

L'Université canadienne Canada's university Software Security Research Group (SSRG), University of Ottawa In collaboration with IBM



The "Game Hack" Scam

Emad Badawi, Guy-Vincent Jourdan, Gregor v. Bochmann Iosif-Viorel Onut, Jason Flood University of Ottawa

June 13, 2019

←□→

Rational. software



The Problem

2

We provide an analysis of a social engineering scam targeting games players:

the Game-Hack Scam (GHS).

GHS in a nutshell:

- 1. Attackers claim that they can hack a specific game and provide the victim with free, unlimited resources or other advantages for their favorite game.
- 2. To obtain these claimed advantages, the victims are asked to complete one or more tasks, called "offers".
- 3. These so-called offers include, but are not limited to, subscriptions to questionable services and installation of executable files on the victim's device.



Games have "resources"



PUBG

3



Subway Surfers





My Talking Tom



Why Players Buy Resources?

- ✤ Used to buy in game outfits.
- ✤ Used to by in game extra lives.
- Used to by in game helper tools.





Candy Crush



Toon Blast



🔶 C 🔒 https://www.change.org/p/legit-candy-crush-saga-online-generator-2018-candy-crush-saga-hack-app-generate... 😭 🌀 🛄 🥥

IBM

GHS at Work

change.org Lancer une pétition

une pétition Parcourir les pétitions Nous soutenir

Se connecter

Candy Crush Saga Hack App Generate Unlimited Gold FREE Online Generator

Scottie Marcie a lancé cette pétition adressée à LEGIT Candy Crush Saga Online Generator 2018

Use our Candy Crush Saga Hack App now to obtain unlimited Gold to your account! This hack tool is the only reliable option and not only this, it is also secure and free to utilize! We also ensured that this hack tool is safe from viruses. We're using this precaution for safety reasons. Players may use all the equipment within our website without having to jailbreak and root the devices. This easy to use hack tool has been doing a beta test that has been exclusive to professional gamers for a couple weeks and it's just been released publicly after multiple requests.

Access Candy Crush Saga Hack App Here http://bit.ly/2Ey6K0Q http://bit.ly/2Ey6K0Q http://bit.ly/2Ey6K0Q

15 ont signé. Allez jusqu'à 100 !	
Prénom	
Nom de famille	
E-mail	
Gatineau, J8Z Canada	Ø

 Faire apparaître mes nom et commentaire sur cette pétition

Signez cette pétition

En signant, vous acceptez les <u>conditions d'utilisation</u> et la <u>politique d'utilisation des données</u> de Change.org et vous acceptez de recevoir de temps en temps des e-mails à propos de campagnes



114

uOttawa

GHS at Work

GHS instance (GHSi)

19

C https://cpbldi.com	m/c26a2bb			\$	G	냈	0
Elite Private Hacking 1	Fools!						
Home > Dashboard >	Generate Unlimited Resources						
Generate	Unlimited Resources						
V2.01.85 Gen	erate Unlimited Resources		100 -	Usage 214 Today		¢	,
LUsername	PaperTest		50 -	a a a			1
🔀 Resources	111		0 -				
Device	Select Device	(🕓 His	story			
Anti-Ban	✓ Enabled		_	trojans283 gener	rated		
Target Server	💎 Gatineau, Quebec		\checkmark	Success (1) few sec	> onds a	go	
Download	Download Not Required			exalted274 gene ~8M Resources Failed () few secon	rated)	
	Cenerate Resources		~	clapper388 gene ~49M Resources Success ① few seco	ratec S onds a	go	



uOttawa

GHS at Work

GHS instance (GHSi)





С

uOttawa

GHS at Work

"Content Locker" with list of tasks to be completed

13

https://cpbldi.com/c26a2bb		☆	C i	<u>a</u> 🔾		
me > Dashboard > Generate Unlimited Resources						
Human Verification Required						
Surveys Human Verification		View More				
Be the first to get the Samsung Galaxy S9!		© 2 m	in	Ð		
Receive your \$50 Visa Gift Card & 24-pack of your choice!	Receive your \$50 Visa Gift Card & 24-pack of your choice!					
Watch full episodes of your favorite TV shows live & on-demand with CB	S All Access	() 5 m				
Verification concluded automatically upon survey completion. Surveys for your count	ry typically take	e 2-3 minutes.				
		73M Resource	S onds ago	,		
		voundsj272 ger 50M Resource	nerated s onds ago	,		
	V V C	ernacu215 gen 44M Resource huccess () few sec	erated s onds ago	,		



GHS at Work

Congratulations!

You have FREE access to the hottest new releases

Sign Up For Free Now!

a site

FRE MEMBERSHIP

Age

Buse

Mathemany movies as

Yutch as many movies as

Task: subscription to a site

1.0



uOttawa

GHS at Work

> Windows PC Repair

Reimage - How to Repair Windows 10

Problem: If your system has been infected with Viruses, Spyware or Malware, it may needs to be corrected. The Reimage patented technology is the only PC Repair program of its kind that actually reverses damage done to your operating system. This process eliminates the need to reinstall Windows.

