

Scam Email

دانشگاه فردوسی مشهد

مرکز فناوری اطلاعات و ارتباطات دانشگاه

بهار 1398

Scam چیست؟

Scam به فعالیت های غیرقانونی در سطح اینترنت گفته می شود که به منجر به کلاهبرداری از افراد و کاربران می شود. Scamها اشکال مختلفی در دنیای دیجیتال دارند و اگر کاربران به آنها توجه نکنند می تواند منجر به خساراتی مانند دزدیدن پول و یا از دست دادن اطلاعات شخصی افراد شود. فرستندگان Scam از تلفن، ایمیل، پیامک و خدمات پستی برای برای تماس با مردم استفاده می کنند.

نمونه ای از ایمیل Scam با موضوع "این حساب کاربری آلوده شده است."

این نمونه ای از ایمیل Scam است که با عنوان "آلوده شدن حساب کاربری" برای شناسه های مختلف ارسال می شود و Scammer ها امیدوارند که بتوانند از این طریق افراد را فریب دهند. این ایمیل در واقع ادعا می کند که از قربانی خود یک سری تصاویر ضبط شده تهیه کرده که در صورت عدم پرداخت مبلغ خاصی آنها را انتشار می دهند.



همانطور که در متن این نامه ملاحظه می کنید، طراح این کلاهبرداری خود را به عنوان یک هکر معرفی می کند که ظاهرا ایمیل کاربر را هک کرده است. این کلاهبردار ادعا می کند که او یک برنامه مخرب را در سیستم عامل نصب کرده است که وب کم هک شده و از صفحه اسکرین فرد قربانی در حال بازدید از یک وب سایت پورنوگرافی فیلم گرفته است. این نرم افزار مخرب که یک Keylogger است قادر به نظارت بر فعالیت های کامپیوتری کاربران و ضبط فیلم ها با استفاده از وب کم کامپیوتر می باشد. این برنامه همچنین میتواند، رمزهای عبور مختلف را سرقت کند. نکته اصلی این ایمیل این است با فریب دادن مردم به اعتقاد بر این که فیلمی از آنها ضبط شده است، مورد استفاده قرار میدهد. کلاهبردار ادعا میکند که یک ویدیویی تهیه کرده است که فرد قربانی و ویدیویی که او تماشا می کند، به طور همزمان دیده شوند. این مهاجمان تهدید میکنند که این فیلم را به تمام مخاطبین فرد قربانی ارسال خواهند کرد، مگر اینکه در عرض 48 ساعت (1000 دلار) در Bitcoins دریافت کنند و در نامه نیز یک آدرس یولی Bitcoin ارائه کردهاند.

نکته ای که باید مورد توجه قرار دهید این است که این گونه ایمیلها را نادیده بگیرید. هیچ یک از ادعاهایی که Scammer بیان کرده است، قابل اعتماد نیست. سیستم شما با نرم افزارهای مخرب آلوده نشده و شناسه ایمیل نیز هک نشده است.

	خلاصه از تهدید
این شناسه ایمیل آلوده شده است	نام يا عنوان
فیشینگ، کلاهبرداری، مهندسی اجتماعی، تقلب	نوع تهديد
خرید های آنلاین غیر مجاز، گذرواژه های حساب کاربری	علائم
آنلاین، سرقت هویت، دسترسی غیر قانونی از رایانه شخصی	
ايميل هاي فريبنده، تبليغات پاپ آپ آنلاين، موتورهاي	روش های توزیع
جستجوگر مسموم، دامنه های اشتباه گرفته شده	
از دست دادن اطلاعات خصوصی حساس، از دست دادن پول،	خسارت
سرقت هويت.	
برای از بین بردن عواقب احتمالی نرمافزار مخرب، اسکن کردن	روش حذف
سیستم با Spyhunter توصیه می شود.	

فایل های اجرا شده (exe.) و غیره هستند. هدف اصلی این ایمیل ها این است که افراد را فریب دهد تا فایل پیوست را باز کنند. هنگام باز شدن، برنامه های مخربی را دانلود و نصب می کنند. این برنامه های مخرب برای سرقت اطلاعات شخصی، اطلاعات مربوط به مرور گر، انتشار ویروس ها و انجام اقدامات دیگر است که می تواند منجر به از دست رفتن اطلاعات، مسائل مربوط به حریم خصوصی و سایر مشکلات شود.

