

Hakiranje bez hakiranja

Robert Petrunić

Sadržaj

- Je li moguće „haknuti” nešto bez hakiranja?
 - Nekoliko primjera
- DEMO(i)
 - Uglavnom je predavanje demo bazirano ...

Primjer koji ste najvjerojatnije svi vidjeli

- Ima li ovdje hakiranja?
 - Ako ima - kakvog?
- Pogledajmo koliko je ljudi platilo
 - <https://www.blockchain.com/explorer>
 - 1MZHWPgmUyjmExofPDCmYuVz9kmnTpu6m

Od: [REDACTED]@jastrebarsko.hr>
Datum: 11. rujna 2018. u 20:55:14 CEST
Za: [REDACTED]@jastrebarsko.hr>
Predmet: Es geht um Ihre Sicherheit.

Hallo, lieber Benutzer von jastrebarsko.hr.

Wir haben eine RAT-Software auf Ihrem Gerät installiert.
Zu dieser Zeit ist Ihr E-Mail-Konto gehackt (siehe , jetzt habe ich den Zugriff auf Ihre Konten).
Ich habe alle vertraulichen Informationen von Ihrem System heruntergeladen und ich habe weitere Beweise erhalten.
Die interessantesten Sachen, die ich entdeckt habe, sind Videos von Ihnen auf denen Sie masturbieren.

Ich habe meinen Virus auf die Pornoseite gepostet, und dann haben Sie ihn auf Ihren Betriebssystem installiert.
Als Sie auf den Button "Play" auf Porno-Video geklickt haben, wurde mein Trojaner in diesem Moment auf Ihr Gerät heruntergeladen.
Nach der Installation nimmt Ihre Frontkamera jedes Mal, wenn Sie masturbieren, ein Video auf; zusätzlich wird die Software mit dem von Ihnen gewählten Video synchronisiert.

Zur Zeit hat die Software alle Ihre Kontaktinformationen aus sozialen Netzwerken und E-Mail-Adressen gesammelt.
Wenn Sie alle Daten gesammelt von Ihr System löschen müssen, senden Sie mir \$300 in BTC (Kryptowährung).
Das ist mein Bitcoin Wallet: 1MZHWPgmUyjmExofPDCmYuVz9kmnTpu6m
Sie haben 2 Tage nach dem Lesen dieses Briefes.

Nach Ihrer Transaktion werde ich alle Ihre Daten löschen.
Ansonsten sende ich Video mit deinen Streiche an alle deine Kollegen und Freunde!!!

Und von nun an, seien Sie vorsichtiger!
Bitte besuchen Sie nur sichere Webseiten!
Tschüss!

Isti primjer – drugi iznos

- „Isti” primjer
- Koliko ljudi je platilo?
 - <https://www.blockchain.com/explorer>
 - 1PfbxCJkGNTZC7yFtHHhtPnZyiwQEUqAmu

Od: [REDACTED]@jastrebarsko.hr>
Datum: 26. listopada 2018. u 15:10:54 CEST
Za: [REDACTED]@jastrebarsko.hr>
Predmet: Sicherheitswarnung!

Salut!

Wie Sie es Ihnen schon denken können, ist Ihr Benutzerkonto [REDACTED]@jastrebarsko.hr) gehackt, da ich Ihnen diesen Brief von verschickt habe. :)

Ich bin der Vertreter einer bedeutenden übernationalen Gruppe von Info-Piraten
Im Zeitraum vom 23.07.2018 bis zum 20.10.2018 wurden Sie mit dem Virus den wir erstellen haben über die von Ihnen besuchte Webseite für Erwachsene infiziert.
Derzeit haben wir Zugriff auf alle Ihre Briefwechsel, Konten in sozialen Netzwerken und Messengerdienste.
Überdies, haben wir vollständige Speicherauszüge von diesen Daten.

Wir sind uns Ihrer „kleinen und großen Geheimnisse“ bewusst, o, ja... Sie haben das ganze heimliche Leben.
Wir haben geguckt und aufgezeichnet, wie Sie Spaß auf Webseiten für Erwachsene hatten. Lieber Himmel, was für Geschmack und Leidenschaften haben Sie... :)

Aber die interessanteste Sache ist, dass wir Sie periodenweise auf der Web-Kamera Ihres Computers aufgenommen haben. Die Web-Kamera wurde mit dem synchronisiert, was Sie
Ich bin der Meinung, dass Sie nicht wollen, dass Ihre Freunde und Angehörigen alle Ihre Heimlichkeiten sehen, und natürlich die Person, die Ihnen am nächsten ist.

Senden Sie \$552 auf unsere Kryptowährung Bitcoin Wallet: 1PfbxCJkGNTZC7yFtHHhtPnZyiwQEUqAmu
Ich gebe mein Wort, dass wir in diesem Fall alle Ihre Geheimnisse löschen werden!

Ab dem Zeitpunkt, in dem diese Nachricht gelesen ist, funktioniert der Timer!
Sie haben 2 Tage, um das obengedachte Geld zu bezahlen.

