

Osnovna analiza zlonamjernog softvera pomoću *online* alata

CERT.hr-PUBDOC-2019-7-383

Sadržaj

1	UVOD	3
2	ANALIZA ZLONAMJERNOG SOFTVERA ALATOM <i>VIRUSTOTAL</i>	4
2.1	ANALIZA LEGITIMNOG SOFTVERA	7
2.2	ANALIZA POTENCIJALNO NEŽELJENOG SOFTVERA	9
2.3	ANALIZA LEGITIMNOG SOFTVERA KOJI SE MOŽE ZLOUPOTRIJEBITI	10
2.4	ANALIZA ZLONAMJERNOG SOFTVERA	11
3	ANALIZA ZLONAMJERNOG SOFTVERA ALATOM <i>HYBRID ANALYSIS</i>	14
3.1	ANALIZA ZLONAMJERNOG SOFTVERA	15
4	ZAKLJUČAK	22

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument vlasništvo je Nacionalnog CERT-a. Namijenjen je javnoj objavi te se svatko smije njime koristiti i na njega se pozivati, ali isključivo u izvornom obliku, bez izmjena, uz obvezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima povreda je autorskih prava CARNET-a, a sve navedeno u skladu je sa zakonskim odredbama Republike Hrvatske.

1 Uvod

Prilikom svakodnevnog pretraživanja interneta postoji rizik od susreta sa zlonamjernim datotekama/programima koji mogu naštetiti računalu.

Iako korisnik ne bi svjesno preuzeo zlonamjerni softver, napadači koriste razne metode kako bi prevarili i naveli korisnika da ga preuzme na svoje računalo – lažno reklamiraju programe, iskorištavaju ranjivosti web preglednika, šalju sumnjive privitke putem e-pošte i društvenih mreža i sl.

Antivirusni softver, koji najčešće dolazi automatski instaliran s operacijskim sustavom, prva je linija obrane i sposoban je klasificirati zlonamjerne datoteke te o tome upozoriti korisnika. Antivirusni će softver presuditi je li datoteka opasna ili nije, a ponekad će dati i nešto više informacija o prijetnji.

No, ponekad postoji potreba za detaljnijim istraživanjem datoteke, npr. ako sumnjamo u odluku antivirusnog softvera, ako nas preciznije zanima o kakvoj se prijetnji radi te općenito ako želimo provjeriti je li datoteka koju želimo otvoriti zlonamjerna. U tom slučaju dostupni su nam razni brzi i besplatni *online* alati koji se mogu jednostavno koristiti bez ikakvih instalacija i ne zahtijevaju veliko stručno znanje.

Dostupan je veći broj takvih alata i osnovne funkcionalnosti im se većim dijelom preklapaju. U ovom dokumentu opisan će se dva ovakva široko korištena *online* alata – *VirusTotal* i *Hybrid Analysis*. Također, demonstrirat će se analiza sigurnih i zlonamjernih datoteka i interpretirati rezultati.

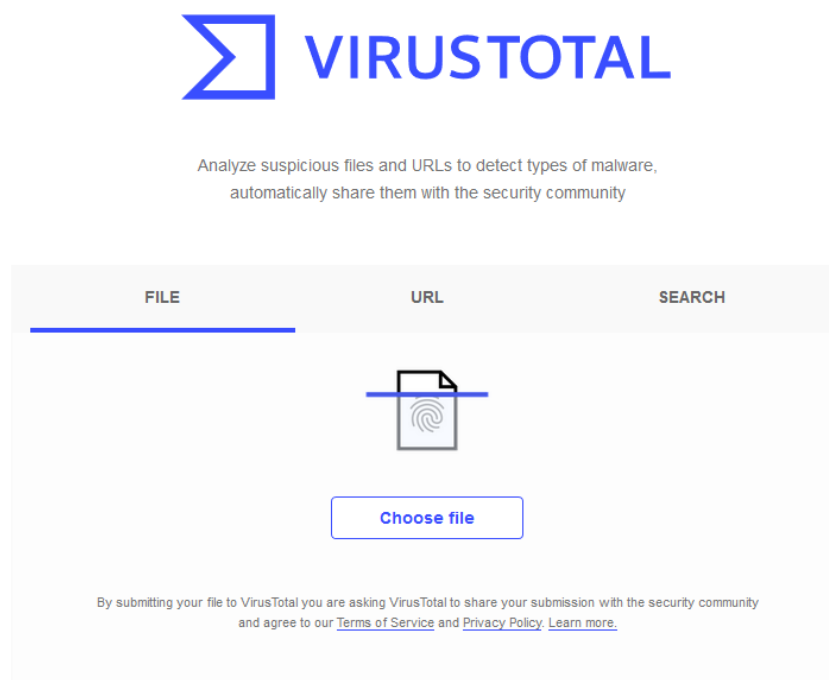
2 Analiza zlonamjernog softvera alatom *VirusTotal*

VirusTotal je web stranica koja korisniku omogućuje skeniranje sumnjivih datoteka ili URL-ova kako bi potvrdio ili odbacio pretpostavku da su zlonamjerne. Objedinjuje više od 70 antivirusnih softvera i skenera raznih proizvođača kako bi poboljšao svoje sposobnosti detekcije, među kojima su i neki od najpoznatijih poput Avasta, McAfee, Malwarebytesa, Bitdefendera, ESET-a i Kasperskya. U vlasništvu je Googlea od 2012. godine.

Osim antivirusnih softvera svojih partnera, *VirusTotal* koristi i dodatne alate za statičku i dinamičku analizu datoteka i URL-ova, a uzima u obzir i komentare korisnika vezane uz određenu datoteku ili URL.

Za analizu datoteka i URL-ova koriste se heurističke metode, prepoznavanje zlonamjernog potpisa, analiza metapodataka, identifikacija zlonamjernih signala i slične metode detekcije zlonamjernog softvera.

VirusTotal je dostupan na URL-u <https://www.virustotal.com/>. Kad se stranica učita, pojavljuje se korisničko sučelje prikazano na slici 2.1.



Slika 2.1. Početna stranica alata *VirusTotal*

VirusTotal prilikom svakog učitavanja datoteke računa njen sažetak (engl. *hash*). Sažetak svake različite datoteke je jedinstven, i pomoću njega *VirusTotal* može povezati učitanu datoteku s istim takvim datotekama na koje su naišli i koje su učitali drugi korisnici, ili koje se već nalaze u bazi antivirusnog alata. Na taj je način analiza brža jer se ne mora svaki put pokrenuti skeniranje, već se dohvati posljednje izvješće o datoteci svakog antivirusnog softvera koji ju je već analizirao. Kad bi se bilo koji dio datoteke izmijenio, izmijenio bi se i njen sažetak, *VirusTotal* ne bi uspio pronaći postojeća izvješća, pa bi pokrenuo skeniranje datoteke koje bi potrajalo od nekoliko sekundi do par minuta.

Osim datoteka s datotečnog sustava na računalu, *VirusTotal* je na analizu moguće predati i URL stranice za koju se sumnja da poslužuje zlonamjerni softver ili je zlonamjerna na neki drugi način. Budući da napadači često distribuiraju zlonamjerni softver putem web stranica na koje ih postavljaju, VirusTotalom je moguće provjeriti je li riječ o URL-u na kojem se nalazi zlonamjerni softver, je li riječ o već viđenom *phishing* URL-u, nalazi li se na njemu neki poznati *exploit kit* i sl.

VirusTotalom moguće je skenirati bilo koju vrstu datoteka – izvršne datoteke, PDF-ove, slike, JavaScript kod, Microsoft Office dokumente...

