



بسمه تعالى

مرکز تخصصی آپا دانشگاه رازی گزارش میدهد



راهکارهای مقابله و پیشگیری از باجافزار BTCWare PayDay

گروه خبری:

مقالات آموزشى

نسخهی کامل خبر





## چگونه متوجه شویم سیستم ما توسط باجافزار PayDay آلوده شده است؟

هنگامی که باجافزار BTCWare کامپیوتر شما را آلوده می کند تمام درایوهای شما را جهت یافتن فایلهای مورد هدف اسکن می نماید، آنها را رمز نموده و سپس پسوند PayDay را به آنها اضافه می کند. زمانی که فایلها رمز گذاری شدند دیگر توسط برنامههای معمولی باز نخواهند شد.

پیغامی که پس از رمز شدن فایلها به شما نشان داده می شود شامل دستورالعمل نحوهی اتصال به سرویس رمزگشایی است، جایی که شما می توانید بفهمید چه اتفاقی برای فایل های شما افتاده و اینکه چگونه باید باج را پرداخت نمایید تا فایل های شما رمزگشایی شوند.

## آیا امکان رمزگشایی فایلهای رمز شده با پسوند PayDay.\*وجود دارد؟

خیر، اکنون امکان بازیابی فایلهای رمز شده با پسوند PayDay. وجود ندارد!

باجافزار BTCWare PayDay و BTCWare می کند\_ برای اینکه مطمئن شود کاربر هیچ راهی جز پرداخت از شیوه رمزنگاری AES-265 و RSA استفاده می کند\_ برای اینکه مطمئن شود کاربر هیچ راهی جز پرداخت باج و خرید کلید خصوصی ندارد. کلید عمومی RSA تنها با کلید خصوصی مربوطه رمزگشایی می گردد. از آنجا که کلید AES با استفاده از رمزنگاری RSA مخفی شده است و کلید خصوصی RSA در دسترس نیست، رمزگشایی فایلها آنطور که گفته شده میسر نیست.

با توجه به مدت زمانی که برای شکستن کلید رمزنگاری AES مورد نیاز است، ادعای Brute force نمودن کلید رمزگشایی واقعبینانه نیست. متأسفانه زمانی که کار رمز نمودن دادهها توسط BTCWare PayDay به پایان رسید، دیگر رمزگشایی بدون پرداخت باج امکانپذیر نخواهد بود. از آنجا که کلید خصوصی مورد نیاز برای باز کردن فایلهای رمز شده تنها از طریق مجرمان سایبری امکانپذیر است، ممکن است قربانیان وسوسه شده و بخواهند با پرداخت باج مورد نظر، کلید را خریداری نمایند. با این وجود، انجام این کار ممکن است افراد سودجو





را به ادامهی این عمل و حتی افزایش مبلغ درخواستی تشویق نماید. توصیهی ما این است که شما هیچ پولی به این مجرمان سایبری پرداخت نکنید، و در عوض به آژانس اجرای قانون در کشور خود (پلیس فتا در ایران) این حمله را گزارش دهید.

نحوه حذف باجافزار PayDay



توجه داشته باشید که طی فرآیند حذف باجافزار خطر از دست دادن فایلها وجود دارد، ما نمیتوانیم تضمین کنیم که فایلهای شما قطعاً بازیابی خواهند شد. علاوه بر این، هنگام حذف باجافزار یا تلاش برای بازیابی فایلهای رمز شده این فایلها ممکن است برای همیشه تسخیر شوند.

این مطلب یک راهنمای جامع است که باجافزار BTCWare PayDay را از کامپیوتر شما حذف می کند، با این وجود ما نمی توانیم تضمین کنیم که فایل های شما بازیابی خواهند شد. ما مسئولیت حذف اسناد و فایل های شخصی شما را طی فرآیند حذف باجافزار به عهده نخواهیم گرفت.

برنامههای Malwarebytes و HitmanPro میتوانند این آلودگی را شناسایی و حذف کنند اما نمیتوانند فایلهای رمز شدهی شما را بازگردانند.

گام اول: استفاده از Malwarebytes برای حذف باجافزار BTCWare PayDay

برنامهی ضدبدافزار Malwarebytes یک اسکنر قدرتمند مبتنی بر درخواست است که PayDay را از دستگاه شما حذف خواهد نمود. توجه داشته باشید که این برنامهی ضدبدافزار میتواند همراه با آنتیویروس بر روی سیستم، بدون هیچ تداخلی، اجرا شود.

