





CERT.hr

Sadržaj

UVOD	. 3
INSTALACIJA ALATA CRYPTOSEARCH	. 4
KORIŠTENJE ALATA CRYPTOSEARCH	.7
ZAKLJUČAK	10
	UVOD INSTALACIJA ALATA CRYPTOSEARCH KORIŠTENJE ALATA CRYPTOSEARCH ZAKLJUČAK

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

Porastom korištenja tehnologije u svakodnevnom životu porasla je i njena primjena u protuzakonite svrhe. Primjena tehnologije u kriminalne svrhe često uključuje i napade zlonamjernim softverom. Posebna i danas izrazito raširena vrsta zlonamjernog softvera je *ransomware*. To je ucjenjivačka vrsta programa koja obično prisilno šifrira datoteke na žrtvinom računalu te zatim traži otkupninu u zamjenu za dešifriranje.

U nekim slučajevima *ransomware* napada, moguće je dešifrirati datoteke bez plaćanja otkupnine. To je najčešće rezultat rada sigurnosnih stručnjaka koji na temelju analize određenog *ransomwarea* razviju alat za dešifriranje.

Čak i ako u trenutku napada ne postoji alat za dešifriranje datoteka, postoji mogućnost da će on biti razvijen u budućnosti. Upravo je iz tog razloga nakon *ransomware* napada korisno pohraniti šifrirane datoteke te ih potencijalno kasnije dešifrirati kada takav alat bude dostupan. Kako bi navedeni proces identifikacije i pohrane šifriranih datoteka bio lakši, razvijen je alat CryptoSearch.

CryptoSearch je alat koji omogućava automatsku identifikaciju te kopiranje ili premještanje datoteka šifriranih *ransomwareom*. Rad alata CryptoSearch temelji se na servisu <u>ID-Ransomware</u> koji omogućava identifikaciju *ransomwarea* korištenog za šifriranje datoteka putem raznih vrsta "potpisa". Baza potpisa koju koristi servis ID-Ransomware, pa time i alat CryptoSearch, redovito se ažurira s potpisima novootkrivenog *ransomwarea*.

2 Instalacija alata CryptoSearch

Alat CryptoSearch dostupan je za Windows operacijske sustave (Windows Vista i novije) te ga je moguće pokrenuti i na 32-bitnoj i 64-bitnoj inačici sustava. Rad s alatom i primjeri korištenja u ovom dokumentu bit će demonstrirani na operacijskom sustavu Windows 10, no postupak je analogan i za druge inačice operacijskog sustava. CryptoSearch je dostupan kao izvršna datoteka te ne zahtijeva instalaciju.

1. Za preuzimanje alata CryptoSearch potrebno je posjetiti <u>BleepingComputer Web</u> <u>stranice</u> i pritisnuti zelenu tipku *Download now* kao što je prikazano na slici 1.

🗄 🖅 🔳 Download Crypto	oSearcł 🗙 🕂 🗸					- 1	o x
\leftarrow \rightarrow \circlearrowright \land	A https://www.bleepingcomputer.com/dowr	nload/cryptosearch/		□ □ ☆	∱=	L	e
BLEEPING CON	1PUTER	f y & m	Q Search Site		LOGIN	SIGN	UP
NEWS - DOWNL	OADS - VIRUS REMOVAL GUIDES -	TUTORIALS -	DEALS -	FORUMS	MORE -	-	
Home > Downloads > Window	s > Security > Security Utilities > CryptoSearch			1	f 🗾 📴 i	n 👲 🔪	1
				SEARCH DO	OWNLOAD	os —	
				Enter key	words	Se	arch
Author:	DOWNLOAD NOW @BleepingComputer Michael Gillespie						
License:	Free						
Operating System:	Windows Vista/7/8/Windows 10 32-bit program. Can run on both a 32-	bit and 64-bit OS.		PLATFORM	IS		
File Size:	2.38 MBs			🐉 Winde	ows		
Downloads:	7,517			🍏 Mac			
Last Updated:	05/19/18 10:40:08 PM EDT			👌 Linux			
				WEEKLY DO	OWNLOAD	DS IN	

Slika 1: Preuzimanje alata CryptoSearch

CERT.hr

2. Nakon preuzimanja arhive potrebno je otpakirati (eng. *extract*) izvršnu datoteku na proizvoljnu lokaciju na računalu. To je moguće učiniti povlačenjem datoteke (eng. *drag and drop*) *CryptoSearch.exe* iz arhive u željeni direktorij kao što je prikazano na slici 2.



Slika 2: Raspakiravanje izvršne datoteke alata CryptoSearch



3. Pokretanje programa CryptoSearch sada je moguće dvostrukim klikom na ikonu alata nakon čega se otvara grafičko sučelje prikazano na slici 3 te time program postaje spreman za rad.

CryptoSea	rch			-	_		×
File About	t						
Search Option	ons						
Ransomv	ware: 4rw	/5w		~ ~	List F	iles	
O Extension	n:				List C	lean Fold	lers
⊖ Byte Patt	tem:) Start	() En	d
O Search D)irectory 🤇) Search Comp	outer			Search	
Retrieving dat Definitions sa Loaded data o	:a from ID F ved to: C:\\l on 499 rans	lansomware Jsers\ \D omwares	esktop \crypt	osearch-de	finition	s.bin	^
<						:	>
ldle							.:

Slika 3: Grafičko korisničko sučelje alata CryptoSearch

3 Korištenje alata CryptoSearch

Prilikom prvog korištenja alata CryptoSearch, računalo na kojem se koristi mora imati aktivnu vezu na internet zbog preuzimanja baze potpisa *ransomwarea*. Ako postoji veza prilikom budućih pokretanja programa, preuzet će se novi potpisi, a ako ne postoji, koristit će se prethodno preuzeti potpisi.

