ba0jy

DNSMon

Ongoing Credit Card Data Leak [Continues]

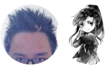
DNSMon is a network-wide DNS malicious domain analysis system we build here at 360Netlab. With the 10%+ total DNS traffic coverage in China, plus the other multi-dimensional security data and security...

· May 14, 2019 · 3 min read

DNSMon

信用卡数据泄漏持续进行中 [快速更新]

DNSMon是一个全网DNS异常发现分析系统。基于我们可以看到的中国地区 10%+ 的DNS流量，加上我们多年积累的其他多维度安全数据以及安全分析能力，我们可以在一个独特的视角来实时监测 全网 每天 正在发生 的事情，我们可以 “看见” 正在发生的威胁。 黑客在行动 5月8号，我们发布文章 <信用卡数据泄漏持续进行中>，揭露了一个通过入侵购物网站来窃取信用卡信息的案例。文章发布后不久，我们发现黑客们开始做调整，原始域名 magento-analytics[.]com 已经下线。 但不久，我们的 DNSMon 系统在UTC时间 2019-05-13 凌晨时候捕捉到该黑客的2个更新，被用于同样的信用卡信息窃取。 更新1: 启动了一个新域名：jqueryextd[.]at 对应的恶意JS链接为 “hxxps://jqueryextd.at/5c21f3dbf01e0.js”，脚本中上报地址也对应的改为了“hxxps://jqueryextd.at/gate.php"

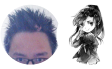


· May 14, 2019 · 3 min read

DNSMon

Ongoing Credit Card Data Leak

Our DNSMon flagged an abnormal domain name magento-analytics[.]com, been used to inject malicious JS script to various online shopping sites to steal the credit card owner/card number/expiration time/ CVV information.



· May 8, 2019 · 6 min read

数据泄漏

信用卡数据泄漏持续进行中

我们的DNSMon发现了一个异常域名 magento-analytics[.]com，通过持续的跟踪，以及和WEB数据的关联，发现该域名通过渗透侵入购物网站，植入自己的JS脚本，实时判定用户信用卡的输入情况，将信用卡的 所有人/卡号/过期时间/CVV 信息回传，实现对信用卡数据的窃取，进而可以盗刷。当前估算，失陷的购物网站应该超过1000+。

· May 8, 2019 · 10 min read