Solution: Scan, diagnose and repair any damage on your PC with powerful technology that not only fixes your Windows Operating System - it reverses the damage already done with a full database of replacement files.

Task: installation of executable



Download Windows 10 Repair Tool

Compatibility: Windows 10, 8.1, 8, 7, Vista, XP, ME, 2000 (32/64) Download File Size: 911KB, Download Time: 1 sec on dsl, 1 min on dial-up

Diagnose & Fix Windows Errors in 3 simple steps

1. <u>Click here to download Windows 10 repair</u> tool.

2. Double click on the setup file and follow the on-











Total downloads: 106,551,102







Methodology

1.5





Methodology/Queries Generator

- Extracted a bag of 1,964 words from our initial set of pages, and manually selected 39 words that relates to GHS.
- 2. Generated 1-, 2- and 3-grams and manually selected **410** queries.
- 3. Extracted a set of **966** games from FB, iTunes, and play store, and permutated them with **9** different queries which generated **8,694** new queries.
- In total, we have generated 9,104 queries, searched daily on
 Google, Yahoo, Bing and 1and1



weeks and it's just been released publicly after multiple requests.

Access Candy Crush Saga Hack App Here

http://bit.ly/2Ey6K0Q

http://bit.ly/2Ey6K0Q

http://bit.ly/2Ey6K0Q

 Faire apparaître mes nom et commentaire sur cette pétition

Signez cette pétition

En signant, vous acceptez les <u>conditions d'utilisation</u> et la <u>politique d'utilisation des données</u> de Change.org et vous acceptez de recevoir de temps en temps des e-mails à propos de campagnes u Ottawa

Methodology/Web Crawler



Search Engine Crawling

→ C ▲ https://www.change.org/p/legit-candy-crush-saga-online-generator-2018-candy-crush-saga-hack-app-generate.... ▲ ● ● 號 ● Change.org Lancer une pétition Parcourir les pétitions Nous soutenir Q Se connecter

Candy Crush Saga Hack App Generate Unlimited Gold FREE Online Generator

Scottie Marcie a lancé cette pétition adressée à LEGIT Candy Crush Saga Online Generato 2018

Use our Candy Crush Saga Hack App now to obtain unlimited Gold to your account! This hack tool is the only reliable option and not only this, it is also secure and free to utilize! We also ensured that this hack tool is safe from viruses. We're using this precaution for safety reasons. Players may use all the equipment within our website without having to jailbreak and root the devices. This easy to use hack tool has been doing a beta test that has been exclusive to professional gamers for a couple weeks and it's just been released publicly after multiple requests.

Access Candy Crush Saga Hack App Here
http://bit.ly/2Ey6K0Q
http://bit.ly/2Ey6K0Q

http://bit.ly/2Ey6K0Q

Prénom Nom de famille E-mail Gatineau, J8Z

15 ont signé. Allez jusqu'à 100 !

Canada

 Faire apparaître mes nom et commentaire sur cette pétition

Signez cette pétition

En signant, vous acceptez les <u>conditions d'utilisation</u> et la <u>politique d'utilisation des données</u> de Change.org et vous acceptez de recevoir de temps en temps des e-mails à propos de campagnes

Extracted URLs Crawling

GHS links were posted in many popular websites including **Jeuxvideo.com**, **change.org**, **pinterest.com**, **linkedin.com** and even **researchgate.net**.





Methodology/Classification Model: SVM

Support-Vector Machine classification based on pages' text.
 96.7%TPR and 2.1%FPR using 10-fold cross-validation on 470 clean pages and 495 GHS pages.



GHS Page



Collected Dataset

Two different crawls were conducted:

1) Collected URL's from different search engines.

#URLs	#Reachable URLs	#English Pages	#1k Alexa Domains URLs	#GHSis	%GHSis
1M	657,578	576,476	326,862 (NO GHSis)	11,969	2.07% (4.7% without 1k Alexa URLs)

2) Extracted URL's from the pages collected in step 1 (excluding pages on 1k Alexa domains).

#URLs	#Crawled URLs	#Reachable URLs	#English Pages	#GHSis	%GHSis
18.5M	1.5M	497,986	378,147	21,353	5.6%



Clustering and Analysis

Several analyses were conducted:

- The relationship between the different GHSis, the scammers who publish them and the games they target.
- Analyzing the Content Lockers, the offers domains and the relationship between the different CLs and the offer domains.
- ✤ GHS and offers domains analysis.
- Bitly Click Through Analysis
- Bitly Monthly URL Clicks and Creation Analysis



GHS Analysis / GHS groups

- Identified 7 identifiers types used for various purposes such as statistics collection (*histats.com*).
- Some identifiers come from the tools used to create GHS templates (*cpabuild.com* and *ogads.com*)
- **4,040** unique IDs, **95.2%** found on fewer than **5** pages.





GHS Analysis / GHS groups 2

- We have **19k** different pages title in a corpus of **33K** GHSIs.
- We found generic titles such as "Generate Resources For Your Game!" in 1,263 GHSIs.
- The analysis is conducted on IDs found on at least 5 GHSIs.