Prilikom učitavanja datoteka, kako se ne bi ugrozila privatnost, potrebno je pripaziti da se ne učitaju i osjetljivi podaci koje te datoteke mogu sadržavati, npr. adresa, OIB, lozinke, brojevi kreditnih kartica i sl. Datoteke koje korisnik pošalje na analizu *VirusTotal* će podijeliti sa svojim partnerima čije alate koristi. Dakle, ako se na *VirusTotal* učita npr. Word dokument s osobnim podacima, taj dokument se prosljeđuje i svim antivirusnim tvrtkama koje surađuju s *VirusTotalom* i korisnicima *VirusTotala*, što znači da praktički postaje javan.

Nakon učitavanja datoteke prikazat će se rezultati skeniranja većeg broja antivirusnih proizvođača koji se ne moraju usuglasiti oko toga je li datoteka zlonamjerna ili nije. Stoga najčešće nije trivijalno interpretirati rezultate niti je moguće dati pouzdan odgovor je li datoteka opasna i o kojoj se prijetnji radi bez daljnje detaljnije analize.

Nakon što se datoteka analizira, generira se izvješće s informacijama koje su prikazane na slici 2.2.:

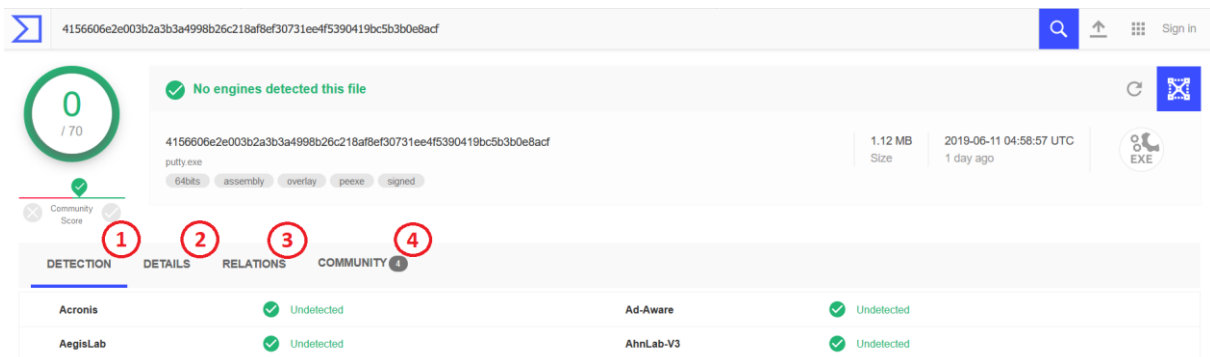
Slika 2.2. Informacije o analiziranoj datoteci

- 1) Broj antivirusnih alata koji su datoteku klasificirali kao opasnu (u ovom slučaju 0) u odnosu na ukupni broj antivirusnih alata koji su skenirali datoteku.
- 2) „Reputacija“: registrirani korisnici koji predstavljaju zajednicu (engl. *VirusTotal Community*) mogu pregledavati i ocjenjivati datoteke koje su učitane na *VirusTotal* kao sigurne ili zlonamjerne, gdje se ukupna ocjena računa ovisno o ocjeni korisnika i korisnikovoj reputaciji. Ako je reputacija negativna (crvena boja), datoteku su korisnici ocijenili kao zlonamjernu, a ako je reputacija pozitivna (zelena boja), datoteku su korisnici ocijenili kao sigurnu.
- 3) Sažetak (engl. *hash*) datoteke izračunat algoritmom SHA-256, čime je datoteka jednoznačno označena i može se prepoznati da je riječ o istoj datoteci čak i ako

ona ima drugi naziv ili ju je na *VirusTotal* sa svog računala učitao neki drugi korisnik.

- 4) Oznake (engl. *tags*) koje opisuju neke karakteristike analizirane datoteke.
- 5) Datum i vrijeme posljednje analize datoteke (ako datoteka nije skenirana, već je dohvaćeno postojeće izvješće, datum i vrijeme označavaju otkad je to izvješće).
- 6) Ikona koja grafički prikazuje vrstu datoteke (PDF, .exe, .docx...).
- 7) Tipka za ponovnu analizu koja će iznova skenirati dokument.

Osim osnovnih informacija, moguće je dobiti uvid i u detaljnije informacije o datoteci i njenom ponašanju koje su grupirane u odjeljke kao što je prikazano na slici 2.3.



Slika 2.3. Odjeljci s detaljnijim informacijama o analiziranoj datoteci

1) DETECTION

Popis svih partnera koji su analizirali datoteku i rezultat analize, pri čemu je moguće sljedeće:

- a. „Undetected“ – alat datoteku nije detektirao kao malicioznu
- b. „Suspicious“ – alat je datoteku označio kao sumnjivu
- c. „Unable to process file type“ – alat ne razumije o kojoj je vrsti datoteke riječ i ne može je analizirati
- d. „Timeout“ – alat je prekoračio dopušteno vrijeme izvršavanja i njegova analiza nije dovršena ni prikazana

2) DETAILS

Dodatne informacije o analiziranoj datoteci poput informacija o potpisu, raznim nazivima pod kojim se ta datoteka pojavljivala kod drugih korisnika, metapodacima, sekcijama, resursima, autoru itd.

3) RELATIONS

VirusTotal tablično i grafički prikazuje sve programe, datoteke i URL-ove uz koje je datoteka vezana, bilo da im pristupa u kodu ili da je tamo već viđena kad se analizirala neka druga datoteka/URL

4) COMMUNITY

Komentari i ocjene korisnika koji čine VirusTotal zajednicu.

Datoteka ne mora uvijek biti ispravno klasificirana te i sam *VirusTotal* upozorava na tzv. *false positives* i *false negatives*. Drugim riječima, datoteka koja je sigurna može biti pogrešno klasificirana kao zlonamjerna (engl. *false positive*), a datoteka koja je zlonamjerna može biti pogrešno klasificirana kao sigurna (engl. *false negative*). Zlonamjerni programi postaju sve sofisticiraniji i čak ni vodećim antivirusnim alatima nije lako dati pouzdan odgovor.

Čak i ako je datoteka ispravno detektirana kao zlonamjerna, detaljnija analiza je neizostavna kako bi se utvrdilo o kakvoj se točno prijetnji radi – nečem kritičnom poput *ransomwarea*, ili ipak nečem poput neželjenih programa ili aplikacija (engl. *Potentially Unwanted Program/Potentially Unwanted Application, PUA/PUP*) koji nisu nužno zlonamjerni.

Neki *VirusTotal*ovi partneri kao zlonamjerne će klasificirati i legitimne alate ako prepoznaju mogućnost da se koriste ili se mogu iskoristiti za zlonamjerne aktivnosti.

U nastavku ovog dokumenta proći će se kroz nekoliko uobičajenih primjera koji će ilustrirati najčešće situacije i pokazati kako ih detaljnije analizirati i pouzdanije odrediti je li riječ o opasnoj ili sigurnoj datoteci.

2.1 Analiza legitimnog softvera

S [poveznice](#) je preuzeta izvršna datoteka alata PuTTY. PuTTY je klijentski program otvorenog koda koji podržava protokole telnet, rlogin i SSH i omogućuje krajnjem korisniku korištenje navedenih protokola i udaljeno upravljanje računalom. Više o PuTTYju moguće je pronaći u prethodnom [dokumentu Nacionalnog CERT-a](#).

Ako je preuzet sa službene stranice, PuTTY može poslužiti kao primjer legitimne, tj. sigurne datoteke.

