2021 1 13

2009

2021 1 13

incaseformat

USB 2010 4

1 2021 1 13

Worm/Win32.Autorun 2010 3 1 10 Incaseformat

21 29

U

RunOnce

2010 CERT (https://www.antiy.cn/research/notice&report/research_report/20210114.html)

4 1 (

2021 1 13)

Ursnif PE Ursnif

Fortinet Ursnif

C2

Word Ursnif C2

Word (https://www.fortinet.com/blog/threat-research/new-variant-of-ursnif-continuously-targeting-italy)

5L-±9Ÿ6 (‹>Ö=T D

URL DLL DLL

RegSvr32.exe

Ursnif

英文标题	CISA: Hackers bypassed MFA to access cloud service accounts
	Sergiu Gatlan
	CISA MFA cookie
	https://www.bleepingcomputer.com/news/security/cisa-hackers-bypassed-mfa-to-access-cloud-service-accounts/