マルウェア対策ラボの現場から
～Stuxnet,Duqu,Flame,Gaussと対峙して思うこと～

マルウェア対策研究人材育成ワークショップ(MWS2012)
(2012年10月31日)

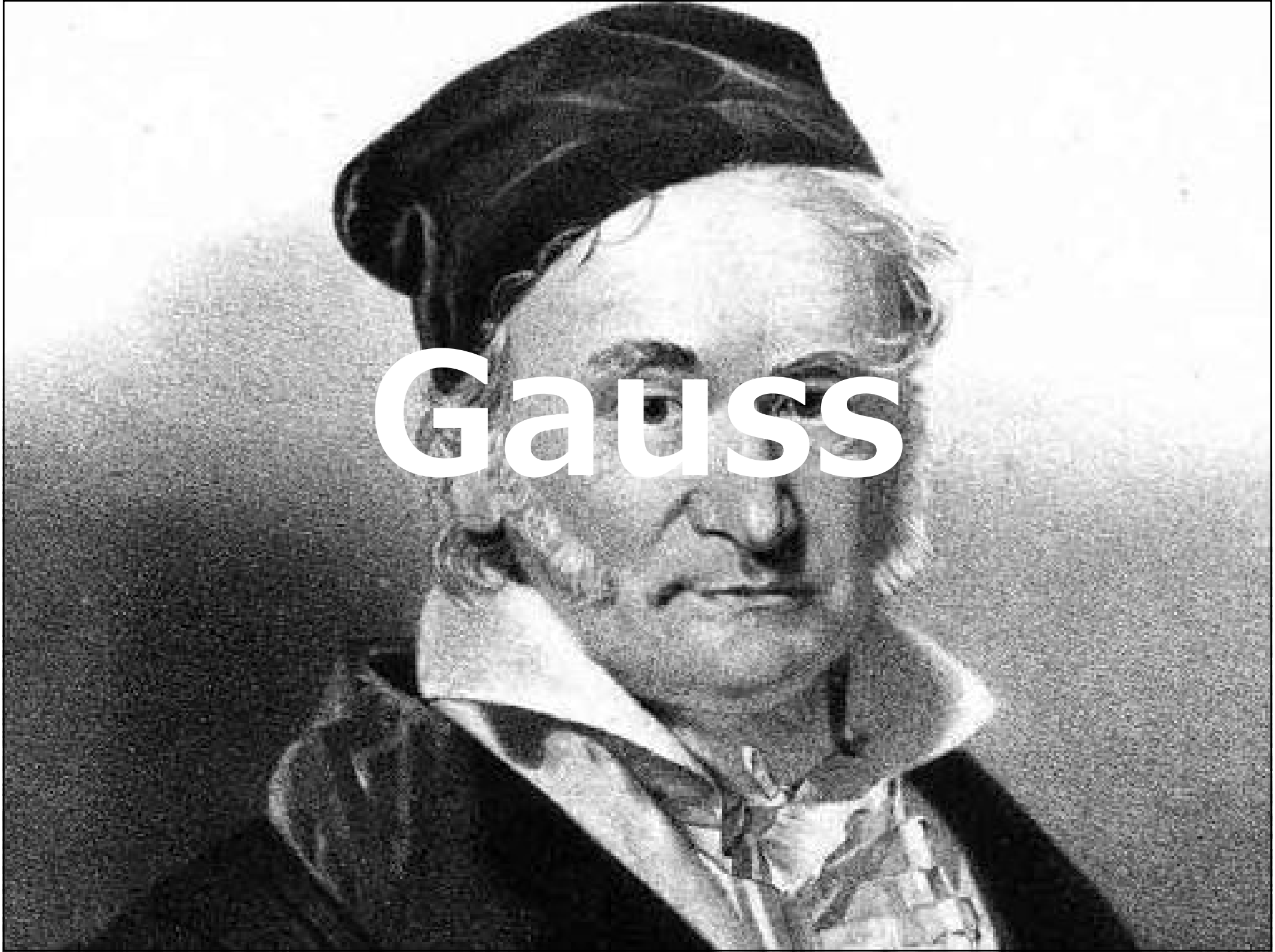
株式会社カスペルスキー
情報セキュリティラボ
チーフセキュリティエヴァンゲリスト