Nakon učitavanja datoteke na *VirusTotal*, vidljivo je kako su se svi alati usuglasili da je riječ o legitimnoj i sigurnoj datoteci. Rezultat analize prikazan je na slici 2.4.

4156606e2e003b2a3b3a4998b26c218af8ef30731ee4f5390419bc5b3b0e8acf

0 / 72

Community Score

✓ No engines detected this file

4156606e2e003b2a3b3a4998b26c218af8ef30731ee4f5390419bc5b3b0e8acf
PuTTY
64bits assembly overlay peexe signed

1.12 MB Size
2019-06-06 09:24:44 UTC
3 days ago

EXE

DETECTION	DETAILS	RELATIONS	COMMUNITY
Acronis	✓ Undetected	Ad-Aware	✓ Undetected
AegisLab	✓ Undetected	AhnLab-V3	✓ Undetected
Alibaba	✓ Undetected	ALYac	✓ Undetected
Antiy-AVL	✓ Undetected	SecureAge APEX	✓ Undetected
Arcabit	✓ Undetected	Avast	✓ Undetected
Avast-Mobile	✓ Undetected	AVG	✓ Undetected
Avira (no cloud)	✓ Undetected	Babable	✓ Undetected
Baidu	✓ Undetected	BitDefender	✓ Undetected
Bkav	✓ Undetected	CAT-QuickHeal	✓ Undetected
ClamAV	✓ Undetected	CMC	✓ Undetected
Comodo	✓ Undetected	CrowdStrike Falcon	✓ Undetected
Cybereason	✓ Undetected	Cylance	✓ Undetected
Cyren	✓ Undetected	DrWeb	✓ Undetected
eGambit	✓ Undetected	Emsisoft	✓ Undetected
Endgame	✓ Undetected	eScan	✓ Undetected

2.4. Rezultat analize sigurne datoteke

Zelena kružnica na vrhu stranice unutar koje piše 0/72 informira korisnika kako nijedan od partnera koji surađuju s *VirusTotalom*, pod čim se misli na antivirusne kompanije, nije klasificirao datoteku kao zlonamjernu ili štetnu. Također, i korisnici koji su analizirali ovu datoteku ocijenili su je kao sigurnu.

Oznaka „**Undetected**“ pored naziva antivirusnog alata govori da alat datoteku ne smatra zlonamjernom.

Ako pogledamo detalje, vidjet ćemo da je datoteka digitalno potpisana i verificirana. Digitalni potpis garantira da potpisana datoteka pripada određenom autoru i da nitko drugi nije neovlašteno izmijenio datoteku.

VirusTotal prikazuje hijerarhiju digitalnih potpisa, kao i sva certifikacijska tijela koja garantiraju za autora datoteke. Na slici 2.5. vidljivo je kako digitalni potpis pripada Simonu Tathamu, programeru koji je razvio PuTTY.

The screenshot shows the VirusTotal interface with the 'DETAILS' tab selected. The 'Signature Info' section is expanded, displaying the following information:

- Signature Verification:** Signed file, valid signature (indicated by a green checkmark).
- File Version Information:**
 - Copyright: Copyright © 1997-2019 Simon Tatham.
 - Product: PuTTY suite
 - Description: SSH, Telnet and Rlogin client
 - Original Name: PuTTY
 - Internal Name: PuTTY
 - File Version: Release 0.71 (with embedded help)
 - Date signed: 1:32 PM 3/16/2019
- Signers:**
 - Simon Tatham (expanded):
 - Name: Simon Tatham
 - Status: Valid
 - Valid From: 12:00 AM 11/13/2018
 - Valid To: 11:59 PM 11/08/2021
 - Valid Usage: Code Signing
 - Algorithm: sha256RSA
 - Serial Number: 7C 11 18 CB BA DC 95 DA 37 52 C4 6E 47 A2 74 38
 - COMODO RSA Code Signing CA
 - Sectigo (formerly Comodo CA)
- Counter Signers:**
 - COMODO SHA-1 Time Stamping Signer
 - Sectigo (UTN Object)

Slika 2.5. Digitalni potpis datoteke

2.2 Analiza potencijalno neželjenog softvera

Kao primjer potencijalno neželjenog softvera preuzet će se instalacijska datoteka programa CCleaner sa stranice Download.com/CNET.

Iako je CCleaner legitiman program namijenjen čišćenju i optimizaciji prostora na računalu, u ovoj instalacijskoj datoteci u paketu dolazi i drugi, potencijalno neželjen softver koji se bez znanja korisnika instalira istovremeno s programom CCleaner.

S obzirom na to da ova datoteka na računalo instalira i dodatni, potencijalno neželjeni softver u sklopu instalacije, ne možemo ju smatrati legitimnim softverom, ali isto tako se ne može smatrati ni pravim zlonamjernim softverom.

Rezultat analize prikazan je na slici 2.6.

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Antiy-AVL	!	Trojan/Win32.Droma	Cyren	! W32/Trojan.DSSE-8486
ESET-NOD32	!	Win32/Bundled.Toolbar.Google.D Potenti...	Acronis	✓ Undetected
Ad-Aware	✓	Undetected	AegisLab	✓ Undetected
AhnLab-V3	✓	Undetected	Alibaba	✓ Undetected
ALYac	✓	Undetected	SecureAge APEX	✓ Undetected
Arcabit	✓	Undetected	Avast	✓ Undetected
Avast-Mobile	✓	Undetected	AVG	✓ Undetected
Avira (no cloud)	✓	Undetected	Babable	✓ Undetected

Slika 2.6. Rezultat analize potencijalno neželjenog softvera

Kao što je vidljivo, nisu se svi alati usuglasili oko toga je li datoteka zlonamjerna ili nije – dva od njih tvrde da je riječ o trojanskom konju, a jedan da je riječ o potencijalno neželjenom softveru (engl. *Potentially Unwanted Program, PUP*) koji ugrađuje Googleovu alatnu traku na web preglednik.

2.3 Analiza legitimnog softvera koji se može zloupotrijebiti

Sa [službene stranice Windows SysInternalsa](#) preuzet je alat PsExec – program koji omogućava udaljeno upravljanje Windows računalima bez potrebe za instalacijom dodatnog softvera.

Zajedno s ostatkom PsTools alata, namijenjen je prvenstveno sistemskim administratorima za obavljanje svakodnevnog posla i tad je legitiman, ali ga ponekad i napadači zloupotrebljavaju u kibernetičkim napadima kako bi se proširili po mreži i u tom je slučaju opasan.

Na slici 2.7. prikazani su rezultati analize.

ad6b98c01ee849874e4b4502c3d7853196f6044240d3271e4ab3fc6e3c08e9a4

2 / 71

2 engines detected this file

ad6b98c01ee849874e4b4502c3d7853196f6044240d3271e4ab3fc6e3c08e9a4

366.16 KB Size

2019-06-09 15:53:21 UTC

3 days ago

PsExec

64bits assembly overlay peexe signed via-tor

Community Score

DETECTION	DETAILS	RELATIONS	COMMUNITY
Sophos AV	❗ PsExec (PUA)	ViRobot	❗ HackTool.PsExec.374944
Acronis	✅ Undetected	Ad-Aware	✅ Undetected
AegisLab	✅ Undetected	AhnLab-V3	✅ Undetected
Alibaba	✅ Undetected	ALYac	✅ Undetected
Antiy-AVL	✅ Undetected	SecureAge APEX	✅ Undetected
Arcabit	✅ Undetected	Avast	✅ Undetected
Avast-Mobile	✅ Undetected	AVG	✅ Undetected
Avira (no cloud)	✅ Undetected	Babable	✅ Undetected

Slika 2.7. Rezultat analize legitimnog softvera koji se može zloupotrijebiti

Iako većina alata datoteku smatra sigurnom, Sophos AV ga je detektirao kao potencijalno neželjenu aplikaciju, a ViRobot kao alat za hakiranje. Obojica su prepoznala da je riječ o alatu PsExec.

