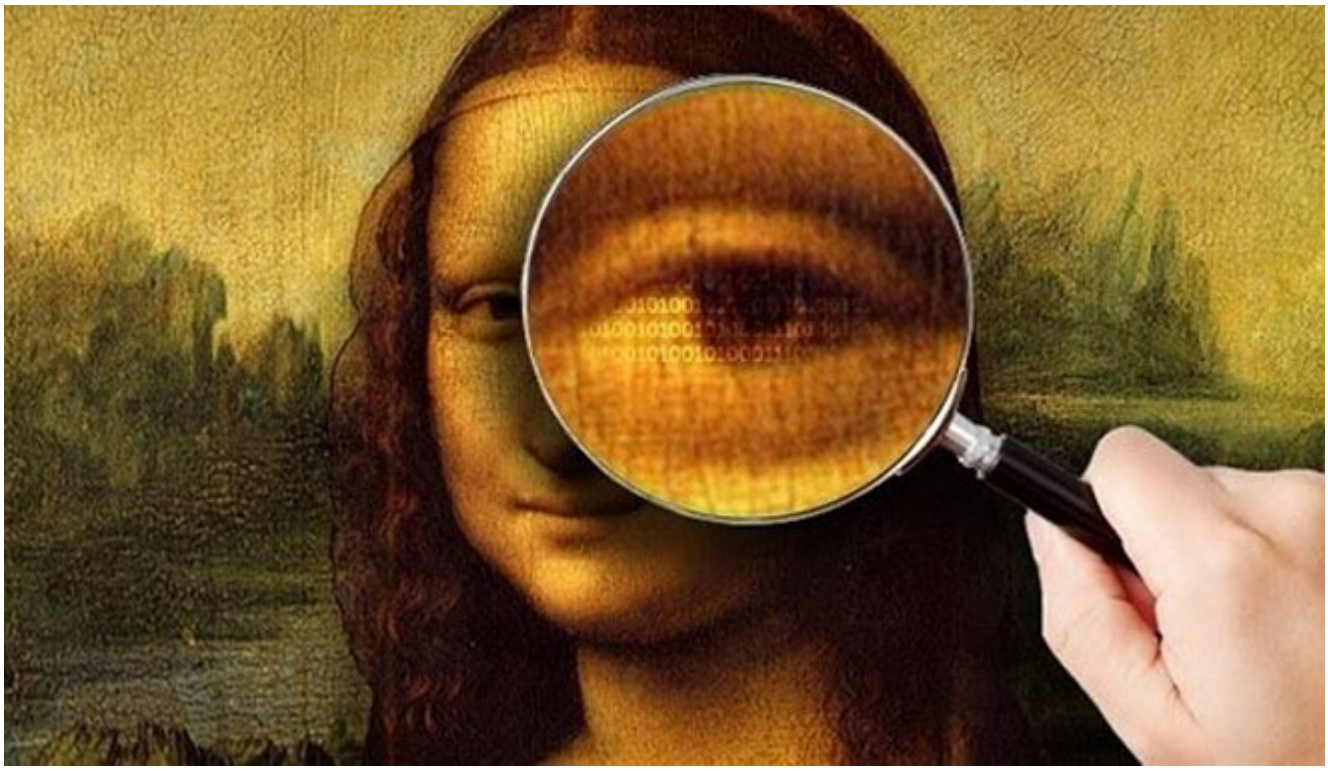
7 Μαΐου 2016

Πώς αποφεύγουν τον εντοπισμό τα Remote Access Trojans;

/ Πεμπτουσία

Image not found or type unknown



Η τέλεια τεχνική για την αποφυγή ανίχνευσης των RATs: Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν fileless malware σε συνδυασμό με στεγανογραφία

Η εταιρεία ασφάλειας SentinelOne ανακάλυψε μια νέα τεχνική που αξιοποιείται από τους προγραμματιστές κακόβουλου λογισμικού, η οποία περιλαμβάνει την απόκρυψη των πιο επικίνδυνων μερών των Remote Access Trojans (*RATs*) στο εσωτερικό της μνήμης του λειτουργικού συστήματος και τη χρήση αρχείων PNG ως configuration files.

Οι ερευνητές παρατήρησαν για πρώτη φορά τη πρακτική αυτή σε μια σειρά από κρατικά επιχορηγούμενες επιθέσεις εναντίον ασιατικών χωρών. Το κακόβουλο λογισμικό που αξιοποιούταν για την πραγματοποίηση των επιθέσεων ήταν το NanoCore (επίσης γνωστό και ως Nancrat), ένα RAT που εντοπίστηκε για πρώτη φορά την άνοιξη του 2014.

Στη συγκεκριμένη εκστρατεία, η απειλή διανεμόταν ως αρχείο EXE, που όταν εκτελούταν εξήγαγε με τη σειρά του ένα δεύτερο εκτελέσιμο. Το πρώτο εκτελέσιμο, το οποίο δεν εμφάνιζε κακόβουλη συμπεριφορά, αποθηκευόταν στο δίσκο, ενώ το δεύτερο εκτελέσιμο εισαγόταν απευθείας στη μνήμη του συστήματος, με τη βοήθεια ενός κρυπτογραφημένου DLL και μιας σειράς από αρχεία PNG.

Σύμφωνα με τους ερευνητές της SentinelOne, και δεδομένου ότι το δεύτερο EXE δεν «αγγίζει» ποτέ τον χώρο αποθήκευσης, οι κλασσικές λύσεις antivirus δεν μπορούν να ανιχνεύσουν την κακόβουλη συμπεριφορά του, και μόνο τα προϊόντα ασφαλείας που σαρώνουν τη μνήμη του λειτουργικού είναι σε θέση να το εντοπίσουν.

Και εάν αναρωτιέστε ποιος είναι ο ρόλος των αρχείων PNG, αυτός έγκειται στην αποθήκευση των ρυθμίσεων που απαιτούνται για τη λειτουργία των RATs. Όλες οι εικόνες που χρησιμοποιούνται είναι απλά ένα χάος από τυχαία pixels, όταν όμως το δεύτερο εκτελέσιμο διαβάσει το περιεχόμενό τους, τα pixels αυτά σχηματίζουν τμήματα του ωφέλιμου φορτίου (payload) του RAT καθώς και τις ρυθμίσεις διαμόρφωσής του (configuration settings).

Πηγή: secnews.gr