Test Phase Duration: 0:03:58 (HH:MM:SS)

Class report:

precision recall f1-score support

alureon 0.2225 0.3042 0.2570 983

banjori 1.0000 1.0000 1.0000 983

bedep 0.3289 0.6724 0.4417 983

ccleaner 0.9889 0.9990 0.9939 983

chinad 0.8385 0.6918 0.7581 983

corebot 0.9938 0.9736 0.9836 983

cryptolocker 0.3662 0.0529 0.0924 983

dircrypt 0.1386 0.0610 0.0847 983

dyre 1.0000 1.0000 1.0000 983

fobber\_v1 0.5222 0.9817 0.6817 983

fobber\_v2 0.2097 0.6155 0.3128 983

gozi\_gpl 0.8862 0.8952 0.8907 983

gozi\_luther 0.8010 0.6592 0.7232 983

gozi\_nasa 0.7291 0.4435 0.5515 983

gozi\_rfc4343 0.5060 0.6846 0.5819 983

kraken\_v1 0.5852 0.7477 0.6565 983

kraken\_v2 0.3860 0.0448 0.0802 983

locky 0.1685 0.1587 0.1634 983

matsnu 0.7721 0.9583 0.8552 983

murofet\_v1 0.7889 0.9583 0.8654 983

murofet\_v2 0.5670 0.9949 0.7223 983

murofet\_v3 1.0000 0.9542 0.9766 983

necurs 0.1820 0.2503 0.2107 983

nymaim 0.8359 0.7874 0.8109 983

padcrypt 0.9017 0.9613 0.9306 983

pizd 0.5455 0.5666 0.5559 983

proslikefan 0.3166 0.4496 0.3716 983

pushdo 0.7452 0.6368 0.6868 983

pykspa 0.3238 0.0346 0.0625 983

pykspa\_noise 0.2262 0.0193 0.0356 983

qadars 0.5661 0.8362 0.6752 983

qakbot 0.5000 0.0031 0.0061 983

ramdo 0.7758 0.9858 0.8683 983

ramnit 0.2185 0.0529 0.0852 983

ranbyus\_v1 0.3571 0.2808 0.3144 983

ranbyus\_v2 0.5287 0.0844 0.1456 983

rovnix 0.9135 0.7202 0.8055 983

shiotob 0.6688 0.2116 0.3215 983

simda 0.4643 0.5351 0.4972 983

sisron 0.9671 0.9878 0.9774 983

suppobox\_1 0.6601 0.5076 0.5739 983

suppobox\_2 0.5927 0.9298 0.7240 983

suppobox\_3 0.8988 0.9756 0.9356 983

symmi 0.9780 0.9969 0.9874 983

tempedreve 0.2171 0.3927 0.2796 983

tinba 0.0000 0.0000 0.0000 983

vawtrak\_v1 0.9457 0.9919 0.9682 983

vawtrak\_v2 0.3232 0.7691 0.4551 983

vawtrak\_v3 0.4564 0.4212 0.4381 983

zeus-newgoz 0.9958 0.9715 0.9835 983

legit 0.4488 0.1740 0.2507 983

accuracy 0.5958 50133

macro avg 0.5951 0.5958 0.5614 50133

weighted avg 0.5951 0.5958 0.5614 50133

F1 Score, Precision and Recall:

Macro Micro

F1 Score 0.561371 0.595795

Precision 0.595149 0.595795

Recall 0.595795 0.595795

Overall accuracy = 0.5957951848084097

Confusion matrix:

alureon banjori bedep ccleaner chinad corebot \

alureon 299 0 2 0 0 0

banjori 0 983 0 0 0 0

bedep 67 0 661 0 3 0

ccleaner 0 0 0 982 0 0

chinad 0 0 6 1 680 1

corebot 0 0 0 0 0 957

cryptolocker 26 0 73 0 1 0

dircrypt 110 0 424 0 0 0

dyre 0 0 0 0 0 0

fobber\_v1 0 0 0 0 0 0

fobber\_v2 275 0 1 0 0 0

gozi\_gpl 0 0 0 0 0 0

gozi\_luther 1 0 2 0 0 0

gozi\_nasa 1 0 6 0 0 0

gozi\_rfc4343 0 0 7 0 0 0

kraken\_v1 18 0 30 0 0 0

kraken\_v2 72 0 62 0 0 0

locky 1 0 0 0 0 0

matsnu 0 0 0 0 0 0

murofet\_v1 0 0 0 0 0 0

murofet\_v2 0 0 0 0 0 0

murofet\_v3 0 0 0 0 0 0

necurs 4 0 14 0 0 0

nymaim 0 0 0 0 0 0

padcrypt 0 0 8 0 0 0

pizd 0 0 0 0 0 0

proslikefan 18 0 0 0 0 0

pushdo 24 0 21 0 0 0

pykspa 20 0 1 0 0 0

pykspa\_noise 22 0 1 0 0 0

qadars 4 0 2 4 9 0

qakbot 13 0 59 0 0 0

ramdo 0 0 0 0 0 0

ramnit 121 0 363 0 0 0

ranbyus\_v1 3 0 75 0 0 0

ranbyus\_v2 0 0 104 0 1 0

rovnix 0 0 0 0 0 0

shiotob 23 0 40 2 115 0

simda 15 0 0 0 0 0

sisron 10 0 0 0 0 0

suppobox\_1 0 0 0 0 0 0

suppobox\_2 0 0 0 0 0 0

suppobox\_3 0 0 0 0 0 0

symmi 0 0 0 0 0 0

tempedreve 81 0 0 0 0 0

tinba 98 0 47 0 0 0

vawtrak\_v1 0 0 0 0 0 0

vawtrak\_v2 4 0 0 0 0 0

vawtrak\_v3 7 0 0 0 0 0

zeus-newgoz 0 0 0 0 2 5

legit 7 0 1 4 0 0

cryptolocker dircrypt dyre fobber\_v1 fobber\_v2 gozi\_gpl \

alureon 0 16 0 0 588 0

banjori 0 0 0 0 0 0

bedep 0 74 0 5 50 0

ccleaner 0 0 0 0 0 0

chinad 0 0 0 27 0 0

corebot 0 0 0 10 0 0

cryptolocker 52 21 0 108 12 1

dircrypt 0 60 0 10 219 0

dyre 0 0 983 0 0 0

fobber\_v1 0 0 0 965 0 0

fobber\_v2 0 14 0 0 605 0

gozi\_gpl 1 0 0 0 0 880

gozi\_luther 0 0 0 0 0 0

gozi\_nasa 0 0 0 0 1 0

gozi\_rfc4343 0 0 0 0 3 2

kraken\_v1 0 11 0 0 112 0

kraken\_v2 1 27 0 0 239 0

locky 7 1 0 6 0 2

matsnu 0 0 0 0 0 0

murofet\_v1 0 0 0 2 0 3

murofet\_v2 1 0 0 0 0 1

murofet\_v3 0 0 0 0 0 0

necurs 14 1 0 37 17 2

nymaim 1 0 0 0 0 28

padcrypt 0 0 0 4 0 0

pizd 0 0 0 0 0 0

proslikefan 1 0 0 1 60 0

pushdo 1 9 0 0 59 1

pykspa 8 8 0 56 58 0

pykspa\_noise 2 11 0 58 61 0

qadars 1 4 0 10 11 0

qakbot 7 3 0 166 28 1

ramdo 0 0 0 0 0 0

ramnit 1 69 0 1 265 0

ranbyus\_v1 30 10 0 68 3 2

ranbyus\_v2 10 1 0 157 0 4

rovnix 0 0 0 0 0 66

shiotob 0 7 0 68 45 0

simda 0 0 0 0 105 0

sisron 0 0 0 0 1 0

suppobox\_1 0 0 0 0 0 0

suppobox\_2 0 0 0 0 0 0

suppobox\_3 0 0 0 0 0 0

symmi 0 0 0 2 0 0

tempedreve 0 0 0 24 146 0

tinba 4 82 0 53 123 0

vawtrak\_v1 0 0 0 0 0 0

vawtrak\_v2 0 2 0 0 43 0

vawtrak\_v3 0 0 0 0 17 0

zeus-newgoz 0 0 0 9 0 0

legit 0 2 0 1 14 0

gozi\_luther gozi\_nasa gozi\_rfc4343 kraken\_v1 kraken\_v2 \

alureon 0 0 0 4 0

banjori 0 0 0 0 0

bedep 3 0 1 10 1

ccleaner 0 0 0 0 0

chinad 0 0 0 0 0

corebot 0 0 0 1 0

cryptolocker 0 0 0 24 3

dircrypt 5 0 0 12 0

dyre 0 0 0 0 0

fobber\_v1 0 0 0 2 0

fobber\_v2 0 0 0 4 0

gozi\_gpl 0 0 2 1 0

gozi\_luther 648 34 235 0 0

gozi\_nasa 62 436 316 0 0

gozi\_rfc4343 62 96 673 2 0

kraken\_v1 1 0 0 735 8

kraken\_v2 0 0 0 249 44

locky 1 0 0 21 14

matsnu 3 9 11 0 0

murofet\_v1 0 0 0 0 0

murofet\_v2 0 0 0 0 0

murofet\_v3 0 0 0 0 0

necurs 0 0 0 9 15

nymaim 1 6 6 1 0

padcrypt 0 1 1 0 0

pizd 0 0 0 0 0

proslikefan 0 0 0 14 3

pushdo 3 0 2 0 0

pykspa 0 0 0 13 1

pykspa\_noise 0 0 0 10 3

qadars 1 0 0 7 0

qakbot 1 0 0 33 5

ramdo 0 0 0 8 0

ramnit 3 0 1 8 0

ranbyus\_v1 0 0 0 24 1

ranbyus\_v2 1 1 1 7 0

rovnix 12 11 75 0 0

shiotob 0 0 0 5 0

simda 0 0 0 4 1

sisron 0 0 0 0 0

suppobox\_1 0 0 0 0 0

suppobox\_2 0 0 0 0 0

suppobox\_3 0 0 0 0 0

symmi 0 0 0 0 0

tempedreve 0 0 0 24 11

tinba 0 0 0 22 4

vawtrak\_v1 0 0 0 1 0

vawtrak\_v2 1 0 0 0 0

vawtrak\_v3 0 0 0 0 0

zeus-newgoz 0 0 0 0 0

legit 1 4 6 1 0

locky matsnu murofet\_v1 murofet\_v2 murofet\_v3 necurs \

alureon 0 0 0 0 0 0

banjori 0 0 0 0 0 0

bedep 0 0 0 4 0 13

ccleaner 0 0 0 0 0 0

chinad 2 0 0 20 0 13

corebot 0 0 0 0 0 0

cryptolocker 64 0 0 167 0 63

dircrypt 0 0 2 3 0 19

dyre 0 0 0 0 0 0

fobber\_v1 0 0 0 0 0 2

fobber\_v2 0 0 0 0 0 0

gozi\_gpl 0 0 4 0 0 0

gozi\_luther 0 22 1 0 0 0

gozi\_nasa 0 100 1 0 0 0

gozi\_rfc4343 0 71 0 0 0 0

kraken\_v1 2 0 0 1 0 2

kraken\_v2 50 0 0 3 0 6

locky 156 0 0 136 0 188

matsnu 0 942 0 0 0 0

murofet\_v1 0 0 942 2 0 29

murofet\_v2 0 0 0 978 0 0

murofet\_v3 0 0 44 0 938 0

necurs 153 0 20 52 0 246

nymaim 1 28 0 1 0 0

padcrypt 0 0 0 0 0 1

pizd 0 0 0 0 0 0

proslikefan 27 0 0 71 0 1

pushdo 13 2 0 1 0 0

pykspa 10 0 0 3 0 0

pykspa\_noise 14 0 0 0 0 2

qadars 3 0 0 0 0 1

qakbot 10 0 171 125 0 98

ramdo 0 0 0 0 0 6

ramnit 0 0 0 2 0 20

ranbyus\_v1 175 0 0 13 0 183

ranbyus\_v2 22 0 0 68 0 422

rovnix 0 3 0 0 0 0

shiotob 0 0 0 0 0 1

simda 8 0 0 0 0 1

sisron 0 0 0 0 0 0

suppobox\_1 0 0 0 0 0 0

suppobox\_2 0 0 0 0 0 0

suppobox\_3 0 0 0 0 0 0

symmi 0 0 0 0 0 0

tempedreve 9 0 0 0 0 0

tinba 203 0 0 74 0 35

vawtrak\_v1 4 0 0 0 0 0

vawtrak\_v2 0 0 0 0 0 0

vawtrak\_v3 0 0 0 0 0 0

zeus-newgoz 0 0 9 0 0 0

legit 0 52 0 1 0 0

nymaim padcrypt pizd proslikefan pushdo pykspa \

alureon 0 2 0 0 8 0

banjori 0 0 0 0 0 0

bedep 0 6 0 0 3 0

ccleaner 0 1 0 0 0 0

chinad 0 2 0 0 0 0

corebot 0 0 0 0 0 0

cryptolocker 0 8 2 2 12 1

dircrypt 0 5 0 0 6 0

dyre 0 0 0 0 0 0

fobber\_v1 0 2 0 0 0 0

fobber\_v2 0 1 0 0 7 0

gozi\_gpl 53 0 0 2 1 0

gozi\_luther 4 0 0 0 3 0

gozi\_nasa 3 0 0 0 1 0

gozi\_rfc4343 4 6 0 0 1 0

kraken\_v1 2 0 0 4 2 0

kraken\_v2 3 6 0 118 5 1

locky 4 9 0 172 23 5

matsnu 0 0 0 0 0 0

murofet\_v1 0 0 0 0 0 0

murofet\_v2 0 0 0 0 2 0

murofet\_v3 0 0 0 0 0 0

necurs 1 6 0 178 19 1

nymaim 774 0 23 2 8 0

padcrypt 1 945 2 0 0 0

pizd 0 0 557 0 0 0

proslikefan 1 1 0 442 6 16

pushdo 8 1 0 21 626 0

pykspa 0 2 2 94 6 34

pykspa\_noise 0 0 0 92 4 30

qadars 0 0 3 0 1 0

qakbot 2 7 0 23 3 4

ramdo 0 0 0 0 0 0

ramnit 0 7 0 0 6 0

ranbyus\_v1 6 5 1 2 21 0

ranbyus\_v2 4 12 0 0 1 0

rovnix 17 0 6 0 0 0

shiotob 0 3 0 1 2 0

simda 12 0 0 113 30 6

sisron 0 0 0 0 0 0

suppobox\_1 0 0 347 0 0 0

suppobox\_2 0 0 59 0 0 0

suppobox\_3 0 0 15 0 0 0

symmi 0 0 0 0 0 0

tempedreve 0 1 1 90 2 6

tinba 1 9 2 6 24 0

vawtrak\_v1 0 0 0 1 0 0

vawtrak\_v2 0 0 0 0 0 0

vawtrak\_v3 0 0 0 0 2 0

zeus-newgoz 0 1 0 0 0 0

legit 26 0 1 33 5 1

pykspa\_noise qadars qakbot ramdo ramnit ranbyus\_v1 \

alureon 0 0 0 0 0 0

banjori 0 0 0 0 0 0

bedep 0 0 0 0 45 0

ccleaner 0 0 0 0 0 0

chinad 0 190 0 5 0 4

corebot 0 0 0 0 0 0

cryptolocker 8 0 0 40 11 165

dircrypt 0 0 1 2 61 1

dyre 0 0 0 0 0 0

fobber\_v1 0 0 0 4 0 0

fobber\_v2 0 0 0 0 0 0

gozi\_gpl 0 0 0 3 0 1