前田　典彦 (まえだ のりひこ)
maeda@kaspersky.co.jp
@z_norihiko

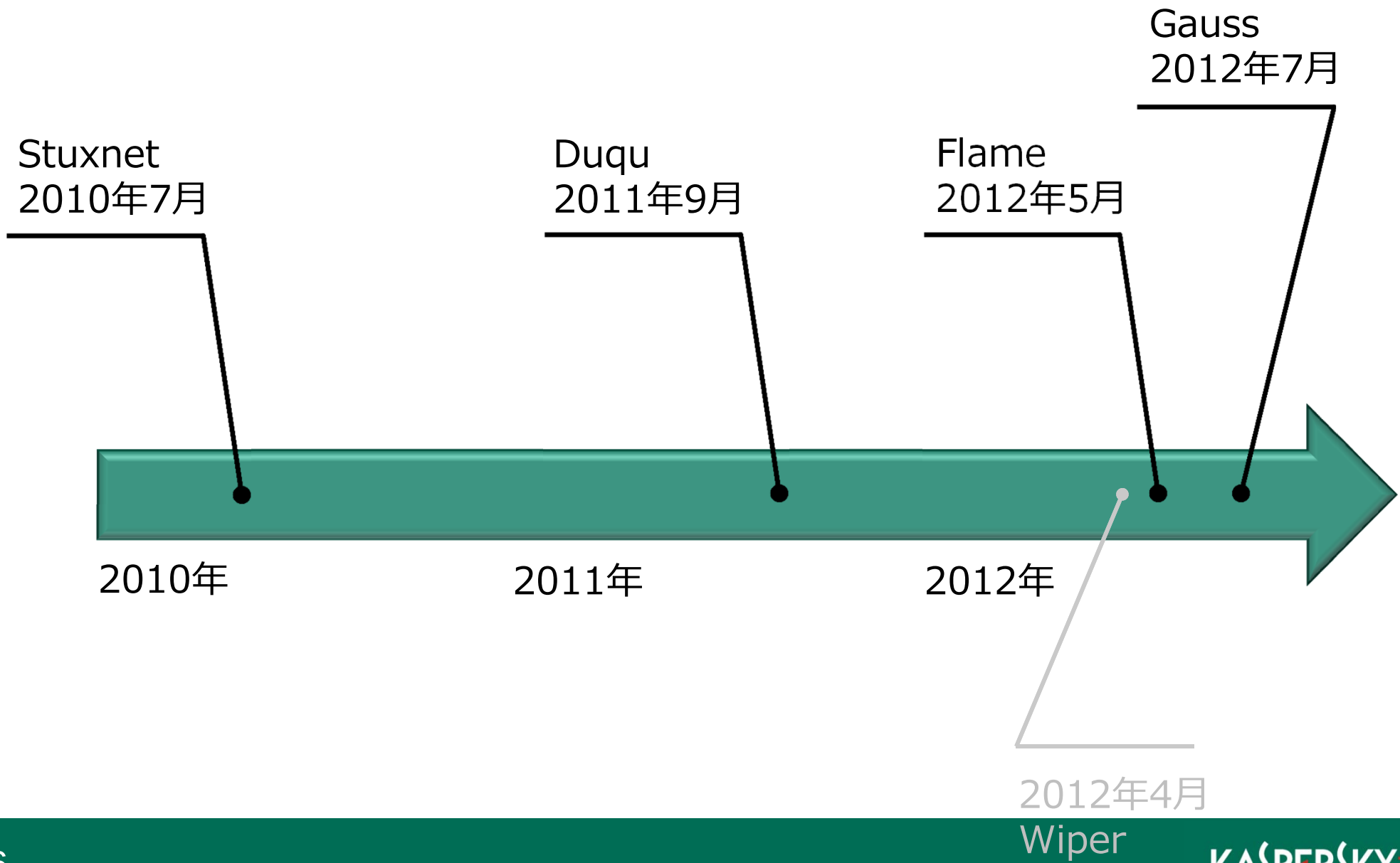
画像出典：The New York Times
※画像はイランの核開発に関するものであり、Stuxnetと直接の関係はありません


