Trickbot

ProximityUntilCache32.tlb

CERT DLL DLL

ProximityUntilCache32.tlb

2017 srv DLL

NSA C2 Internet

VPN

DGA VPN

C2 eee.asf3r23.

cf *.drawal.tk Crypt CERT

NSA

Crypt

%win_dir%\IME\

Crypt\ spoolsv.exe payload

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述木马程序进行有效检测，下为其自动形成的分析报告：

文件名	srv64
文件类型	BinExecute/Microsoft-DLL[-X64]
大小	563 KB
MD5	C70673F416E3C3EE0B194FF0966E0A86
病毒类型	[redacted]
威胁名称	Trojan/Win64.Miner
判定依据	

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=C70673F416E3C3EE0B194FF0966E0A86

IP		IP	
/ ˚ f	Ã¾		

操作系统	内置软件
WinXP SP3 build 2600	IE6 Firefox Google Chrome Office 2003 Flash WPS FoxitReader Adobe Reader

PID		
1980	rundll32.exe	"C:\WINDOWS\system32\rundll32.exe" c:\ec04764149f14d55a23980e61b926009\share\target.dll,DllMain

UDP

rx Wet

rx server security cks

rigi Paganini

Nginx HTTP/2 Nginx 1.9.5
5 5 DoS CVE - 2018 - 16844 CPU
inx dule CVE - 2018 - 16845
MP4 nginx 1.1.3 1.0.7

os / /securityaffairs.co/wordp cking/nginx - server - dos - flaws.html