gozi\_luther 0 0 0 0 3 0

gozi\_nasa 0 0 1 0 2 0

gozi\_rfc4343 0 0 0 0 7 0

kraken\_v1 0 0 0 4 4 2

kraken\_v2 0 0 0 6 2 5

locky 1 0 1 17 1 91

matsnu 0 0 0 0 0 0

murofet\_v1 0 0 0 2 0 0

murofet\_v2 0 0 0 0 0 0

murofet\_v3 0 0 0 0 0 0

necurs 0 0 0 17 1 73

nymaim 1 0 0 1 0 0

padcrypt 0 0 0 9 0 0

pizd 0 0 0 0 0 0

proslikefan 3 2 0 4 0 3

pushdo 2 0 0 1 7 3

pykspa 15 1 0 26 0 18

pykspa\_noise 19 1 0 29 0 11

qadars 0 822 0 22 0 2

qakbot 4 1 3 32 13 19

ramdo 0 0 0 969 0 0

ramnit 0 0 0 1 52 0

ranbyus\_v1 1 3 0 28 11 276

ranbyus\_v2 0 0 0 24 16 39

rovnix 0 0 0 0 0 0

shiotob 1 415 0 0 1 1

simda 2 0 0 0 0 1

sisron 0 0 0 0 0 0

suppobox\_1 0 0 0 0 0 0

suppobox\_2 0 0 0 0 0 0

suppobox\_3 0 0 0 0 0 0

symmi 0 0 0 0 0 0

tempedreve 21 5 0 0 0 1

tinba 6 4 0 3 1 57

vawtrak\_v1 0 0 0 0 0 0

vawtrak\_v2 0 0 0 0 0 0

vawtrak\_v3 0 0 0 0 0 0

zeus-newgoz 0 2 0 0 0 0

legit 0 6 0 0 0 0

ranbyus\_v2 rovnix shiotob simda sisron suppobox\_1 \

alureon 0 0 0 1 0 0

banjori 0 0 0 0 0 0

bedep 3 0 27 0 2 0

ccleaner 0 0 0 0 0 0

chinad 6 0 23 0 0 0

corebot 0 0 0 0 0 0

cryptolocker 11 0 0 7 2 0

dircrypt 6 0 1 0 0 0

dyre 0 0 0 0 0 0

fobber\_v1 0 0 0 0 1 0

fobber\_v2 0 0 4 0 1 0

gozi\_gpl 0 34 0 0 0 0

gozi\_luther 0 0 0 0 0 0

gozi\_nasa 0 10 0 1 0 0

gozi\_rfc4343 0 9 0 0 0 0

kraken\_v1 0 0 0 0 2 0

kraken\_v2 0 0 0 1 1 0

locky 11 0 0 31 3 0

matsnu 0 0 0 0 0 0

murofet\_v1 2 1 0 0 0 0

murofet\_v2 0 0 0 1 0 0

murofet\_v3 0 0 0 0 0 0

necurs 19 1 0 8 0 1

nymaim 0 11 0 2 0 18

padcrypt 3 0 0 0 0 0

pizd 0 0 0 0 0 208

proslikefan 0 0 0 79 1 0

pushdo 0 0 0 19 0 0

pykspa 0 0 1 169 2 0

pykspa\_noise 0 0 0 162 3 0

qadars 0 0 34 0 0 0

qakbot 10 0 2 15 1 0

ramdo 0 0 0 0 0 0

ramnit 2 0 1 0 0 0

ranbyus\_v1 1 0 0 1 2 1

ranbyus\_v2 83 0 1 0 0 0

rovnix 0 708 0 0 0 7

shiotob 0 0 208 0 0 0

simda 0 0 0 526 0 0

sisron 0 0 0 0 971 0

suppobox\_1 0 0 0 0 0 499

suppobox\_2 0 0 0 0 0 9

suppobox\_3 0 0 0 0 0 9

symmi 0 0 0 0 0 0

tempedreve 0 0 2 102 11 1

tinba 0 0 0 1 1 0

vawtrak\_v1 0 0 0 0 0 0

vawtrak\_v2 0 0 0 0 0 0

vawtrak\_v3 0 0 0 0 0 0

zeus-newgoz 0 0 0 0 0 0

legit 0 1 7 7 0 3

suppobox\_2 suppobox\_3 symmi tempedreve tinba vawtrak\_v1 \

alureon 0 0 0 0 0 0

banjori 0 0 0 0 0 0

bedep 0 0 0 0 0 0

ccleaner 0 0 0 0 0 0

chinad 0 0 0 0 0 0

corebot 0 0 15 0 0 0

cryptolocker 1 0 0 92 1 0

dircrypt 0 0 0 0 0 0

dyre 0 0 0 0 0 0

fobber\_v1 0 5 1 1 0 0

fobber\_v2 0 0 0 0 0 0

gozi\_gpl 0 0 0 1 0 0

gozi\_luther 0 0 0 0 0 0

gozi\_nasa 0 0 0 0 0 0

gozi\_rfc4343 0 0 0 0 0 0

kraken\_v1 0 0 0 20 0 0

kraken\_v2 0 0 0 32 1 2

locky 0 0 0 72 0 3

matsnu 0 0 0 0 0 0

murofet\_v1 0 0 0 0 0 0

murofet\_v2 0 0 0 0 0 0

murofet\_v3 0 0 0 0 0 0

necurs 1 0 0 47 0 11

nymaim 11 8 0 0 0 5

padcrypt 0 3 2 0 0 0

pizd 210 8 0 0 0 0

proslikefan 27 0 0 142 0 7

pushdo 0 0 0 7 0 0

pykspa 62 0 0 328 0 1

pykspa\_noise 78 0 0 328 0 0

qadars 1 1 0 17 0 22

qakbot 4 0 1 116 0 0

ramdo 0 0 0 0 0 0

ramnit 0 0 0 0 0 0

ranbyus\_v1 2 0 0 33 1 1

ranbyus\_v2 0 1 0 3 0 0

rovnix 0 77 0 0 0 0

shiotob 7 1 0 30 0 0

simda 1 0 0 16 0 0

sisron 0 0 0 1 0 0

suppobox\_1 135 2 0 0 0 0

suppobox\_2 914 0 0 0 0 0

suppobox\_3 0 959 0 0 0 0

symmi 0 1 980 0 0 0

tempedreve 26 0 3 386 0 2

tinba 2 0 0 103 0 1

vawtrak\_v1 0 0 0 2 0 975

vawtrak\_v2 0 0 0 0 0 0

vawtrak\_v3 0 0 0 0 0 0

zeus-newgoz 0 0 0 0 0 0

legit 60 1 0 1 0 1

vawtrak\_v2 vawtrak\_v3 zeus-newgoz legit

alureon 50 13 0 0

banjori 0 0 0 0

bedep 5 0 0 0

ccleaner 0 0 0 0

chinad 1 0 2 0

corebot 0 0 0 0

cryptolocker 5 0 0 0

dircrypt 28 8 0 0

dyre 0 0 0 0

fobber\_v1 0 0 0 0

fobber\_v2 58 13 0 0

gozi\_gpl 0 0 0 0

gozi\_luther 23 7 0 0

gozi\_nasa 36 6 0 0

gozi\_rfc4343 31 7 0 2

kraken\_v1 15 8 0 0

kraken\_v2 28 9 0 10

locky 0 0 0 6

matsnu 9 9 0 0

murofet\_v1 0 0 0 0

murofet\_v2 0 0 0 0

murofet\_v3 0 0 1 0

necurs 1 0 0 14

nymaim 10 2 0 34

padcrypt 3 0 0 0

pizd 0 0 0 0

proslikefan 19 7 0 27

pushdo 116 27 0 9

pykspa 31 5 0 8

pykspa\_noise 33 6 0 3

qadars 1 0 0 0

qakbot 0 2 0 1

ramdo 0 0 0 0

ramnit 50 10 0 0

ranbyus\_v1 0 0 0 0

ranbyus\_v2 0 0 0 0

rovnix 0 0 1 0

shiotob 5 1 0 1

simda 47 11 0 84

sisron 0 0 0 0

suppobox\_1 0 0 0 0

suppobox\_2 0 0 0 1

suppobox\_3 0 0 0 0

symmi 0 0 0 0

tempedreve 14 5 0 9

tinba 14 2 0 1

vawtrak\_v1 0 0 0 0

vawtrak\_v2 756 177 0 0

vawtrak\_v3 543 414 0 0

zeus-newgoz 0 0 955 0

legit 407 158 0 171

True positive: 29869

Test Phase Duration: 0:03:47 (HH:MM:SS)

Class report:

precision recall f1-score support

alureon 0.2225 0.3042 0.2570 983

banjori 1.0000 1.0000 1.0000 983

bedep 0.3289 0.6724 0.4417 983

ccleaner 0.9889 0.9990 0.9939 983

chinad 0.8385 0.6918 0.7581 983

corebot 0.9938 0.9736 0.9836 983

cryptolocker 0.3662 0.0529 0.0924 983

dircrypt 0.1386 0.0610 0.0847 983

dyre 1.0000 1.0000 1.0000 983

fobber\_v1 0.5222 0.9817 0.6817 983

fobber\_v2 0.2097 0.6155 0.3128 983

gozi\_gpl 0.8862 0.8952 0.8907 983

gozi\_luther 0.8010 0.6592 0.7232 983

gozi\_nasa 0.7291 0.4435 0.5515 983

gozi\_rfc4343 0.5060 0.6846 0.5819 983

kraken\_v1 0.5852 0.7477 0.6565 983

kraken\_v2 0.3860 0.0448 0.0802 983

locky 0.1685 0.1587 0.1634 983

matsnu 0.7721 0.9583 0.8552 983

murofet\_v1 0.7889 0.9583 0.8654 983

murofet\_v2 0.5670 0.9949 0.7223 983

murofet\_v3 1.0000 0.9542 0.9766 983

necurs 0.1820 0.2503 0.2107 983

nymaim 0.8359 0.7874 0.8109 983

padcrypt 0.9017 0.9613 0.9306 983

pizd 0.5455 0.5666 0.5559 983

proslikefan 0.3166 0.4496 0.3716 983

pushdo 0.7452 0.6368 0.6868 983

pykspa 0.3238 0.0346 0.0625 983

pykspa\_noise 0.2262 0.0193 0.0356 983

qadars 0.5661 0.8362 0.6752 983

qakbot 0.5000 0.0031 0.0061 983

ramdo 0.7758 0.9858 0.8683 983

ramnit 0.2185 0.0529 0.0852 983

ranbyus\_v1 0.3571 0.2808 0.3144 983

ranbyus\_v2 0.5287 0.0844 0.1456 983

rovnix 0.9135 0.7202 0.8055 983

shiotob 0.6688 0.2116 0.3215 983

simda 0.4643 0.5351 0.4972 983

sisron 0.9671 0.9878 0.9774 983

suppobox\_1 0.6601 0.5076 0.5739 983

suppobox\_2 0.5927 0.9298 0.7240 983

suppobox\_3 0.8988 0.9756 0.9356 983

symmi 0.9780 0.9969 0.9874 983

tempedreve 0.2171 0.3927 0.2796 983

tinba 0.0000 0.0000 0.0000 983

vawtrak\_v1 0.9457 0.9919 0.9682 983

vawtrak\_v2 0.3232 0.7691 0.4551 983

vawtrak\_v3 0.4564 0.4212 0.4381 983

zeus-newgoz 0.9958 0.9715 0.9835 983

legit 0.4488 0.1740 0.2507 983

accuracy 0.5958 50133

macro avg 0.5951 0.5958 0.5614 50133

weighted avg 0.5951 0.5958 0.5614 50133

F1 Score, Precision and Recall:

Macro Micro

F1 Score 0.561371 0.595795

Precision 0.595149 0.595795

Recall 0.595795 0.595795

Overall accuracy = 0.5957951848084097

Confusion matrix:

alureon banjori bedep ccleaner chinad corebot \

alureon 299 0 2 0 0 0

banjori 0 983 0 0 0 0

bedep 67 0 661 0 3 0

ccleaner 0 0 0 982 0 0

chinad 0 0 6 1 680 1

corebot 0 0 0 0 0 957

cryptolocker 26 0 73 0 1 0

dircrypt 110 0 424 0 0 0

dyre 0 0 0 0 0 0

fobber\_v1 0 0 0 0 0 0

fobber\_v2 275 0 1 0 0 0

gozi\_gpl 0 0 0 0 0 0

gozi\_luther 1 0 2 0 0 0

gozi\_nasa 1 0 6 0 0 0

gozi\_rfc4343 0 0 7 0 0 0

kraken\_v1 18 0 30 0 0 0

kraken\_v2 72 0 62 0 0 0

locky 1 0 0 0 0 0

matsnu 0 0 0 0 0 0

murofet\_v1 0 0 0 0 0 0

murofet\_v2 0 0 0 0 0 0

murofet\_v3 0 0 0 0 0 0

necurs 4 0 14 0 0 0

nymaim 0 0 0 0 0 0

padcrypt 0 0 8 0 0 0

pizd 0 0 0 0 0 0

proslikefan 18 0 0 0 0 0

pushdo 24 0 21 0 0 0

pykspa 20 0 1 0 0 0

pykspa\_noise 22 0 1 0 0 0

qadars 4 0 2 4 9 0

qakbot 13 0 59 0 0 0

ramdo 0 0 0 0 0 0

ramnit 121 0 363 0 0 0

ranbyus\_v1 3 0 75 0 0 0

ranbyus\_v2 0 0 104 0 1 0

rovnix 0 0 0 0 0 0

shiotob 23 0 40 2 115 0

simda 15 0 0 0 0 0

sisron 10 0 0 0 0 0

suppobox\_1 0 0 0 0 0 0

suppobox\_2 0 0 0 0 0 0

suppobox\_3 0 0 0 0 0 0

symmi 0 0 0 0 0 0

tempedreve 81 0 0 0 0 0

tinba 98 0 47 0 0 0

vawtrak\_v1 0 0 0 0 0 0

vawtrak\_v2 4 0 0 0 0 0

vawtrak\_v3 7 0 0 0 0 0

zeus-newgoz 0 0 0 0 2 5

legit 7 0 1 4 0 0

cryptolocker dircrypt dyre fobber\_v1 fobber\_v2 gozi\_gpl \

alureon 0 16 0 0 588 0

banjori 0 0 0 0 0 0

bedep 0 74 0 5 50 0

ccleaner 0 0 0 0 0 0

chinad 0 0 0 27 0 0

corebot 0 0 0 10 0 0

cryptolocker 52 21 0 108 12 1

dircrypt 0 60 0 10 219 0

dyre 0 0 983 0 0 0

fobber\_v1 0 0 0 965 0 0

fobber\_v2 0 14 0 0 605 0

gozi\_gpl 1 0 0 0 0 880

gozi\_luther 0 0 0 0 0 0

gozi\_nasa 0 0 0 0 1 0

gozi\_rfc4343 0 0 0 0 3 2

kraken\_v1 0 11 0 0 112 0

kraken\_v2 1 27 0 0 239 0

locky 7 1 0 6 0 2

matsnu 0 0 0 0 0 0

murofet\_v1 0 0 0 2 0 3

murofet\_v2 1 0 0 0 0 1

murofet\_v3 0 0 0 0 0 0

necurs 14 1 0 37 17 2

nymaim 1 0 0 0 0 28

padcrypt 0 0 0 4 0 0

pizd 0 0 0 0 0 0

proslikefan 1 0 0 1 60 0

pushdo 1 9 0 0 59 1

pykspa 8 8 0 56 58 0

pykspa\_noise 2 11 0 58 61 0

qadars 1 4 0 10 11 0

qakbot 7 3 0 166 28 1

ramdo 0 0 0 0 0 0

ramnit 1 69 0 1 265 0

ranbyus\_v1 30 10 0 68 3 2

ranbyus\_v2 10 1 0 157 0 4

rovnix 0 0 0 0 0 66

shiotob 0 7 0 68 45 0

simda 0 0 0 0 105 0

sisron 0 0 0 0 1 0

suppobox\_1 0 0 0 0 0 0

suppobox\_2 0 0 0 0 0 0

suppobox\_3 0 0 0 0 0 0

symmi 0 0 0 2 0 0

tempedreve 0 0 0 24 146 0

tinba 4 82 0 53 123 0

vawtrak\_v1 0 0 0 0 0 0

vawtrak\_v2 0 2 0 0 43 0

vawtrak\_v3 0 0 0 0 17 0

zeus-newgoz 0 0 0 9 0 0

legit 0 2 0 1 14 0

gozi\_luther gozi\_nasa gozi\_rfc4343 kraken\_v1 kraken\_v2 \

alureon 0 0 0 4 0

banjori 0 0 0 0 0

bedep 3 0 1 10 1

ccleaner 0 0 0 0 0

chinad 0 0 0 0 0

corebot 0 0 0 1 0

cryptolocker 0 0 0 24 3

dircrypt 5 0 0 12 0

dyre 0 0 0 0 0

fobber\_v1 0 0 0 2 0

fobber\_v2 0 0 0 4 0

gozi\_gpl 0 0 2 1 0

gozi\_luther 648 34 235 0 0

gozi\_nasa 62 436 316 0 0

gozi\_rfc4343 62 96 673 2 0

kraken\_v1 1 0 0 735 8

kraken\_v2 0 0 0 249 44

locky 1 0 0 21 14

matsnu 3 9 11 0 0

murofet\_v1 0 0 0 0 0

murofet\_v2 0 0 0 0 0

murofet\_v3 0 0 0 0 0

necurs 0 0 0 9 15

nymaim 1 6 6 1 0

padcrypt 0 1 1 0 0

pizd 0 0 0 0 0

proslikefan 0 0 0 14 3

pushdo 3 0 2 0 0

pykspa 0 0 0 13 1

pykspa\_noise 0 0 0 10 3

qadars 1 0 0 7 0

qakbot 1 0 0 33 5

ramdo 0 0 0 8 0

ramnit 3 0 1 8 0

ranbyus\_v1 0 0 0 24 1

ranbyus\_v2 1 1 1 7 0

rovnix 12 11 75 0 0

shiotob 0 0 0 5 0

simda 0 0 0 4 1

sisron 0 0 0 0 0

suppobox\_1 0 0 0 0 0

suppobox\_2 0 0 0 0 0

suppobox\_3 0 0 0 0 0

symmi 0 0 0 0 0

tempedreve 0 0 0 24 11

tinba 0 0 0 22 4

vawtrak\_v1 0 0 0 1 0

vawtrak\_v2 1 0 0 0 0

vawtrak\_v3 0 0 0 0 0

zeus-newgoz 0 0 0 0 0

legit 1 4 6 1 0

locky matsnu murofet\_v1 murofet\_v2 murofet\_v3 necurs \

alureon 0 0 0 0 0 0

banjori 0 0 0 0 0 0

bedep 0 0 0 4 0 13

ccleaner 0 0 0 0 0 0

chinad 2 0 0 20 0 13

corebot 0 0 0 0 0 0

cryptolocker 64 0 0 167 0 63

dircrypt 0 0 2 3 0 19

dyre 0 0 0 0 0 0

fobber\_v1 0 0 0 0 0 2

fobber\_v2 0 0 0 0 0 0

gozi\_gpl 0 0 4 0 0 0

gozi\_luther 0 22 1 0 0 0

gozi\_nasa 0 100 1 0 0 0

gozi\_rfc4343 0 71 0 0 0 0

kraken\_v1 2 0 0 1 0 2

kraken\_v2 50 0 0 3 0 6

locky 156 0 0 136 0 188

matsnu 0 942 0 0 0 0

murofet\_v1 0 0 942 2 0 29

murofet\_v2 0 0 0 978 0 0

murofet\_v3 0 0 44 0 938 0

necurs 153 0 20 52 0 246

