



Korisnik Windowsa 7 i Outlooka 2007 pokupio je *Locky Ransomware* nametnika. Ali nekim "čudom" ostale su mu netaknute *.ps*t (*Personal Storage Table*) datoteke, u koje korisnici spremaju poruke na svom računalu. Malo je misteriozno da *Locky* nije zahvatio *.pst* datoteke koje inače <u>prema popisu</u> [1] pronalazi i kriptira. Ponadali smo se povratku velike količine dokumenata iz arhivskih e-mail poruka, ali nije sve teklo glatko.



Nakon početnog oduševljenja korisnika i uvoza "preživjelih" arhiva na "svježe" instalirani sustav, počinje otkrivanje "nedostataka". Korisnik je očekivao da ćemo spasiti više sadržaja. Čini mu se da ima manje poruka, a nedostaju i "kontakti", sve ovo uzimamo s rezervom te objašnjavamo da je to cijela arhiva onog što je imao na prethodnom sustavu. Ne isključujemo mogućnost da je *Locky* nešto kriptirao ako se nalazilo van standardnih *Outlook* i arhivskih *.pst* datoteka. Korisnik se polako miri sa činjenicom da se nešto i ne može izvući. Međutim kako sistemac želi sve dodatno provjeriti, iako osobno nije korisnik *MS Outlook* klijenta, obavlja dodatne provjere.



Proučavajući MS dokumentaciju saznajemo da se sve vezano uz *MS Outlook, mail*, kalendar i kontakti nalazi u *.pst* datotekama. Nema izdvojenih datoteka koje sadrže imenik ili neke druge informacije. Iz iskustva s *Outlook Expressom,* kada smo prebacivali korisnike *Windowsa XP* na drugi mail klijent, imenici su se nalazili u *.wab* datotekama (*Windows Address Book*), izvan arhivskih *.dbx* datoteka. Po novom sve se nalazi unutar jedinstvene *.pst* datoteke koju korisnik smatra "nepotpunom". Odlučili smo u testnom okruženju napraviti pokus s korisnikovim *.pst* datotekama.

S korisnikovog računala smo spasili archive.pst i Outlook.pst datoteke.

$ ightarrow ~ \uparrow = >$ This F	PC > Local Disk (F:) > Outlook			~ Ö
^	Name	Date modified	Type	Size
P Quick access	🗋 ~last~.sharing.xml.obi	28.11.2016. 10:20	OBI File	2 KB
Desktop 🖈	archive	14.12.2016. 11:06	Microsoft Office Outlook Personal Folders	2.093.137 KB
👆 Downloads 🖈	extend.dat	16.7.2014. 6:40	DAT File	1 KB
😫 Documents 🖈	Outlook	13.12.2016. 14:11	Microsoft Office Outlook Personal Folders	3.882.705 KB
📰 Pictures 🛛 🖈	Outlook.sharing.xml.obi	28.11.2016. 10:25	OBI File	2 KB
ClanakAdrese				
Music				
Outlook				
Win10				
OneDrive				
Desktop				
Desktop				
Downloads				
Music				
Distures				
Pictures				
Videos				
Local Disk (C:)				
Local Disk (F:)				
Local Disk (G:)				

Sretna okolnost po korisnika je bila *Auto Archive* opcija koju standardno Outlook ima uključenu. U nekom trenutku korisnik se odlučio na ponuđenu opciju arhiviranja odgovoriti potvrdno i time pohraniti sve poslane poruke od 2012 do danas u archive.pst. *Auto Archive* opcija inače služi tome da se smanje inače nekad ogromne *.pst* datoteke, što email klijentu olakšava čitanje. Čak je, kaže, u jednom trenutku htio zbrisati te arhivirane poruke kao "nepotrebne". *Outlook.pst* sadžava ostatak novih mailova i adresar, kalendar ukoliko su korišteni.

Za testne potrebe napravimo *Outlook* profil bez e-mail računa.



Published on sys.portal (https://sysportal.carnet.hr)







Otvaranjem novog profila stvorena je "prazna" *Outlook.pst* datoteka u korisnikovim skrivenim direktorijima.