Sobald dieses Geld auf unserem Konto ist, werden Ihre Daten sofort vernichtet!
Sofern Geld nicht da ist, werden alle Ihre Briefe und das Video wo sie mit sich spielen automatisch an alle Kontakte gesendet, die in der Zeit der Infektion auf Ihrem Gerät erreichbar sind.
Es tut mir Leid, Sie sollen über ihre Sicherheit nachdenken!
Wir hoffen, dass diese Geschichte lehrt Ihnen, Ihre Geheimnisse korrekt zu bewahren.
Geben Sie acht auf sich!

AHA – utaja poreza

- To će sve prestrašiti
 - Pogotovo u RH
- Koliko ljudi je platilo?
 - <https://www.blockchain.com/explorer>
 - 1Dz7DbQmE7SNm3C5mb9syPcctgZECcCEbL

Šalje: [redacted]@jastrebarsko.hr
Predmet: Incident: E7hC1mB2a*
Datum: 5. travnja 2019. u 05:06:56 CEST
Prima: [redacted]@jastrebarsko.hr

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We Hacked Your Infrastructure.
We Caught Possible Communication.
We Backuped Available DATA And DOCUMENTS.
That you trusting our words, we send this mail to you with YOUR account.

After analyzing documents, We see your illegal activity, HIDING TAXES.

That we do NEXT.
I want two (2) Bitcoin

If you don't pay fees. To my wallet Bitcoin.
1Dz7DbQmE7SNm3C5mb9syPcctgZECcCEbL

We want send this Documents and Proofs to your Tax Department.
And in this time Your network will be DDoS.
Read that in this link
http://en.wikipedia.org/wiki/Denial-of-service_attack

This is our guarantee, that you don't clean evidence and build a protection policy.

If you don't pay by in 7 days, attack will start.
Yours service going down permanently and price to stop will increase to Four (4) BTC,
Price will go up one (1) BTC for every day of the attack.

This is not a joke.

Our attacks are extremely powerful - sometimes over 1 Tbps per second.
And we pass CloudFlare and others remote protections!
So, no cheap protection will help.

Prevent it all with just Two (2) BTC
To my wallet Bitcoin.
1Dz7DbQmE7SNm3C5mb9syPcctgZECcCEbL

Pay strict sum. This is your identification. And we will know that its you.
AND YOU WILL NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.

Time started after open this mail.
To track the reading of a message and the actions in it, I use the facebook pixel.

Svi su oni male bebe za mene

- Ovo sam dobio ja
 - Prvi mail je bio 3500 GBP
 - A ovaj je rekorder – nisam vidio ništa slično
 - astronomskih 4600 GBP
- Koliko ljudi je platilo?
 - <https://www.blockchain.com/explorer>
 - 14qiiiMCEqUzxccF6ByHfCF2V83XoSAUXE

From: 11000642.edu@unmae.vandalucia.es
Sent: Thursday 25 October, 22:00
Subject: RE: ODGOVOR
To: 11000642.edu@unmae.vandalucia.es

Valjda se pitate zašto primate ovu poruku e-pošte?

Bilo bi vrlo korisno za vašu privatnost ako ga niste zanemarili.

Postavio sam zlonamjerni softver na web-lokaciju za odrasle (... P ... 0 ... r ... n web-lokacija) i kao što ste posjetili i gledali videozapis na koji je vaš uređaj pogođen stavljajući spyware na vaš uređaj. Što vas je snimilo s kamerom i snimalo omogućuje da vidim točno ono što vidite.

To je također utjecalo na vaš smartphone putem Exploit. Stoga nemojte misliti na jednu minutu da to možete zaobići ponovnim instaliranjem OS-a. Već ste zabilježeni.

Nakon toga su moji zlonamjerni prikupili sve vaše glasnike, e-poštu i društvene mreže.

Pretpostavljam da ovo nije dobra vijest?

No nemojte se previše brinuti, postoji način na koji možemo riješiti ovaj problem s privatnošću. Sve što trebam je Bitcoin plaćanje od **E4,600 GBP** što mislim da je fer cijena s obzirom na okolnosti.

Adresa za uplatu je: 14qiiiMCEqUzxccF6ByHfCF2V83XoSAUXE

Ako ne razumijete bitcoin, idite na YouTube i potražite "kako kupiti bitcoin" ili google za "lokalne bitcoine", to je prilično jednostavno za napraviti.

Imate samo 48 sati nakon čitanja ove e-pošte za slanje plaćanja (budite upoznani da znam kad ste otvorili i pročitali ovu poruku e-pošte, postavio sam sliku piksela koja mi omogućuje da znate kada ste točno otvorili poruku koji dan i vrijeme).

Ako odlučite zanemariti ovu poruku e-pošte, nemam izbora nego proslijediti videozapis svim prikupljenim kontaktima koje imate na svom računaru e-pošte, kao i postavljati na svoje račune društvenih medija i poslati ih kao osobnu poruku s dostupan na internetu, putem YouTubea i web mjesta za odrasle. s obzirom na vašu reputaciju, vrlo sumnjam da želite biti izloženi vašoj obitelji / prijateljima / suradnicima tijekom ovog trenutnog vremena.

