SUBJECT: Exit Relay Scanner Logs

FROM: Network Intelligence and Technical Evaluation Team 4

TO: Division 79

MESSAGE CONTENTS:

Our investigation on a coordinated action to deanonymize dark web users has produced the following malicious activity logs from our exit relay scanners. We require analyst assistance to find evidence of a group of operatives working together in these logs. If we can then identify the name of the ISP responsible for hosting the malicious nodes, we can proceed to the next phase of the operation.

IP address	Problem	Fingerprint
176.99.12.246	HTTPS MitM	12FR4323
83.172.8.4	HTTPS MitM	FV32TV54
92.63.102.68	SSH & HTTPS MitM	DC43TV32
121.54.175.51	sslstrip	HF4823NX
117.18.118.136	DNS censorship	KJ73HDN2
46.254.19.140	SSH & HTTPS MitM	NB389NCB
89.128.56.73	sslstrip	KN483XCZ
178.211.39	HTML injection	45NC293N
196.207.11.33	SSH & HTTPS MitM	OI0239MC
93.170.130.194	HTTPS MitM	KM239NCV
196.207.11.83	SSH & HTTPS MitM	2837BCTV
24.84.118.132	OpenDNS	TVR4736B
207.98.174.40	OpenDNS	MN3874BC
196.207.11.182	SSH & HTTPS MitM	KM483BVT

37.143.14.176	XMPP MitM	K2238BCY
196.207.11.145	SSH & HTTPS MitM	LM4837BC
85.23.243.147	IMAPS anti virus	23TVB38V
132.248.80.171	IMAPS anti virus	543KMCNT
196.207.11.104	SSH & HTTPS MitM	283NTBVC
54.200.102.199	sslstrip	938KMNTV
121.121.82.198	DNS censorship	563BVHTM
37.143.8.242	sslstrip	88YCB54B
196.207.11.134	SSH & HTTPS MitM	KN47BTVN
196.207.11.129	SSH & HTTPS MitM	09IKM382B
37.143.11.220	SSH MitM	TY65BTN43
198.50.244.31	sslstrip	XZ4738TBV
196.207.11.57	SSH & HTTPS MitM	849TBNJKN
188.120.228.103	DNS censorship	43TJNVM09
62.109.22.20	sslstrip	LCMDN3389