nymaim 1 28 0 1 0 0

padcrypt 0 0 0 0 0 1

pizd 0 0 0 0 0 0

proslikefan 27 0 0 71 0 1

pushdo 13 2 0 1 0 0

pykspa 10 0 0 3 0 0

pykspa\_noise 14 0 0 0 0 2

qadars 3 0 0 0 0 1

qakbot 10 0 171 125 0 98

ramdo 0 0 0 0 0 6

ramnit 0 0 0 2 0 20

ranbyus\_v1 175 0 0 13 0 183

ranbyus\_v2 22 0 0 68 0 422

rovnix 0 3 0 0 0 0

shiotob 0 0 0 0 0 1

simda 8 0 0 0 0 1

sisron 0 0 0 0 0 0

suppobox\_1 0 0 0 0 0 0

suppobox\_2 0 0 0 0 0 0

suppobox\_3 0 0 0 0 0 0

symmi 0 0 0 0 0 0

tempedreve 9 0 0 0 0 0

tinba 203 0 0 74 0 35

vawtrak\_v1 4 0 0 0 0 0

vawtrak\_v2 0 0 0 0 0 0

vawtrak\_v3 0 0 0 0 0 0

zeus-newgoz 0 0 9 0 0 0

legit 0 52 0 1 0 0

nymaim padcrypt pizd proslikefan pushdo pykspa \

alureon 0 2 0 0 8 0

banjori 0 0 0 0 0 0

bedep 0 6 0 0 3 0

ccleaner 0 1 0 0 0 0

chinad 0 2 0 0 0 0

corebot 0 0 0 0 0 0

cryptolocker 0 8 2 2 12 1

dircrypt 0 5 0 0 6 0

dyre 0 0 0 0 0 0

fobber\_v1 0 2 0 0 0 0

fobber\_v2 0 1 0 0 7 0

gozi\_gpl 53 0 0 2 1 0

gozi\_luther 4 0 0 0 3 0

gozi\_nasa 3 0 0 0 1 0

gozi\_rfc4343 4 6 0 0 1 0

kraken\_v1 2 0 0 4 2 0

kraken\_v2 3 6 0 118 5 1

locky 4 9 0 172 23 5

matsnu 0 0 0 0 0 0

murofet\_v1 0 0 0 0 0 0

murofet\_v2 0 0 0 0 2 0

murofet\_v3 0 0 0 0 0 0

necurs 1 6 0 178 19 1

nymaim 774 0 23 2 8 0

padcrypt 1 945 2 0 0 0

pizd 0 0 557 0 0 0

proslikefan 1 1 0 442 6 16

pushdo 8 1 0 21 626 0

pykspa 0 2 2 94 6 34

pykspa\_noise 0 0 0 92 4 30

qadars 0 0 3 0 1 0

qakbot 2 7 0 23 3 4

ramdo 0 0 0 0 0 0

ramnit 0 7 0 0 6 0

ranbyus\_v1 6 5 1 2 21 0

ranbyus\_v2 4 12 0 0 1 0

rovnix 17 0 6 0 0 0

shiotob 0 3 0 1 2 0

simda 12 0 0 113 30 6

sisron 0 0 0 0 0 0

suppobox\_1 0 0 347 0 0 0

suppobox\_2 0 0 59 0 0 0

suppobox\_3 0 0 15 0 0 0

symmi 0 0 0 0 0 0

tempedreve 0 1 1 90 2 6

tinba 1 9 2 6 24 0

vawtrak\_v1 0 0 0 1 0 0

vawtrak\_v2 0 0 0 0 0 0

vawtrak\_v3 0 0 0 0 2 0

zeus-newgoz 0 1 0 0 0 0

legit 26 0 1 33 5 1

pykspa\_noise qadars qakbot ramdo ramnit ranbyus\_v1 \

alureon 0 0 0 0 0 0

banjori 0 0 0 0 0 0

bedep 0 0 0 0 45 0

ccleaner 0 0 0 0 0 0

chinad 0 190 0 5 0 4

corebot 0 0 0 0 0 0

cryptolocker 8 0 0 40 11 165

dircrypt 0 0 1 2 61 1

dyre 0 0 0 0 0 0

fobber\_v1 0 0 0 4 0 0

fobber\_v2 0 0 0 0 0 0

gozi\_gpl 0 0 0 3 0 1

gozi\_luther 0 0 0 0 3 0

gozi\_nasa 0 0 1 0 2 0

gozi\_rfc4343 0 0 0 0 7 0

kraken\_v1 0 0 0 4 4 2

kraken\_v2 0 0 0 6 2 5

locky 1 0 1 17 1 91

matsnu 0 0 0 0 0 0

murofet\_v1 0 0 0 2 0 0

murofet\_v2 0 0 0 0 0 0

murofet\_v3 0 0 0 0 0 0

necurs 0 0 0 17 1 73

nymaim 1 0 0 1 0 0

padcrypt 0 0 0 9 0 0

pizd 0 0 0 0 0 0

proslikefan 3 2 0 4 0 3

pushdo 2 0 0 1 7 3

pykspa 15 1 0 26 0 18

pykspa\_noise 19 1 0 29 0 11

qadars 0 822 0 22 0 2

qakbot 4 1 3 32 13 19

ramdo 0 0 0 969 0 0

ramnit 0 0 0 1 52 0

ranbyus\_v1 1 3 0 28 11 276

ranbyus\_v2 0 0 0 24 16 39

rovnix 0 0 0 0 0 0

shiotob 1 415 0 0 1 1

simda 2 0 0 0 0 1

sisron 0 0 0 0 0 0

suppobox\_1 0 0 0 0 0 0

suppobox\_2 0 0 0 0 0 0

suppobox\_3 0 0 0 0 0 0

symmi 0 0 0 0 0 0

tempedreve 21 5 0 0 0 1

tinba 6 4 0 3 1 57

vawtrak\_v1 0 0 0 0 0 0

vawtrak\_v2 0 0 0 0 0 0

vawtrak\_v3 0 0 0 0 0 0

zeus-newgoz 0 2 0 0 0 0

legit 0 6 0 0 0 0

ranbyus\_v2 rovnix shiotob simda sisron suppobox\_1 \

alureon 0 0 0 1 0 0

banjori 0 0 0 0 0 0

bedep 3 0 27 0 2 0

ccleaner 0 0 0 0 0 0

chinad 6 0 23 0 0 0

corebot 0 0 0 0 0 0

cryptolocker 11 0 0 7 2 0

dircrypt 6 0 1 0 0 0

dyre 0 0 0 0 0 0

fobber\_v1 0 0 0 0 1 0

fobber\_v2 0 0 4 0 1 0

gozi\_gpl 0 34 0 0 0 0

gozi\_luther 0 0 0 0 0 0

gozi\_nasa 0 10 0 1 0 0

gozi\_rfc4343 0 9 0 0 0 0

kraken\_v1 0 0 0 0 2 0

kraken\_v2 0 0 0 1 1 0

locky 11 0 0 31 3 0

matsnu 0 0 0 0 0 0

murofet\_v1 2 1 0 0 0 0

murofet\_v2 0 0 0 1 0 0

murofet\_v3 0 0 0 0 0 0

necurs 19 1 0 8 0 1

nymaim 0 11 0 2 0 18

padcrypt 3 0 0 0 0 0

pizd 0 0 0 0 0 208

proslikefan 0 0 0 79 1 0

pushdo 0 0 0 19 0 0

pykspa 0 0 1 169 2 0

pykspa\_noise 0 0 0 162 3 0

qadars 0 0 34 0 0 0

qakbot 10 0 2 15 1 0

ramdo 0 0 0 0 0 0

ramnit 2 0 1 0 0 0

ranbyus\_v1 1 0 0 1 2 1

ranbyus\_v2 83 0 1 0 0 0

rovnix 0 708 0 0 0 7

shiotob 0 0 208 0 0 0

simda 0 0 0 526 0 0

sisron 0 0 0 0 971 0

suppobox\_1 0 0 0 0 0 499

suppobox\_2 0 0 0 0 0 9

suppobox\_3 0 0 0 0 0 9

symmi 0 0 0 0 0 0

tempedreve 0 0 2 102 11 1

tinba 0 0 0 1 1 0

vawtrak\_v1 0 0 0 0 0 0

vawtrak\_v2 0 0 0 0 0 0

vawtrak\_v3 0 0 0 0 0 0

zeus-newgoz 0 0 0 0 0 0

legit 0 1 7 7 0 3

suppobox\_2 suppobox\_3 symmi tempedreve tinba vawtrak\_v1 \

