650-614-1705
www.menlosecurity.com
support@menlosecurity.com

Menlo Labs Threat Bulletin

Bulletin: 2021-002

Date: 04/12/2021

Name: USPS/Amazon Phishing

Classification: Credential Phishing

Summary

Menlo Labs has been tracking a malicious campaign that is targeting both mobile and desktop users in what appears to be an organized spam operation campaign.

Technical Details

Infection Vector

Mobile users who click on these malicious links in text messages are redirected to a credential phishing page that attempts to phish for USPS/FedEX/Amazon credentials. Desktop users are redirected to a site that then prompts the user into downloading malicious browser extensions.

IOCs

IPs

47[.]243[.]34[.]151
47[.]242[.]142[.]35
47[.]242[.]110[.]196
3[.]233[.]37[.]12
104[.]21[.]29[.]241

650-614-1705
www.menlosecurity.com
support@menlosecurity.com

Menlo Labs Threat Bulletin

URLs (Mobile)

hxxp[://]w7fzc[.]info/fU8rPoxD35
hxxp[://]w4fza[.]info/jdSdORwYco
hxxp[://]t9fzc[.]info/Hxpl1o5BD2
hxxp[://]eb31g[.]com/kbLAFmo4Ir
hxxp[://]gh18n[.]com/LtEYd8wmA5
hxxps[://]usps-na[.]winnerof[.]today/mm/u25k7hbp/index[.]php
hxxps[://]ups-na[.]winnerof[.]today/mm/k9bcvi9c/index[.]php?clickid=out&crid=80002437&cg=T2B8T38q0npYJ7&source=187425779&target=ts5603-sms-a-3-us&camid=59639&br=Unknown&ca=Unknown&lpkey=160d173c74f1044011&clickcost=0[.]06&s2=de03b2tbzdubgi47eb&s3=27&s4=80002437&s5=US&s6=1&domain=redirect[.]winnerof[.]today&uclick=2tbzdubgi4&uclickhash=2tbzdubgi4-2tbzdubgi4-16ir-0-e2ci-gmzwwj-gmikwj-d5d8f8&user=bc9b36b878374b8e85cc3f2ece0f9aa6&country=en
hxxps[://]fedex-na[.]winnerof[.]today/mm/h26slqns/index[.]php

URLs (Desktop)

hxxps[://]boot-upextremely-bestprogressivefile[.]best/uim0AfFkHwfxTeqfd8Q4XELJ60aE4zNesPm7hMpvzaU?cid=71c7b44bf1e965b9afc7a61c63d26f98&sid=14872535
hxxps[://]boot-upnewest-bestextremelyfile[.]best/yJmtjUqT15z23HF9oHcxRXL0hiJfhbK010nUOq99M60?cid=09e93672f5d209ac48f4f7751a109c6f&sid=14872535
hxxps[://]boot-uporiginal-bestoverlyfile[.]best/zlzPDmrPvKfxNouZCNqRJx5_rYYjjCCQlcH7LCSRvH0?clck=4012283291112656 25&sid=3877104
hxxps[://]boot-upgreatly-bestlatestfile[.]best/rRoVk9jjBC9piCZuupV3NpxwMio9v49EQjoUcwvEXJQ?cid=65562769b11b8011f6c59dce3b2f751d&sid=15888588

650-614-1705
www.menlosecurity.com
support@menlosecurity.com

Menlo Labs Threat Bulletin

Conclusion

Menlo Security's cloud security platform protects against this threat. The platform's unique *Isolate ReadOnly* capability completely eliminates credential phishing attacks. When the Menlo platform renders a website in this mode, the user is unable to input any credentials on that website, thereby preventing credential theft. With the recent announcement of our Mobile Isolation solution, these powerful capabilities are now extended to protect Mobile devices, against such attacks.

Menlo labs proactively monitors threats and updates the platform accordingly with IOCs. IOCs in this campaign have been added to the product and are now categorized as Phishing. Customers are recommended to set their policy for threat categories, across isolated and application web requests, to block.