Security Alert:
Critical

EventTracker
Actionable Security Intelligence

Contoso - EventTracker: Critical potential breach by unknown process from low reputation IP

Summary

Time: 2017-11-20 00:54:51

Description: Network connection established between GNET-SL-WKSTN61.contoso.local and 197.231.203.6 by an unknown process FileZillaServer.exe.

Event ID:8009

Cause: This event is generated when a network connection is established between a local system and a remote IP address by an unknown process.

Resolution: Check to see if the process is known and safe, and then add to the whitelist. If it is unknown and unsafe, terminate the process and block these IP addresses.

This alert is provided to you by EventTracker, your partner for

Actionable Security Intelligence.

Need further guidance? Visit the

EventTracker Knowledgebase or

contact us

Full Details

Time:	2017-11-20 00:54:51
Type:	Info
Computer:	GNET-SL-WKSTN61.contoso.local
Asset Value:	Low
Source:	EventTracker
Event ID:	8009
User:	N/A\battled
Description:	Unknown process FileZillaServer.exe launched on GNET-SL-WKSTN61.contoso.local is connecting to 197.231.203.6. User Name: CONTOSO\battled Process Details:- Process Name: FileZillaServer.exe Process ID: 10800 Image File Name: C:\Program Files (x86)\FileZillaServer\Phone\FileZillaServer.exe Local Address: GNET-SL-WKSTN61.contoso.local Local Port : 17166 Remote Address: 197.231.203.6 Remote Port: 443 Reputation provider: Borderware Borderware Overall Reputation Details:- Reputation Score: 100 Reverse DNS: none ISP Location: Hargeysa,WoqooyiGalbeed,Somalia Reputation Detail [Email]:- Clean: 0% Viruses: 1.82% Spam: 98.18% Malformed Messages: 0% Suspicious Messages: 0%