alureon 0 0 0 0 0 0

banjori 0 0 0 0 0 0

bedep 0 0 0 0 0 0

ccleaner 0 0 0 0 0 0

chinad 0 0 0 0 0 0

corebot 0 0 15 0 0 0

cryptolocker 1 0 0 92 1 0

dircrypt 0 0 0 0 0 0

dyre 0 0 0 0 0 0

fobber\_v1 0 5 1 1 0 0

fobber\_v2 0 0 0 0 0 0

gozi\_gpl 0 0 0 1 0 0

gozi\_luther 0 0 0 0 0 0

gozi\_nasa 0 0 0 0 0 0

gozi\_rfc4343 0 0 0 0 0 0

kraken\_v1 0 0 0 20 0 0

kraken\_v2 0 0 0 32 1 2

locky 0 0 0 72 0 3

matsnu 0 0 0 0 0 0

murofet\_v1 0 0 0 0 0 0

murofet\_v2 0 0 0 0 0 0

murofet\_v3 0 0 0 0 0 0

necurs 1 0 0 47 0 11

nymaim 11 8 0 0 0 5

padcrypt 0 3 2 0 0 0

pizd 210 8 0 0 0 0

proslikefan 27 0 0 142 0 7

pushdo 0 0 0 7 0 0

pykspa 62 0 0 328 0 1

pykspa\_noise 78 0 0 328 0 0

qadars 1 1 0 17 0 22

qakbot 4 0 1 116 0 0

ramdo 0 0 0 0 0 0

ramnit 0 0 0 0 0 0

ranbyus\_v1 2 0 0 33 1 1

ranbyus\_v2 0 1 0 3 0 0

rovnix 0 77 0 0 0 0

shiotob 7 1 0 30 0 0

simda 1 0 0 16 0 0

sisron 0 0 0 1 0 0

suppobox\_1 135 2 0 0 0 0

suppobox\_2 914 0 0 0 0 0

suppobox\_3 0 959 0 0 0 0

symmi 0 1 980 0 0 0

tempedreve 26 0 3 386 0 2

tinba 2 0 0 103 0 1

vawtrak\_v1 0 0 0 2 0 975

vawtrak\_v2 0 0 0 0 0 0

vawtrak\_v3 0 0 0 0 0 0

zeus-newgoz 0 0 0 0 0 0

legit 60 1 0 1 0 1

vawtrak\_v2 vawtrak\_v3 zeus-newgoz legit

alureon 50 13 0 0

banjori 0 0 0 0

bedep 5 0 0 0

ccleaner 0 0 0 0

chinad 1 0 2 0

corebot 0 0 0 0

cryptolocker 5 0 0 0

dircrypt 28 8 0 0

dyre 0 0 0 0

fobber\_v1 0 0 0 0

fobber\_v2 58 13 0 0

gozi\_gpl 0 0 0 0

gozi\_luther 23 7 0 0

gozi\_nasa 36 6 0 0

gozi\_rfc4343 31 7 0 2

kraken\_v1 15 8 0 0

kraken\_v2 28 9 0 10

locky 0 0 0 6

matsnu 9 9 0 0

murofet\_v1 0 0 0 0

murofet\_v2 0 0 0 0

murofet\_v3 0 0 1 0

necurs 1 0 0 14

nymaim 10 2 0 34

padcrypt 3 0 0 0

pizd 0 0 0 0

proslikefan 19 7 0 27

pushdo 116 27 0 9

pykspa 31 5 0 8

pykspa\_noise 33 6 0 3

qadars 1 0 0 0

qakbot 0 2 0 1

ramdo 0 0 0 0

ramnit 50 10 0 0

ranbyus\_v1 0 0 0 0

ranbyus\_v2 0 0 0 0

rovnix 0 0 1 0

shiotob 5 1 0 1

simda 47 11 0 84

sisron 0 0 0 0

suppobox\_1 0 0 0 0

suppobox\_2 0 0 0 1

suppobox\_3 0 0 0 0

symmi 0 0 0 0

tempedreve 14 5 0 9

tinba 14 2 0 1

vawtrak\_v1 0 0 0 0

vawtrak\_v2 756 177 0 0

vawtrak\_v3 543 414 0 0

zeus-newgoz 0 0 955 0

legit 407 158 0 171

True positive: 29869

Test Phase Duration: 0:04:37 (HH:MM:SS)

Class report:

precision recall f1-score support

alureon 0.2225 0.3042 0.2570 983

banjori 1.0000 1.0000 1.0000 983

bedep 0.3289 0.6724 0.4417 983

ccleaner 0.9889 0.9990 0.9939 983

chinad 0.8385 0.6918 0.7581 983

corebot 0.9938 0.9736 0.9836 983

cryptolocker 0.3662 0.0529 0.0924 983

dircrypt 0.1386 0.0610 0.0847 983

dyre 1.0000 1.0000 1.0000 983

fobber\_v1 0.5222 0.9817 0.6817 983

fobber\_v2 0.2097 0.6155 0.3128 983

gozi\_gpl 0.8862 0.8952 0.8907 983

gozi\_luther 0.8010 0.6592 0.7232 983

gozi\_nasa 0.7291 0.4435 0.5515 983

gozi\_rfc4343 0.5060 0.6846 0.5819 983

kraken\_v1 0.5852 0.7477 0.6565 983

kraken\_v2 0.3860 0.0448 0.0802 983

locky 0.1685 0.1587 0.1634 983

matsnu 0.7721 0.9583 0.8552 983

murofet\_v1 0.7889 0.9583 0.8654 983

murofet\_v2 0.5670 0.9949 0.7223 983

murofet\_v3 1.0000 0.9542 0.9766 983

necurs 0.1820 0.2503 0.2107 983

nymaim 0.8359 0.7874 0.8109 983

padcrypt 0.9017 0.9613 0.9306 983

pizd 0.5455 0.5666 0.5559 983

proslikefan 0.3166 0.4496 0.3716 983

pushdo 0.7452 0.6368 0.6868 983

pykspa 0.3238 0.0346 0.0625 983

pykspa\_noise 0.2262 0.0193 0.0356 983

qadars 0.5661 0.8362 0.6752 983

qakbot 0.5000 0.0031 0.0061 983

ramdo 0.7758 0.9858 0.8683 983

ramnit 0.2185 0.0529 0.0852 983

ranbyus\_v1 0.3571 0.2808 0.3144 983

ranbyus\_v2 0.5287 0.0844 0.1456 983

rovnix 0.9135 0.7202 0.8055 983

shiotob 0.6688 0.2116 0.3215 983

simda 0.4643 0.5351 0.4972 983

sisron 0.9671 0.9878 0.9774 983

suppobox\_1 0.6601 0.5076 0.5739 983

suppobox\_2 0.5927 0.9298 0.7240 983

suppobox\_3 0.8988 0.9756 0.9356 983

symmi 0.9780 0.9969 0.9874 983

tempedreve 0.2171 0.3927 0.2796 983

tinba 0.0000 0.0000 0.0000 983

vawtrak\_v1 0.9457 0.9919 0.9682 983

vawtrak\_v2 0.3232 0.7691 0.4551 983

vawtrak\_v3 0.4564 0.4212 0.4381 983

zeus-newgoz 0.9958 0.9715 0.9835 983

legit 0.4488 0.1740 0.2507 983

accuracy 0.5958 50133

macro avg 0.5951 0.5958 0.5614 50133

weighted avg 0.5951 0.5958 0.5614 50133

F1 Score, Precision and Recall:

Macro Micro

F1 Score 0.561371 0.595795

Precision 0.595149 0.595795

Recall 0.595795 0.595795

Overall accuracy = 0.5957951848084097

Confusion matrix:

alureon banjori bedep ccleaner chinad corebot \

alureon 299 0 2 0 0 0

banjori 0 983 0 0 0 0

bedep 67 0 661 0 3 0

ccleaner 0 0 0 982 0 0

chinad 0 0 6 1 680 1

corebot 0 0 0 0 0 957

cryptolocker 26 0 73 0 1 0

dircrypt 110 0 424 0 0 0

dyre 0 0 0 0 0 0

fobber\_v1 0 0 0 0 0 0

fobber\_v2 275 0 1 0 0 0

gozi\_gpl 0 0 0 0 0 0

gozi\_luther 1 0 2 0 0 0

gozi\_nasa 1 0 6 0 0 0

gozi\_rfc4343 0 0 7 0 0 0

kraken\_v1 18 0 30 0 0 0

kraken\_v2 72 0 62 0 0 0

locky 1 0 0 0 0 0

matsnu 0 0 0 0 0 0

murofet\_v1 0 0 0 0 0 0

murofet\_v2 0 0 0 0 0 0

murofet\_v3 0 0 0 0 0 0

necurs 4 0 14 0 0 0

nymaim 0 0 0 0 0 0

padcrypt 0 0 8 0 0 0

pizd 0 0 0 0 0 0

proslikefan 18 0 0 0 0 0

pushdo 24 0 21 0 0 0

pykspa 20 0 1 0 0 0

pykspa\_noise 22 0 1 0 0 0

qadars 4 0 2 4 9 0

qakbot 13 0 59 0 0 0

ramdo 0 0 0 0 0 0

ramnit 121 0 363 0 0 0

ranbyus\_v1 3 0 75 0 0 0

ranbyus\_v2 0 0 104 0 1 0

rovnix 0 0 0 0 0 0

shiotob 23 0 40 2 115 0

simda 15 0 0 0 0 0

sisron 10 0 0 0 0 0

suppobox\_1 0 0 0 0 0 0

suppobox\_2 0 0 0 0 0 0

suppobox\_3 0 0 0 0 0 0

symmi 0 0 0 0 0 0

tempedreve 81 0 0 0 0 0

tinba 98 0 47 0 0 0

vawtrak\_v1 0 0 0 0 0 0

vawtrak\_v2 4 0 0 0 0 0

vawtrak\_v3 7 0 0 0 0 0

zeus-newgoz 0 0 0 0 2 5

legit 7 0 1 4 0 0

cryptolocker dircrypt dyre fobber\_v1 fobber\_v2 gozi\_gpl \

alureon 0 16 0 0 588 0

banjori 0 0 0 0 0 0

bedep 0 74 0 5 50 0

ccleaner 0 0 0 0 0 0

chinad 0 0 0 27 0 0

corebot 0 0 0 10 0 0

cryptolocker 52 21 0 108 12 1

dircrypt 0 60 0 10 219 0

dyre 0 0 983 0 0 0

fobber\_v1 0 0 0 965 0 0

fobber\_v2 0 14 0 0 605 0

gozi\_gpl 1 0 0 0 0 880

gozi\_luther 0 0 0 0 0 0

gozi\_nasa 0 0 0 0 1 0

gozi\_rfc4343 0 0 0 0 3 2

kraken\_v1 0 11 0 0 112 0

kraken\_v2 1 27 0 0 239 0

locky 7 1 0 6 0 2

matsnu 0 0 0 0 0 0

murofet\_v1 0 0 0 2 0 3

murofet\_v2 1 0 0 0 0 1

murofet\_v3 0 0 0 0 0 0

necurs 14 1 0 37 17 2

nymaim 1 0 0 0 0 28

padcrypt 0 0 0 4 0 0

pizd 0 0 0 0 0 0

proslikefan 1 0 0 1 60 0

pushdo 1 9 0 0 59 1

pykspa 8 8 0 56 58 0

pykspa\_noise 2 11 0 58 61 0

qadars 1 4 0 10 11 0

qakbot 7 3 0 166 28 1

ramdo 0 0 0 0 0 0

ramnit 1 69 0 1 265 0

ranbyus\_v1 30 10 0 68 3 2

ranbyus\_v2 10 1 0 157 0 4

rovnix 0 0 0 0 0 66

shiotob 0 7 0 68 45 0

simda 0 0 0 0 105 0

sisron 0 0 0 0 1 0

suppobox\_1 0 0 0 0 0 0

suppobox\_2 0 0 0 0 0 0

suppobox\_3 0 0 0 0 0 0

symmi 0 0 0 2 0 0

tempedreve 0 0 0 24 146 0

tinba 4 82 0 53 123 0

vawtrak\_v1 0 0 0 0 0 0

vawtrak\_v2 0 2 0 0 43 0

vawtrak\_v3 0 0 0 0 17 0

zeus-newgoz 0 0 0 9 0 0

legit 0 2 0 1 14 0

gozi\_luther gozi\_nasa gozi\_rfc4343 kraken\_v1 kraken\_v2 \

alureon 0 0 0 4 0

banjori 0 0 0 0 0

bedep 3 0 1 10 1

ccleaner 0 0 0 0 0

chinad 0 0 0 0 0

corebot 0 0 0 1 0

cryptolocker 0 0 0 24 3

dircrypt 5 0 0 12 0

dyre 0 0 0 0 0

fobber\_v1 0 0 0 2 0

fobber\_v2 0 0 0 4 0

gozi\_gpl 0 0 2 1 0

gozi\_luther 648 34 235 0 0

gozi\_nasa 62 436 316 0 0

gozi\_rfc4343 62 96 673 2 0

kraken\_v1 1 0 0 735 8

kraken\_v2 0 0 0 249 44

locky 1 0 0 21 14

matsnu 3 9 11 0 0

murofet\_v1 0 0 0 0 0

murofet\_v2 0 0 0 0 0

murofet\_v3 0 0 0 0 0

necurs 0 0 0 9 15

nymaim 1 6 6 1 0

padcrypt 0 1 1 0 0

pizd 0 0 0 0 0

proslikefan 0 0 0 14 3

pushdo 3 0 2 0 0

pykspa 0 0 0 13 1

pykspa\_noise 0 0 0 10 3

qadars 1 0 0 7 0

qakbot 1 0 0 33 5

ramdo 0 0 0 8 0

ramnit 3 0 1 8 0

ranbyus\_v1 0 0 0 24 1

ranbyus\_v2 1 1 1 7 0

rovnix 12 11 75 0 0

shiotob 0 0 0 5 0

simda 0 0 0 4 1

sisron 0 0 0 0 0

suppobox\_1 0 0 0 0 0

suppobox\_2 0 0 0 0 0

suppobox\_3 0 0 0 0 0

symmi 0 0 0 0 0

tempedreve 0 0 0 24 11

tinba 0 0 0 22 4

vawtrak\_v1 0 0 0 1 0

vawtrak\_v2 1 0 0 0 0

vawtrak\_v3 0 0 0 0 0

zeus-newgoz 0 0 0 0 0

legit 1 4 6 1 0

locky matsnu murofet\_v1 murofet\_v2 murofet\_v3 necurs \

alureon 0 0 0 0 0 0

banjori 0 0 0 0 0 0

bedep 0 0 0 4 0 13

ccleaner 0 0 0 0 0 0

chinad 2 0 0 20 0 13

corebot 0 0 0 0 0 0

cryptolocker 64 0 0 167 0 63

dircrypt 0 0 2 3 0 19

dyre 0 0 0 0 0 0

fobber\_v1 0 0 0 0 0 2

fobber\_v2 0 0 0 0 0 0

gozi\_gpl 0 0 4 0 0 0

gozi\_luther 0 22 1 0 0 0

gozi\_nasa 0 100 1 0 0 0

gozi\_rfc4343 0 71 0 0 0 0

kraken\_v1 2 0 0 1 0 2

kraken\_v2 50 0 0 3 0 6

locky 156 0 0 136 0 188

matsnu 0 942 0 0 0 0

murofet\_v1 0 0 942 2 0 29

murofet\_v2 0 0 0 978 0 0

murofet\_v3 0 0 44 0 938 0

necurs 153 0 20 52 0 246

nymaim 1 28 0 1 0 0

padcrypt 0 0 0 0 0 1

pizd 0 0 0 0 0 0

proslikefan 27 0 0 71 0 1

pushdo 13 2 0 1 0 0

pykspa 10 0 0 3 0 0

pykspa\_noise 14 0 0 0 0 2

qadars 3 0 0 0 0 1

qakbot 10 0 171 125 0 98

ramdo 0 0 0 0 0 6

ramnit 0 0 0 2 0 20

ranbyus\_v1 175 0 0 13 0 183

ranbyus\_v2 22 0 0 68 0 422

rovnix 0 3 0 0 0 0

shiotob 0 0 0 0 0 1

simda 8 0 0 0 0 1

sisron 0 0 0 0 0 0

suppobox\_1 0 0 0 0 0 0

suppobox\_2 0 0 0 0 0 0

suppobox\_3 0 0 0 0 0 0

symmi 0 0 0 0 0 0

tempedreve 9 0 0 0 0 0

tinba 203 0 0 74 0 35

vawtrak\_v1 4 0 0 0 0 0

vawtrak\_v2 0 0 0 0 0 0

vawtrak\_v3 0 0 0 0 0 0

zeus-newgoz 0 0 9 0 0 0

legit 0 52 0 1 0 0

nymaim padcrypt pizd proslikefan pushdo pykspa \

alureon 0 2 0 0 8 0

banjori 0 0 0 0 0 0

bedep 0 6 0 0 3 0

ccleaner 0 1 0 0 0 0

chinad 0 2 0 0 0 0

corebot 0 0 0 0 0 0

cryptolocker 0 8 2 2 12 1

dircrypt 0 5 0 0 6 0

dyre 0 0 0 0 0 0

fobber\_v1 0 2 0 0 0 0

fobber\_v2 0 1 0 0 7 0

gozi\_gpl 53 0 0 2 1 0

gozi\_luther 4 0 0 0 3 0

gozi\_nasa 3 0 0 0 1 0

gozi\_rfc4343 4 6 0 0 1 0

kraken\_v1 2 0 0 4 2 0

kraken\_v2 3 6 0 118 5 1

locky 4 9 0 172 23 5

matsnu 0 0 0 0 0 0

murofet\_v1 0 0 0 0 0 0

murofet\_v2 0 0 0 0 2 0