جلوگیری از نصب نرم افزارهای مخرب یا malware چگونه است؟

هر ایمیل را به دقت بررسی کنید، به خصوص اگر آن ایمیل حاوی پیوست یا لینک باشد. این ایمیل ها معمولا با عنوان رسمی و قانونی ارائه می شوند اما اغلب بی اهمیتند. اگر یک ایمیل به نظر مشکوک یا از یک آدرس ناشناس دریافت کردید، آن را باز نکنید. علاوه بر این، نرم افزارها را از منابع معتبر دانلود نمایید. برای حفظ امنیت رایانه، نرم افزار آنتی ویروس معتبر بر روی سیستم نصب شده و همیشه فعال باشد.

حذف برنامه های مخرب برای جلوگیری از عواقب احتمالی

حذف دستی بدافزارهای ممکن است یک روند طولانی و پیچیده باشد که نیاز به مهارت های پیشرفته کامپیوتری دارد. Spyhunter یک ابزار حرفه ای حذف نرم افزارهای مخرب است که برای از بین بردن برنامه های مخرب توصیه می شود و دانلود آن را از طریق لینک زیر امکان پذیر است: https://www.pcrisk.com/download-spyhunter-5

نحوه حذف نرم افزارهای مخرب چگونه است؟

.برای حذف بدافزارها استفاده از Spyhunter توصیه می شود. اگر می خواهید بدافزار را به صورت دستی حذف کنید، اولین گام این است که نام نرم افزارهای مخرب را که می خواهید حذف کنید شناسایی کنید .در ادامه یک مثال از یک برنامه مشکوک در حال اجرا بر روی یک کامپیوتر کاربر آمده است:

Pr	ocesses Perfor	mance	App history	Startup	Users	Details	Services			
		^			4%	34	4%	0%	0%	
Na	me				CPU	Men	nory	Disk	Network	
	Microsoft	Window	vs Search Prot		0%	0,1	мв	0 MB/s	0 Mbps	
	Parallels C	oheren	ce service		0%	0,1	мв	0 MB/s	0 Mbps	
>	Parallels C	oheren	ce service		0%	0,1	мв	0 MB/s	0 Mbps	
	Parallels C	oheren	ce service (32		0%	0,2	мв	0 MB/s	0 Mbps	
	🍓 Parallels C	Control (Center		0%	2,1	мв	0 MB/s	0 Mbps	- 1
	Parallels T	ools			0%	1,1	мв	0 MB/s	0 Mbps	
>	Parallels T	ools Ser	vice		0%	0,3	мв	0 MB/s	0 Mbps	
>	🔳 Runtime I	Broker			0%	1,7	мв	0 MB/s	0 Mbps	- 1
	Runtime I	Broker			0%	2,4	мв	0 MB/s	0 Mbps	
>	🥪 Spooler S	ubSyste	m App		0%	0	мв	0 MB/s	0 Mbps	
	🏂 trickbot-ti	rojan-sa	mple (32 bit)		0%	0,4	мв	0 MB/s	0 Mbps	
	Usermode	Font D	river Host		0%	0,5	мв	0 MB/s	0 Mbps	
	🔳 Usermode	e Font D	river Host		0%	0	мв	0 MB/s	0 Mbps	
	Windows	Audio D	evice Graph Is		0%	0,3	мв	0 MB/s	0 Mbps	
	Windows	Defende	er notification		0%	0,1	мв	0 MB/s	0 Mbps	
	Windows	Defend	or ConortCoroou		0%	0	MR	O MR/c	0 Mhos	

با استفاده از Task Manager لیست برنامه های در حال اجرا بر روی رایانه خود را چک کنید، سپس مراحل زیر را ادامه دهید:

مرحله 1:

دانلود برنامهای با نام Autoruns این برنامه، لیست تمام برنامه های نصب شده در سیستم و رجیستری را نشان می دهد :

