ERIS

木马程序

Ł ˛ Ï BD ƒ ᶐɻ YARA
Ɱ ᶐɻ Ḥ ᶐɻ ë ᶐɻ ̈ Ḥ ᶐɻ Ɱ
ч ƒ ᶐɻ ŭ ᶐɻ˜ (WinXP) ᶐɻ ᶍ ¡ Dž ŕ , ₈ Ԓ
ƒ ᶐɻ й ᶐɻ ᶐɻ `H

髭貌生物分析

	5 1 580 5333d1 a 262dc e0 221 4ec	N	a a N
	7888a d fa 2a1 4f0 53a1 5a220	N bb	N

購謥运行环境

in	ic E c is o ild o le e ÿc l o it d d d

髭 硏 E 髂鐘息

IP		IP	
192.168.122.111	137	192.168.122.255	137
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

購常见行为

安天周观察
APT
2019 07 29 (193) 4 antiylab

“ ”

7 17 “ 2019 “ ” “ “ CNCERT/CC ” ” 2004 2019 4 103 11 CERT 69 5 18 12 CNCERT 12 6 CNCERT C è ɜ CNCERT ˜ ≠ Î ı Ω N è ьa dz æ Ɔ æ ɽ ɽ

7 22

2010

Comodo Antivirus SYSTEM CVE-2019-3970 CmdAgent.exe CVE-2019-3973 Comodo Antivirus Comodo Antivirus Advanced 12.0.0.6810 11.0.0.6582 CVE-2019-3969 CVE-2019-3971 memcpy NULL CVE-2019-3972 https://www.tenable.com/security/research/tra-2019-34

类 型	内 容
	DLTMiner
英文标题	CB TAU Technical Analysis: DLTMiner Campaign Targeting Corporations in Asia
	JARED MYERS
	Carbon Black DLTMiner DLTMiner 2019 1 RDP
	https://www.carbonblack.com/2019/07/23/cb-tau-technical-analysis-dltminer-campaign-targeting-corporations-in-asia/

ʁ CER . ɟ Ï ⁒.. 8 γ ‴ ˆ م 6 γ PC ˆ م ẅ ĩ

为何说事件响应必须采用“杀伤链”视角

Stan Engelbrecht/文 安天技术公益翻译组/译