

Esercizio 2 M5 D5

ThreatConnect, una nota azienda di sicurezza informatica provider di una piattaforma di TI, utilizza un sistema di valutazione delle informazioni basato su sei livelli:

Confermata (90-100): l'informazione risulta è confermata da diverse sorgenti e la minaccia risulta reale a valle della valutazione

Probabile (70-89): la minaccia non è stata ancora confermata, ma molti dei segnali indicano una probabilità alta che essa sia reale

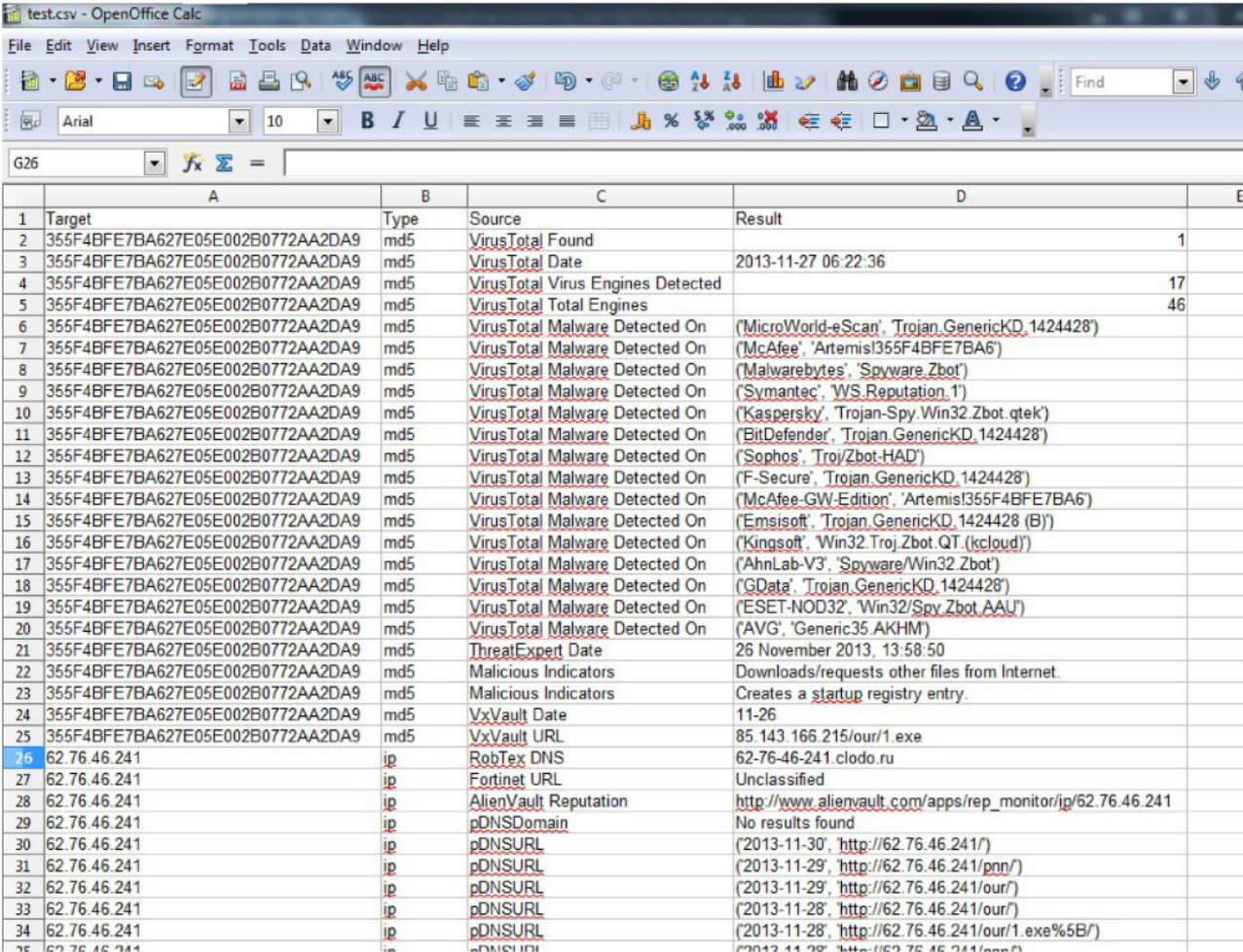
Possibile (50-69): alcune delle informazioni indicano un grado di veridicità concreto, ma non ci sono ancora evidenze per confermare la minaccia

