PIOLINK

정보탈취 악성코드

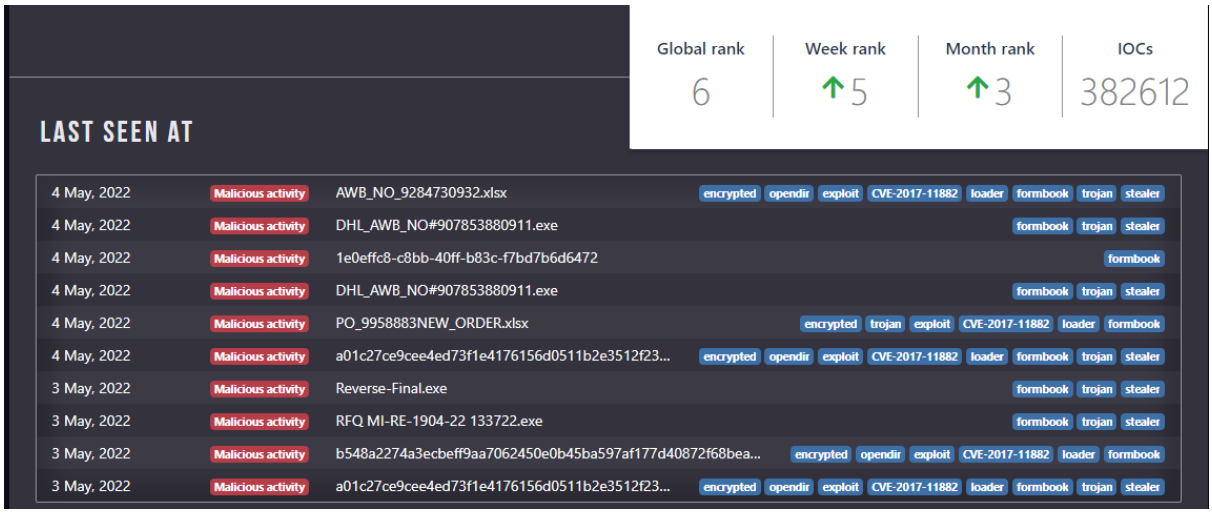
(InfoStealer)

침해대응센터

정보 탈취 악성코드 (InfoStealer)

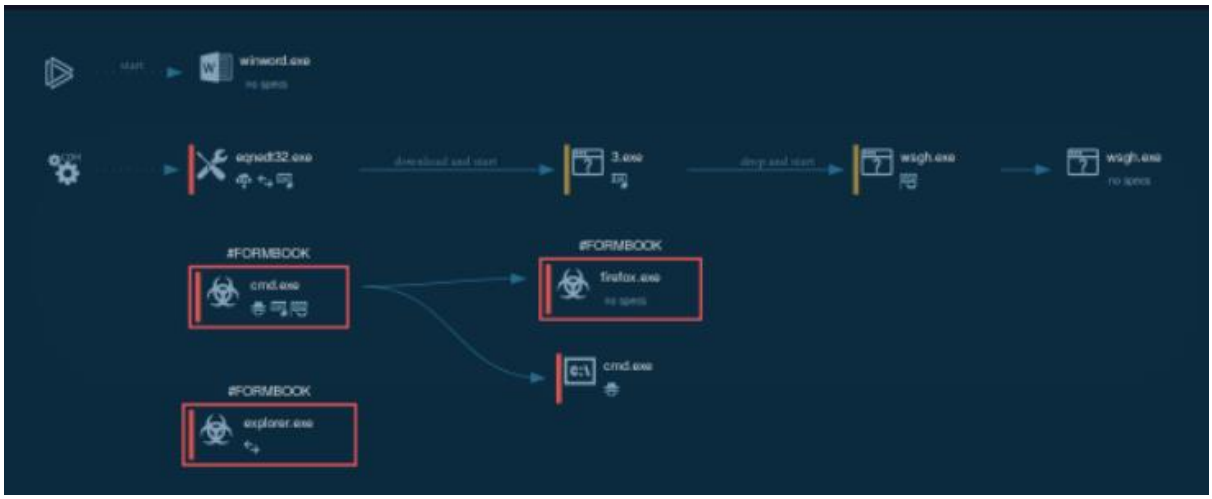
FormBook

감염된 PC의 사용자 정보를 유출하는 인포스틸러 악성코드가 국내에서 가장 많이 유포되는 악성코드로 나타났다. 22년도 상반기 동안 국내에서 가장 활발하게 유포되는 인포스틸러 악성코드는 Formbook, AgentTesla, Lokibot, BeamWinHTTP, SnakeKeyLogger, Redline등이 있다.



