

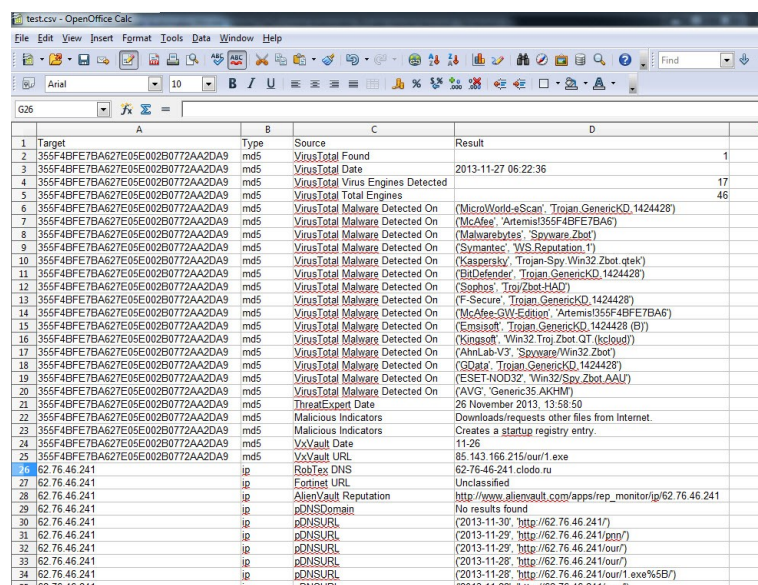
Livello di reputazione: In questo livello, le minacce vengono valutate in base alla loro reputazione o al loro status. Le fonti di dati possono includere elenchi di indirizzi IP o domini noti per essere associati a comportamenti dannosi o indesiderati. Le minacce con una reputazione negativa possono essere identificate e monitorate.

Livello di rilevanza: Qui le minacce vengono valutate in base alla loro rilevanza per un'organizzazione o un settore specifico. Si tiene conto dei fattori come il tipo di minaccia, l'industria interessata, le vulnerabilità esistenti e altre informazioni specifiche per determinare l'impatto potenziale di una minaccia su un'organizzazione.

Livello di pericolosità: Questo livello valuta la pericolosità o l'efficacia delle minacce. Si considerano fattori come le capacità tecniche della minaccia, le tattiche utilizzate, la diffusione geografica, il livello di sofisticazione e il potenziale danno che possono causare.

Livello di affidabilità delle fonti: In questo livello, si valuta l'affidabilità e la credibilità delle fonti di informazioni sulle minacce. Si possono considerare fattori come l'autenticità delle fonti, la loro esperienza nel settore, la qualità delle informazioni fornite e la loro storicità nel fornire informazioni accurate.

Livello di impatto: Questo livello valuta l'impatto potenziale delle minacce sulle operazioni di un'organizzazione. Si considerano gli obiettivi dell'organizzazione, i beni critici, la catena di fornitura, la reputazione aziendale e altri fattori che possono essere influenzati in caso di compromissione o attacco.



