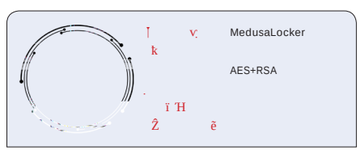
2020 7 20 (239)
antiynews@antiy.cn



“ HOW_TO_RECOVER_DATA.html ”

USER_ID

CERT

MedusaLocker

2019 9

IEP

MedusaLocker

VPN

MedusaLocker MedusaLocker AES+RSA

APPDATA \Roaming\ MedusaLocker

“ Readinstructions ”

MedusaLocker

木马程序

	269.exe
	BinExecute/Microsoft.EXE[:X86]
	338 KB
KB3	3EA4DFE71D3BDB4B0A5B0D472433628A
	[redacted]
-	Trojan/Script.AGeneric
	Trojan/Win32.Kryptik

, ,	
.....	.....

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

DLL	



3.

ATT&CK

ATT&CK

ATT&CK

EDR

0day

/

ATT&CK

EDR

EDR

EDR

ATT&CK

EDR

ATT&CK

ATT&CK

ATT&CK

ATT&CK

ATT&CK

1.

2019 ATT&CK

2019

2.

2020 7 20 (239)
antiynews@antiy.cn

	M00nD3V Logger
英文标题	Deep Dive Into the M00nD3V Logger
	Rohit Chaturvedi&Naveen Selvan
	https://www.zscaler.com/blogs/research/deep-dive-m00nd3v-logger