[그림] 1 Formbook

Formbook 악성코드는 다크웹에서 서비스형 악성코드(MaaS)로 배포되고 있으며 지속적으로 버전 업그레이드를 하고 있다 피싱 메일의 첨부 파일을 통해 유포되며 정상 프로세스에 인젝션되어 사용자 계정 정보를 탈취 하는 등의 행위를 하기도 한다.



[그림] 2 Formbook Lifecycle

IoC 정보

IP

35[.]242[.]251[.]130	104[.]219[.]248[.]46	162[.]159[.]138[.]85	162[.]159[.]137[.]85	172[.]217[.]18[.]115
213[.]186[.]33[.]19	188[.]114[.]97[.]7	217[.]160[.]0[.]174	151[.]139[.]128[.]11	104[.]18[.]47[.]230
141[.]193[.]213[.]20	199[.]36[.]158[.]100	143[.]204[.]98[.]82	35[.]186[.]245[.]55	143[.]204[.]98[.]18
143[.]204[.]98[.]59	143[.]204[.]101[.]42	217[.]160[.]0[.]91	13[.]107[.]246[.]45	

Domains

sp-ao[.]shortpixel[.]ai

boatshowradio[.]com

alem[.]be

forms[.]gle

cevent[.]net

www[.]wash-wear[.]com

asl-company[.]ru

www[.]macartegrise[.]eu

dualstack[.]reddit[.]map[.]fastly[.]net

www[.]billerimpex[.]com

accounts[.]home[.]sophos[.]com

marvel-b1-cdn[.]bc0a[.]com

etools[.]page

nanmmachineapcnds[.]firebaseapp[.]com

valdia[.]quatiappcn[.]pw

input[.]noibu[.]com

biggi[.]nigelmidnightrappers[.]com

js[.]pusher[.]com

zoominfo[.]widget[.]insent[.]ai

tls-ech-experiment-c[.]cloudflareresearch[.]com

Hash Sha-256

348EF19495451DAF907EDA76F4AC395779E287AFAAACFEA0DF07F048EFC20109

6AB3AC24A4DDFA9FA1CF94315AB384193CDDB9F4E1B1DB6C8F31B650F3F067D5

9187706072F008A27C26421791F57EC33A59B44B012500B2DB3EEB48136FB2DA

6770C75026C53334EBA0AB25938787CD72513B720C0782EF49E2FE316BB7D470

7D13EE531A347B669460FA3BAAFCD42C93FCDEB44E8D7C8A59AA3BA36AB5E17E

01453B5C19F88FFEB1ED1C9AB3AA63879C3967CD25CE03AD15C5435E027F185A

E4D96258C51CC4E4196C566E116077E7DC443A153E2AB651268CCD09C003D792