Duqu


Flame


Gauss

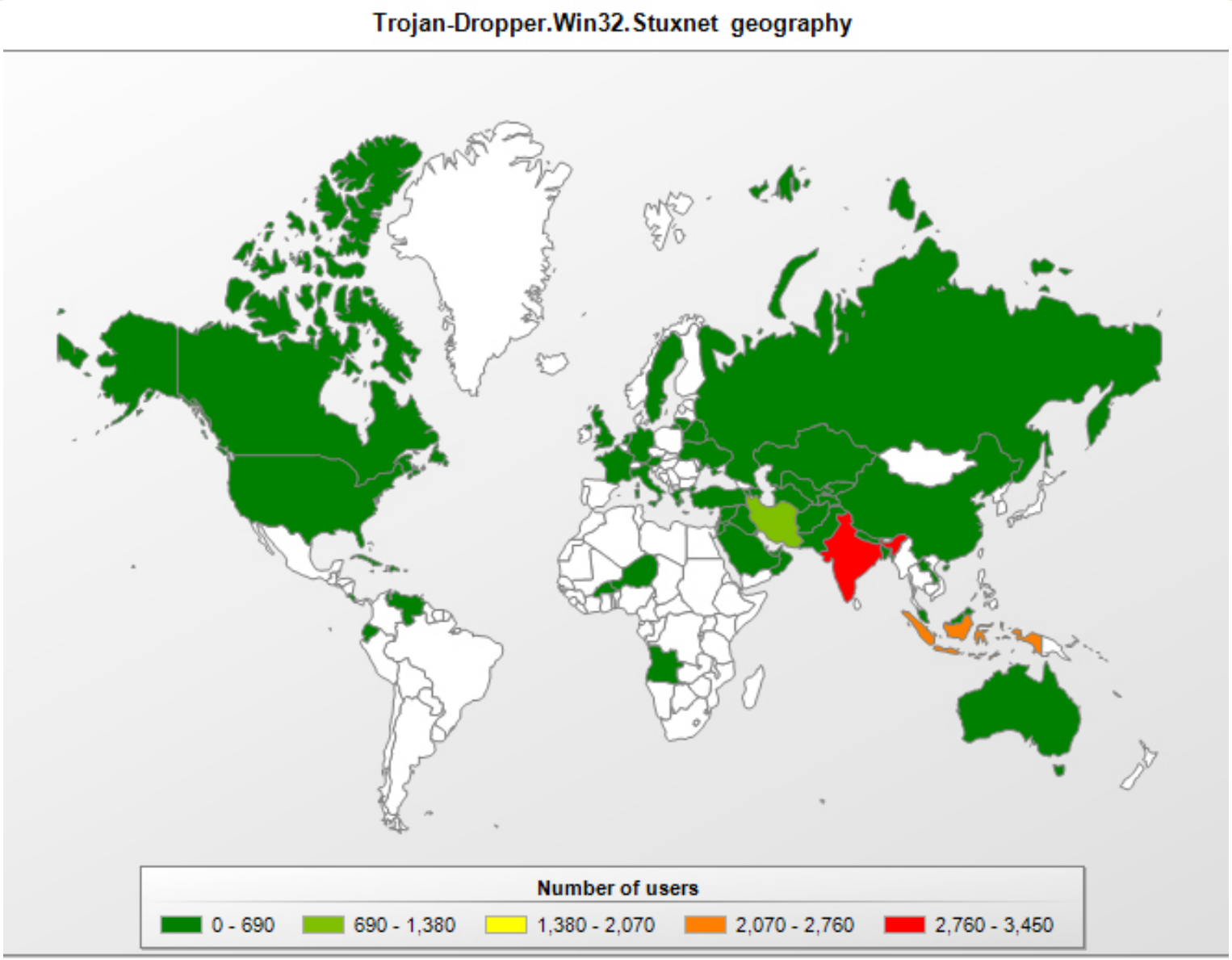
検出timeline



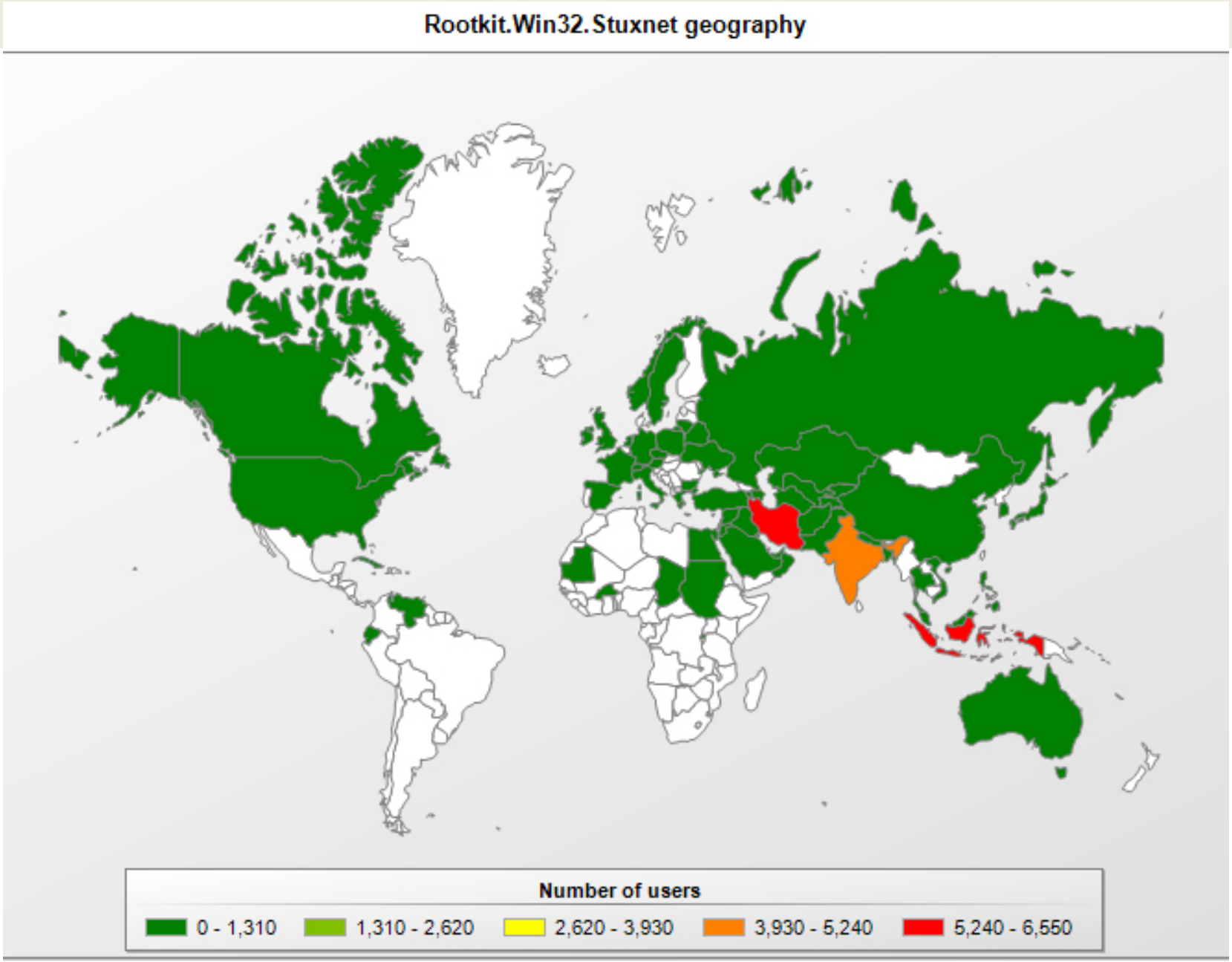
Stuxnet
Duqu
Flame
Gauss
?