Incerta (30-49): la valutazione dell'informazione è possibile, ma sono necessarie più informazioni per identificare la minaccia

Improbabile (2-29): la valutazione dell'informazione è possibile, ma non è la scelta più logica, data la presenza di informazioni discordanti

Screditata (1): la valutazione ha confermato che la minaccia non è reale

PARTE 2



	A	B	C	D	E
1	Target	Type	Source	Result	
2	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal Found		1
3	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal Date	2013-11-27 06:22:36	
4	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal Virus Engines Detected		17
5	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal Total Engines		46
6	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal Malware Detected On	(MicroWorld-eScan', Trojan.GenericKD.1424428')	
7	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal Malware Detected On	(McAfee', 'ArtemisI355F4BFE7BA6')	
8	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal Malware Detected On	(Malwarebytes', 'Spyware.Zbot')	
9	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal Malware Detected On	(Symantec', 'VWS.Reputation.1')	
10	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal Malware Detected On	(Kaspersky', Trojan-Spy.Win32.Zbot.qtek')	
11	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal Malware Detected On	(BitDefender', Trojan.GenericKD.1424428')	
12	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal Malware Detected On	(Sophos', 'Troj/Zbot-HAD')	
13	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal Malware Detected On	(F-Secure', Trojan.GenericKD.1424428')	
14	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal Malware Detected On	(McAfee-GW-Edition', 'ArtemisI355F4BFE7BA6')	
15	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal Malware Detected On	(Emsisoft', Trojan.GenericKD.1424428 (B))	
16	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal Malware Detected On	(Kingsoft', 'Win32.Troj.Zbot.QT.(kcloud)')	
17	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal Malware Detected On	(AhnLab-V3', 'Spyware/Win32.Zbot')	
18	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal Malware Detected On	(GData', Trojan.GenericKD.1424428')	
19	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal Malware Detected On	(ESET-NOD32', 'Win32/Spy.Zbot.AAU')	
20	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal Malware Detected On	(AVG', 'Generic35.AKHM')	
21	355F4BFE7BA627E05E002B0772AA2DA9	md5	ThreatExpert Date	26 November 2013, 13:58:50	
22	355F4BFE7BA627E05E002B0772AA2DA9	md5	Malicious Indicators	Downloads/requests other files from Internet.	
23	355F4BFE7BA627E05E002B0772AA2DA9	md5	Malicious Indicators	Creates a startup registry entry.	
24	355F4BFE7BA627E05E002B0772AA2DA9	md5	VxVault Date	11-26	
25	355F4BFE7BA627E05E002B0772AA2DA9	md5	VxVault URL	85.143.166.215/our/1.exe	
26	62.76.46.241	ip	RobTex DNS	62-76-46-241.clodo.ru	
27	62.76.46.241	ip	Fortinet URL	Unclassified	
28	62.76.46.241	ip	AlienVault Reputation	http://www.alienvault.com/apps/rep_monitor/ip/62.76.46.241	