📙 🛃 📮 🗸 Outlook						-	×
File Home Share	View						~ 0
$\leftarrow \rightarrow \neg \uparrow \square$ > This	s PC > Local Disk (C:) > Users > user > App	Data > Local > Mic	osoft > Outlook		~ Õ	Search Outlook	Q,
Ouick access	Name	Date modified	Туре	Size			
	() Outlook	15.12.2016. 9:42	Microsoft Office	265 KB			
Desctop //	Outlook.sharing.xml.obi	15.12.2016. 9:42	OBI File	2 KB			
Downloads							
Documents #							
Music							
Music Outlack							
- Unidok							
Wie10							
- WIND							
a OneDrive							
This PC							
Desktop							
Documents							
Downloads							
Music							
E Pictures							
Videos							
Local Disk (C:)							
Network							
📲 Homearoup 👻							_
2 items 1 item selected 2	65 KB						1

Uvezimo *Outlook.pst* i *archive.pst* na način.

File --> Import and Export ... --> Import from another program or file --> Import a file --> Personal Folder File(.pst) --> Browse...

U našem slučaju arhivski *Outlook.pst* sa vanjskog diska F: uvozimo u *Personal folders*.



Published on sys.portal (https://sysportal.carnet.hr)





Backup i migriranje klijenata elektroničke pošte 1.dio Published on sys.portal (https://sysportal.carnet.hr)

😼 Outlook Today - Microsoft	Outlook				- 🗆 ×
Eile Edit View Go I	ools <u>A</u> ctions <u>H</u> elp	0 0 0 0 0			Type a question for help •
: Da Men . Ma Da searce	address books •	🛞 🗄 : 🕲 Dack 💿	🛛 🔄 🖬 🔍 outbolctoday		·
Mail «	🧐 Personal Fo	lders - Outlook To	day		
Favorite Folders 🔅		15. prosinca 2016.			Cystomize Outlook Today
Sent Items					
Mail Folders 🔅	Calendar		Tasks		Messages
All Mail Items					Inbox 0
Personal Folders		mport Personal Folders		×	Outbox 0
Deleted items			Select the folder to import from: Calendar Calendar Contacts Deleted Items Drafts Include subfolders Import items into the current folder Import items into the same folder in Personal Folders < Back Finish	Filter	
🖂 Mail					
Calendar					
S Contacts					
🟹 Tasks					
u 🖬 🖉 -					~
Done					

Isti postupak primjenimo za archive.pst i uvezemo podatke u Archive Folders.



Published on sys.portal (https://sysportal.carnet.hr)

😼 Outlook Today - Microsoft	Outlook		- 🗆 X
Eile Edit View Go Is	ols Actions Help		Type a question for help
🔂 New • 🌐 🛄 Search	address books 🔹 📦 📻 🥘 Back 🤅	🛛 🔄 🙆 😋 outlook:today -	
Mail «	🧐 Personal Folders - Outlook 1	oday	
Favorite Folders 🔅	(>>) 15. prosinca 2016		Customize Outlook Today
Sent Items	Colorday	Taska	Harran
Mail Folders 🙁	Calendar	12585	riessages
Al Mail Items +			Drafts 0
Personal Folders Poleted Items Dualts whox (1) whox (1) whox (2) whox (3) Coutbox PosS Feeds Sent Items Sent Items Sent Folders		Import Personal Folders Select the folder to inport from: Select the folders Calendar Calendar Seleted items Source terms	X Outbex 0
A 144			
Calendar			
Contacts			
💙 Tasks			
🖬 🖬 🗹 🔹			~
Done			

Na kraju uvoza sve poruke "slijepe" u jednu zajedničku listu e-mail poruka iako su uvezene kao posebne datoteke.

😼 Sent Items - Microsoft Out	tlook			– 🗆 X
Elle Edit View Go I	ools Actions Help			Type a question for help
🕞 New • 🤀 🦉 🗙 🛛	Beply 🕞 Reply to All 🔒 Forward	🔡 🏹 🔝 Search address books	· • • .	
Mail «	Sent Items		RE: FW: FW:	To-Do Bar » ×
Favorite Folders :	Search Sent Items	0 • X	A CONTRACTOR OF THE OWNER OF THE	prosinac 2016
Sent Items	Arranged By: Date	Newest on top 👻 🌥	Sent: det 24.11.2016 7:48	20 29 30 1 2 3 4
Mail Folders 🔅	E village	10.12.2012		5 6 7 8 9 10 11 12 13 14 15 16 17 18
All Mail Items 🔹	Ca tagetting	17.12.2012		19 20 21 22 23 24 25 26 27 28 29 30 31 1
Deleted Items	A 100	17.12.2012		2345678
Junk E-mail		17.12.2012		
RSS Feeds	Career and	17.12.2012		No upcoming appointments.
Search Folders	Carl Table Contraction of Contraction	17.12.2012 @ 0 \?		
	Ca tagétera:	17.12.2012		
	Real March 1	14.12.2012		Arranged By: Due Date A
	Ca tan Manu:	14.12.2012		There are no items to show in this view.
		14.12.2012		
		14.12.2012		
	Carl Name (1997)	14.12.2012	And the second	
📄 Mail	2	13.12.2012		
Calendar	Careful and the second	13.12.2012		
Contacts		12.12.2012	And the second	
📝 Tasks	A	12.12.2012	Seattle	
🖌 🖬 🖉 -	Company of the local division of the local d	• 40	Name and Address of the Address of t	
3505 Items				