KASPERSKY lab

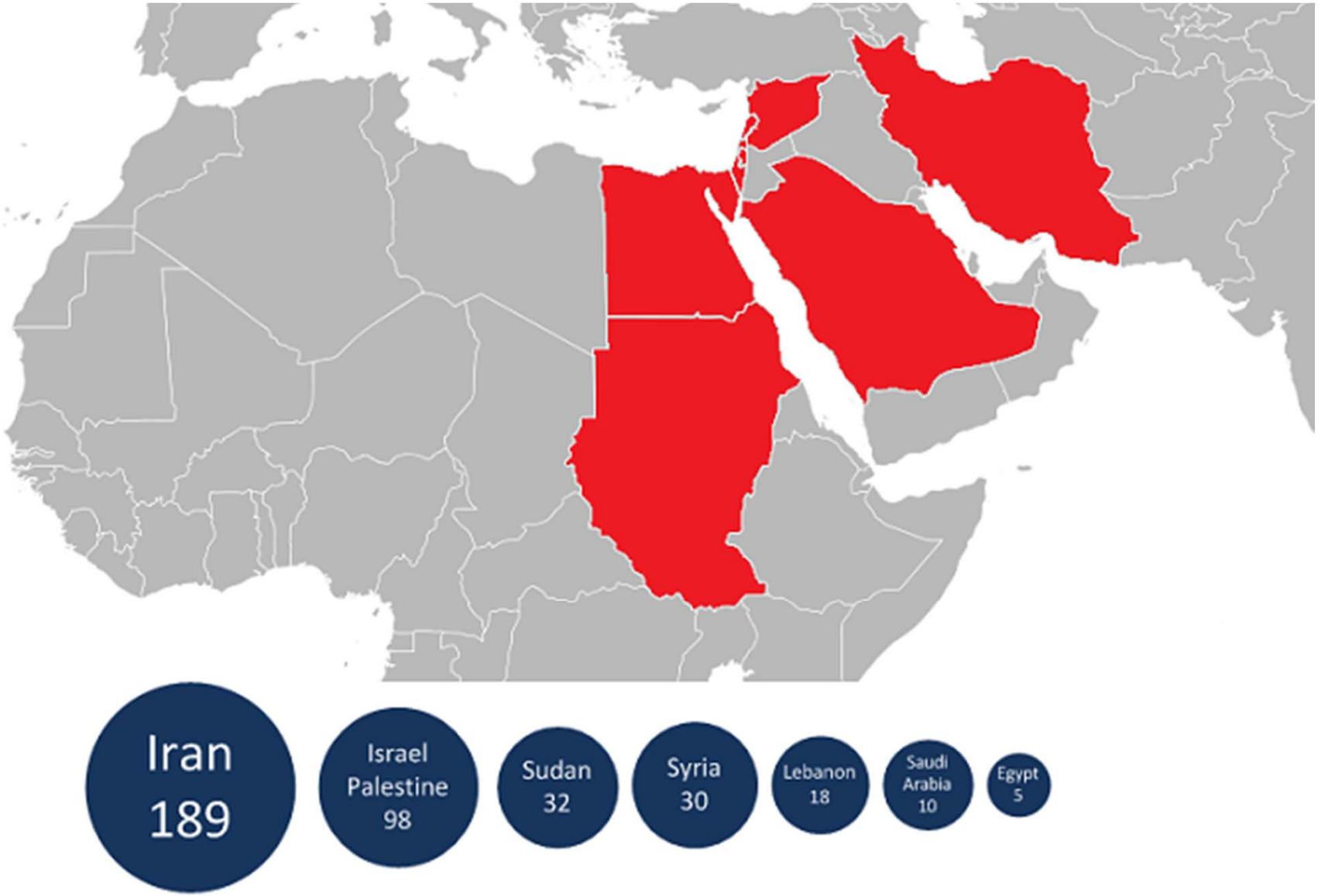
Stuxnet検出状況（当時）



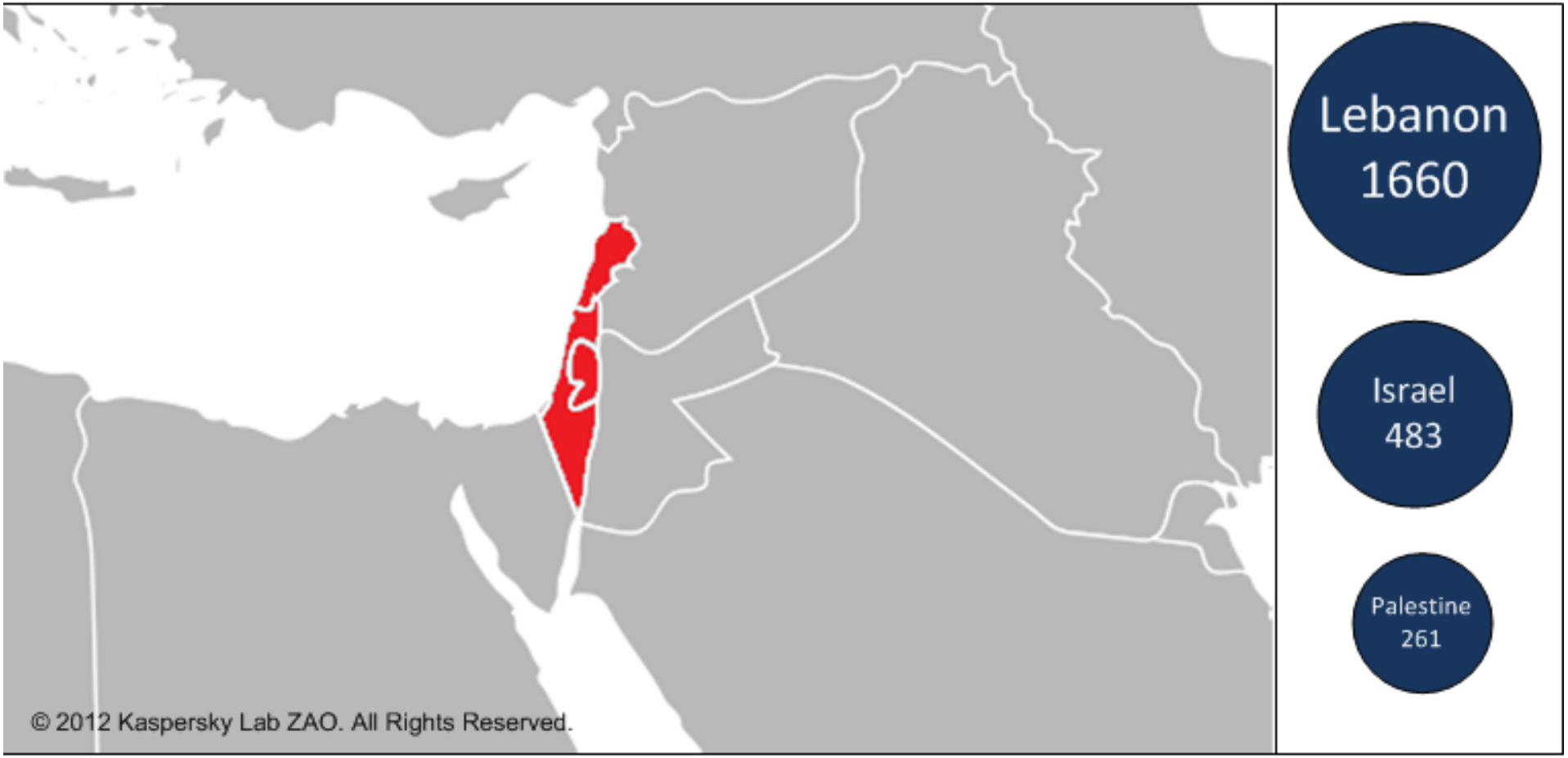