To je upozorenje navedeno i na stranici alata:

„Napomena: neki antivirusni skeneri upozoravaju korisnika da je jedan ili više PsTools alata zaraženo 'remote admin' virusom. Nijedan PsTool alat ne sadrži viruse, ali su zabilježeni slučajevi kad su ih virusi koristili u napadu i zato kod nekih antivirusnih skenera aktiviraju obavijest o virusu.“

2.4 Analiza zlonamjernog softvera

S [poveznice](#) je preuzet zlonamjerni softver Infostealer.Dexter, trojanski konj koji prikuplja informacije sa žrtvinog računala.

NAPOMENA: Zbog rizika od zaraze računala, ne preporučujemo preuzimanje i rad s pravim zlonamjernim softverom bez odgovarajućeg predznanja, prethodnog iskustva i mjera opreza. Ako se ipak odlučite pratiti korake u dokumentu i samostalno analizirati softver, obavezno to činite isključivo u virtualnom računalu.

Na slici 2.8. prikazani su rezultati analize.

4eabb1adc035f035e010c0d0d259c683e18193f509946652ed8aa7c5d92b6a92

66.5 KB Size | 2019-06-09 23:45:32 UTC | 2 days ago

win32.exe

Community Score: 57 / 70

57 engines detected this file

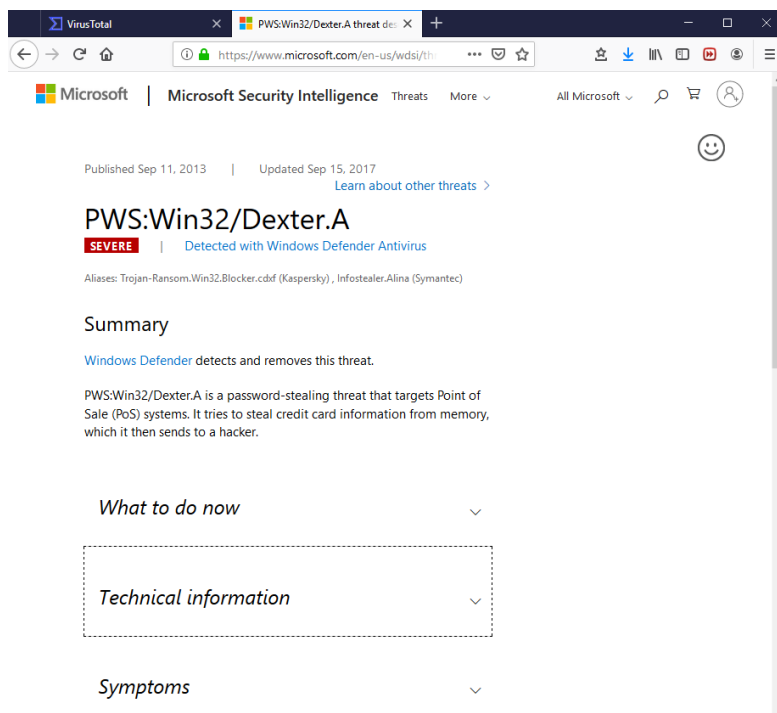
DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Acronis		Suspicious	Ad-Aware	Dropped:Trojan.AgentWDCR.COP
AegisLab		Trojan.Win32.Generic.4lc	AhnLab-V3	Trojan/Win32.Agent.R66523
Alibaba		PWSteal.Win32/Dexter.4d9f032c	Antiy-AVL	Trojan/Win32.Invader
SecureAge APEX		Malicious	Arcabit	Trojan.AgentWDCR.COP
Avast		Win32.Dexter-I [Trj]	AVG	Win32.Dexter-I [Trj]
Avira (no cloud)		TR/Hijacker.Gen	BitDefender	Dropped:Trojan.AgentWDCR.COP
CAT-QuickHeal		TrojanPWS.Dexter.A4	Comodo	TrojWare.Win32.Poxters.A@5s5ve5
CrowdStrike Falcon		Win/malicious_confidence_100% (W)	Cybereason	Malicious.f0c2b3
Cylance		Unsafe	DrWeb	Trojan.Packed.21724
eGambit		Trojan.Generic	Emsisoft	Dropped:Trojan.AgentWDCR.COP (B)
Endgame		Malicious (high Confidence)	eScan	Dropped:Trojan.AgentWDCR.COP
ESET-NOD32		A Variant Of Win32/Poxters.E	F-Prot	W32/Heuristic-KPPIEldorado

2.8. Rezultati analize zlonamjernog softvera

Skoro svi antivirusni alati su se usuglasili kako je riječ o zlonamjernoj datoteci. Također, i korisnici su je ocijenili kao zlonamjernu, što se vidi time što je *community score* izrazito negativan.

Kako bi se pronašlo više detalja o čemu je riječ, može se posjetiti stranica neke konkretne antivirusne tvrtke koja je sudjelovala u skeniranju. Primjerice, informacije o ovom zlonamjernom softveru dostupne su u [Microsoftovoj](#), [TrendMicrovoj](#) i [ESETovoj](#) enciklopediji prijetnji.

Primjerice, Microsoftov alat za ovu datoteku kaže da je riječ o zlonamjernom softveru „PWS:WIN32/Dexter.a“. Na Microsoftovoj enciklopediji prijetnji koja se nalazi na [ovoj poveznici](#) možemo pretražiti prijetnje po ključnoj riječi, ili možemo koristiti uobičajenu tražilicu kao što je Google. Na slici su 2.8. prikazani rezultati pretrage.



The screenshot shows a web browser window displaying the Microsoft Security Intelligence page for the threat PWS:Win32/Dexter.A. The page includes the following information:

- Published Sep 11, 2013 | Updated Sep 15, 2017
- Severity: **SEVERE** | Detected with Windows Defender Antivirus
- Aliases: Trojan-Ransom.Win32.Blocker.cdf (Kaspersky), Infostealer.Alina (Symantec)
- Section: **Summary**
 - Windows Defender detects and removes this threat.
 - PWS:Win32/Dexter.A is a password-stealing threat that targets Point of Sale (PoS) systems. It tries to steal credit card information from memory, which it then sends to a hacker.
- Section: **What to do now** (collapsed)
- Section: **Technical information** (collapsed)
- Section: **Symptoms** (collapsed)

2.8. Rezultati pretrage za PWS:Win32/Dexter.A

Osim kratkog opisa, navedeni su i daljnji koraci koje korisnik može poduzeti ako je zaražen ovim trojanskim konjem, tehničke informacije koje objašnjavaju što se točno dogodilo na računalu prilikom instalacije zlonamjernog softvera, i simptomi prema kojima je moguće prepoznati da je računalo zaraženo.

3 Analiza zlonamjernog softvera alatom *Hybrid Analysis*

Hybrid Analysis besplatna je web aplikacija u vlasništvu tvrtke CrowdStrike koja nudi uslugu analize datoteka i pomoć pri detekciji zlonamjernog softvera.

Dok je *VirusTotal* primarno fokusiran na usporedbu rezultata analize više antivirusnih alata, glavna funkcionalnost alata *Hybrid Analysis* je detaljnija statička i dinamička analiza datoteke koja može dati pobliži uvid u to što datoteka radi i na koji je način zlonamjerna.

Statička analiza je provjeravanje sadržaja datoteke bez pokretanja koda i njome se skupljaju informacije poput popisa znakovnih nizova koji se pojavljuju, potpisa (engl. *signatures*), sažetka (engl. *hash*) itd.