Na lokaciji *Local Disk(C:)->Users->user->Appdata->Local->Microsoft->Outlook* se nalazi sad značajno veća *Outlook.pst* datoteka koja sadržava sve što smo uvezli s vanjskog diska na testni *MS*



Outlook profil.

📊 🛃 🚽 Vutlook						
File Home Share	View					
← → ~ ↑ 🔄 > This PC > Local Disk (C:) > Users > user > AppData > Local > Microsoft > Outlook						
^	Name	Date modified	Type	Size		
📌 Quick access	avtend dat	15 12 2016 0.59	DAT File	1 // 2		
🔜 Desktop 🛛 🖈	C Outlook	15.12.2016.10.51	Microsoft Office	2,539,537 KB		
🕂 Downloads 🖈	Outlook.sharing.xml.obi	15.12.2016. 9:42	OBI File	2 KB		
🗄 Documents 🖈						
📰 Pictures 🛛 🖈						
ClanakAdrese						
👌 Music						
Outlook						
Win10						
a OneDrive						
This PC						
Desktop						
Documents						
🕂 Downloads						
b Music						
E Pictures						
Videos						
Local Disk (C:)						
Local Disk (F:)						
Local Disk (G:)						
3 items 1 item selected 2,4	42 GB					

Provjeravamo Contacts, i dalje je prazan.



Published on sys.portal (https://sysportal.carnet.hr)

Scontacts - Microsoft Outle	ok	-		×				
Elle Edit View Go Tools Actions Help Type a question for he								
Se New + 🚓 🖄 X 🐁 + 🔢 ♥ 🔯 Search address books 🔹 💀 👷								
Contacts «	Search Contacts Search Contact	fts	ρ	• 8				
All Contact Items 🔹	There are no items to show in this view.			123				
My Contacts A								
S Contacts	Double-click here to create a new Contact.			b				
Current View 🔶				с.				
O Business Cards				d				
Address Cards				÷				
Detailed Address Cards Detailed Address Cards				9				
O By Category				h				
O By Company								
O By Location								
Outlook Data Files				k				
Add New Group				<u> </u>				
Customize Current View				-				
				P				
				9				
				•				
				5				
				t				
				U				
				¥				
				The second secon				
A Mail				Y				
				z				
Calendar								
Contacts								
📝 Tasks								
📃 🖬 🗹 🔹	4		Þ	80				
0 Items								

Pretpostavljamo da je uzrok nije *Locky Ransomware* nego "nešto drugo". Nudimo korisniku da iz postojećih poruka pokušamo izvući e-mail adrese svih koji su slali i primali njegove e-mail poruke. Pokušavamo se snaći sa nekim *MS Outlook* uputama da prikupimo adrese, uglavnom većina nudi izvoz adresa iz svih postojećih e-mail poruka uz komercijalne alate kao *free trial* opciju. Dopušteno je samo isprobati alat, za više trebalo bi kupiti softver. Imamo više iskustva sa *Thunderbird* email klijentom za kojeg postoje neke dodatne *free* ekstenzije za koje mislimo da mogu odraditi ono što bi htjeli.

Prebacivanju MS Outlook arhiva u Thunderbird mail klijent opisati ćemo u slijedećem članku. [2]

uto, 2017-01-24 09:02 - Goran Šljivić**Kuharice:** <u>Windows</u> [3] Kategorije: <u>sys.kuharica</u> [4] Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1720



- [1] http://www.enigmasoftware.com/lockyfileextensionransomware-removal/
- [2] https://sysportal.carnet.hr/node/1721
- [3] https://sysportal.carnet.hr/taxonomy/term/18
- [4] https://sysportal.carnet.hr/taxonomy/term/69