شما می توانید ضدبدافزار Malwarebytes را از لینک زیر دانلود نمایید:

https://www.malwarebytes.com/mwb-download





۲. پس از دانلود، تمامی برنامههای خود را ببندید، سپس بر روی آیکون موجود بر روی دسکتاپ خود به
 نام " mbam-setup " دابل کلیک کنید تا نصب آغاز گردد.



ممکن است هنگام نصب با پیغام User Account Control به صورت زیر مواجه گردید که از شما می پرسد

آیا می خواهید این فایل اجرا شود یا خیر، اگر این اتفاق افتاد باید بر روی "Yes " کلیک کنید تا نصب ادامه یابد.

User Account Control		>
Do you want to allow th changes to your device	nis app to make ?	
Malwarebytes		
Verified publisher: Malwarebyte	es Corporation	
File origin. Hard drive on this c	omputer	
Show more details		
Show more details Yes	No	÷

۳. زمانی که نصب آغاز شد، صفحه ی نصب ضدبدافزار Malwarebytes را خواهید دید که شما را از طریق

فرآیند نصب راهنمایی خواهد نمود.







جهت نصب ضدبدافزار Malwarebytes بر روی سیستم دستورات زیر را با کلیک بر روی "Next" دنبال کنید.



۴. پس از نصب، Malwarebytes به طور خودکار شروع به کار کرده و پایگاه دادهی آنتیویروس را آپدیت

خواهد کرد. جهت آغاز اسکن سیستم، میتوانید بر روی دکمهی "Scan Now" کلیک کنید.





Halwarebytes   TRIAL	Activate License Upgrade New
Or Daahbinand	Real-Time Protection       Image: Comparison of the protection: On         Image: Web protection: On       Image: Comparison of the protection: On         Image: Mail and the protection: On       Image: Comparison of the protection: On         Image: Comparison of the protection: On       Image: Comparison of the protection: On
Settings Awesome! You're protected.	Scan Status III III C ( Last Scan: None Next scheduled scan: 12/9/16 2:00 AM Updates: Current
Your premium trial ends in 13 days Upgrade Now	Protection History Tems scanned: 0 Scan detectors: 0 Real-Time detectors: 390
Upgrade Now Scan Now	Terro scanned: 0 Scan detections: 0 Real-Time detections: 390

۵. با کلیک بر روی دکمهی "Scan Now" ضدبدافزار شروع به اسکن کرده و کامپیوتر شما را برای یافتن بدافزار Malwarebytes
 ۱۰۰ بدافزار BTCWare PayDay. اسکن خواهد نمود. زمانی که ضدبدافزار Malwarebytes در حال اسکن است صفحهای مانند تصویر زیر نشان داده خواهد شد.

Malware	DYTES I TRIAL				Activa	te License	Upgradil Now
Dashboard	Threat Scan						
🎯 scan	0	0	0	0	0	0	0
🛞 Quarantine	Check for Updates	Pre-Scan Operations	Scan Memory	Scan Startup Files	Scan Registry	Scan File System	Heuristics Analysis
Reports	the second call and the						
() Settings	Currently Scanning: Items Scanned: Time Ebosed:	Heuristics Ana 274,282	lysia				
	Threats Identified:	© 8					
	View Identified T	hreats				Pause	Cancel

۶. زمانی که اسکن به پایان رسید، شما با صفحهای مطابق تصویر زیر که نشان دهنده ی آلود گیهای بدافزاری
 (آلود گی ناشی از باجافزار PayDay) شناسایی شده توسط این ضدبدافزار است مواجه خواهید شد.





به منظور حذف برنامههای مخربی که توسط این برنامه یافت شده است، بر روی دکمهی " Remove " کلیک نمایید. Selected" کلیک نمایید.

