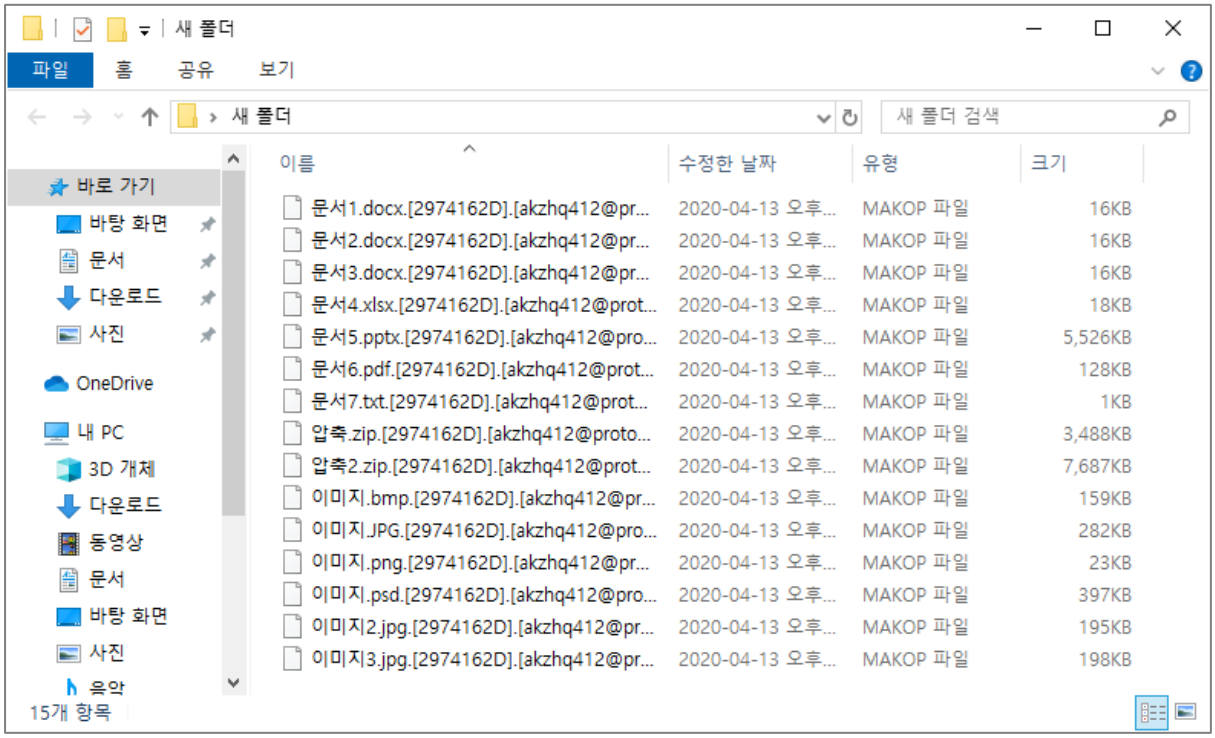
Today's Ransomware –Makop

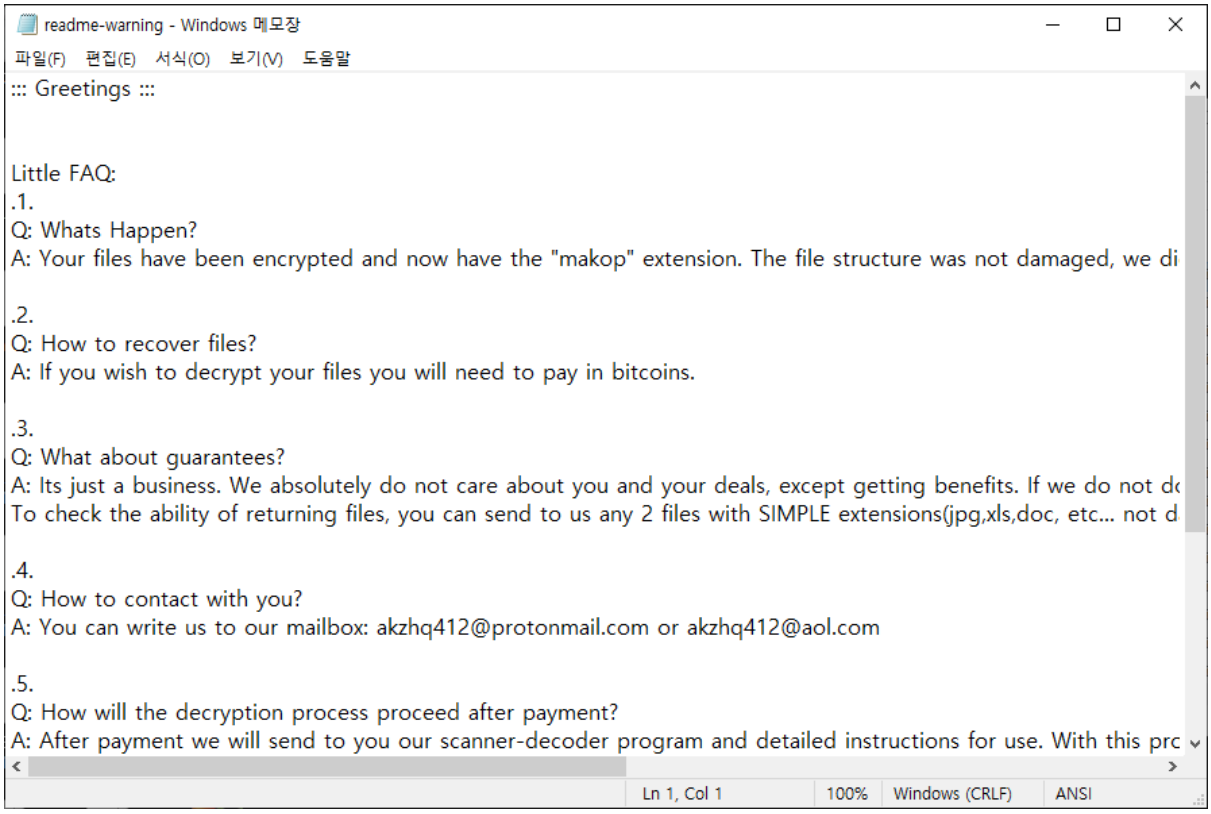
Apr. 13, 2020

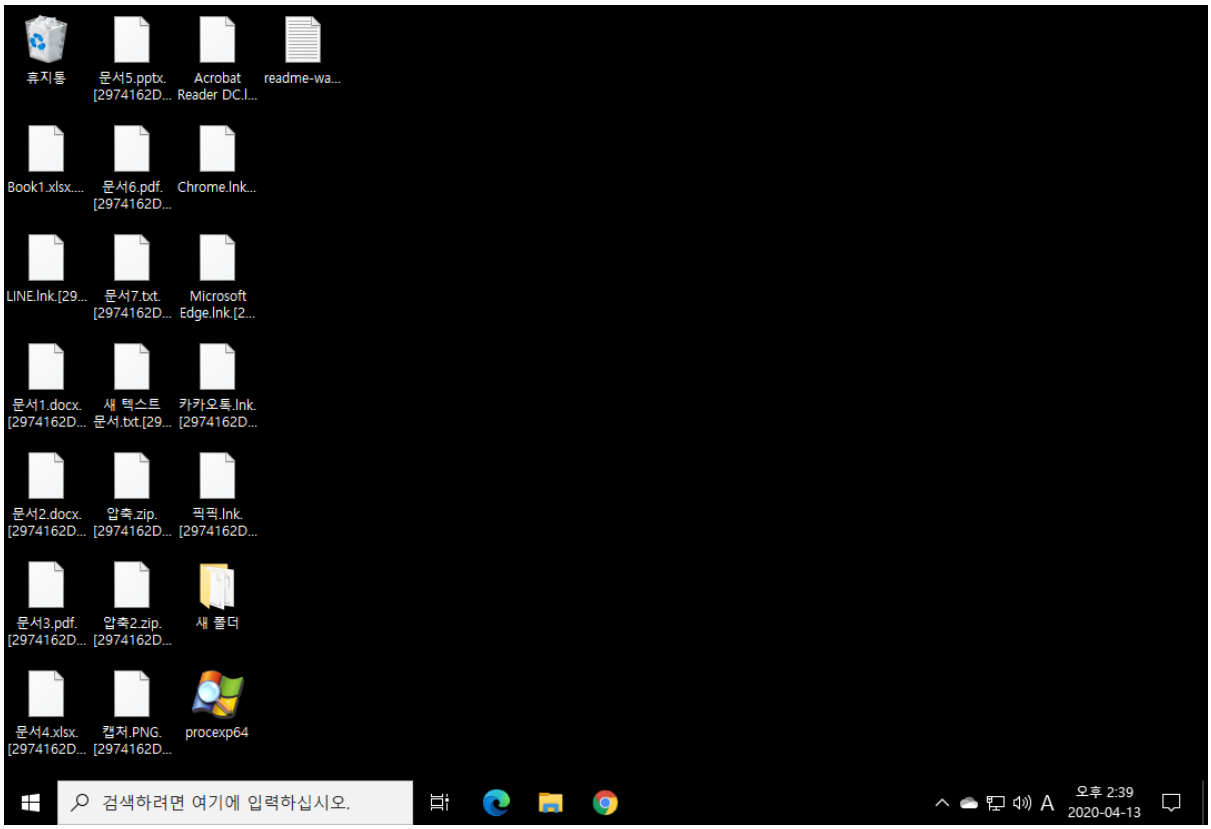
1. Blocked by trueEP®

2. Victim in case trueEP® was not installed - All file name's extensions were changed to [2974162D].[akzhq412@protonmail.com].makop