29	62.76.46.241	ip	pDNSDomain	No results found	
30	62.76.46.241	ip	pDNSURL	('2013-11-30', ' http://62.76.46.241/)	
31	62.76.46.241	ip	pDNSURL	('2013-11-29', ' http://62.76.46.241/pnn/)	
32	62.76.46.241	ip	pDNSURL	('2013-11-29', ' http://62.76.46.241/our/)	
33	62.76.46.241	ip	pDNSURL	('2013-11-28', ' http://62.76.46.241/our/)	
34	62.76.46.241	ip	pDNSURL	('2013-11-28', ' http://62.76.46.241/our/1.exe%5B/)	
35	62.76.46.241	ip	pDNSURL	('2013-11-28', ' http://62.76.46.241/our/)	

```
1
2           Results found for: 355F4BFE7BA627E05E002B0772AA2DA9
3 [+] MD5 found on VT: 1
4 [+] Scan date submitted: 2013-11-27 06:22:36
5 [+] # of virus engines detected on: 17
6 [+] # of total scan engines: 46
7 [+] Malware detected on: ('MicroWorld-eScan', 'Trojan.GenericKD.1424428')
8 [+] Malware detected on: ('McAfee', 'Artemis!355F4BFE7BA6')
9 [+] Malware detected on: ('Malwarebytes', 'Spyware.Zbot')
10 [+] Malware detected on: ('Symantec', 'WS.Reputation.1')
11 [+] Malware detected on: ('Kaspersky', 'Trojan-Spy.Win32.Zbot.qtek')
12 [+] Malware detected on: ('BitDefender', 'Trojan.GenericKD.1424428')
13 [+] Malware detected on: ('Sophos', 'Troj.Zbot-HAD')
14 [+] Malware detected on: ('F-Secure', 'Trojan.GenericKD.1424428')
15 [+] Malware detected on: ('McAfee-GW-Edition', 'Artemis!355F4BFE7BA6')
16 [+] Malware detected on: ('Emsisoft', 'Trojan.GenericKD.1424428 (B)')
17 [+] Malware detected on: ('Kingsoft', 'Win32.Troj.Zbot.QT.(kcloud)')
18 [+] Malware detected on: ('AhnLab-V3', 'Spyware/Win32.Zbot')
19 [+] Malware detected on: ('GData', 'Trojan.GenericKD.1424428')
20 [+] Malware detected on: ('ESET-NOD32', 'Win32/Spy.Zbot.AAU')
21 [+] Malware detected on: ('AVG', 'Generic35.AKHM')
22 [+] Hash found at ThreatExpert: 26 November 2013, 13:58:50
23 [+] Malicious Indicators from ThreatExpert: Downloads/requests other files from Internet.
24 [+] Malicious Indicators from ThreatExpert: Creates a startup registry entry.
25 [+] Date found at VXVault: 11-26
26 [+] URL found at VXVault: 85.143.166.215/our/1.exe
27           Results found for: 62.76.46.241
28 [+] A records from Robtex.com: 62-76-46-241.clodo.ru
29 [+] Fortinet URL Category: Unclassified
30 [+] Found in AlienVault reputation DB: http://www.alienvault.com/apps/rep_monitor/ip/62.76.46.241
31 No results found for: [+] pDNS data from VirusTotal:
32 [+] pDNS malicious URLs from VirusTotal: ('2013-11-30', 'http://62.76.46.241/')
33 [+] pDNS malicious URLs from VirusTotal: ('2013-11-29', 'http://62.76.46.241/pnn/')
34 [+] pDNS malicious URLs from VirusTotal: ('2013-11-29', 'http://62.76.46.241/our/')
35 [+] pDNS malicious URLs from VirusTotal: ('2013-11-28', 'http://62.76.46.241/our/')
36 [+] pDNS malicious URLs from VirusTotal: ('2013-11-28', 'http://62.76.46.241/our/1.exe%5B/')
37 [+] pDNS malicious URLs from VirusTotal: ('2013-11-28', 'http://62.76.46.241/pnn/')
38 No results found for: [+] Blacklist from IPVoid:
39 [+] ISP from IPVoid: ROSNIROS Russian Institute for Public Networ...
40 [+] Country from IPVoid: (RU) Russian Federation
41           Results found for: 62.76.46.242
42 [+] A records from Robtex.com: 62-76-46-242.clodo.ru
```