250626_TnD Soft IoC (Indicators of Compromise) report

1) This report summarizes the reputation findings based on the provided indicators of compromise (IoCs). The reputation of the IP address is assessed using the Abuseipdb score, and Virustotal provides the number of vendor reports. 2) We provide these IoCs as valuable resources to assist in your security efforts. While these tools may require careful consideration for integration within your unique environment, we offer technical support throughout the process. The effectiveness can vary based on your specific system configuration and complexity. We aim to support you while acknowledging that performance may differ across different environments.

Indicator	Type	Malware Title	AbuseIPDB Score	VirusTotal Score
coppergold.ru.com	hostname	Win32.Webdialer.Dialer.Porn	0	1
kotolantopeni.cz	domain	PDF.MalwareX.generic	0	N/A
dpfremovalnottingham.com	domain	Trojan.PDF.Phishing.R	0	1
220.89.98.213	ipv4	Telnet Login attempt	71	5
186.91.102.134	ipv4	Telnet Login attempt	100	5
120.56.83.240	ipv4	Telnet Login attempt	45	1
117.193.58.174	ipv4	Telnet Login attempt	54	2
848a803509a300b2e4ce3548b504c117	filehash-md5	Win32.Webdialer.Dialer.Porn	N/A	N/A
883ae9e4842f1622fa04f9e283abf4e7	filehash-md5	PDF.MalwareX.generic	N/A	N/A
a0dc9fd4ffe3cfd0abca78e9a82f3348	filehash-md5	Trojan.PDF.Phishing.R	N/A	13
21ef4f8234f400e647e2f126e31b4d42	filehash-md5	PDF.MalwareX.generic	N/A	N/A
7ef4e61b4b1fb32bede3b5220e75c0df	filehash-md5	PDF.MalwareX.generic	N/A	7
0a7dde8a4cd450e7f9c0b65ca7a4dd114f091965	filehash-sha1	Win32.Webdialer.Dialer.Porn	N/A	N/A
b5eeb39c1c487623a6975bd3d5ce3421b706f270	filehash-sha1	PDF.MalwareX.generic	N/A	N/A
56357393d9b941f28eb57363a73dc2346726ee0c	filehash-sha1	Trojan.PDF.Phishing.R	N/A	13
53685e14a7381adeeca66bb130338d56ef6677b4	filehash-sha1	PDF.MalwareX.generic	N/A	N/A
b4b1eae1429a46171fb508461e40041eb78765b1	filehash-sha1	PDF.MalwareX.generic	N/A	7