(https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns (لینک نرم افزار

Filter:				_			
Codecs 🔄 Boot Execute	e 📑 Image Hijac	ks 🖄 AppInit	MownDLLs	Winlogon	🧠 Win:	sock Pr	oviders
la Print Monitors	A Providers	Network Providers	imw 📷	R Sidebar	Gadgets	J	Office
🖅 Everything 🛛 😹 Logon	🚼 Explorer	进 Internet Explore	r 🛛 🙆 Scheduled	Tasks	Services	3	Drivers
utorun Entry Wicrosoft/Windows\ Wicrosoft/Windows\ Wicrosoft/Windows\ Wicrosoft/Windows\ Wicrosoft/Windows\ Wicrosoft/Windows\ Wicrosoft/Windows\ Wicrosoft/Windows\ Wicrosoft/Windows\ Wicrosoft/Windows\ Wicrosoft/Windows\ Wicrosoft/Windows\ Wicrosoft/Windows\	Description Windows host pr Microsoft Malwar Microsoft Malwar Microsoft Malwar Microsoft Malwar Windows host pr Windows Media Standalone Upda	Publisher Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor	Image Path c:\windows\syste c:\program files\w c:\program files\w c:\program files\w c:\program files\w c:\windows\syste c:\program files\w c:\users\tomas\a	Timestamp 02/04/32 05:: 25/11/12 13:: 25/11/12 13:: 25/11/12 13:: 25/11/12 13:: 02/04/32 05:: 23/07/18 20:: 01/06/18 17:- 02/04/15 14:1	Virus 35 39 39 39 39 39 35 28 40	Total	
KI M/System/CurrentControl	Set\Services		c.iusersitomasia	13/06/18 14.0	03		
	Google Update S Google Update S Mozilla Maintena OpenVPN Servic Parallels Cohere Parallels Tools S Windows Defend Service KMSELD	Google Inc. Google Inc. Mozilla Foundation The OpenVPN Pr Parallels Internati Parallels Internati Microsoft Corpor @ByELDI	c:\program files (c:\program files (c:\program files (c:\program files (c:\program files (c:\program files (c:\program files\w c:\program files\k	17/06/15 01:4 17/06/15 01:4 05/06/18 21:3 07/08/14 13:4 20/05/18 22:5 20/05/18 22:5 20/05/18 22:5 20/09/28 03:3 22/07/15 04:5	46 46 24 10 09 21 32	7	>

مرحله 2: کامپیوتر خود را در حالت Safe Mode راه اندازی مجدد کنید.

Advanced Boot Options

Choose Advanced Options for: Windows 7 (Use the arrow keys to highlight your choice.)

Repair Your Computer

Safe Mode

Safe Mode with Networking Safe Mode with Command Prompt

Enable Boot Logging Enable low-resolution video (640x480) Last Known Good Configuration (advanced) Directory Services Restore Mode Debugging Mode Disable automatic restart on system failure Disable Driver Signature Enforcement

Start Windows Normally

کاربران ویندوز XP و ویندوز 7:

کامپیوتر خود را در حالت Safe Mode راهاندازی کنید. سپس مجدد سیستم را Restart کنید. در طول فرایند شروع به کار کامپیوتر خود، کلید F8 را بر روی صفحه کلید خود چند بار فشار دهید تا منویWindows فرایند شروع به کار کامپیوتر خود، کنید و در نهایت Safe Mode with Networking را از لیست انتخاب نمایید.

کاربران ويندوز 8:

سیستم را در حالت Safe Mode راهاندازی نمایید. از منوی Settings گزینه Advanced startup options را انتخاب نمایید. در پنجره "General PC Settings" باز شده، "Advanced startup" را انتخاب کنید. روی دکمه "Restart now" کلیک کنید .در حال حاضر رایانه شما به حالت "Advanced Startup options menu" راه اندازی مجدد خواهد شد .روی دکمه "Troubleshoot" کلیک کنید و سپس دکمه "Advanced options" را انتخاب کنید .در صفحه option و تب «Startup settings» رفته و سیستم را انتخاب کنید . کنید.سیستم شما به صفحه تنظیمات راه اندازی مجدد خواهد رفت. دکمه "F5 را بزنید تا سیستم در حالت امن با شبکه راه اندازی شود.

