

Beware of Phishing Emails Disguised as Project Proposals

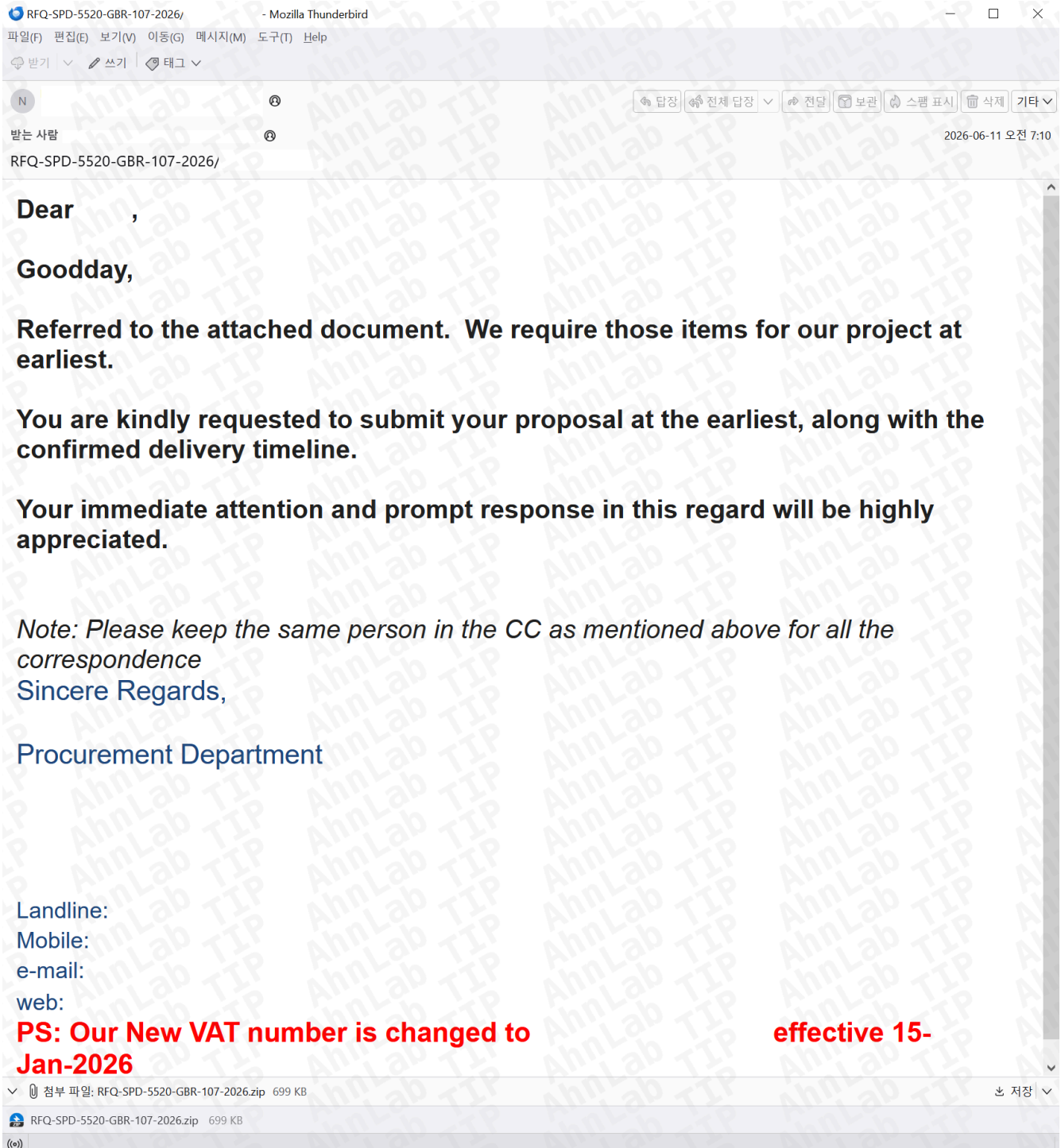
A asec.ahnlab.com/en/94433

ATCP

July 8, 2026



The AhnLab Security intelligence Center (ASEC) recently confirmed that phishing emails disguised as project proposals are being circulated. The body of the email pretends to request that the proposal and confirmed delivery schedule be submitted as soon as possible, and prompts the recipient to download the attached compressed file.



