

Αυτή ήταν η εικόνα που αντίκρυσαν χιλιάδες χρήστες μετά την επίθεση του ransomware WannaCry.



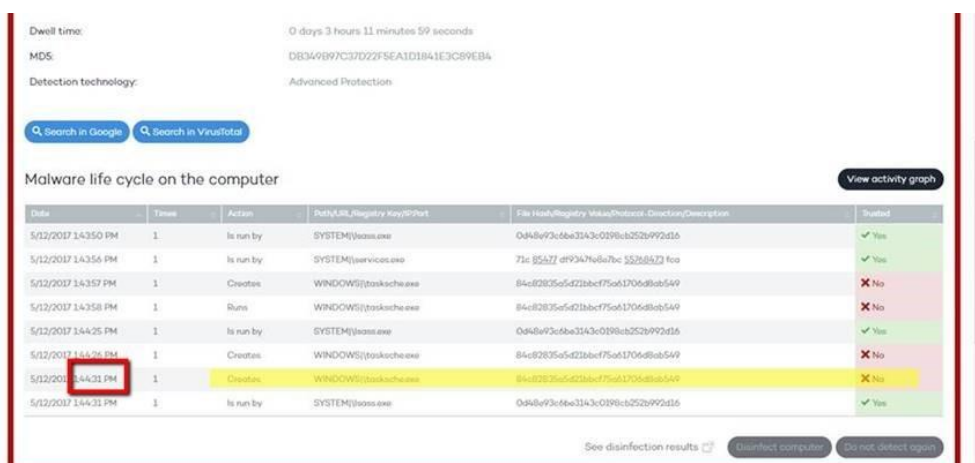
Γιατί πήρε τόσο έκταση το πρόβλημα:

1. Οι παραδοσιακές λύσεις antivirus επέτρεψαν την εκτέλεση του άγνωστου κακόβουλου προγράμματος.
2. Τα εμβόλια Ransomware, anti-exploits και HIPS απέτυχαν να προστατεύσουν εκατομμύρια υπολογιστές.

Αναρωτιέστε αν υπάρχει τρόπος να αποφύγετε να είστε ένα από τα θύματα αντίστοιχων κυβερνο-επιθέσεων στο μέλλον?

Η μοναδική λύση ασφαλείας που μπόρεσε να αποκλείσει άμεσα την επίθεση WannaCry ήταν η λύση EDR της Panda Security "Adaptive Defense / Adaptive Defense 360".

Δείτε παρακάτω ένα χαρακτηριστικό παράδειγμα για το πώς το Adaptive Defense / Adaptive Defense 360 μπλόκαρε αμέσως την επίθεση σε ένα από τους πελάτες που το χρησιμοποιούν, την Παρασκευή 12/05/2017 στις 1:43:50.



Date	Time	Action	Path\URL_Registry Key\Port	File Hash\Registry Value\Process...Description	Status
5/12/2017	1:43:50 PM	Is run by	SYSTEM\services.exe	0468973c66e3143c0198c525b992d16	✓ Yes
5/12/2017	1:43:56 PM	Is run by	SYSTEM\services.exe	71c85a77e9934768a7bc55268527fca	✓ Yes
5/12/2017	1:43:57 PM	Creates	WINDOWS\taskcache.exe	84c82835c5422b6ef750d1706d80b549	✗ No
5/12/2017	1:43:58 PM	Runs	WINDOWS\taskcache.exe	84c82835c5422b6ef750d1706d80b549	✗ No
5/12/2017	1:44:25 PM	Is run by	SYSTEM\services.exe	0468973c66e3143c0198c525b992d16	✓ Yes
5/12/2017	1:44:26 PM	Creates	WINDOWS\taskcache.exe	84c82835c5422b6ef750d1706d80b549	✗ No
5/12/2017	1:44:31 PM	Creates	WINDOWS\taskcache.exe	84c82835c5422b6ef750d1706d80b549	✗ No
5/12/2017	1:44:31 PM	Is run by	SYSTEM\services.exe	0468973c66e3143c0198c525b992d16	✓ Yes

Βεβαιωθείτε ότι έχετε επενδύσει σε μια λύση Cyber Security που είναι σε θέση να ταξινομήσει οποιαδήποτε τρέχουσα διαδικασία σε goodware, malware και άγνωστη (οποιαδήποτε άγνωστη διαδικασία δεν θα πρέπει να επιτρέπεται να εκτελείται μέχρι να κατηγοριοποιηθεί από ένα εργαστήριο malware). Η ταξινόμηση πρέπει να γίνεται αυτόματα! Άλλες λύσεις ασφαλείας αντιθέτως ταξινομούν μόνο κακόβουλο λογισμικό ή πιθανές ύποπτες διεργασίες.