Malware	bytes	TRIA			Active	te License Opgrade Nov
Dashboard	Thre	at Sca	n Results: 58 of 58 ider	ntified threats a	re selected	
🎯 50m	To quar Cancel	More info	selected threats, click Quarantine Se rmation	elected if you don't we	nt to quarantine (	any of the detected threats, click
🛞 Quarantine	20	500	Threat Type Patentially Unwanted Program	Threat PUP.Optional.R	Object Type File	Location C/USERS/MALWARETIPS/
Reports	12	0	Potentially Universed Program	PUP.Optional.Y	File	CIV/SERSIMALWARETIPS\
	1	0	Patentially Unwanted Program	PUP.Opsional.Y	File	C:UROGRAMDATAINTUS
203 Settings		0	Potentially Linwarted Program	PUP.Optional.Y	File	CIWINDOWS/SYSTEM32
	1	0	Potentially Unwanted Program	PUP.Optional.D	Registry K.,	HKLMISOFTWAREWOW6
	1	8	Malware	Rogue.ForcedE	File	C:UUSERSUMALWARETUPSU
		$\otimes$	Malware	Rogue.ForcedE	File	C:\Users\MelwareTips\Ap
		8	Malware	Rogue.ForcedE	File	C:/Users'iMalwareTips'Ap
		$\otimes$	Malware	Rogue.ForcedE	File	CiVUsers'iMalwareTips'Ap
	1	8	Mahvare	Rogue.ForcedE	File	C:\Users\MalwareTips\Ap
	1	8	Malware	Rogue.ForcedE	File	CiUsersiMalwareTipsiAp

ضدبدافزار Malwarebytes اکنون تمامی فایلهای مخرب و کلیدهای رجیستری را که یافته است قرنطینه می کند. هنگام حذف فایلها، ضدبدافزار ممکن است جهت حذف برخی از فایلها نیاز به راهاندازی مجدد داشته باشد. بنابراین اگر پیغامی در خصوص ریستارت کردن سیستم به شما نشان داده شد اجازهی این









پس از اینکه سیستم ریستارت شد، شما باید ضدبدافزار Malwarebytes را باز کرده و مجدداً اسکن را

بزنید تا مطمئن شوید خطری سیستم شما را تهدید نمی کند.

گام دوم: با HitmanPro سیستم خود را دوباره بررسی نمایید

HitmanPro بدافزارها، ابزارهای تبلیغاتی مزاحم، باتها و سایر تهدیدات را یافته و آنها را حذف مینماید، در حدی که حتی ممکن است بهترین آنتیویروسها را نیز از بین ببرد. این برنامه برای اجرا در کنار آنتیویروسها، فایروالها و دیگر برنامههای امنیتی طراحی شده است.

۱. می توانید HitmanPro را از لینک زیر دانلود نمایید:

https://www.hitmanpro.com/en-us/hmp.aspx

۲. بر روی فایل به نام "HitmanPro.exe" (برای نسخههای ۳۲ بیتی ویندوز) یا " (برای نسخههای ۶۴ بیتی ویندوز) دابل کلیک کنید. (برای نسخههای ۶۴ بیتی ویندوز) دابل کلیک کنید.



برای نصب HitmanPro بر روی کامپیوتر، روی دکمهی "Next" کلیک کنید.







۳. اکنون HitmanPro شروع به اسکن سیستم شما، جهت یافتن بدافزارها خواهد نمود.

C:\WINDOW\$\system32\sfc.dll		
Service_KMS.exe EBB0 British C:\Program Files\KMSpico\	😵 Malware ූෆ	Delete 🛨 🔺
cvsmon32.exe E00 E01 C\Program Files (x86)\Software Guardian\	😵 Trojan	Delete 🕶
gcpum.dll C:\Users\MalwareTips\AppData\Local\Temp\is-9EIFB.tmp\	😵 Riskware	Delete 🕶
InoDII.dll C-\Users\MalwareTips\AppData\Local\Temp\is-0JKOJ.tmp\	😵 Trojan	Quarantine 👻
gcpum.dll C:\Users\MalwareTips\AppData\Locaf\Temp\is-0JKOJ.tmp\	😵 Riskware	Delete 🕶
1.exe C:\Users\MalwareTips\Desktop\Malware\	😵 Riskware	Delete 🕶
InoDII.dll C:\Users\MalwareTips\AppData\Local\Temp\is-9EIFB.tmp\	😵 Trojan	Quarantine 👻
5.exe C:\Users\MalwareTips\Desktop\Malware\	😵 Trojan	Delete 🛩
32.exe Chiltersi MalwareTinci Deskton Malwaret	😵 Riskware	Delete 🕶 🗸
dentified Threats: 24 (Traces: 51)		46 ltem





۴. زمانی که اسکن به پایان رسید، مطابق تصویر زیر لیستی از تمام بدافزارهایی که برنامه شناسایی

کرده به شما نشان داده خواهد شد. برای حذف بدافزار بر روی دکمهی "Next" کلیک کنید.