Stuxnet検出状況（当時）



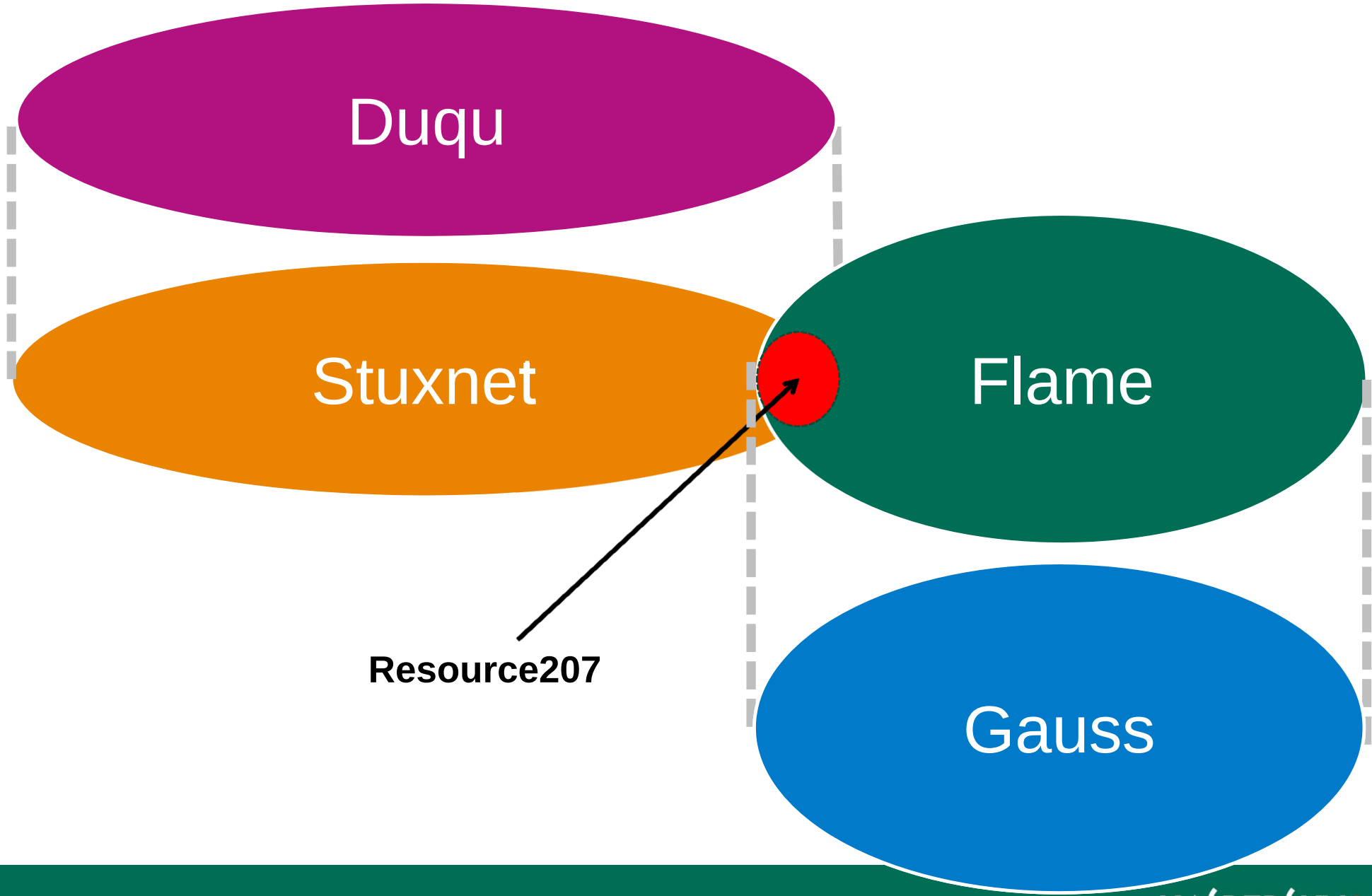
Flame検出状況(当初)



