

Indicators of Compromises (IOC) table:

Tablo 1: UNK_FistBump Network Indicators

Indicator	Type	Description	First Seen
166.88.61[.]35	IP Address	Cobalt Strike C2	May 2025
hxxps://sheets[.]googleapis[.]com:443/v4/spreadsheets/1z8ykHVYh9DFb_BFDA9c4Q2ojfrglfq1v797Y5576Y	URL	Voldemort Google Sheets C2	May 2025
hxxps://sheets[.]googleapis[.]com:443/v4/spreadsheets/14H0Gm6xgc2p3gpIB5saDyzSDqpVMKGBKIdkVGh2y1bo	URL	Voldemort Google Sheets C2	June 2025
john.doe89e@gmail[.]com	Email	Malware Delivery	May 2025
hxxps://3008[.]filemail[.]com /api/file/get?...	Delivery URL	Filemail staging URL	May 2025

Tablo 3: UNK_DropPitch Network Indicators

Indicator	Type	Description	First Seen
amelia_w_chavez@proton[.]me	Email	Malware Delivery	April 2025
lisan_0818@outlook[.]com	Email	Malware Delivery	May 2025
moctw[.]info	Domain	Malware Delivery	April 2025
ema.moctw[.]info	Domain	C2	April 2025
Error! Hyperlink reference not valid.	Domain	C2	June 2025
80.85.156[.]234	IP Address	C2	April 2025
82.118.16[.]72	IP Address	C2	April 2025
45.141.139[.]222	IP Address	C2	May 2025
80.85.156[.]237	IP Address	C2	June 2025
80.85.154[.]48	IP Address	C2	June 2025

Table 5: UNK_SparkyCarp Network Indicators

Indicator	Type	Description	First Seen
accshieldportal[.]com	Domain	Credential Phishing Domain	March 2025
acesportal[.]com	Domain	Tracking Pixel Domain	March 2025
hxxps://ttot.accshieldportal[.]com/v3/ls/click/?c=b5c64761	URL	Credential Phishing URL	March 2025
hxxps://aqrm.accshieldporta l[.]com/v2/account/validate/?vid=35f46f46	URL	Credential Phishing URL	March 2025
menglunwaluegg226@prot on[.]me	Email	Malware Delivery	March 2025
lonelyboymaoxcz231@prot on[.]me	Email	Malware Delivery	March 2025