Zapravo možete ići u policiju, ali ti ljudi vjerojatno neće učiniti ništa, najznačajnije stvari koje mogu učiniti je zaključavanje novčanika i uskraćiti će druge ljude od mogućnosti plaćanja. Stoga razmislite dvaput prije nego što budete radili glup.

Ako primim uplatu, svi će materijali biti uništeni i nikad više nećete čuti od mene. Ako ne dobivam sredstva iz praktički bilo kojeg razloga, kao što je nemogućnost slanja novca na novčanik na mojoj listi - vaš će se ugled uništiti. Zato je brz.

Imajte na umu da je ovdje moj Bitcoin adresa za prijenos računa - 14qiiiMCEqUzxccF6ByHfCF2V83XoSAUXE

Nemojte pokušavati stupiti u vezu sa mnom jer koristim e-poštu žrtve koja je bila sjeckana i izložena. Samo odgovorite ako ste obavijestili da ste izvršili uplatu ili imate pitanja o uplati, a zatim kliknite odgovor.

Ako ne vjerujete i želite dokaz samo odgovoriti na ovu poruku e-pošte s "PROOF" i ja ću poslati vaš videozapis na 5 vaših kontakata putem e-pošte i objaviti na vašem Facebook zidu. U kojem ćete ga moći ukloniti jednom, ne zauvijek.

A sad malo dobrog starog haktivizma

- Support PewDiePie!
- Nemam riječi ...
 - Stvarno? Za to smo se borili?
 - Će ode ovaj svijet ...
- OK, OK,
 - Ovo je hakiranje
 - ALI ljudi moji - PewDiePie
 - Nekad su se ljudi borili za bitnije stvari
 - Bolji život
 - Legalizaciju ganĎe
 - ...
- NAJGORE OD SVEGA SLIJEDI
 - DEMO

Thousands of Google Chromecast Devices Hijacked to Promote PewDiePie

January 03, 2019 Mohit Kumar



YOUR Chromecast/Smart TV is exposed to the public internet and is exposing sensitive information about you!

To find out more about what to do and how to fix this, visit

<https://bit.ly/CastHack> for more

information

You should also Subscribe to Pewdiepie

Greetings from @HackerGiraffe and @j3ws3r

Made by rosk2006



Modriča ... Optima ... Sint 2001

AUTHORIZATIONRETURNPAGE	System.String	aspx	
APP_VERSION	System.String	RN:0.0.0.0	
LOGIN	System.String	m	
READWRITE	System.Decimal	1	
AUTHORIZATION	System.Boolean	True	
USER_ID	System.Decimal		
MY_PARTNER_ID	System.Decimal		
DISPLAY_NAME	System.String		
EMAIL	System.String	lhr>	
ACCOUNT_TYPE	System.String	PARTNER	
orderselection.REGION_ID	System.Decimal	--	
MY_REGION_ID	System.Decimal		
MY_INV_ADDRESS_ID	System.Decimal	631328	
orderselection.FILTERED_PARTNER_ID	System.String	0	8)
ASP.order_aspx.ddlPageSize	System.String		
NEWORDER_CONTRACTNR	<null>	<null>	
NEWORDER_ORDERBY	<null>	<null>	
NEWORDER_WOTYPE	<null>	<null>	
NEWORDER_WOPROPERTIES	<null>	<null>	it(s)
NEWORDER_REQUESTID	<null>	<null>	
EQUIP_SRC_GROUP_VISIBLE	System.String	getAssets	
EQUIP_DES_GROUP_VISIBLE	System.String	getAssets	
WorkOrderValue.Text	System.String	PRIVATNO_SKLADIŠTE	
CTRL_CUSTOMER_NAME	System.String	Rješavanje smetnje - Rezidencijala	
CTRL_CUSTOMER_ADDRESS	System.String	Kristijan	
IPhone	System.String	Mar 52000 Pičan	
INSTALATION_ADDRESS_ID	System.String	+385000000	
IContractNumberValue	System.Decimal	1436359	
IIdStatusi.SelectedValue	System.String	1707000004	
PARTNER_ID	System.String	PARK	
WorkOrderNumberValue.Text	System.Decimal		
WORK_ORDER_NR	System.String	4453639.ERR.2	
PRIORITY_ID	System.String	4453639.ERR.2	
CONTRACT_ID	System.String	N	
WORK_ORDER_PATH	System.String	4453639	
SELF_INSTALATION	System.String	NA	
WORK_ORDER_TYPE_ID	System.Decimal	0	
WORK_ORDER_GROUP	System.Decimal	3	
EQUIP_SRC_ADDRESS_ID	System.String	ERROR	
EQUIP_DES_ADDRESS_ID	System.Decimal	631328	
EQUIP_SRC_APPROVE_DATE	System.Decimal	1436359	
EQUIP_DES_APPROVE_DATE	<null>	<null>	
	<null>	<null>	

A sad - DEMO

- 😊
 - Malo shodan-a

Hvala na pažnji!