Startup Settings

Press a number to choose from the options below:

Use number keys or functions keys F1-F9.

- 1) Enable debugging
- 2) Enable boot logging
- 3) Enable low-resolution video
- 4) Enable Safe Mode

5) Enable Safe Mode with Networking

- 6) Enable Safe Mode with Command Prompt
- 7) Disable driver signature enforcement
- 8) Disable early launch anti-malware protection
- 9) Disable automatic restart after failure

Press F10 for more options Press Enter to return to your operating system

كاربران ويندوز 10:



مرحله 3: فایل Autoruns.exe را دانلود و اجرا کنید.

ile Home Shar	e View Extract					~ (
· → ~ ↑ 🚺 > T	This PC > Downloads > Au	toruns	~	ව Search Aut	oruns	۶
recess	Name	Туре	Compressed	Password pr	Size	710.1
Desktop	autoruns	Compiled HTML Hel	42 KB	No		50 K
Documents	Autoruns64	Application Application extension	367 KB 307 KB	No		847 K 733 K
Music	autorunsc autorunsc64	Application Application	270 KB 314 KB	No No		635 K 747 k
Videos	Eula	Text Document	4 KB	No		8 K
This PC						
🥩 Network	4			14		

مرحله 4:

در برنامه Autoruns بر روی گزینه "Options" در بالای صفحه کلیک کنید و گزینه " Autoruns در برنامه Locations" و "Refresh" کلیک کنید.

THE PETERS LIPSTON	ns Heln							
	Filter							
	rinter.							
🖸 d 🔍 🗖	Boot Execute	Image Hij	jacks 🛐 AppInit	KnownDLLs	Winlog	on 🚳 W	insock Pr	oviders
Print a	irs 🌒 LS	A Providers	Network Provider	s 🗃 WMI	Sideba	ar Gadgets	1	Office
C Everything	Logon	Explorer	A Internet Explor	er 🙆 Scheduled	Tasks	Services		Drivers
Autorun Entry	380 S	Description	Publisher	Image Path	Timestam	v Vi	usTotal	
HKLMISYSTE	M\CurrentContr	olSet\Control\Safe	Boot\AlternateShell	indge i dui	06/03/18 1	9:03	astolat	
Cm cmd.exe	3	Windows Comma	Microsoft Corpor	c:\windows\syste	23/01/15 2	2:14		
HKLM\SOFTW	ARE\Microsoft	Windows\Current	Version\Run		06/03/18 1	9:03		
Security	Health	Windows Defend	Microsoft Corpor	c:\program files\w	. 26/09/20 2	1:44		
HKLM\SOFTW	ARE\Wow6432	Node\Microsoft\W	/indows\CurrentVersid	on\Run	06/03/18 1	9:03		
🖂 🍐 Parallel	s Tools Center	Parallels Control	Parallels Internati.	c:\program files (20/05/18 2	2:08		
HKCU\SOFTW	ARE\Microsoft	Windows\Current	Version\Run		06/03/18 1	9:19		
🗹 👝 OneDriv	/e	Microsoft OneDri	ve Microsoft Corpor	c:\users\tomas\a	01/06/18 1	7:41		
HKCU\SOFTW	ARE\Microsoft	Windows\Current	Version\RunOnce		13/06/18 1	4:11		
Uninsta	II 18.065.032	Windows Comma	Microsoft Corpor	c:\windows\syste	23/01/15 2	2:14		-
Uninsta	II 18.065.032	Windows Comma	Microsoft Corpor	c:\windows\syste	23/01/15 2	2:14		
HKLM\SOFTW	ARE\Microsoft\	Active Setup\Insta	alled Components		06/03/18 1	9:03		
Microso	ft Windows			File not found: C:				
🔽 📄 n/a		Windows host pr.	Microsoft Corpor	c:\windows\syste	02/04/32 0	5:35		
HKLM\SOFTW	ARE\Wow6432	Node\Microsoft\A	ctive Setup\Installed	Components	06/03/18 1	9:12		
Google 👸 Google	Chrome	Google Chrome I	Google Inc.	c:\program files (12/06/18 0	5:52		
🗹 📄 n/a		Windows host pr.	Microsoft Corpor	c:\windows\sysw	24/02/29 0	9:39		
🗳 HKLM\Software	e\Classes*\She	IIEx\ContextMent	uHandlers		28/05/18 1	1:11		
C								>

مرحله 5:

لیست ارائه شده توسط نرم افزار Autoruns را بررسی کنید و فایل بدافزاری را که می خواهید از بین ببرد پیدا کنید.