5840A26FF1EFF0A0A9F9AF023B4BA78C29B48E9319363E5A7EDD90D83FAC3A59

84793A0ABAFB1359181904EF25ECC2AA98520BD224113DAE140D9E631BD6B77E

3BA7AD2A718413AB6D36DD156BBDD5AC1BCCA860F039B14C4CB4382AEE58BC88

7D39FF7529F7332C14740D39770CA4C230F5B8D92D06383DB8C9919156C5CEBC

C122639D652908B10751CB546A1C48E753427AA4D74F6A638FCB6C829B65E12F

019ACFBD71AEC2E6623FF1A9FDE8459504571CEE05F1C0CA9E87E45FD10B88D0

AFB058FDD8AA200FE754289C9B48D8876F4BBD7CBCEFC964742D76C32A990340

85D5B151523B0270E76F1F31ECF1AF9AEA0D1F0E32B169D219A43D7B79DE3D7F

547B16CC95ED3EF76F60797580FDB30DB3DBCA66FDD2B393E1D8C4E720E3B0BF

A981EDCC04257C8FE7F77707C3F588D55A30BE17619F54C7281E22DF94B73D24

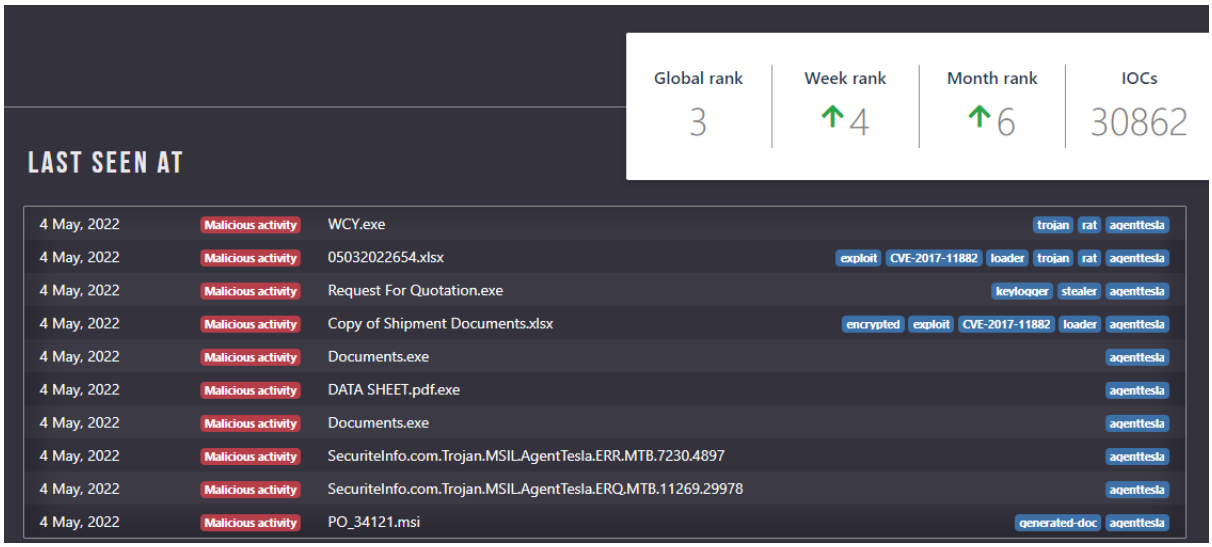
4A679E555DBCD9DF0BBA37A432FF366811281897C2E1482A7844BE9BC9FA39A6

A7FA2F72E5B82E5CF437C0B43886851F317836414FE709C73E40578574D419F3

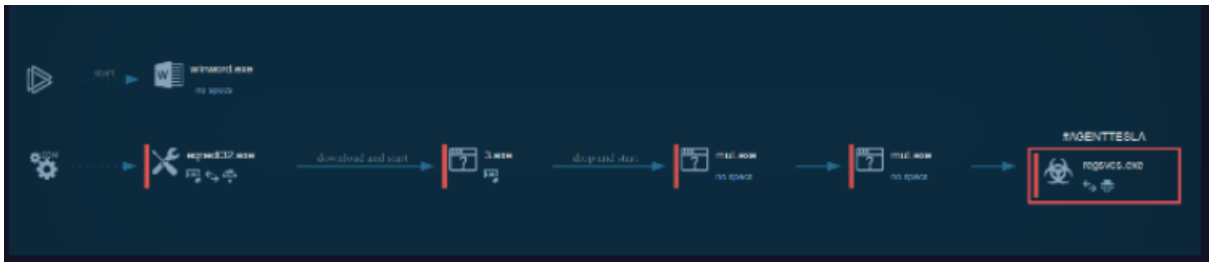
C2C8EB14B3A0B789A287440954AE52E8F72A5B0CFF922ACA1302EEFFF3DD689F

Agent Tesla

해당 악성코드는 피싱 이메일로 유포되고 있으며 첨부 파일에는 악성 매크로가 포함 된 문서 파일이 존재한다 문서를 실행 하게 되면 악성 C&C서버에서 악성코드를 다운로드 하며 키보드 입력값, 화면캡처, 계정 정보 저장 등 사용자의 정보를 탈취 한다[.] 이 악성코드는 전용 웹사이트에서 합법적인 소프트웨어로 위장하여 판매되고 있다.



[그림] 3 Agent Tesla



[그림] 4 Agent Tesla Lifecycle

IoC 정보

IP

198[.]54[.]117[.]218	209[.]99[.]40[.]222	204[.]11[.]56[.]48	216[.]40[.]42[.]5	45[.]56[.]79[.]23
185[.]220[.]245[.]14	103[.]195[.]185[.]58	194[.]195[.]211[.]98	66[.]96[.]162[.]143	192[.]185[.]174[.]179
208[.]91[.]198[.]225	198[.]7[.]58[.]222	173[.]231[.]198[.]30	198[.]54[.]117[.]216	198[.]12[.]123[.]178
204[.]11[.]58[.]28	103[.]21[.]59[.]27	108[.]170[.]27[.]202	192[.]227[.]170[.]162	199[.]79[.]62[.]18