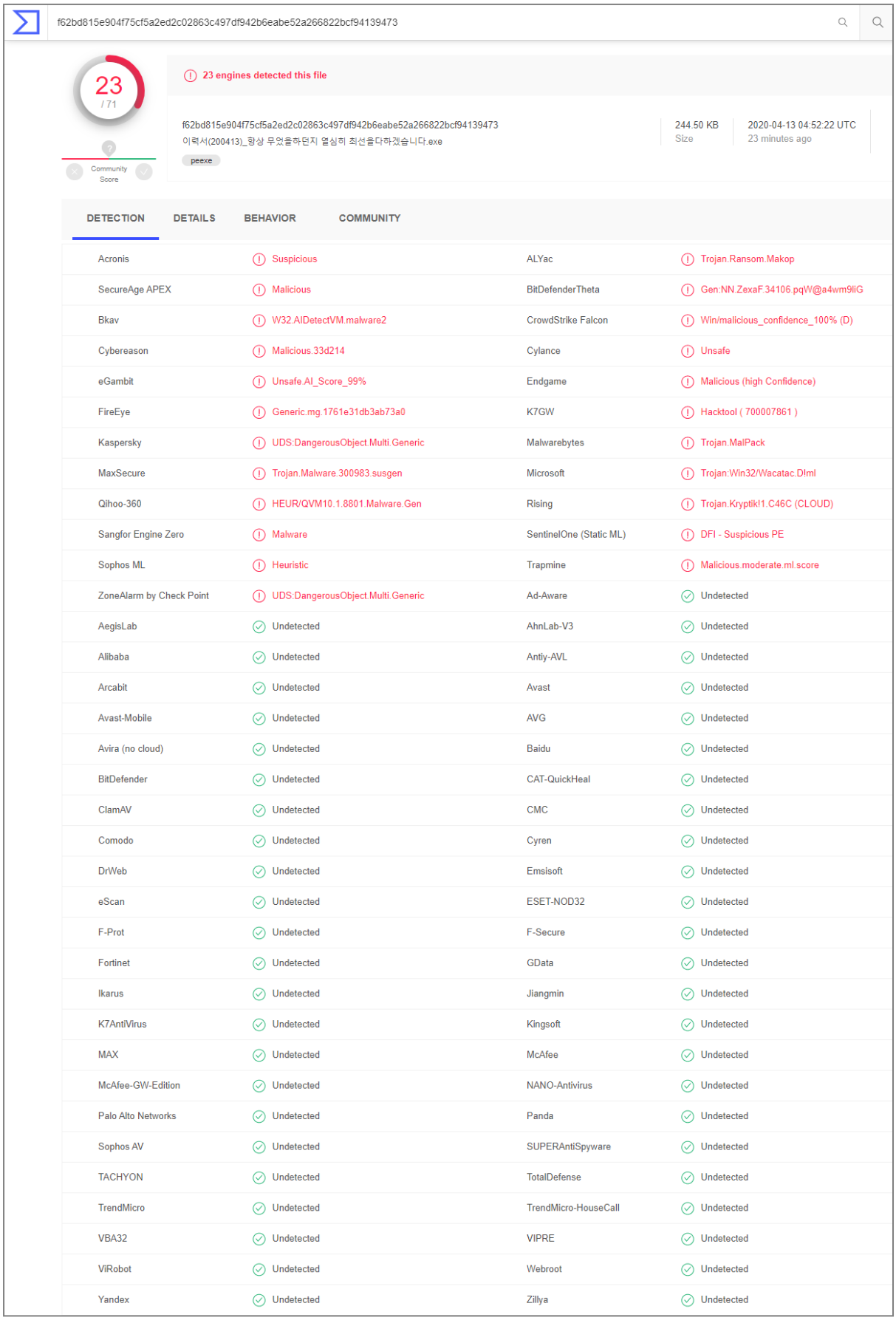


3. Screen of Victim





4. The results of Virus Total


f62bd815e904f75cf5a2ed2c02863c497df942b6eabe52a266822bcf94139473
23
/ 71
Community Score
23 engines detected this file
f62bd815e904f75cf5a2ed2c02863c497df942b6eabe52a266822bcf94139473
이력서(200413)_항상 무었을하던지 열심히 최선을다하겠습니다.exe
peexe
244.50 KB
Size
2020-04-13 04:52:22 UTC
23 minutes ago
DETECTION
DETAILS
BEHAVIOR
COMMUNITY
Acronis Suspicious
ALYac Trojan.Ransom.Makop
SecureAge APEX Malicious
BitDefenderTheta Gen:NN.ZexaF.34106.pqW@a4wm9liG
Bkav W32.AIDetectVM.malware2
CrowdStrike Falcon Win/malicious_confidence_100% (D)
Cybereason Malicious.33d214
Cylance Unsafe
eGambit Unsafe.AI_Score_99%
Endgame Malicious (high Confidence)
FireEye Generic.mg.1761e31db3ab73a0
K7GW Hacktool (700007861)
Kaspersky UDS:DangerousObject.Multi.Generic
Malwarebytes Trojan.MalPack
MaxSecure Trojan.Malware.300983.susgen
Microsoft Trojan:Win32/Wacatac.D!ml
Qihoo-360 HEUR/QVM10.1.8801.Malware.Gen
Rising Trojan.Kryptik!1.C46C (CLOUD)
Sangfor Engine Zero Malware
SentinelOne (Static ML) DFI - Suspicious PE