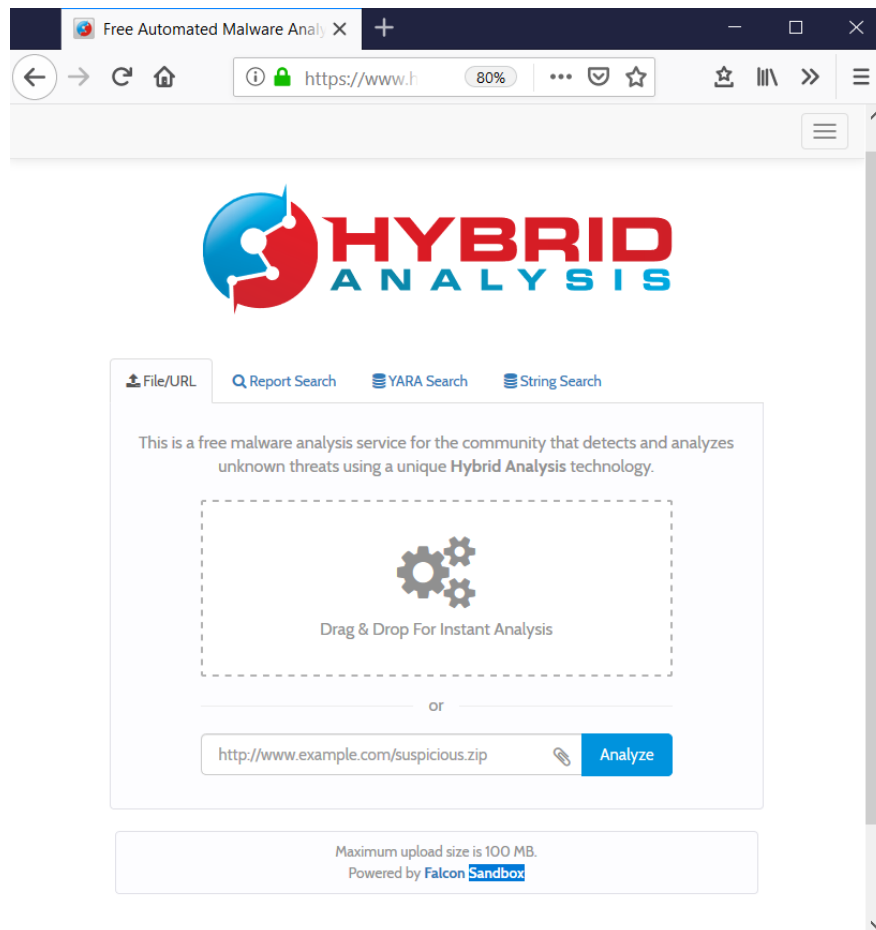
Dinamička analiza pokreće program u sigurnom okruženju (engl. *sandbox*), i prati što on radi unutar sustava i koje su posljedice njegovih aktivnosti. Kad je riječ o analizi zlonamjernog softvera, dinamičkom analizom dobiju se vrlo korisne informacije – obrasci ponašanja programa. *Hybrid Analysis* koristi *Falcon Sandbox* za pokretanje datoteke i evidenciju njenog ponašanja.

Iako se *VirusTotal* i *HybridAnalysis* idejno razlikuju, alati su prisiljeni nuditi sve više funkcionalnosti kako bi ostali konkurentni, tako da se već danas većina funkcionalnosti ovih i njima sličnih alata preklapaju.

Na analizu je moguće predati bilo koju vrstu izvršne datoteke, Office datoteke, PDF, APK, JAR, HTML, JS, VB, itd.

U trenutku pisanja ovog dokumenta podržana je analiza na operacijskim sustavima Windows XP, Vista, 7, 8, 10, Linux (Ubuntu 16.04) i statička analiza za Android APK datoteke.

Alat je dostupan na URL-u <https://www.hybrid-analysis.com/>. Kad se stranica učita, pojavljuje se korisničko sučelje prikazano na slici 3.1.



Slika 3.1. Korisničko sučelje alata Hybrid Analysis

Funkcionalnost učitavanja datoteke/URL-a ili pretraživanja postojećeg izvještaja slična je kao na *VirusTotalu*. Kao i kod *VirusTotala*, prilikom učitavanja potrebno je pripaziti na osjetljive podatke jer će učitane datoteke postati javne. Iako je u *Hybrid Analysisu* moguće ne dati dopuštenje da se datoteka podijeli s trećim stranama, rezultati analize koji obuhvaćaju pronađene znakovne nizove, izvršavanje programa i analizu memorije uvijek će biti javno dostupni.

Za razliku od *VirusTotala*, *Hybrid Analysis* na početnom sučelju nudi i mogućnosti pretraživanja znakovnih nizova i YARA potpisa iz njihove baze u analiziranoj datoteci.

Također, na *Hybrid Analysisu* je moguće odabrati okolinu, tj. operacijski sustav unutar kojeg će se datoteka pokrenuti.

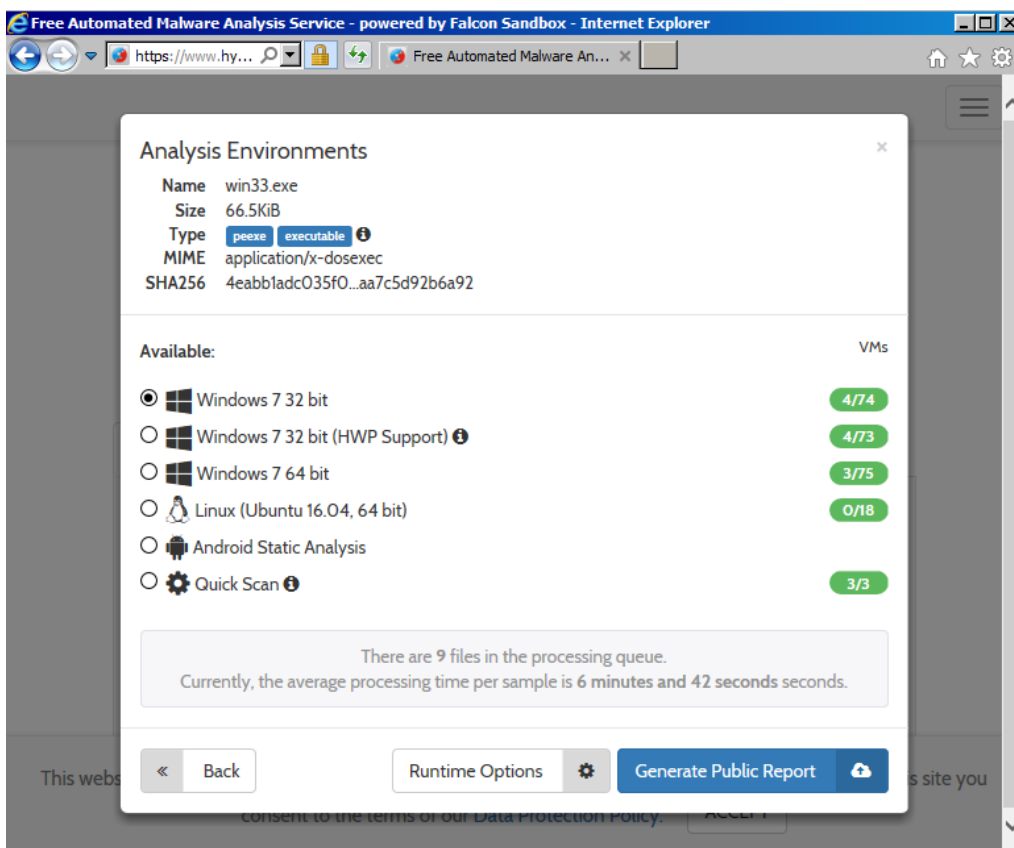
U nastavku dokumenta demonstrirat će se analiza zlonamjernog softvera alatom *Hybrid Analysis*.

