EVILNUM

CERT 666
C2 IP
EVILNUM EVILNUM
lnk
CMD
.Net JS
EVILNUM Cookie
JavaScript EVILNUM Internet
.Net VPN
.Net VPN
JS
C2 CERT
GitHub

β γ

Ł Ï BD Ǝ ᘜ ɻ YARA ᘜ Ǝ ſ
Ɱ ᘜ ɻ Ł Ꮋ ᘜ ɻ ë ᘜ ɻ Ł ѽ ᘜ Ǝ BD Ǝ ᘜ ɻ ů ᘜ Ł ≡
ᘜ ɻ Ǝ ᘜ ɻ ů ᘜ ɻ ˝ (WinXP) ҽ ſ
ᘜ ɻ ˝ Ѓ Win7 x86 Є ᘜ ɻ й ᘜ ɻ ѝ HW

◆ 概要信息

	bee6c5a506d6fb2cc129443c74b7676fbb9a79b53b92b2cac4c7fb8209592714
	BinExecute/Microsoft.EXE[:X86]
	21 KB
KB3	8147EAD27C482AC705318B275A9B6830
	木马程序
-	Trojan/Win32.Occamy

https://antiy.pta.center/_lk/details.html?hash=8147EAD27C482AC705318B275A9B6830

◆ 运行环境

WinXP 5.1.2600 Service Pack 3 Build 2600	IE6 Firefox Google Chrome Ofŷce 2003 Flash WPS FoxitReader Adobe Reader

◆常见行为

◆ UDP 信息

CCTGA 2018

CNCERT

类 型	内 容
	0day
	New zero-day vulnerability CVE-2019-0859 in win32k.sys
	Vasily Berdnikov, Boris Larin, Anton Ivanov
	2019 3 win32k.sys 0day CVE-2019-0859 CreateWindowEx Use-After-Free 64 Windows HMValidateHandle ASLR Base64 PowerShell PowerShell PowerShell shellcode shellcode CreateThread shellcode shellcode HTTP shell 3
	https://securelist.com/new-win32k-zero-day-cve-2019-0859/90435/