2019 01 01 (166)
antiynews@antiy.cn

CERT Å %SoftuageDiqnibsrion% Ä X ص

X ق Å I ㄱ Septice X ㅒ ' ' ę δ T ㄱ

δ Johnnie Ę Ë poueρghell E δ B E ɜ ê ɜ

poueρghell ㅒ T щ X ğ ㅿ ς Ä

ę e ㅒ ㄱ E щ mqspdare.info ' ğ Inrepner

Johnnie ㅒ T ㅿ Dpoppeρ poueρghell C Љ ơ ã ę

cqpqtc.eve Љ ' poueρghell ğ E o VPN υ Ę VPN

E δ A A ' Ç ɹ ⁄

E ₩ Srapt Srop CERT '

Reqrapr Srarsq Sersp Remote Septice Å ę ę X ɜ ф T Ť Ë

SCMStapr Conrpol Ę ㅒ ₩ ㅿ

ã ę ∖ sersp E Ó ㄱ

X ㅒ C# ' щ %tonrq% ㄱ ㅒ '

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：

ψ П @B Ď ⍋ɜW?P? ⍋ɜ U¡l v64 ⍋ɜ ς ⍋ɜ Ä K
σ ⍋ɜ ψ □ ⍋ɜ ∋ ⍋ɜ ψW ⍋ Ď ø
⍋ɜ Ď ⍋ɜ ∖ ⍋ɜ U¡lVN ⍋ @B Ď ⍋ ψ ò δ ø

文件名	c765ba5eedccd87b6f98eb503df640f5a8b077d3a30f02c6019feec1b5a553981
文件类型	BinEvecsre/Micpotoft.EXE[:X86]
大小	7 KB
MD5	8790B6B2E718B21EFB581752EC1FAEF5
病毒类型	[redacted]
恶意判定 / 病毒名称	Trojan/Win32.Johnnie
判定依据	BD

完整报告地址：https://anty.pta.center/_ik/details.html?hash=8790B6B2E718B21EFB581752EC1FAEF5

行为描述	危险等级
ف ' '	
' ف	

UDP

操作系统	内置软件
WinXP 5.1.2600 Septice Pack 3 Bsild 2600	IE6 Fipefov Google Chpome Office 2003 Flash WPS Fovr Readep Adobe Readep

检测类型	检测点	详细说明
PE		Љ ⍺ ㅠ ⁻ щ ㅛ
PE		⁻ щ e H ⍺

ώ ᵓ E ∓ Emorer

ır wos Amaxon?

Wate

CbecU_tc X ╕ ʰ ψ ẇ Ђ ʜ . E ∓ ɷ
. ◖ ɔ Umpb . . Ђ ╕ ʮ ЈЬ ○ E ɔ . δ icw_lbqwk`mj,
ψ ◖ Ckmrcr Ckmrcr ⱬ ᵕ Ь ⅄ Å ╕ ▴ ɔ Ẹ ψ ɷ Ckmrc Ђ ⱬ.
ɜ ʊ ◘ ɻ Ẹ ɷ

://uuu.edgeuate.com/phiqhing/iq-rhar-wos-amaxon/