3.1 Analiza zlonamjernog softvera

S [poveznice](#) je preuzet zlonamjerni softver Infostealer.Dexter, trojanski konj koji prikuplja informacije sa žrtvinog računala. U nastavku će se pokazati analiza softvera alatom *Hybrid Analysis*.

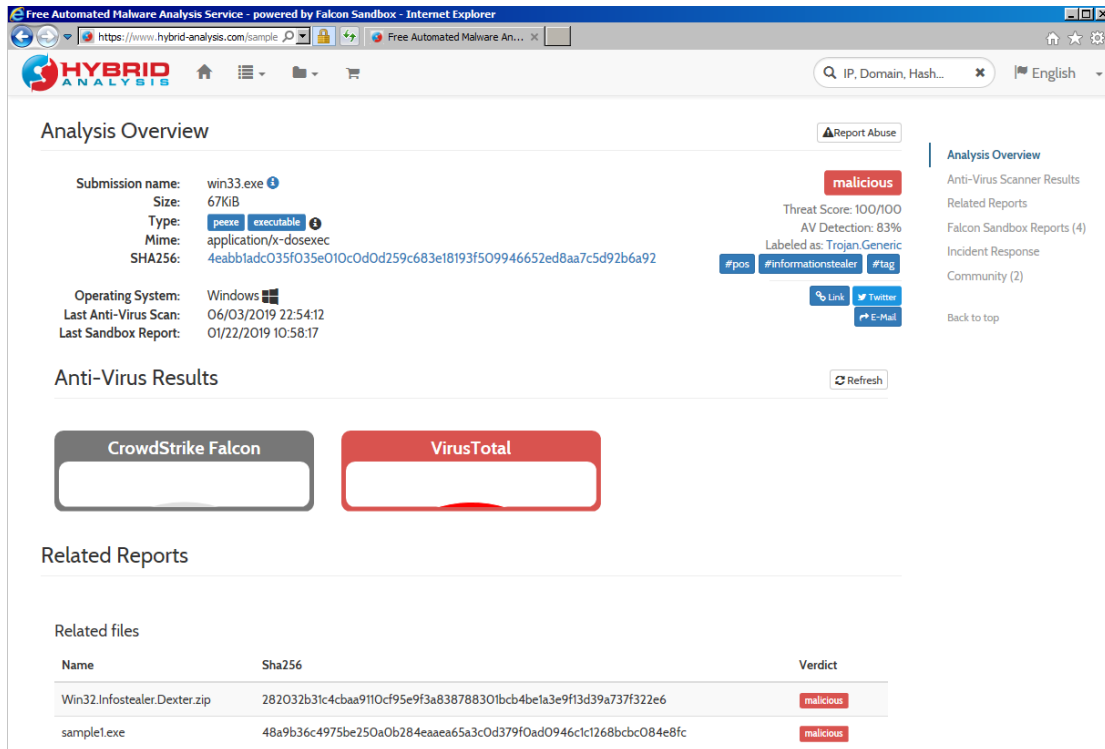
NAPOMENA: Zbog rizika od zaraze računala, ne preporučujemo preuzimanje i rad s pravim zlonamjernim softverom bez odgovarajućeg predznanja, prethodnog iskustva i mjera opreza. Ako se ipak odlučite pratiti korake u dokumentu i samostalno analizirati softver, obavezno to činite isključivo u virtualnom računalu.

Odabrat ćemo analizu na Windows 7 32-bitnom računalu sa zadanim postavkama izvršavanja kao što je prikazano na slici 3.2.



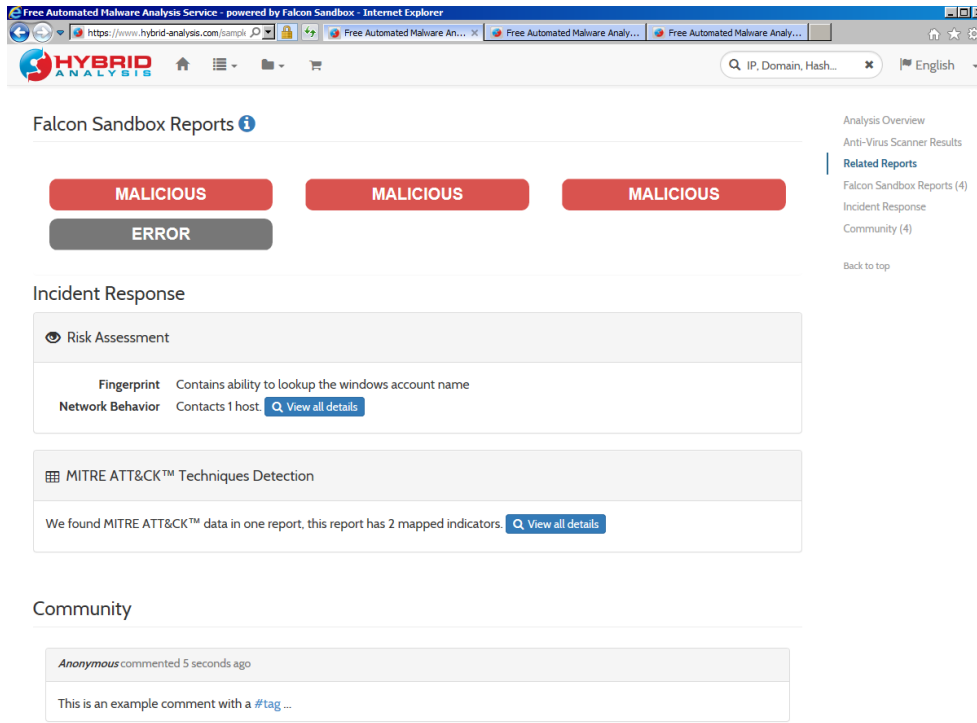
Slika 3.2. Odabir okoline za pokretanje datoteke

Prvi dio izvješća analize, prikazan na slici 3.3., sličan je kao i na alatu VirusTotal. Štoviše, *Hybrid Analysis* ima ugrađen prikaz rezultata *VirusTotal* i *CrownStrike Falcon* analize datoteke.



Slika 3.3. Prvi dio izvještaja analize alatom Hybrid Analysis

Za razliku od *VirusTotala*, drugi dio izvještaja rezultati su analize nakon pokretanja datoteke na odabranom operacijskom sustavu.



Slika 3.4. Drugi dio izvještaja analize alatom Hybrid Analysis

Poput *VirusTotala*, ni *Hybrid Analysis* neće svaki put iznova analizirati datoteku ako prema njenom sažetku pronađe već postojeći izvještaj. U ovom slučaju postoje četiri izvještaja za istu datoteku. Tri izvještaja zaključila su da je riječ o zlonamjernom softveru (MALICIOUS), dok 4. izvještaj nije uspio dovršiti analizu (ERROR).

Detalji dinamičke analize mogu se vidjeti klikom na „MALICIOUS“ tipku, a čine ih:

- 1) Indikatori (zlonamjerni, sumnjivi ili informativni)
- 2) Vizualizacija sadržaja i strukture datoteke
- 3) Učitane datoteke
- 4) Pronađeni znakovni nizovi

Indikatori

Hybrid Analysis popisuje indikatore zlonamjernog i sumnjivog ponašanja. Također, korisnika će obavijestiti i o informativnim indikatorima – ponašanje koje ne mora biti zlonamjerno ni sumnjivo, ali može pomoći pri analizi.

