

Gafgyt Tel/
SSH IP
Gafgyt NetCore 53413 33.04% 26.08%
17.82%
NetCore NetCore
2014
NetCore 53413/UDP
Gafgyt 33230 “ ”
Gafgyt C2
“ NetCore 53413/UDP Gafgyt
” 53413
Gafgyt



1 18

“ 2017
”

“
”

“
”

木马程序

ŵ ş f O . ş. ⅜ u Ƒ / ľ . ض

Windows XP 5.1.2600 Service Pack 3 Build 2600

IE6 Firefox Google Chrome
Office 2003 Flash WPS FoxitReader
Adobe Reader

源 IP	源端口	目的 IP	目的端口
127.0.0.1	null	127.0.0.1	2000

中文标题	RubyMiner Monero Cryptominer 24 30
英文标题	RubyMiner Monero Cryptominer affected 30% of networks worldwide in just 24h
作者及单位	Pierluigi Paganini; SecurityAffairs
内容概述	RubyMiner Windows Linux PHP Microsoft IIS Ruby on Rails Monero POST base64 bash cronjob shell robots.txt cryptominer robots.txt RubyMiner kill web robots.txt
链接地址	http://securityaffairs.co/wordpress/67865/malware/rubyminer-monero-cryptominer.html