	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.GeneticKD.1424428)
7	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal	Malware Detected On	(McAfee, Artemis355F4BFE7BA6)
8	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal	Malware Detected On	(Malwarebytes, Spyware.Zbot)
9	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal	Malware Detected On	(Symantec, W32.Reputation.1)
10	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal	Malware Detected On	(Kaspersky, Trojan-Spy.Win32.Zbot.gtek)
11	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal	Malware Detected On	(BitDefender, Trojan.GeneticKD.1424428)
12	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal	Malware Detected On	(Sophos, Troy.Zbot.HAQ)
13	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal	Malware Detected On	(F-Secure, Trojan.GeneticKD.1424428)
14	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal	Malware Detected On	(McAfee-SW-Edition, Artemis355F4BFE7BA6)
15	355F4BFE7BA627E05E002B0772AA2DA9	md5	VirusTotal	Malware Detected On	(Emsisoft, Trojan.GeneticKD.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.GeneticKD.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/our1.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_monitorip/62.76.46.241
29	62.76.46.241	ip	pDNSDomain		No results found
30	62.76.46.241	ip	pDNSURL		(2013-11-29, http://62.76.46.241/)
31	62.76.46.241	ip	pDNSURL		(2013-11-29, http://62.76.46.241/pnp/)
32	62.76.46.241	ip	pDNSURL		(2013-11-29, http://62.76.46.241/our1/)
33	62.76.46.241	ip	pDNSURL		(2013-11-28, http://62.76.46.241/our1/)
34	62.76.46.241	ip	pDNSURL		(2013-11-28, http://62.76.46.241/our1.exe%5B/)
35	62.76.46.241	ip	pDNSURL		(2013-11-28, http://62.76.46.241/our1.exe%5B/)

```
1
2
3 Results found for: 355F4BFE7BA627E05E002B0772AA2DA9
4
5 [+] MDS found on VT: 1
6 [+] Scan date submitted: 2013-11-27 06:22:36
7 [+] # of virus engines detected on: 17
8 [+] # of total scan engines: 46
9 [+] Malware detected on: ('MicroWorld-eScan', 'Trojan.GenericKD.1424428')
10 [+] Malware detected on: ('McAfee', 'Artemis!355F4BFE7BA6')
11 [+] Malware detected on: ('Malwarebytes', 'Spyware.Zbot')
12 [+] Malware detected on: ('Symantec', 'WS.Reputation.1')
13 [+] Malware detected on: ('Kaspersky', 'Trojan-Spy.Win32.Zbot.qsak')
14 [+] Malware detected on: ('BitDefender', 'Trojan.GenericKD.1424428')
15 [+] Malware detected on: ('Sophos', 'Trojan.Zbot-HAD')
16 [+] Malware detected on: ('F-Secure', 'Trojan.GenericKD.1424428')
17 [+] Malware detected on: ('McAfee-GW-Edition', 'Artemis!355F4BFE7BA6')
18 [+] Malware detected on: ('Emsisoft', 'Trojan.GenericKD.1424428 (B)')
19 [+] Malware detected on: ('Kingsoft', 'Win32.Trojan.Zbot.QT.(kcloud)')
20 [+] Malware detected on: ('AhnLab-V3', 'Spyware/Win32.Zbot')
21 [+] Malware detected on: ('GData', 'Trojan.GenericKD.1424428')
22 [+] Malware detected on: ('ESET-NOD32', 'Win32/Spy.Zbot.AAU')
23 [+] Malware detected on: ('AVG', 'Generic35.AKHM')
24 [+] Hash found at ThreatExpert: 26 November 2013, 13:58:50
25 [+] Malicious Indicators from ThreatExpert: Downloads/requests other files from Internet.
26 [+] Malicious Indicators from ThreatExpert: Creates a STARTUP registry entry.
27 [+] Date found at VXVault: 11-26
28 [+] URL found at VXVault: 85.143.166.215/our/1.exe
29
30 Results found for: 62.76.46.241
31
32 [+] A records from Robtex.com: 62-76-46-241.clodo.ku
33 [+] Fortinet URL Category: Unclassified
34 [+] Found in AlienVault reputation DB: http://www.alienvault.com/apps/rep_monitor/ip/62.76.46.241
35
36 No results found for: [+] pDNS data from VirusTotal:
37
38 [+] pDNS malicious URLs from VirusTotal: ('2013-11-30', 'http://62.76.46.241/')
39 [+] pDNS malicious URLs from VirusTotal: ('2013-11-29', 'http://62.76.46.241/pnn/')
40 [+] pDNS malicious URLs from VirusTotal: ('2013-11-29', 'http://62.76.46.241/our/')
41 [+] pDNS malicious URLs from VirusTotal: ('2013-11-28', 'http://62.76.46.241/our/')
42 [+] pDNS malicious URLs from VirusTotal: ('2013-11-28', 'http://62.76.46.241/our/1.exe%5B/')
43 [+] pDNS malicious URLs from VirusTotal: ('2013-11-28', 'http://62.76.46.241/pnn/')
44
45 No results found for: [+] Blacklist from IPVoid:
46
47 [+] ISP from IPVoid: ROSNIROS Russian Institute for Public Netw...
48 [+] Country from IPVoid: (RU) Russian Federation
49
50 Results found for: 62.76.46.242
51
52 [+] A records from Robtex.com: 62-76-46-242.clodo.ru
```