Domains

boatshowradio[.]com

www[.]brandimise[.]com

www[.]jimasun[.]online

www[.]furrylamb[.]com

www[.]clvilworksnsw[.]com

www[.]metaphilippines[.]com

www[.]spartanboardgames[.]com

www[.]timschindler[.]com

www[.]senz[.]design

www[.]synovusbanc[.]online

www[.]twiningss[.]com

www[.]justpita[.]net

www[.]123moviesflix[.]club

www[.]thefutureofxec[.]com

www[.]synovous-us[.]online

www[.]letsblessthismess[.]com

www[.]cleanenergymorocco[.]com

www[.]carstation[.]toys

www[.]xetaprotocol[.]com

www[.]buyhomemade[.]biz

Hash Sha-256

9EEAC4773D7F0E7F4303BAED25C04F0B138E55F9FA7E7C718E3E6599A2E41513

F40B127BD9693265582906BCABEA1F967597B4047D9E2A9C247B3AF84D1DBB73

4C7CE63CD966E72E5D94F6DC8B0F82CEC35B88B1A8D24305C52A7106CDAD5AD9

1A3BBF6F2ABFA4DC657A51EEDF5FA2D6CEF29C9461520990DEB36B97614EB2CF

D06E6E4FFB45128AC788CEA4094BDD7C91841FE588D9EE04E4EBE98CCDE37E29

224B1D257B5D2EBB67515CE2367E1CC25254601BC594B6008DCB67275DBA1212

9C00D71B81182C896E3C8F63D6A877C6BE8B1FBED3C9B6A510E2ABC959B8CF5F

D6E1A688DAA6611F7FF1EBF6724C3CCDABC18B97B1F606EC7BC141D8B81E1082

C2D65EA1C6FA3C75597C5A27931C94FFBF4BEA5BAA3B4447B5A0F7AEFEA52665

6AB9B209FDD5FBD49F97A187BE268836BA85FF7C4B070A288B44FCBC6E45F659

702A898F99FDCF56D29F5A9D4C54794C09880F7B000488A1F9F4C2259E520BEE

830AB27291A13C25DBF7FAA79E8C0D9984B572A06547B13D63195751A82F006A

EC02B1EAE63869AF607BB857C14BFDB7D0ACD823E203BE20AA9E6E5874B6ECF1

CFE8BE1E8C9102BB38319AE52E3EC3F51ED7330F447DA51A7A7E791F8A1CF966

78C432566D05D206897F549145494B9524298AAE8EE5E96578B980F6085E7759

2015FD8944FF2B72D2E09DD0AF7344283F1D9BFA4CA8A07E04E34AED7CD52421

E46D797785EE0837FBE4F643F1F8BFE3331306C3B46B2505B72E2E562B6B8525

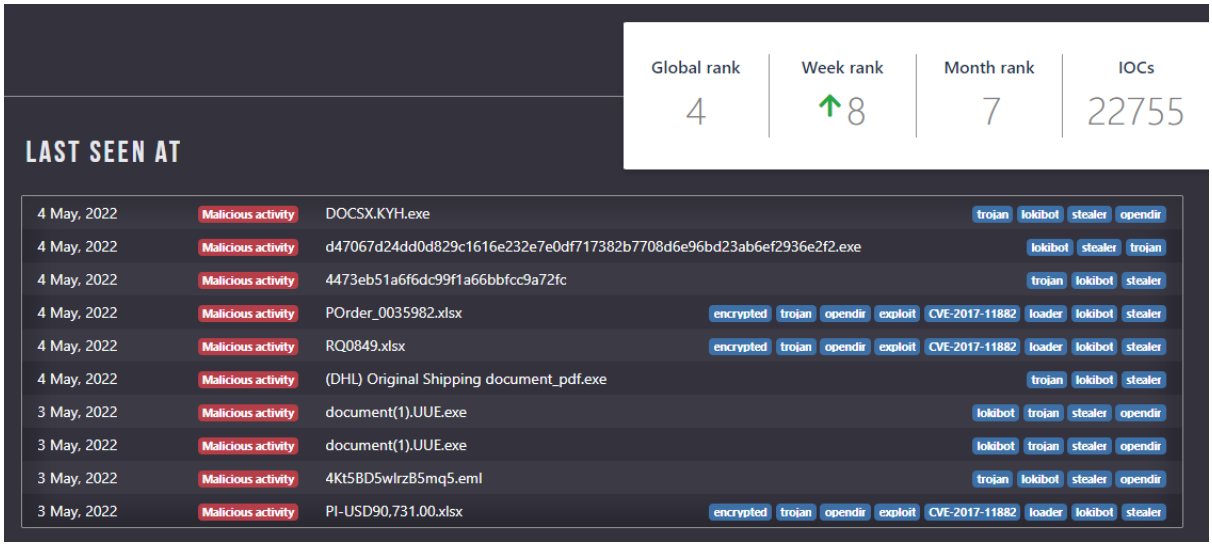
6F246950E4551705A3839EC78388104DE1038307A399E7566C81851394734977