murofet\_v3 0 0 0 0 0 0

necurs 1 6 0 178 19 1

nymaim 774 0 23 2 8 0

padcrypt 1 945 2 0 0 0

pizd 0 0 557 0 0 0

proslikefan 1 1 0 442 6 16

pushdo 8 1 0 21 626 0

pykspa 0 2 2 94 6 34

pykspa\_noise 0 0 0 92 4 30

qadars 0 0 3 0 1 0

qakbot 2 7 0 23 3 4

ramdo 0 0 0 0 0 0

ramnit 0 7 0 0 6 0

ranbyus\_v1 6 5 1 2 21 0

ranbyus\_v2 4 12 0 0 1 0

rovnix 17 0 6 0 0 0

shiotob 0 3 0 1 2 0

simda 12 0 0 113 30 6

sisron 0 0 0 0 0 0

suppobox\_1 0 0 347 0 0 0

suppobox\_2 0 0 59 0 0 0

suppobox\_3 0 0 15 0 0 0

symmi 0 0 0 0 0 0

tempedreve 0 1 1 90 2 6

tinba 1 9 2 6 24 0

vawtrak\_v1 0 0 0 1 0 0

vawtrak\_v2 0 0 0 0 0 0

vawtrak\_v3 0 0 0 0 2 0

zeus-newgoz 0 1 0 0 0 0

legit 26 0 1 33 5 1

pykspa\_noise qadars qakbot ramdo ramnit ranbyus\_v1 \

alureon 0 0 0 0 0 0

banjori 0 0 0 0 0 0

bedep 0 0 0 0 45 0

ccleaner 0 0 0 0 0 0

chinad 0 190 0 5 0 4

corebot 0 0 0 0 0 0

cryptolocker 8 0 0 40 11 165

dircrypt 0 0 1 2 61 1

dyre 0 0 0 0 0 0

fobber\_v1 0 0 0 4 0 0

fobber\_v2 0 0 0 0 0 0

gozi\_gpl 0 0 0 3 0 1

gozi\_luther 0 0 0 0 3 0

gozi\_nasa 0 0 1 0 2 0

gozi\_rfc4343 0 0 0 0 7 0

kraken\_v1 0 0 0 4 4 2

kraken\_v2 0 0 0 6 2 5

locky 1 0 1 17 1 91

matsnu 0 0 0 0 0 0

murofet\_v1 0 0 0 2 0 0

murofet\_v2 0 0 0 0 0 0

murofet\_v3 0 0 0 0 0 0

necurs 0 0 0 17 1 73

nymaim 1 0 0 1 0 0

padcrypt 0 0 0 9 0 0

pizd 0 0 0 0 0 0

proslikefan 3 2 0 4 0 3

pushdo 2 0 0 1 7 3

pykspa 15 1 0 26 0 18

pykspa\_noise 19 1 0 29 0 11

qadars 0 822 0 22 0 2

qakbot 4 1 3 32 13 19

ramdo 0 0 0 969 0 0

ramnit 0 0 0 1 52 0

ranbyus\_v1 1 3 0 28 11 276

ranbyus\_v2 0 0 0 24 16 39

rovnix 0 0 0 0 0 0

shiotob 1 415 0 0 1 1

simda 2 0 0 0 0 1

sisron 0 0 0 0 0 0

suppobox\_1 0 0 0 0 0 0

suppobox\_2 0 0 0 0 0 0

suppobox\_3 0 0 0 0 0 0

symmi 0 0 0 0 0 0

tempedreve 21 5 0 0 0 1

tinba 6 4 0 3 1 57

vawtrak\_v1 0 0 0 0 0 0

vawtrak\_v2 0 0 0 0 0 0

vawtrak\_v3 0 0 0 0 0 0

zeus-newgoz 0 2 0 0 0 0

legit 0 6 0 0 0 0

ranbyus\_v2 rovnix shiotob simda sisron suppobox\_1 \

alureon 0 0 0 1 0 0

banjori 0 0 0 0 0 0

bedep 3 0 27 0 2 0

ccleaner 0 0 0 0 0 0

chinad 6 0 23 0 0 0

corebot 0 0 0 0 0 0

cryptolocker 11 0 0 7 2 0

dircrypt 6 0 1 0 0 0

dyre 0 0 0 0 0 0

fobber\_v1 0 0 0 0 1 0

fobber\_v2 0 0 4 0 1 0

gozi\_gpl 0 34 0 0 0 0

gozi\_luther 0 0 0 0 0 0

gozi\_nasa 0 10 0 1 0 0

gozi\_rfc4343 0 9 0 0 0 0

kraken\_v1 0 0 0 0 2 0

kraken\_v2 0 0 0 1 1 0

locky 11 0 0 31 3 0

matsnu 0 0 0 0 0 0

murofet\_v1 2 1 0 0 0 0

murofet\_v2 0 0 0 1 0 0

murofet\_v3 0 0 0 0 0 0

necurs 19 1 0 8 0 1

nymaim 0 11 0 2 0 18

padcrypt 3 0 0 0 0 0

pizd 0 0 0 0 0 208

proslikefan 0 0 0 79 1 0

pushdo 0 0 0 19 0 0

pykspa 0 0 1 169 2 0

pykspa\_noise 0 0 0 162 3 0

qadars 0 0 34 0 0 0

qakbot 10 0 2 15 1 0

ramdo 0 0 0 0 0 0

ramnit 2 0 1 0 0 0

ranbyus\_v1 1 0 0 1 2 1

ranbyus\_v2 83 0 1 0 0 0

rovnix 0 708 0 0 0 7

shiotob 0 0 208 0 0 0

simda 0 0 0 526 0 0

sisron 0 0 0 0 971 0

suppobox\_1 0 0 0 0 0 499

suppobox\_2 0 0 0 0 0 9

suppobox\_3 0 0 0 0 0 9

symmi 0 0 0 0 0 0

tempedreve 0 0 2 102 11 1

tinba 0 0 0 1 1 0

vawtrak\_v1 0 0 0 0 0 0

vawtrak\_v2 0 0 0 0 0 0

vawtrak\_v3 0 0 0 0 0 0

zeus-newgoz 0 0 0 0 0 0

legit 0 1 7 7 0 3

suppobox\_2 suppobox\_3 symmi tempedreve tinba vawtrak\_v1 \

alureon 0 0 0 0 0 0

banjori 0 0 0 0 0 0

bedep 0 0 0 0 0 0

ccleaner 0 0 0 0 0 0

chinad 0 0 0 0 0 0

corebot 0 0 15 0 0 0

cryptolocker 1 0 0 92 1 0

dircrypt 0 0 0 0 0 0

dyre 0 0 0 0 0 0

fobber\_v1 0 5 1 1 0 0

fobber\_v2 0 0 0 0 0 0

gozi\_gpl 0 0 0 1 0 0

gozi\_luther 0 0 0 0 0 0

gozi\_nasa 0 0 0 0 0 0

gozi\_rfc4343 0 0 0 0 0 0

kraken\_v1 0 0 0 20 0 0

kraken\_v2 0 0 0 32 1 2

locky 0 0 0 72 0 3

matsnu 0 0 0 0 0 0

murofet\_v1 0 0 0 0 0 0

murofet\_v2 0 0 0 0 0 0

murofet\_v3 0 0 0 0 0 0

necurs 1 0 0 47 0 11

nymaim 11 8 0 0 0 5

padcrypt 0 3 2 0 0 0

pizd 210 8 0 0 0 0

proslikefan 27 0 0 142 0 7

pushdo 0 0 0 7 0 0

pykspa 62 0 0 328 0 1

pykspa\_noise 78 0 0 328 0 0

qadars 1 1 0 17 0 22

qakbot 4 0 1 116 0 0

ramdo 0 0 0 0 0 0

ramnit 0 0 0 0 0 0

ranbyus\_v1 2 0 0 33 1 1

ranbyus\_v2 0 1 0 3 0 0

rovnix 0 77 0 0 0 0

shiotob 7 1 0 30 0 0

simda 1 0 0 16 0 0

sisron 0 0 0 1 0 0

suppobox\_1 135 2 0 0 0 0

suppobox\_2 914 0 0 0 0 0

suppobox\_3 0 959 0 0 0 0

symmi 0 1 980 0 0 0

tempedreve 26 0 3 386 0 2

tinba 2 0 0 103 0 1

vawtrak\_v1 0 0 0 2 0 975

vawtrak\_v2 0 0 0 0 0 0

vawtrak\_v3 0 0 0 0 0 0

zeus-newgoz 0 0 0 0 0 0

legit 60 1 0 1 0 1

vawtrak\_v2 vawtrak\_v3 zeus-newgoz legit

alureon 50 13 0 0

banjori 0 0 0 0

bedep 5 0 0 0

ccleaner 0 0 0 0

chinad 1 0 2 0

corebot 0 0 0 0

cryptolocker 5 0 0 0

dircrypt 28 8 0 0

dyre 0 0 0 0

fobber\_v1 0 0 0 0

fobber\_v2 58 13 0 0

gozi\_gpl 0 0 0 0

gozi\_luther 23 7 0 0

gozi\_nasa 36 6 0 0

gozi\_rfc4343 31 7 0 2

kraken\_v1 15 8 0 0

kraken\_v2 28 9 0 10

locky 0 0 0 6

matsnu 9 9 0 0

murofet\_v1 0 0 0 0

murofet\_v2 0 0 0 0

murofet\_v3 0 0 1 0

necurs 1 0 0 14

nymaim 10 2 0 34

padcrypt 3 0 0 0

pizd 0 0 0 0

proslikefan 19 7 0 27

pushdo 116 27 0 9

pykspa 31 5 0 8

pykspa\_noise 33 6 0 3

qadars 1 0 0 0

qakbot 0 2 0 1

ramdo 0 0 0 0

ramnit 50 10 0 0

ranbyus\_v1 0 0 0 0

ranbyus\_v2 0 0 0 0

rovnix 0 0 1 0

shiotob 5 1 0 1

simda 47 11 0 84

sisron 0 0 0 0

suppobox\_1 0 0 0 0

suppobox\_2 0 0 0 1

suppobox\_3 0 0 0 0

symmi 0 0 0 0

tempedreve 14 5 0 9

tinba 14 2 0 1

vawtrak\_v1 0 0 0 0

vawtrak\_v2 756 177 0 0

vawtrak\_v3 543 414 0 0

zeus-newgoz 0 0 955 0

legit 407 158 0 171

True positive: 29869