Gauss検出状況(当初)



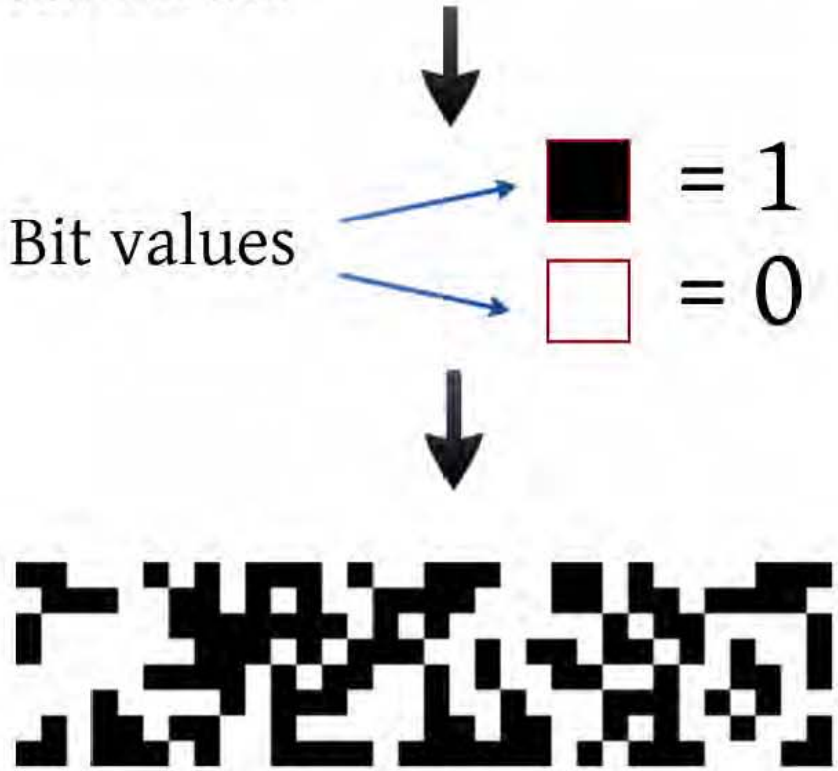
Stuxnet, Duqu, Flame, Gauss

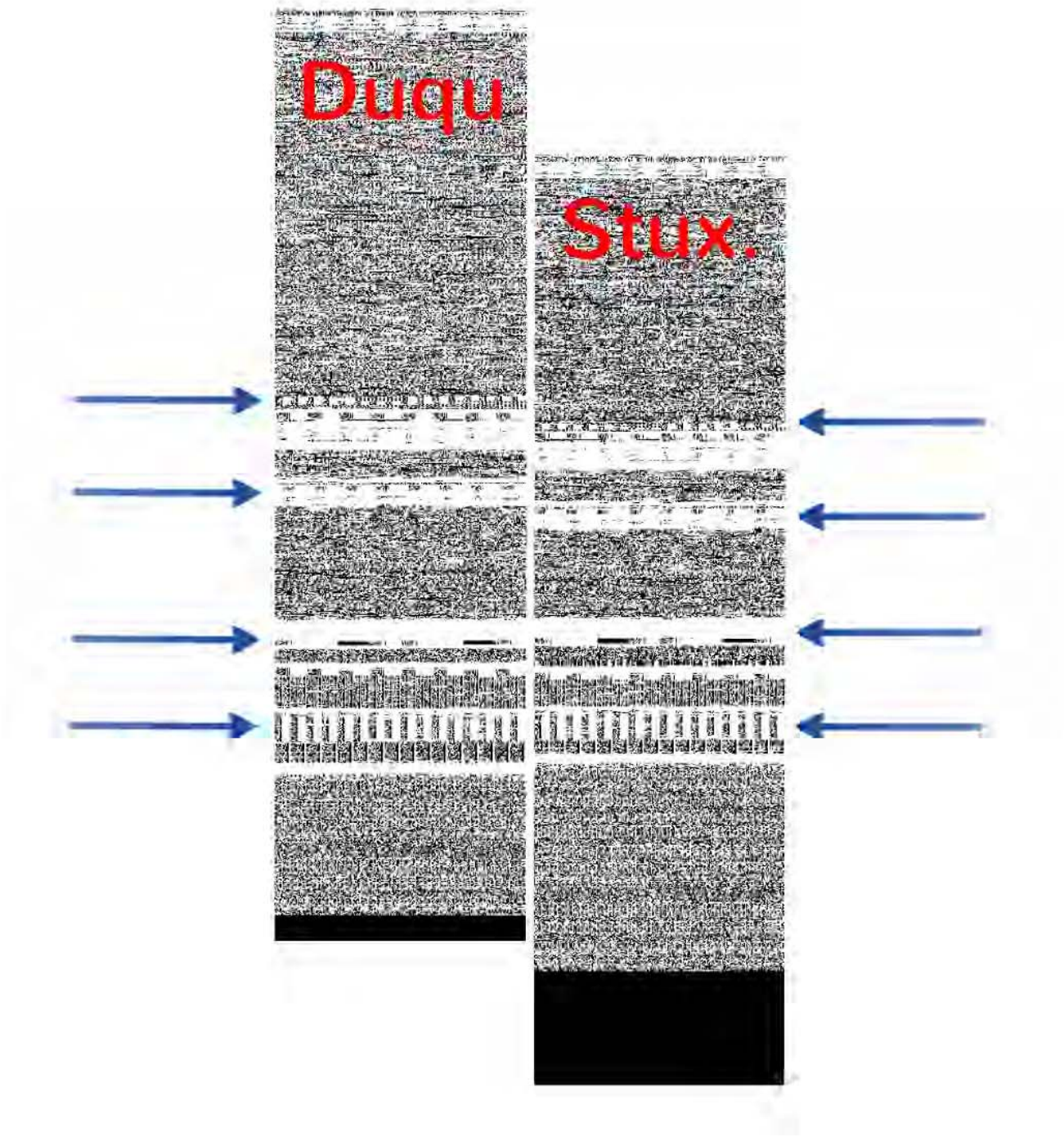


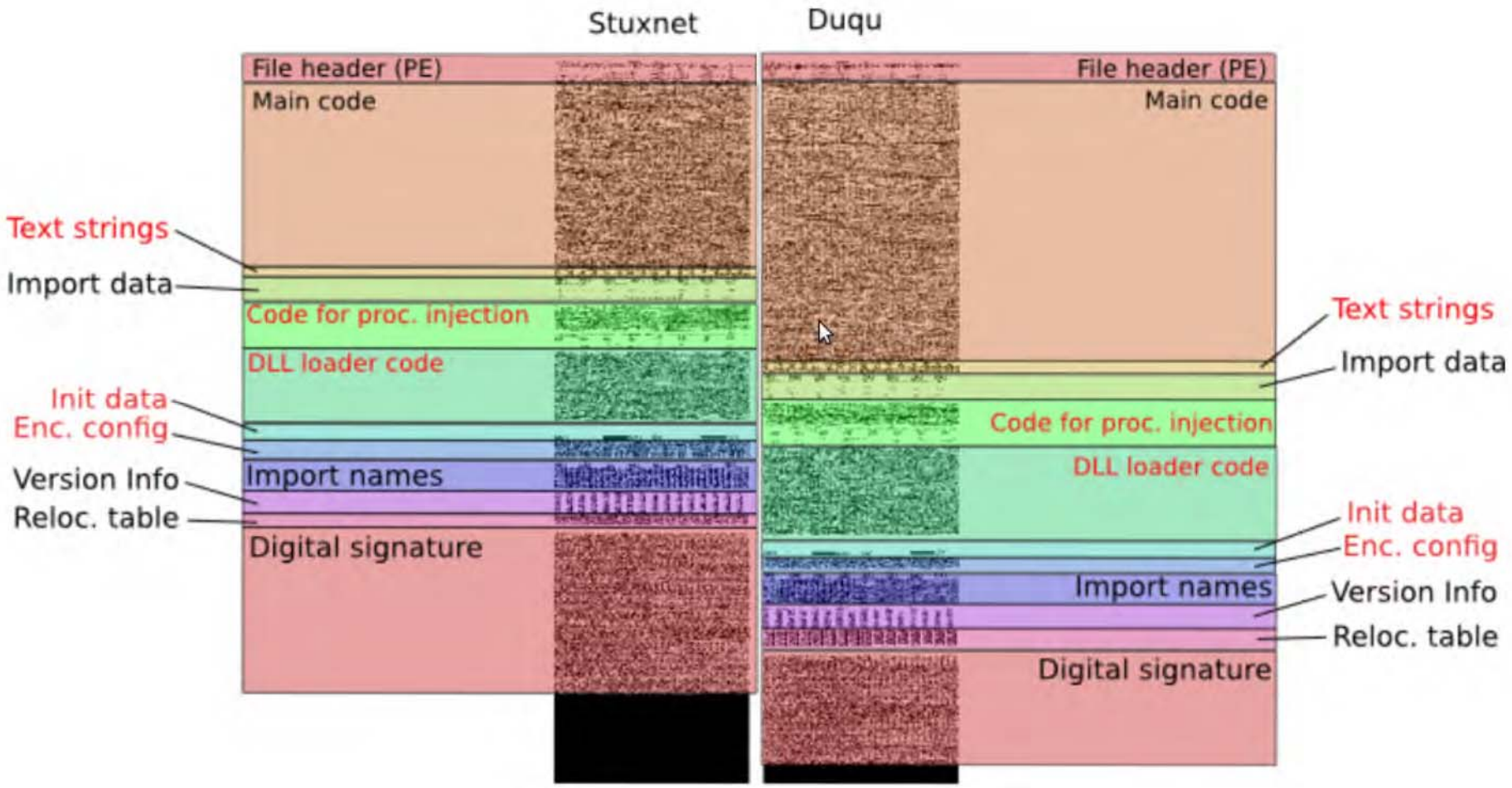
DuquとStuxnet

Game of Binary Similarity

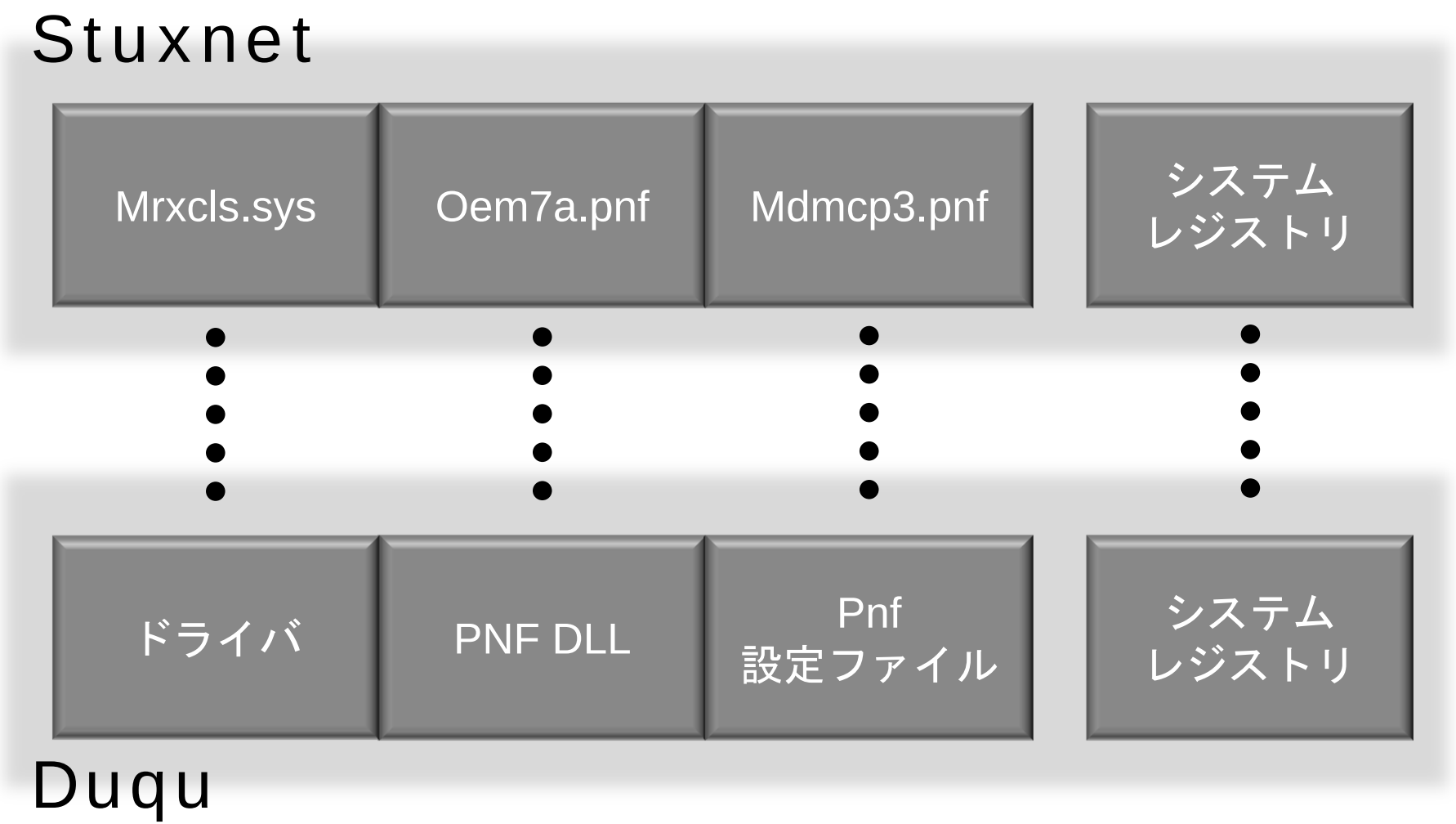
10100011 00101110 01100111 11100001 11001110 11001010
01100011 01111011 11000001 01011111 10000001 10000110
10000001 11101011 10110100 10010101 11100000 00110101
01100101 10110010 00001000 00011101 10001001 00101011
11011010 00000100 10011011 10010010 10111011 10111100
01011111 11000111







DuquとStuxnetの構成相関



最後に

KASPERSKY lab

最後に

- 検体の収集
- 如何に迅速に解析できるか
- 如何に早期検出できるか
- 攻撃の全体像を把握するには

CnCをハッキングとか、したいと思ったりしますよね！？

ありがとうございました

株式会社カスペルスキー

前田　典彦
maeda@kaspersky.co.jp
@z_norihiko

マルウェア対策研究人材育成ワークショップ(MWS2012)
2012年10月31日

KASPERSKY lab