DFEEA21B02AC4AE062E090CB4D22E921B572DB69AEF76BB26B7FC9477628F3EC

11E386BC1A3CDB9CA413E3E285C36D744A8B218033530D1976BB973685702C11

Lokibot

Lokibot 악성코드는 Agent Tesla, Formbook등의 악성코드와 비슷하게 대부분 스팸 메일을 통해 유포 되고 있다 안티바이러스 제품의 탐지를 우회하기 위해 닷넷 외형의 패커로 패킹되어 유포 되고 있다.



[그림] 5 Lokibot

유포되는 Lokibot 악성코드는 실행파일(exe)이 포함된 압축파일(zip) 혹은 문서 파일 (docx, pptx, xls)등이 있다 해당 악성코드는 사용자 PC의 메일, 웹 브라우저, 패스워드 관리 프로그램등의 사용자 정보를 수집하여 악성 C&C 서버로 전송하는 역할을 하고 있다 더 나아가 원격 조종으로 감염자 PC에서 추가적인 악성 행위를 시도 하기도 한다.

[그림] 6 Lokibot Lifecycle

IoC 정보

IP

204[.]11[.]56[.]48	209[.]99[.]40[.]222	172[.]67[.]171[.]141	185[.]53[.]179[.]29	192[.]124[.]249[.]18
45[.]133[.]200[.]3	103[.]21[.]59[.]27	192[.]168[.]100[.]227	192[.]169[.]69[.]25	104[.]18[.]32[.]77
185[.]55[.]227[.]103	199[.]33[.]112[.]226	173[.]239[.]8[.]164	66[.]96[.]149[.]17	167[.]88[.]160[.]226
198[.]23[.]213[.]114	72[.]52[.]238[.]62	204[.]93[.]178[.]31	192[.]168[.]100[.]27	69[.]90[.]160[.]170