The second secon					11 - 41 - N	
Autoruns - Sysinternals: www	w.sysinternals.com			20 -1 0		×
File Entry Options Help						
🛃 😰 👬 🛃 🗙 Ķ Filter:						
Print Monitors Boot Execute	Providers 🔮 Netwo	ork Providers AppInit 🔇	WMI Sideba KnownDLLs Winlogo	r Gadgets n 🗳 Wi	nsock Provid	ice ders
Everything 🛃 Logon	🚼 Explorer 🛛 😂 Inte	rnet Explorer	Scheduled Tasks	Services	📕 Driv	ers
Autorun Entry Image: State	Description Public Vindows host pr Micro Vindows PowerS Micro Vindows PowerS Micro Vindows host pr Micro Microsoft Malwar Micro Microsoft Malwar Micro Microsoft Malwar Micro Vindows host pr Micro Vindows host pr Micro Vindows host pr Micro	sher II soft Corpor c soft Corpor c	mage Path Timestal :\windows\syste 02/04/32 :\windows\syste 02/11/68 :\windows\syste 02/04/32 :\windows\syste 02/04/32 :\windows\syste 02/04/32 :\windows\syste 02/04/32 :\windows\syste 02/04/32 :\program files\w 25/11/12 :\program files\w 25/11/12 :\program files\w 25/11/12 :\program files\w 25/11/12 :\program files\w 23/07/18	mp 05:35 05:35 05:35 05:35 16:42 05:35 11:06 11:06 05:35 13:39 13:39 13:39 13:39 13:39 13:39	VirusTotal	
HKLM/System/CurrentControls	Delete Copy Jump to Entry	Ctrl+D Ctrl+C	sers\tomas\a 28/08/15 13/06/18 rogram files (17/06/15 rogram files (17/06/15	14:03 14:09 01:46 01:46 21-24		v
trjdlcot-trokan-sanpm	Verify Image Check VirusTotal				,	
"C:\Users\tomas\AppD Ready.	Process Explorer Search Online Find	Ctrl+M Ctrl+F	.exe" vs Entries Hidden.			
	Properties	Alt+Enter				

پس از حذف نرم افزارهای مخرب از طریق نرم افزار Autoruns (این امر تضمین می کند که نرم افزارهای مخرب در راه اندازی بعدی سیستم اجرا نمی شوند)، شما باید نام بدافزار را در رایانه خود جستجو کرده و آن را حذف کنید.

File Home	Share	View	Search Tools Search	Application Tools Manage	trjdlcot-trokan-sa	npmf.e	exe - Search Res	ults in Thi	- 0	× ~ (
⊢ → × ↑ 🛢	Search	h Results	in This PC				ٽ ~	trjdlcot-trokan-	sanpmf.exe	×
 Quick access Desktop Downloads Documents Pictures Music Videos OneDrive This PC 	* * * *		trjdlco C:\Users	<mark>t-trokan-sanpı</mark> s∖tomas∖AppData	<mark>nf</mark> ∖Roaming∖winapp	• •	Open Run as administ Troubleshoot co Pin to Start Share Open on Mac Show in Finder Share on Give access to Restore previou	trator ompatibility is versions	> >	
Network 1 item 1 item selected 423 KB	5			Send to Cut Copy Create shortcut Delete Rename		>				
						_	Open file locati	on		

کامپیوتر خود را در حالت عادی راهاندازی کنید. برای اطمینان از اینکه کامپیوتر شما فاقد نرمافزارهای مخرب است، مجدد سیستم را با Spyhunter اسکن نمایید.