CERT XOR Process

M00nD3V Logger M00nD3V Logger Explorer Process Hacker SMTP/ FTP/

URL Crypto.dll

M00nD3V Logger 5000

zip "99ed2fc7-0fdc-42ef-8b82-78d1c7c554e3" Rijndael256

M00nD3V Logger StubConfig Base64

SMTP/FTP/ SbieDll.dll Wireshark

BouncyCastle AceQualifier AccessDenied M00nD3V “ WorldSid ” Logger

β γ

BD YARA Win7 x86 BD WinXP)

	c23b33ddb4e0cfa52b9242648f5cb7a6ee916b4ba1e6f547d8d5ef543dccbb9d
	BinExecute/Microsoft.EXE[:X86]
	250 KB
KB3	BF8801BCD5A196744CCD0F863F84DF71
	[redacted]
-	Trojan[Spy]/MSIL.Siplog.B
	BD

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

DLL	

“ ”

antiynews@antiy.cn

	Ghost Squad Hackers	ESA
英文标题	Ghost Squad Hackers defaced a second European Space Agency (ESA) site in a week	
	Pierluigi Paganini	
	https://securityaffairs.co/wordpress/106111/hacking/esa-site-defaced-again.html	