Domains

majul[.]com

boatshowradio[.]com

www[.]lieebherr[.]com

booking[.]msg[.]bluhotels[.]com

booking[.]msg[.]bluhotels[.]com

pool[.]ug

www[.]gaffney-krroese[.]com

89gospel[.]com

millsmiltinon[.]com

office-archive-index[.]com

vladisfoxlink[.]ru

officeupgrade[.]org

grab-indonesia[.]com

broomingkingpoiuty[.]tk

mahikuchen[.]com

epsondriversforwindows[.]com

myinvestgroup[.]com

www[.]dicemention[.]com

www[.]rdppath[.]com

coreupdate[.]msoftupdates[.]com

Hash Sha-256

8CB097F0F995471541DE31F532D3E82B8308A0F2A504CF2BD0F8D4D981E2F369

9B134C393A0C62F6315F33BF58187167C24E14313BB20CC7E660BE3FEA1ABF05

5FA667E9B3AD3E183B65DCC3A10B983AC3B3282253C878C1779D7BDB9517355F

FF22D46135D75DC4E049A167E2A73A09F8C60A45EB93265ADF2F4FEB4A69DFAB

36F2FF4CC96257ED1162123AF197601669F978B483FEFC90F7C07772E1DD6A50

4FCB98C0D290235F50B5AD42CCD1D6514621AE40028CB965966AB586EF85D201

9AA58085341801686EA971B05C378D033B918417238C9C9DFCEB8C79DBE25AC0

45A72A9288FA594CBC38D7719AA0D44413DDE06DDA165B86DB143C5269AA6190

F2CE8DED83182F7F428CC8007429788FC17C54975D2C38EB7E46A21B84CA07F5

4EB6180BE03B71D0D63F458795A479EAE12DF53E6298D817C0BD24740995B389

BBABD9CB468B540C686F5777A6640F1CF8AA725FEAF3D12C569B1479F0BD2151

72F46C69DF5DAD8BC33C6D7CA8AE68B8A679447F8809EF3BBD63CE16AF445530

71E81F5B53A5B12D0DE6B1870166F2DD78FE61DADC7EC783AA6C3DAB103F0462

1A3BBF6F2ABFA4DC657A51EEDF5FA2D6CEF29C9461520990DEB36B97614EB2CF

5D840A9F5693E9156A461651C6D07E6D4171BF5A7E277487966E2013D2B20E34

AF8FD10B749EA99DB1BB4A6A2D7EE79F6B03726B2866A652F8BADE94D83440B8

AE88A45A8652BE603EC1D99C02B3030FE62BA055213075BFDB75C71D4F47B65C

74B0946B5310B7A6A5BFC00486172F6C2E492AB8CEF6022075F0BB1E2DF5F452

ABEAB6295037593783BC8746EAF467A11B0D246549F8EDE95E9C2A3D55E91D01

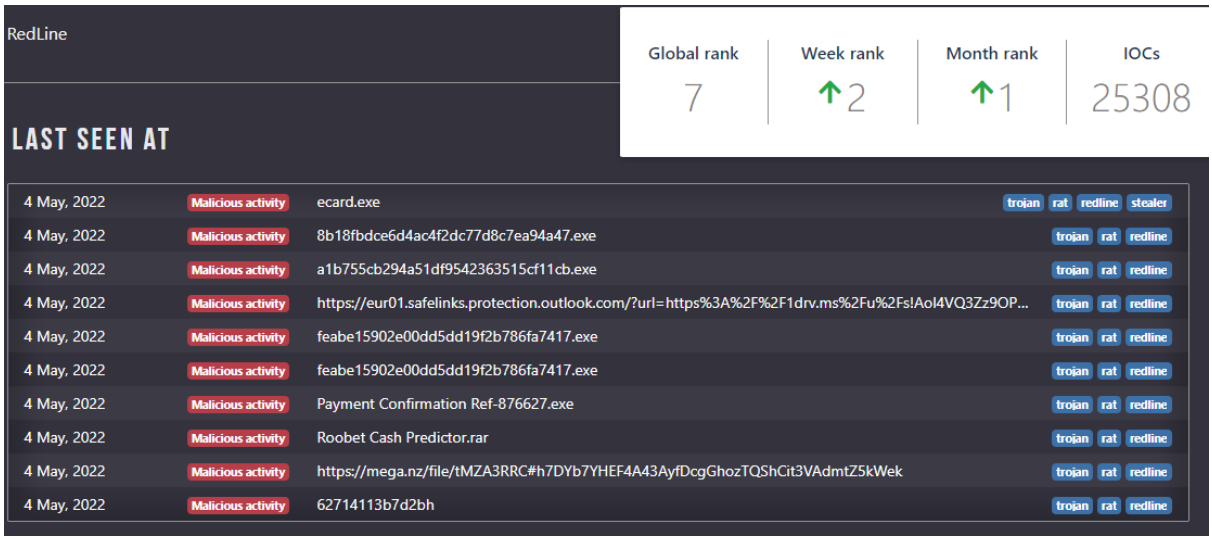
F8739A401C2A32

76DF0B47253199CEFD60F9D50F0EC006268FA53DD4FDAAD85A

RedLine

RedLine Stealer 악성코드는 20년 3월 코로나 이슈를 악용한 피싱 메일부터 시작하여 피싱 웹사이트나 악성코드를 추가 다운로드 하는 방식 등을 이용하여 유포 된 것으로 알려졌다.

구글 광고나 사진 편집 프로그램, 게임 핵 등을 위장하는 방식을 이용하여 유포된 사례가 다수 발견되고 있다.



[그림] 7 RedLine

RedLine Stealer는 정보탈취 악성코드로 피해자 PC가 감염 된다면 PC정보, 파일, 브라우저, 암호화폐 지갑 및 소프트웨어 등 감염환경의 다양한 정보들을 탈취한다.

이 악성코드는 사용자가 의심없이 파일을 다운로드 받아 실행하도록 유도하고 있으며, 정식 판매 광고 뿐만 아니라 크랙 된 버전도 유포되고 있어 각별한 주의가 필요하다. 출처가 불분명한 파일을 실행할 때는 매우 각별한 주의가 필요하다.

[그림] 8 RedLine Lifecycle

IoC 정보

IP

95[.]181[.]164[.]53	193[.]161[.]193[.]99	193[.]106[.]191[.]78	45[.]63[.]105[.]161	194[.]87[.]71[.]4
91[.]121[.]67[.]60	135[.]181[.]129[.]119	38[.]91[.]106[.]103	62[.]204[.]41[.]177	192[.]168[.]100[.]121
23[.]202[.]231[.]167	3[.]14[.]182[.]203	46[.]175[.]145[.]22	45[.]87[.]63[.]175	104[.]168[.]44[.]52
185[.]200[.]191[.]18	62[.]197[.]136[.]229	51[.]79[.]188[.]112	89[.]105[.]217[.]44	