Content Locker (CL) / Offers Analysis

- Analysis conducted on 42 seemingly unrelated GHSis (different domains).
- Identified only 14 unique CLs.
- 41% of the GHSis CLs belongs to cpabuild.com and ogads.com.
- ✤ 115 offers Domains were collected.
- 22% of the domains reached by all 14 CLs, and 75% of the domains reached by at least 12 CLs.
- Offers domains targets mainly surveys and online subscription websites such as music, movies and books websites.





GHS and Offers domains Analysis

- Email/Phone reaching out with **10** different offers websites with online bookstore as a service:
 - 1) 9 out of the 10 has the same reply "A representative will follow-up with you as soon as possible. You can view the tickets progress online."
 - Only 1 website replied back asking to create a free account with a visa with at least 50\$ to check the offered content.
 - 3) Similar case with a direct call, all sites has similar auto response with a repeated cycle. We succeeded once to get a human response with similar answer as in **2**.



GHS and Offers domains Analysis

Blacklists analysis

Malwaredomains: http://www.malwaredomains.com/	SANS: https://isc.sans.edu/suspicious_domains.html			
abuse.ch: <u>https://abuse.ch/</u>	Malc0de database: http://m	nalc0de.com/database/		
malwaredomainlist: https://www.malwaredomainlist.com	virus total	google safe browsing		

- Only **225** (**6.7%**) of the GHS domains are blacklisted.
- 91 (79%) of the Content locker domains are blacklisted.
 - average black listing time is **506** days from registration day.
 - Only **1** domain was blacklisted in less than **100** days.



Bitly Analytics

- Collected 2,215 GHSIs shortened using Bitly.
- ✤ 99% of the URLs has at least 2 clicks.
- Total # of clicks is 3,894,964 with average clicks of 1,774 per URL.
- 20% of the links register clicks over a period of a year or more.
- By extrapolation, we estimate that these links have been clicked through at least 60 million times.





Bitly Monthly URL Clicks and Creation Analysis

- The first active Bitly URL was seen in mid-2014.
- The GHS URL creation and clicks peaked in early 2018.
- GHS Bitly URLs had 575k clicks in September 2018 only.
- US, India and Indonesia had the highest # of clicks with 22.67%, 10.37% and 6.7% respectively.
- Direct, jeuxvideo.com and piktochart.com are the top referrals with 77.17%, 5.81% and 3.36% respectively.





Limitations and Future Work

- ✤ Our work is based on GHS corpus that we have collected as a starting point.
 - ✤ We plan to do a more systematic and exhaustive study of this scam.
- ✤ The analysis was focused on the GHS and the final offers.
 - ✤ A more study of the Malware part is to be conducted.
 - ✤ More analysis of the offer side of the scam.



Conclusion

- ✤ Reported the first systematic investigation of what we call the "Game Hack" Scam GHS.
- ✤ GHS attackers use popular websites to publish links leading to this type of scam.
- The targeted websites are social media, streaming sites, blogs, and even unrelated sites such as change.org or researchgate.net
- Over a period of 5 months we uncovered over 3k GHS domains and over 100 different offer domains.
- ✤ attackers use pre-built templates to create their attacks. They also target different games
- ✤ We estimate that these links have been clicked through at least 60 million times.
- ✤ Current Blacklists are ineffective against GHS.



The "Game Hack" Scam

Emad Badawi¹, Guy-Vincent Jourdan¹, Gregor Bochmann¹, Iosif-Viorel Onut², and Jason Flood³

¹ Faculty of Engineering, University of Ottawa, Ottawa, Canada {ebadawi,GuyVincent.Jourdan,Bochmann}@uottawa.ca ² IBM Centre for Advanced Studies, Ottawa, Canada vioonu@ca.ibm.com ³ IBM Security Data Matrices, Dublin, Ireland floodjas@ie.ibm.com

Abstract. Game Hack Scam (GHS) is a cyberattack in which the attacker attempts to convince the victim, often a child or a young adult, that they will be provided with free, unlimited resources or other advantages for their favorite game. To obtain these claimed advantages, the victims are asked to complete one or more tasks, called "offers". These so-called offers include, but are not limited to, subscriptions to questionable services and installation of executable files on the victim's device. Although recent research has provided important insights into different types of scam such as "Technical Support Scam", "Survey Scam", and "Romance Scam", to the best of our knowledge GHS has not been studied up to now.

In this paper, we report the first systematic study of GHS. We use a data-driven approach to investigate and gain knowledge on this type of scam: we formulated GHS-related search queries, and used multiple search engines to collect data about the websites to which GHS victims are directed when they search online for various game hacks and tricks. We analyze the collected data to provide new insight into GHS, and research the extent of this scam. We show that GHS attackers abuse social media, streaming sites, blogs, and even unrelated sites such as *change.org* or *researchgate.net* to carry out their attacks and reach a

You can find me at: ebadawi@uottawa.ca

Or access our website: <u>http://ssrg.site.uottawa.ca</u>

Access our full dataset at: http://ssrg.site.uottawa.ca/ghsicwe2019/

Thanks!

ANY QUESTIONS?