‰ώ Ð Ғ ô A_pbgl_j ل 4 ت و h ئ p Ř

CERT GUID %TEMP%\[random]. CERT
ini %APPDATA%\Microsoft\
Cardinal Windows\IEConfig .lnk
2017 Carp .lnk
C:\Windows\System32\
WindowsPowerShell\v1.0\powershell.exe
-windowstyle hidden “ %APPDATA%\
Cardinal 1.7.2 Microsoft\Windows\IEConfig\[random]\
sqlreader.exe sqlreader.exe
.Net
.Net Internet
RegSvcs.exe RegAsm. VPN
dll exe VPN
.Net dll
” strings ”

dll dll Cookie

β γ

BD YARA BD

(WinXP) Win7 x86

◆概要信息

安天周观察
2019 04 15 (179) 4 antiylab

“
” “ ” G20
24
“ G20
” G20
“
“ ” “ ” “ 2005
” ”
60
2016 G20

类 型	内 容
	Mirai IoT
	Mirai Compiled for New Processors Surfaces in the Wild
	Ruchna Nigam
	Mirai Altera Nios II OpenRISC Tensilica Xtensa Xilinx MicroBlaze Mirai