Pokretanjem programa CryptoSearch otvara se jednostavno grafičko sučelje koje nudi niz opcija za pretraživanje datoteka.

1. Ako je poznato kojim su *ransomwareom* datoteke šifrirane, moguće je izabrati pretraživanje po vrsti *ransomwarea* pritiskom na opciju *Ransomware* i odabirom naziva vrste iz padajućeg izbornika kao što je prikazano na slici 4.

Search Options Ransomware: 	Satan ~	🗹 List Files
O Extension:		List Clean Folders
O Byte Pattern:		Start O End

Slika 4: Pretraživanje po vrsti ransomwarea

2. Pretraživanje po nastavcima datoteka moguće je pritiskom na opciju *Extension* i upisivanjem željenog nastavka kao što je prikazano na slici 5.

Search Options		
O Ransomware:	Satan 🗸	🗹 List Files
Extension:	.mp4	List Clean Folders
O Byte Pattern:		● Start ○ End

Slika 5: Pretraživanje po ekstenzijama

Neki *ransomware* programi mijenjaju nastavke šifriranih datoteka u niz znakova karakterističan samo za taj program što može olakšati identifikaciju i pronalazak šifriranih datoteka. Također, ova opcija može se koristiti za pretragu pomoću uzorka u imenu datoteka (eng. *filename pattern*).



3. Pretraživanje po uzorku bajtova moguće je pritiskom na opciju *Byte Pattern* i upisivanjem željenog uzorka kao što je prikazano na slici 6. Opcije *Start* i *End* označavaju je li uzorak potrebno tražiti na početku ili kraju datoteke.



Slika 6: Pretraživanje po uzorku bajtova

Uzorak bajtova upisuje se kao niz heksadekadskih brojeva koji predstavlja niz bajtova na početku ili kraju datoteka. Neki od *ransomwarea* promijenit će zaglavlje ili podnožje tako da sve datoteke koje su njime šifrirane sadržavaju određeni uzorak bajtova.

Neovisno o odabranoj metodi pretraživanja postoji nekoliko opcija prikazanih na slici 7.

- 1. *List Files* ako je opcija označena ispisuju se šifrirane datoteke; inače se ispisuju samo direktoriji koji sadrže šifrirane datoteke
- 2. *List Clean Folders* ako je opcija označena ispisat će se i pretraženi direktoriji koji ne sadrže šifrirane datoteke
- 3. *Search Directory* pretraživanje određenog direktorija koji se može izabrati iz skočnog prozora
- 4. Search Computer pretraživanje cijelog računala

Search Options				
Ransomware:	Satan 🗸	🗹 List Files		
O Extension:	.mp4	List Clean Folders		
O Byte Pattern:	DEADBEEF	● Start ○ End		
O Search Director	y 💿 Search Computer	Search		

Slika 7: Dodatne opcije

Pritiskom na tipku *Search* započinje pretraga s odabranim parametrima. Nakon završetka pretraživanja CryptoSearch ispisuje rezultat: pronađene datoteke. Rezultat ovisi o prethodno opisanim opcijama te između ostaloga sadrži i broj direktorija koji sadrže šifrirane datoteke, broj šifriranih datoteka, broj pretraženih direktorija te broj provjerenih datoteka što je prikazano na slici 8.



Jednom kada je pretraživanje završeno, pritiskom na tipku *File* na navigacijskoj traci otvara se padajući izbornik koji nudi sljedeće opcije:

- 1. *Export List* mogućnost spremanja popisa pretraženih ili šifriranih datoteka u tekstualnu datoteku
- 2. *Archive* mogućnost kopiranja ili premještanja pretraženih ili šifriranih datoteka na novu lokaciju radi arhiviranja

CryptoSearch				\times		
File About						
Export List 🔹 🕨						
Archive 🕨	Encrypted Files		t Files			
Refresh Network	Clean Files		t Clean Fo	olders		
Load Definition File	() 9	art O F	nd		
Search Directory Search Computer Search						
Directory selected: C:\Test	Directory selected: C:\Test					
Searching for files encrypted by Satan						
Complete, found 0 encrypted folders with 0 encrypted files (0B) Also found 0 clean folders with 0 clean files (0B)						
<				>		
Search Complete .:						

Slika 8: Rezultati pretraživanja i *File* izbornik

Odabirom jedne od opcija moguće je zadati lokaciju na koju je potrebno pohraniti datoteke. Ako je izabrana opcija *Archive,* potrebno je definirati trebaju li se datoteke kopirati ili premjestiti. Odabirom opcije *No* datoteke će se kopirati, dok odabirom opcije *Yes* će biti premještene kao što je vidljivo na slici 9.



Slika 9: Kopiranje ili premještanje datoteka



4 Zaključak

Nakon *ransomware* napada, čak i ako u tom trenutku nije dostupan program za dešifriranje datoteka, postoji mogućnost da će takav program biti naknadno razvijen. Zato je korisno pohraniti šifrirane datoteke na sigurno mjesto u nadi da će ih kasnije biti moguće dešifrirati.

CryptoSearch automatizira postupak identifikacije i pohrane datoteka šifriranih *ransomwareom* te na taj način može olakšati i ubrzati navedeni proces. Kako se njegov rad temelji na servisu ID-Ransomware, potpisi koje koristi u svom radu bit će redovito ažurirani što ga čini korisnim kako za starije, tako i za nove i buduće *ransomware* programe. Iako je CryptoSearch suštinski jednostavan, on nudi jedinstven skup funkcionalnosti koristan u velikom broju situacija zaraze *ransomwareom*.