Malicious Indicators 5	Suspicious Indicators 3
External Systems <ul style="list-style-type: none"> Sample was identified as malicious by a large number of Antivirus engines <ul style="list-style-type: none"> details: 12/15 Antivirus vendors marked sample as malicious (80% detection rate) 59/71 Antivirus vendors marked sample as malicious (83% detection rate) source: External System relevance: 10/10 Sample was identified as malicious by at least one Antivirus engine 	Anti-Reverse Engineering <ul style="list-style-type: none"> PE file has unusual entropy sections
Pattern Matching <ul style="list-style-type: none"> YARA signature match 	Network Related <ul style="list-style-type: none"> Found potential IP address in binary/memory
Unusual Characteristics <ul style="list-style-type: none"> References suspicious system modules 	Remote Access Related <ul style="list-style-type: none"> Contains references to WMI/WMIC
Hiding 1 Malicious Indicators <p><small>All indicators are available only in the private subinterface or standalone version.</small></p>	Unusual Characteristics <ul style="list-style-type: none"> Imports suspicious APIs
	Informative 1 <ul style="list-style-type: none"> Network Related <ul style="list-style-type: none"> Found potential URL in binary/memory

Slika 3.5. Popis indikatora koje je pronašao Hybrid Analysis za zlonamjerni softver Infosec.Dexter

Klikom na indikator može se saznati više detalja o tome zašto i na koji način analizirana datoteka zadovoljava kriterij za određenu vrstu indikatora.

Za zlonamjerni softver Infosec.Dexter pronađeni su sljedeći zlonamjerni indikatori:

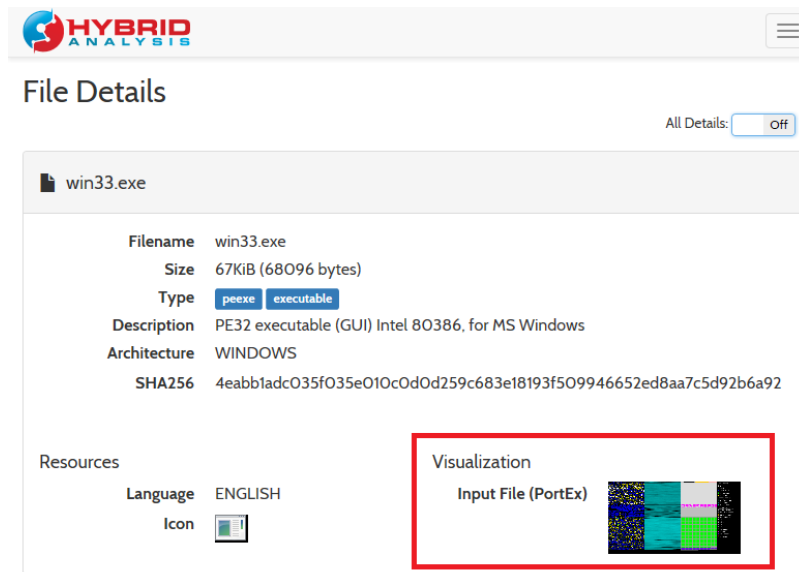
- Velik broj antivirusnih alata klasificirao ga je kao zlonamjernog
- Uzorak se podudara s YARA potpisom koji *Hybrid Analysis* ima u svojoj bazi kao potpis zlonamjernog softvera
- Zabilježene su neuobičajene karakteristike

Također, pronađeni su i sljedeći sumnjivi indikatori:

- neuobičajena entropija sekcija
- pronađena IP adresa u memoriji
- referenciranje na WMI/WMIC
- učitavanje sumnjivih API-ja

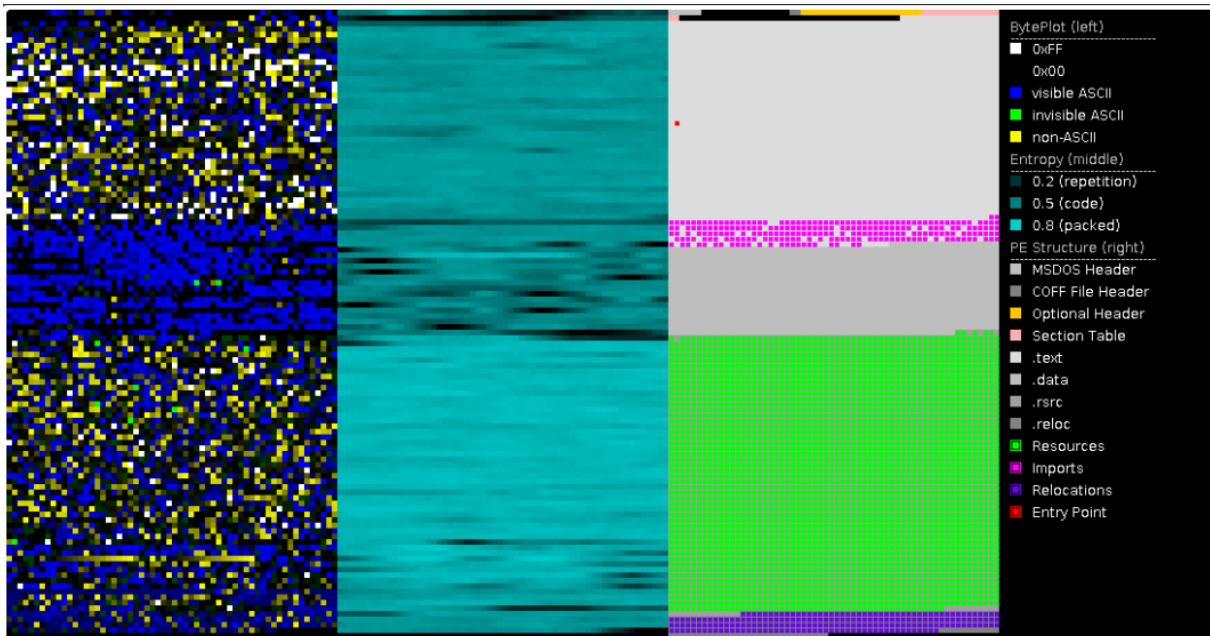
Vizualizacija sadržaja i strukture datoteke

Vizualizacija sadržaja i strukture datoteke može pomoći otkriti je li dio datoteke pakiran/kriptiran, što je uobičajeno za zlonamjerni softver koji na taj način pokušava sakriti zlonamjerni dio koda od antivirusnih alata. Vizualizaciju sadržaja moguće je pronaći u odjeljku *File Details* kao što je prikazano na slici 3.6.