Scan results Malicious software was detected. Close all applications and click renain programs may terminate unexpectedly.	Next to remove the malicious so	Im oftware. During removal,	28
Service_KMS.exe IIIII Enter C:/Program Files/KMSpico/	😵 Malware	Delete 🕈	^
cvsmon32.exe and and C:\Program Files (x86)\Software Guardian\	😵 Trojan	Delete 🕶	
gcpum.dll C:\Users\MalwareTips\AppData\Local\Temp\Is-9EIFB.tmp\	😵 Riskware	Delete 🕶	
InoDil.dll C:\Users\MalwareTips\AppData\Local\Temp\is-03KOJ.tmp\	😵 Trojan	Quarantine 👻	
gcpum.dll C\Users\MalwareTips\AppData\Local\Temp\is-0IKQJ.tmp\	😵 Riskware	Delete 🛩	
1,exe C:\Users\MalwareTips\Desktop\Malware\	😵 Riskware	Delete 👻	
InoDII.dll Ci\Users\MalwareTips\AppData\Local\Temp\\s-9EIFB.tmp\	😵 Trojan	Quarantine 👻	
5.exe C:\Users\MalwareTips\Desktop\Malware\	😵 Trojan	Delete 👻	
32.exe CVI (sets) MahwateTips) Desktop) Mahwate)	😵 Riskware	Deleté 💌	•
dentified Threats: 107 (Traces: 138)		133 it.	m

۵. برای اینکه برنامه به مدت ۳۰ روز به صورت آزمایشی فعال شود بر روی دکمهی " Activate free

license" کلیک کنید، و تمامی فایلهای مخرب را از سیستم خود حذف کنید.

Product Activation				
Activate your copy of Hi	tmanPro to remove malicious software.			
Please enter the product XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	key that you received when you purchased HitmanPro ir XXXXX. Activation will register the product key to this com	n the field below in fo puter.	rmat	
Product Key:		Activa	te	
	I do not have a product key			
This one-time lic	encense ense is valid for thirty days			
This one-time lic	tense is valid for thirty days			
This one-time lic	t activated.			
This one-time lic	t activated.			





### گام سوم: بازگردانی فایلهای رمز شده توسط BTCWare PayDay با نرمافزارهای بازیابی

#### روش اول: بازگردانی فایلهای رمز شده توسط BTCWare PayDay با BTCWare ا

BTCWare PayDay تلاش می کند تمام کپی های Shadow را زمانی که شما برای اولین بار پس از آلوده

شدن، هرگونه فایل اجرایی را باز می کنید حذف نماید. خوشبختانه، این آلودگی همیشه قادر به حذف کردن

کپیهای Shadow نیست، بنابراین شما باید سعی کنید فایلهای خود را با استفاده از این روش بازگردانید.

۱. شما میتوانید ShadowExplorer از لینک زیر دانلود نمایید:

http://www.shadowexplorer.com/downloads.html

۲. زمانی که ShadowExplorer را دانلود و نصب کردید، می توانید با دنبال کردن ویدئوی راهنمایی که در

لینک زیر آمده است نحوهی بازگردانی فایلهای رمز شده را با استفاده از این روش ببینید:

https://www.youtube.com/watch?v=oaXtQ6rbvxA

روش دوم: بازگردانی فایلهای رمز شده توسط BTCWare PayDay از طریق نرمافزار بازگردانی فایل Recuva

هنگامی که فایلها توسط BTCWare PayDay. رمز شدند، باجافزار ابتدا یک کپی از فایلها ایجاد می کند، کپی را رمز کرده و سپس فایلهای اصلی را پاک می کند. بنابراین شما می توانید از نرمافزارهای باز گردانی فایل مانند Recuva استفاده کنید.

می توانید با دنبال کردن ویدئوی راهنمایی که در لینک زیر آمده است نحوه باز گردانی فایل های رمز شده را با استفاده از Recuva ببینید:

https://www.youtube.com/watch?v=LeEICG0zWqY





# چگونه از آلوده شدن کامپیوتر خود توسط این باجافزار جلوگیری کنیم؟

به منظور حفاظت از سیستم در مقابل باجافزار BTCWare PayDay همیشه باید یک آنتیویروس بر روی سیستم نصب داشته باشید و نیز همیشه از فایلهای شخصی خود بکآپ بگیرید. روش حفاظتی دیگر این است که از برنامهای به نام HitmanPro.Alert استفاده کنید که از اجرای هر گونه بدافزار رمزکنندهی فایل جلوگیری میکند.

در ویدئویی که در لینک زیر آمده است نحوهی نصب و کار با این برنامه توضیح داده شده است:

https://www.youtube.com/watch?v=XrSP-CMjuFk

منبع:

https://malwaretips.com/blogs/remove-btcware-payday-ransomware/#prevent