[Figure 1] Phishing email body

When a user downloads and decompresses the attached compressed file, they will find JS malware disguised as a proposal, as shown in [Figure 2].


```

$ARXyTm="";foreach($HqqOfu in @(123,161,155,156,141,149,86,117,137,150,137,143,141,149,141,150,156,86,108,157,156,151,149,137,156,14
179,187,190,183,182)){ $TuvsMh=[char]($HqqOfu-82)};$OkEmse=[PSObject].Assembly.('GetT'+$ype')($ARXyTm);$oZDduA=$OkEmse.('GetF'+$ie'+
1069743kF5DHAWRDurr+$env:PYBrc5K008k+$env:6L2ob0Ww91+$env:d201Gyrf0TtPlqXzw4+$env:exclu82PlVlRyszM5X+$env:AFhsv9p1rTMBLE2sM+$env:Xa
B66Zk6x062cuzQ+$env:clYy3eIrxlJdofa+$env:fRUAKyioVoyxE+$env:LWzq5N0QNifc+$env:OkIUggRrNlks4Yr46+$env:djEQeQKwthKpuBjOx6oJ+$env:EfHqQ
$env:LqjKQxZVs2sR91+$env:vXSHqQ6KdZk7+$env:8xuttoGhhPPDJh+$env:00gv1f618Bp+$env:UatpbmuzTzCB9Jd12TQh+$env:o8jZfDR8fagy3eIon+$env:1gQ
coj8SovvYnwfy3vJ+$env:FSSyXUzNw5OcD81Z255N+$env:dDFT58WN7S5XHR+$env:HmfnsYGLXJlZ+$env:VHpC8SGcmMP2VM+$env:9ynSo6rtMTSMYG2SGA+$env:
ZjcvkGIAiMgu9hu59bFb+$env:t32J6bj78f0wr+$env:flioPtY3CFz4wFuY+$env:c4eLHX6gDziXLBdWU+$env:c3JlQuS0ilxCOJGY+$env:i6kWUUSM1VqkBraCN+$e
$env:M1Zx1ltd9eT4+$env:dBlYtFSuX9uWqWV17+$env:aj9FkwV8kKahvkl+$env:thTnXZsHdrNHdgfXh+$env:f85Uz3efOvu4uPNk+$env:L7Ob8kk0BB2Soh1+$e
zq9ByLMZAmD7+$env:OODPrUmibJcDop80tTFz+$env:cx0DNHd170rtmYxDR+$env:zsoEafZY5YJMWGRRe5r+$env:XabUqalksj101F+$env:j4A04brbPSVvJluKL+$e
zxtN2s0EkyL6uqsEJbzy+$env:Gbx5BuLb3udNdzt+$env:sPCwuzZcGBCEO+$env:ixec4DxaymHRZL0u8+$env:2569m3Jdeglyua2+$env:gwU69L156s4D4OF+$env:
ObdDVITG5b+$env:g3NEAxerlr3z+$env:oST2XHgE9c4+$env:cnTx8EHNNetr+$env:BCWmqVV10FoWvU+$env:3UmABcn8KqR9fWuOq54+$env:Arzau0SokeH96+$env:
uqTpeoDM3+$env:gq0JhLYELN3MF+$env:cPeGSSGsU1bnwm+$env:99WbFiwPtZo72PlZ+$env:4sSVQK9RGUfLvyy+$env:YwU8YFYmXZwxvosU+$env:01g56SFLGz9eF
hdSXi7ryDGHoXl405wP+$env:P5Cm5yoeXiko3lt8aVh+$env:OgKUAS2QAQt+$env:ru2LzmLG2TSnL+$env:vwtuCEm32YFyfbE+$env:dIYxD0ZvrW+$env:hxE2xhd
9mp0lFS1juvZtCGDsL+$env:dB1YW7xmsGUNcca8V+$env:8B0BncaVEbh1Da9P8Kv+$env:lArc8mzPzRTXsDVElUM+$env:nZXAdbfhZFU7dBPXuQ+$env:92oYxLdUoZ
mBW4uFWe5NhMUTWVr+$env:hUWY80CSK00+$env:QPohvedjeKSyjs9FNs+$env:QbHd48wsoLulTqh+$env:op83EzOSMnG+$env:cxOP16fsIMsMvPUC0+$env:CY20Bd
0yMyGKAk80+$env:BGUvF8BCglU0R+$env:M153tLiwdGhQ761wU+$env:tldQfWGVdQoFxrM+$env:aQ9pKQg8Zsya+$env:MZYcJgVlJwBgVyiZv4+$env:1PoFqr6LVer
fWKzB2k0DN8vNRFnGz+$env:TSfzBvZta5d+$env:lFKE6a4tWZ2a1eKRDj9u+$env:YBTEB6PpPaS2pW4ix0RQ+$env:k4UaBRnv0NvjaLogw+$env:Gd9vJdWh9VejuME
+$env:tGutMbP3G097pVCb0zs+$env:8UVn9SzipNJv3t6MtJPh+$env:1KvQ2FUOLQ13IMukHtuK+$env:m3Ap6FgNsjBlrBy8Eu+$env:E8VHJCQWq8Vfao+$env:f48V
PPmwLxtYj7NVAvFOWCZ+$env:Y0wpSba2Xa+$env:VVprDLi25Kvsj2k+$env:kZDZzeuYQNTsADuLFGXx+$env:myE6UwW12E+$env:FRFeILGyy6A6IOUs+$env:SyK8ZW
$env:HDFmZuhbvKuYx0v+$env:bAfWfoqLlCrhJUmRk+$env:L35sgZc0Rz6qXnss8+$env:fxjgUtm3axc9BK+$env:Y2jnd4d4Ld+$env:6XZuvxo9ZLP+$env:Zhd0KT
$env:lrJye7qCnhtil+$env:2EbU7QqvLNQqPE+$env:TsdGA8hiEVCbB+$env:200Y3Ebw5gRzhosKO+$env:21yCGkUL2keT9ps5p+$env:yRUYY0iYm+$env:VgtT2I0
:e26A0f1GVD800X4+$env:G0sxPa04wW8zPQ+$env:v8BbTWTOBRBj4+$env:xgeIVLW8dchvdz8J4+$env:OlQl0zFHZgak1yb6Ggq+$env:XsnmX2S5tPQx+$env:VeXAU
jJXyNrAnnlAywnr+$env:IGBulKPX0zWecZxao3+$env:k6T2ajSWmgrPcYnM+$env:TUL7R4EL791mxYZ+$env:LlEmrHQGRlfyIflw+$env:70AGNzrlgBI+$env:4brFY
QNo2UdKZT2cLxJE+$env:FwIQOMQsRmBV6m3Lx1fts+$env:g6BXJFwNag2IOfjc+$env:Phdfx6cA8h+$env:x6hBlndqyIvVfh4f+$env:r5JnwgTJSTcn5k4aYBh+$env:
ab9J2w3y2p+$env:UfjdXOYreFaH50+$env:icB40uKu923j2KPsck+$env:2lhxYZxrIX+$env:CQaEdTtUBEB5kVkkJ+$env:NwOPVDZPUTVnMH+$env:JVW2s2zgJ0v4
nqJlFlzWnFoGCR+$env:KBse3WFOUIDy+$env:AT48DjASjtkJmm1qaxcE+$env:6dxq1RlohUCSgXe+$env:hFYTwXYtxA2g2bFExF9+$env:BxwNgVsmLy1B+$env:DzhTV
IcwJY300DReS1Is2L+$env:bkrILNpEkeJPGGJu+$env:2DK8Tc4nyTRU1W76n+$env:Efbis6zgeNzqk7K+$env:EyqeR3l9peT15Fsygn+$env:CbaIljGk2Oye7ov+$env:
8ynkRCC5MV0f7t0lGEq1+$env:GhdVkdSwzV4+$env:OHRHr54oNXZQQ8+$env:Rb6BTy8KZulvBanTPF+$env:r0lHqVJqLpNdRaxCBW5+$env:P66dSwP6D3a+$env:3f
EmhjIRZlpMCSOKSTCAu+$env:sc2qgr13hh5jVocKv+$env:nloYgfuTFgg+$env:mXusBVnwL512RYRTu+$env:DQdmA7FL1FlwIGV+$env:kKQcXMR9BQIZw8+$env:Hay