Domains

rippr[.]cc

www[.]armantus[.]com

wiki[.]gamedetectives[.]net

recommendations[.]loopclub[.]io

assets[.]loopclub[.]io

proxoexploits[.]com

api[.]thundermods[.]com

shpr[.]co

theonecdn[.]com

psoeiras[.]net

2gvkhkatxu2iwio2cpro2rcrzh[.]com

21ypuxcv4gagi1k5eksm4ky1oh[.]com

2ah35terytseq3jgkvrakntoda[.]com

rgww1uvsk1blrxfvcir2nitpyd[.]com

nqd5zp4wgxk4f3inzhsy0g5iqa[.]com

waybes5qfjv5jbgqbhqg00i5hh[.]com

1uinnlqs144rlg4excqk1d45vc[.]com

xdzrut0u1repk11ukesujaybdf[.]com

jlpapzfuk35ldqpcqiswidaobb[.]com

petjiklshoapvx5dnjskq3fzuh[.]com

HASH Sha-256

6CE5F204A91D345A9AD811053B6557D5A187AA76DF44FEA5BB2A972BCE333C5D

7F210F9961B8BA954050558FA4B85120C876D304AAE0D3EDBB6576F0FA2661BE

C4269933FA6CD9B0A4BDA4981B659ED808C473B5AC2A2C27ED739AD36656F142

0F4B95A37B553B42F04C8530C0863C2A77D5ECF968976673CCDE973E7CA379A0

58274C41A987C806022F227B6DF900BB1BD3FAB9A7A87A3D34A5BD4F1B58980D

CF5E49420A700BBAB22878909E97B0ABA6F3E418E5C7EBBA98092157DE8A7350

FBC227EEE18134FF00CEB5D441E50EB3BCE71047E17D19823681E2DE64E4709B

29FF166AA81E12BB122B7D8CAB563E6E74DC662F206866A7C0F1214D2FF579C6

A9A8AF6A7973F0BB681937D63D6E6910E70FB4F3D9BBF86B9765EE9BAE61527B

EADDA092BA0C3EB11ECF0AEBBE7C305BAD2F675A760AB7EE0E58908E63D458BF

357F63389B69CBF2DAABDE47DA3F43B0BD853FEBCEF627373DF182D08C3A1D26

4035294BF7F0FF54530E66DB45DFE19EC280D03D14EA5E0BAB72AB6F8690A8B8

A2BED9BE9E8D978AC01029BB1EDC5949CB9EC9A455C36D561026EF7954CF99DB

60FF4EDB80ADDC2DE4A37FA61E4C811DAA8ADA05FE6DF70F024A3B916D2C2615

15A59C4AC664D9378A28620FD635B1C70D8B62FD8E8933E1128718B31E67345D

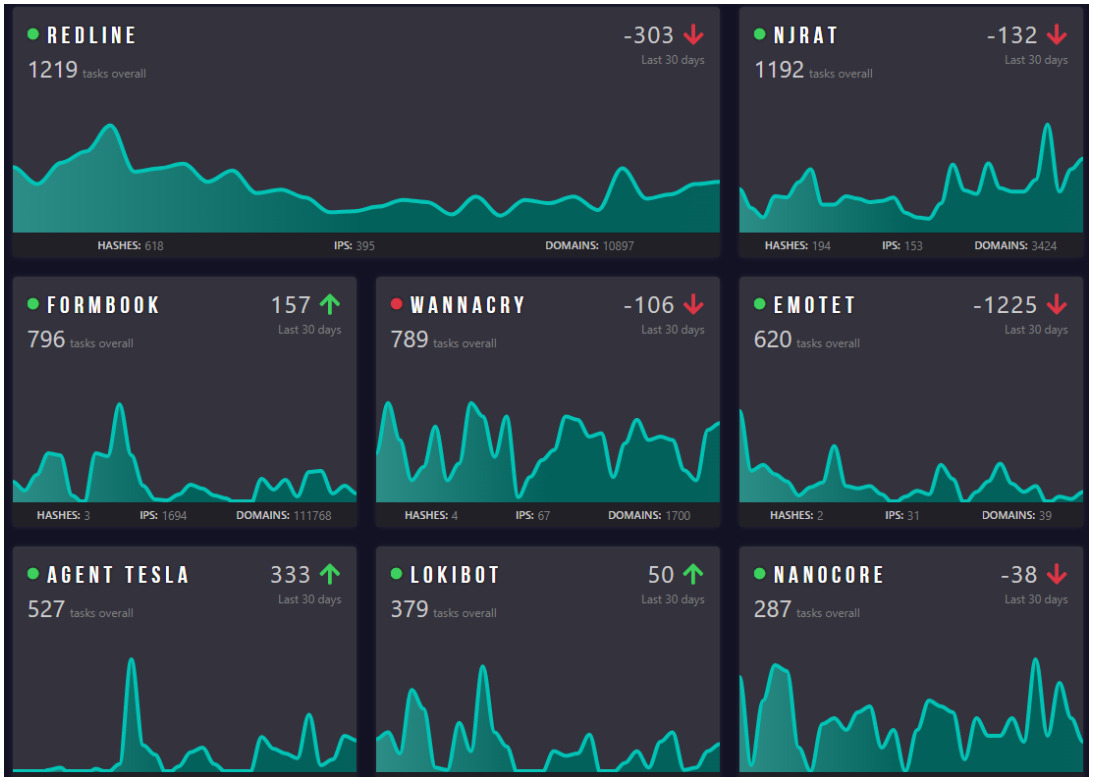
DC96D93AD1C83DCE26DC847E4A842485642533F0DC6151F564425DBA0B1BF753