3.6. Opcija vizualizacije datoteke

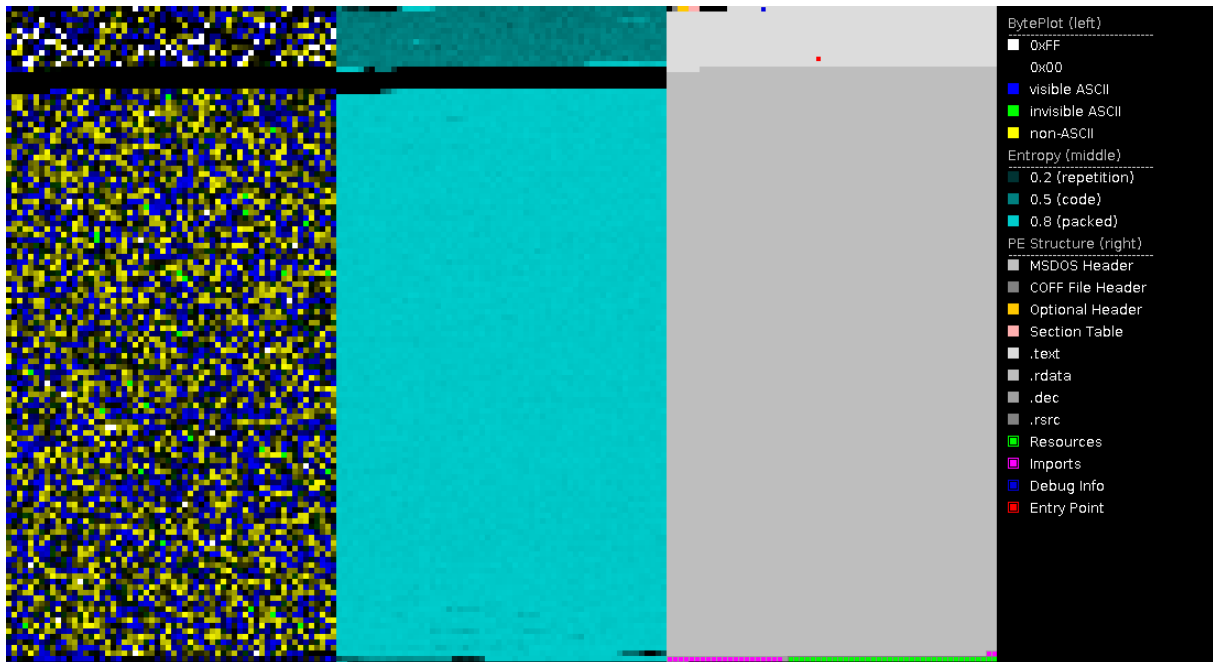
Vizualizacija analiziranog zlonamjernog softvera Dexter koju je generirao alat Hybrid Analysis prikazana je na slici 3.7. U ovom slučaju zlonamjerni softver nije pakiran – to je moguće naslutiti iz srednjeg stupca na slici koji prikazuje kako datoteka ne sadrži velike blokove podataka visoke entropije.



Slika 3.7. Vizualizacija zlonamjernog softvera Dexter

Na slici 3.8. prikazana je vizualizacija jednog drugog zlonamjernog softvera koji je pakiran – u ovom slučaju, na srednjem dijelu slike vidljivo je da se datoteka velikim

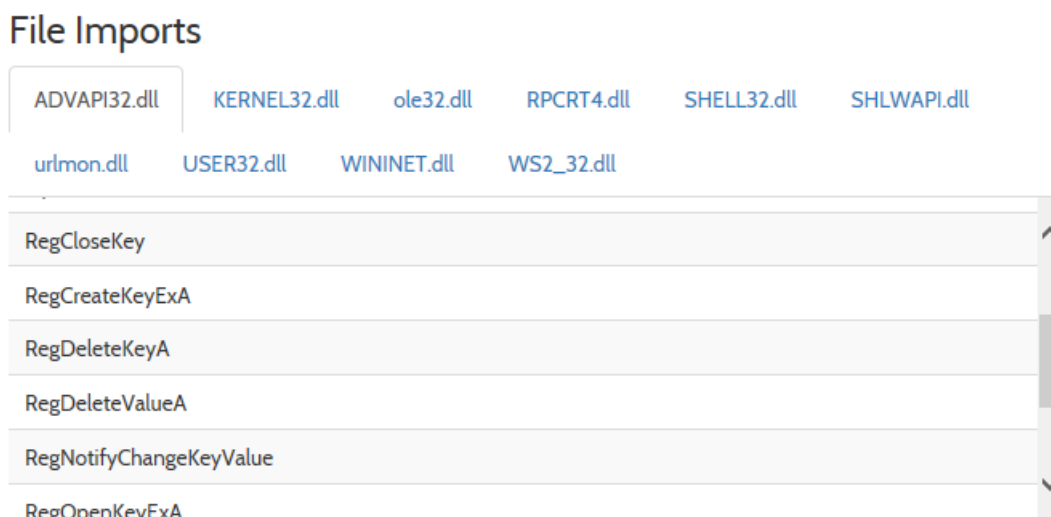
dijelom sastoji od podataka visoke entropije, tj. od naizgled nasumičnih podataka. Iz toga je moguće naslutiti da su ti podaci komprimirani i/ili šifrirani.



Slika 3.8. Vizualizacija jednog pakiranog zlonamjernog softvera

Uvezene biblioteke

Hybrid Analysis popisuje biblioteke (engl. *libraries*) koje analizirana datoteka uvozi (engl. *import*) i operacija koje one mogu obaviti. Na slici 3.9. popisane su biblioteke, a klikom na određenu biblioteku prikazuju se operacije koje ona omogućava – npr. biblioteka *ADVAPI32.dll*, između ostaloga, omogućava stvaranje i brisanje ključeva u *registryju*.



Slika 3.9. Popis uvezenih biblioteka i operacija koje one omogućavaju

Pronađeni znakovni nizovi

Hybrid Analysis izdvojiti će i pronađene znakovne nizove (engl. *strings*) prikazane na slici 3.10. Korisnik može pregledati sve pronađene znakovne nizove, ili samo one koje je alat

odredio kao „zanimljive“. Zanimljive u ovom slučaju znači da mogu ukazati na zlonamjerno ponašanje. Odabirom opcije za prikaz više detalja (*All Details*) pokazat će se i lokacije na kojima se određeni znakovni niz pojavljuje.

Extracted Strings

Search

All Details: Off

Download All Memory Strings (1.6KiB)

All Strings (400) Interesting (136)

!#\$%&()*+,-./0123

!p"6kC@%\$6

!This program cannot be run in DOS mode.\$

%s%s%s.exe

()*+,-./

(/clr) fXuncb*

.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

.exe;.bat;.reg;.vbs;

/w19218317418621031041543/gateway.php

O(O-080BOGORO\OpOzO

004080<0@ODOHOLOPOTOXO\O`OdOhOLOH1x1

1%1*151:1@1H1

3.10. Pronađeni znakovni nizovi

4 Zaključak

Iako su antivirusni alati, zajedno s redovitim ažuriranjem operacijskog sustava i aplikacija, u pravilu dovoljni za zaštitu korisnika od većine zlonamjernog softvera, razlozi zbog kojih je određena datoteka klasificirana kao zlonamjerna nisu uvijek prikazani korisniku.

Ponekada se nađemo u situaciji da neku datoteku antivirusni program nije klasificirao kao zlonamjernu, no svejedno ju ne želimo pokrenuti prije no što provjerimo o čemu je riječ. Ponekada se nađemo i u situaciji da naidemo na zlonamjerni softver, ali nas zanima detaljnije o kakvoj se prijetnji radi.

U takvim situacijama besplatni *online* alati poput *VirusTotal* i *Hybrid Analysis* mogu pomoći provjeriti je li datoteka zlonamjerna odnosno o kakvoj je točno prijetnji riječ.

Iako nisu jedini, *VirusTotal* i *Hybrid Analysis* su popularni, široko rasprostranjeni i često korišteni alati koji ne zahtijevaju nikakvu instalaciju, brzi su, pružaju informacije o ponašanju datoteke, s tim da se *VirusTotal* više oslanja na svoje partnere i rezultate njihove analize, a *Hybrid Analysis* na detaljniju dinamičku i statičku analizu.

Detaljniji popis postojećih alata za analizu zlonamjernog softvera koji funkcioniraju na sličan način kao *VirusTotal* i *Hybrid Analysis* dostupan je na [ovoj poveznici](#).