A TLC srl
Via 1° Maggio, 26 / 60131 Ancona (Italy)
Tel. +39 071 250651 / Fax +39 071 2506518
www.aethra.com - info@aethra.com

Chiarimento riguardo all'articolo "Aethra Botnet" apparso su Voidsec.com

Aethra Telecommunications desidera fare chiarezza relativamente a quanto riportato nell'articolo "Aethra Botnet" pubblicato sul blog Voidsec.com, con particolare riferimento a successivi rilanci incompleti e/o non corretti.

E' opportuno sottolineare che non esiste evidenza alcuna di brecce di sicurezza e/o di software malevoli installati all'interno degli apparati presenti presso le reti dei clienti Aethra Telecommunications, come invece lasciato intendere da alcune citazioni dell'articolo stesso.

Aethra Telecommunications ha verificato, anche alla luce di un costruttivo scambio di informazioni con gli autori dell'articolo originale, che gli eventi descritti sono riconducibili all'abilitazione (di default sino alla versione 5.6.18 del sistema operativo ATOS NT) di una funzionalità specifica che, se non debitamente protetta come da prassi tramite l'impiego di una *access list*, potrebbe prestarsi ad un uso potenzialmente malevolo realizzando quanto segnalato dagli autori dell'articolo.

La descrizione di tale potenziale problematica era già stata segnalata da Aethra Telecommunications in data 28 Gennaio 2015 in un bollettino tecnico presente all'interno dell'area download del sito www.aethra.com e inviato direttamente ai propri clienti.

Aethra Telecommunications realizza router dedicati alla clientela business rivolgendo un'attenzione particolare proprio alle problematiche di sicurezza di reti ed apparati e si rende disponibile per qualsiasi chiarimento o integrazione.

Link all'articolo originale su Voidsec.com: http://voidsec.com/aethra-botnet/
Link al bollettino tecnico: http://www.aethra.com/site/wp-content/uploads/2015/02/SSH-Service-Access.pdf

Luca Messina

CTO/CMO

Aethra Telecommunications

A TLC S.R.L.

Ancona 26/01/2016

Clarification on the “Aethra Botnet” article published on Voidsec.com

Aethra Telecommunications intends to clarify what has been reported on the “Aethra Botnet” article published in the Voidsec.com blog, in particular with regards to some of the third party posts that followed up and referred to the original article in a non-correct / non-complete way.

It is important to underline the fact that there is no evidence whatsoever of security breaches and / or malware present in any of the Aethra Telecommunications routers installed in the customers’ networks, contrary to what some of the subsequent posts seemed to imply.

Aethra Telecommunications verified, also thanks to a productive exchange of information with the authors of the original article, that the events described in the Voidsec.com post can be attributed to a specific functionality provided by our routers (enabled by default in the ATOS NT operating system up to version 5.6.18). In case this feature is not duly protected as in any good practice by the use of *access lists*, it could be potentially exploited in order to realize what has been described in the article.

This potential issue had already been detailed by Aethra Telecommunications in a technical bulletin issued on Jan, 28 2015 that can be found on the Aethra Telecommunications website download area and had been directly sent to our customers.

Aethra Telecommunications designs business-class routers with particular attention to the security of networks and devices, and is available for any clarification on the topic.

Link to the original article on Voidsec.com: http://voidsec.com/aethra-botnet/
Link to the technical bullettin: http://www.aethra.com/site/wp-content/uploads/2015/02/SSH-Service-Access.pdf

Luca Messina

CTO/CMO

Aethra Telecommunications

A TLC S.R.L.

Ancona 26/01/2016