Sophos ML Heuristic
Trapmine Malicious.moderate.ml.score
ZoneAlarm by Check Point UDS:DangerousObject.Multi.Generic
Ad-Aware Undetected
AegisLab Undetected
AhnLab-V3 Undetected
Alibaba Undetected
Antiy-AVL Undetected
Arcabit Undetected
Avast Undetected
Avast-Mobile Undetected
AVG Undetected
Avira (no cloud) Undetected
Baidu Undetected
BitDefender Undetected
CAT-QuickHeal Undetected
ClamAV Undetected
CMC Undetected
Comodo Undetected
Cyren Undetected
DrWeb Undetected
Emsisoft Undetected
eScan Undetected
ESET-NOD32 Undetected
F-Prot Undetected
F-Secure Undetected
Fortinet Undetected
GData Undetected
Ikarus Undetected
Jiangmin Undetected
K7AntiVirus Undetected
Kingsoft Undetected
MAX Undetected
McAfee Undetected
McAfee-GW-Edition Undetected
NANO-Antivirus Undetected
Palo Alto Networks Undetected
Panda Undetected
Sophos AV Undetected
SUPERAntiSpyware Undetected
TACHYON Undetected
TotalDefense Undetected
TrendMicro Undetected
TrendMicro-HouseCall Undetected
VBA32 Undetected
VIPRE Undetected
ViRobot Undetected
Webroot Undetected
Yandex Undetected
Zillya Undetected