for them to spot malicious emails Vs actual orders. But they don't just rely on traditional antivirus, they have **Sentry Defender** to keep them safe and properly protected!