```

[Figure 4] Part of the obfuscated PowerShell script

Once executed, SnakeKeylogger—an Infostealer—collects various types of information from the infected system, such as web browser data, system information, and keylogging data, and transmits it externally through SMTP or Telegram. The C2 server information used is as follows.

SnakeKeylogger C2

- Mail Server: mail.Trimnt[.]Com
- ID: nova3@mnt[.]Com
- Email To: keishstanford5@gmail[.]Com

```

1249 // Token: 0x06000058 RID: 88 RVA: 0x0000436C File Offset: 0x0000256C
1250 public static void Start()
1251 {
1252     COVIDPickers.Chrome_Speed();
1253     COVIDPickers.Torch_Speed();
1254     COVIDPickers.CocCoc_Speed();
1255     COVIDPickers.QQ_Speed();
1256     COVIDPickers.xVast_Speed();
1257     COVIDPickers.QIPSurf_Speed();
1258     COVIDPickers.Microsoft_Speed();
1259     COVIDPickers.Chromium_Speed();
1260     COVIDPickers.Blisk_Speed();
1261     COVIDPickers.Brave_Speed();
1262     COVIDPickers.Nichrome_Speed();
1263     COVIDPickers.Kometa_Speed();
1264     COVIDPickers.Superbird_Speed();
1265     COVIDPickers.Opera_Speed();
1266     COVIDPickers.Comodo_Speed();
1267     COVIDPickers.Cent_Speed();
1268     COVIDPickers.Chedot_Speed();
1269     COVIDPickers.Ghost_Speed();
1270     COVIDPickers.Iron_Speed();
1271     COVIDPickers.UC_Speed();
1272     COVIDPickers.BlackHawk_Speed();
1273     COVIDPickers.Citrio_Speed();

```

[Figure 5] SnakeKeylogger malware Main

Response Guide

1. Verify the Sender

Verify that the sender's email address uses an official domain.

2. Check Hyperlinks and Attachments

If the email body contains an image that prompts you to click on it, check the linked URL first before clicking. Suspicious URLs often redirect to legitimate pages via third-party sites rather than directly from official pages, so examine them carefully. Additionally, if there are attachments, check for suspicious file extensions (.Exe, .Vbs, .Js, etc.).

3. Be Cautious When Entering Sensitive Information

If you are asked to provide sensitive information, such as login credentials, always verify that the page's URL is that of the official site before entering any information. If the page is not official, it is highly likely to be a suspicious URL, so caution is required. In particular, check the page's security certification (HTTPS, padlock icon) before entering sensitive information, and never enter any information if you have any doubts.

MD5

0cbfcc3573399368a2a9abcfa42af134

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

