SLUB

CERT \ProgramData\update\

GitHub

SLUB gist cmd

GitHub tokens

Slack ʎ ʞ DT Ǝ

SLUB

Q

DLL PowerShell

^

SLUB

CVE-2015-1701

SLUB Internet

VPN

木马程序 β VPN ʏ

3 20

Ł ˬ Ï BD ɟ ᒐ ɻ YARA ᒐ ɟ ſ

Ɱ ᒐ ɻ Ł Ḥ ᒐ ɻ ë ᒐ ɻ Ł ѽ ˢ BD ɟ ᒐ ɻ Ů ᒐ Ł ≡

ᒐ ɻ ɟ ᒐ ɻ Ů ᒐ ɻ ˝ (WinXP) ᵩ ſ

ᒐ ɻ ˝ Ѓ Win7 x86 Є ᒐ ɻ й ᒐ ɻ ˋHW

文件名	43221eb160733ea694b4fdda70e7eab4a86d59c5f9749fd2f9b71783e5da6dd7
文件类型	BinExecute/Microsoft.DLL[:X86]
	837 KB
KB3	F3004DDAEF5B8C18883E716DDA966141
	[redacted]

- Trojan/Win32.RunDll

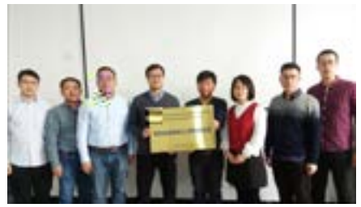
IP		IP	
192.168.122.111	1025	192.168.122.1	53
192.168.122.1	53	192.168.122.111	1025
0.0.0.0	68	255.255.255.255	67
192.168.122.111	138	192.168.122.255	138
192.168.122.1	67	192.168.122.111	68
192.168.122.111	137	192.168.122.255	137
192.168.122.111	123	13.65.88.161	123

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=F3004DDAEF5B8C18883E716DDA966141

PE	tls	PE TLS
PE	GCC	GCC GCC

UDP

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 04 月 01 日 (总第 177 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费流





中文标题	ZOLL 27
	ZOLL notiÿes over two hundred thousand patients of data exposure
作者及单位	Ryan Stewart
内容概述	ZOLL 2018 11 8 2018 12 28 ZOLL ZOLL 1 ZOLL ZOLL 277,319
接地址	https://cyware.com/news/zoll-notiÿes-over-two-hundred-thousand-patients-of-data-exposure-2e67a78a