83DEDC781457C9DD7B9DB68494163D944000ECCB1691C41E7DE989A1AE761282

BCFBCAFB6A9A4C9B927C314911D6FB2DF0124F3E84C5BDE424F17F0024E650E4

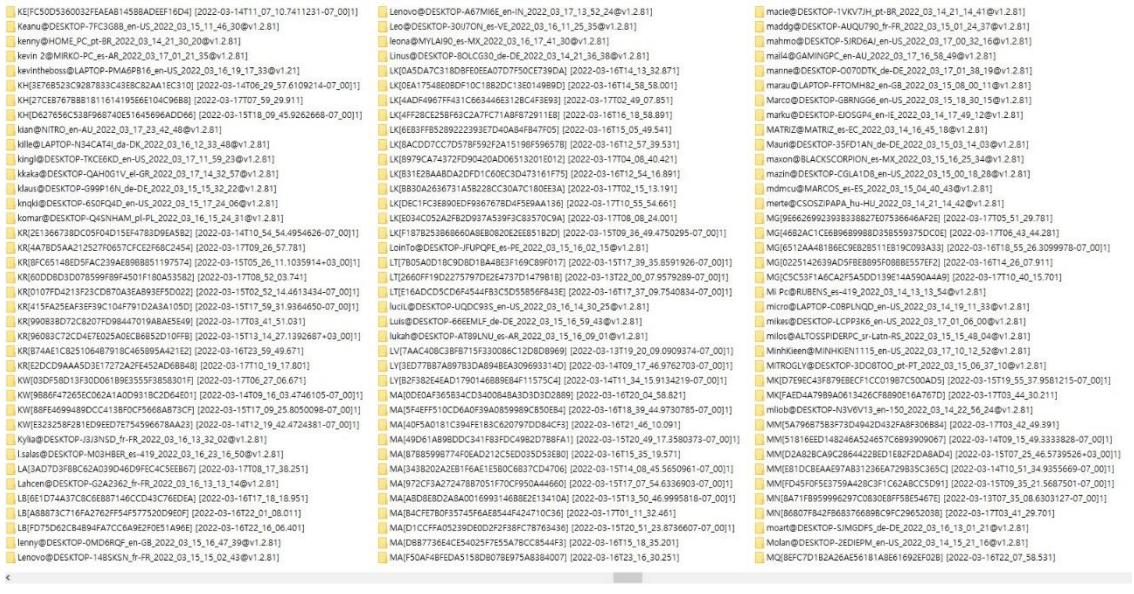
DD9194CF20F72E8F2F0B2FD08C9A4175E222B18DE4738B43AA9274F5111CB01B

9726C9A4D1E5C61B6A195FBDBFAF8E52253620CC2FB5E198F57C4269EBCFE7A1



[그림] 9 최근 한달 간 통계

최근 한 달간 유행하는 악성코드 유형에 대한 통계를 봤을 때 InfoStealer 악성코드가 대거 포진 되어 있는 것을 확인할 수 있다 InfoStealer 악성코드는 제 2차 타깃형 공격을 위한 사전 공격으로 많이 사용되고 있어 업무 메일에 첨부되어 있는 문서 파일이나 실행 파일 등을 실행을 하는데 있어서 각별한 주의가 필요하며 InfoStealer 악성코드로 인한 정보 유출이 심각하게 발생하고 있다.



[그림] 10 인포스틸러 감염으로 인한 유출 정보

참고 사이트

https://any.run/

https://asec.ahnlab.com/ko/33759/