# Game of Threats

## How cybercriminals use popular TV shows to spread malware

## Introduction

While the way we consume TV content is rapidly changing, the content itself remains in high demand, and users resort to any means available to get at it – including illegal and non-ethical ones like the use of pirated stuff. The world is embracing the idea of paying for entertainment more and more with the development of paid subscription networks like Netflix or Apple Music. Yet many countries are still fighting the battle against illegally distributed content. In December 2018, Australia's Federal Court issued an injunction requiring local internet providers to block 181 pirate domains linked to 78 websites full of files infringing copyright regulations. At the beginning of 2019, Brazil's Ministry of Justice brought on board the Federal Police of Brazil (Polícia Federal) to launch an anti-piracy operation targeting the illegal distribution of music, movies and TV shows. These are just two of the many initiatives introduced both by governments and the private sector all over the world to combat the problem.

However, despite these measures, copyright-infringing content is still readily available. According to the latest Annual Piracy Report by Muso – a global technology company providing anti-piracy, market analytics and audience connection solutions – the numbers of pirated content consumers are growing. The company registered more than 300 billion visits to pirate websites in 2017 alone. An 1.6% increase from 2016 and an international trend: the US supplied the greatest number of pirate website visitors with 27.9 billion visits per year, followed by Russia, 20.6 billion (a 46% increase from 2016), and India, whose residents visited pirate websites 17 billion times. A major share of pirated content still comes from downloadable files: a 2019 WebKontrol report claims that torrent websites are still leading in Russia in terms of volume of pirated content, followed by file-hosting and streaming services. Moreover, the share of links to illegal content posted on torrent websites grew 14% from 2018 (38% from 24%), overtaking streaming websites.

Being a lucrative source of content, torrents also prove to be a popular way of distributing malicious code, and there are many studies on how cybercriminals exploit that opportunity. According to the results of one such study published in 2015, bootlegged content represents 35% of files shared via BitTorrent, with more than 99% of the analyzed counterfeit files linked to either malware or scam websites. The recent findings by Kaspersky Lab and independent researchers have confirmed the continuation of this trend.

But what kind of content is being targeted? Originally, torrent trackers were the 'go-to' places for those seeking pirated versions of games and other software, as well as recent Hollywood blockbusters. Yet in recent years TV shows have become an extremely popular type of content among viewers all around the world – sometimes even more popular than Hollywood movies. According to the Muso report, TV content is clearly of interest to one third of all users consuming copyright-infringing content: TV shows remain the most popular product among users with 106.9 billion visits last year, followed by music (73.9 billion) and films (53.2 billion).

Such popularity has not escaped the eye of cybercriminals, either. To find out exactly how they capitalize on the rise in illegal downloads of TV content, we have researched the landscape of malware threats disguised as new episodes of popular TV shows distributed through torrent

websites. Our goal was to see which TV series were the most popular with the malware pushers and to take a closer look at what kind of threats are distributed that way.

## Methodology and key findings

To make sure the TV series we focused on were high in demand and sufficiently relevant, we made a list of the most popular TV shows in 2018 using various public sources like IMDB, Rotten Tomatoes and other online ratings sources, plus the most pirated TV shows, also suggesting how popular a particular show may be. We listed a total of 45 titles, but as some of the more popular ones appeared in several different rankings at the same time, we made a few revisions and came up with a final list of 31 TV shows (according to various public ratings like IMDB, Rotten Tomatoes, TorrentFreak, etc., in an alphabetic order).

1. Altered Carbon
2. American Horror Story
3. Arrow
4. Better Call Saul
5. Daredevil
6. DC's Legends of Tomorrow
7. Doctor Who
8. Game of Thrones
9. Grey's Anatomy
10. Homeland
11. House of Cards
12. Killing Eve
13. Legends of Tomorrow
14. Modern Family
15. Roseanna
16. Sharp Objects
17. Stranger Things
18. Suits
19. Supernatural
20. The Big Bang Theory
21. The Flash
22. The Good Doctor
23. The Good Place
24. The Handmaid's Tale
25. The Haunting of Hill House
26. The Walking Dead
27. The X-files
28. This Is Us
29. Vikings
30. Westworld
31. Young Sheldon

We then ran each title against our threat database. Using aggregated threat statistics from the Kaspersky Security Network (KSN) – the infrastructure dedicated to processing cybersecurity-related data streams from millions of volonteers around the world – we checked whether the users who had agreed to share threat statistics with KSN had ever encountered malware when dealing with the corresponding TV show titles.

Next, we identified the episodes of the most popular TV shows used to diguise malware to find out whether there was any correlation between the number and order of episodes in any given season and the malware pushers' interest in them.

In addition, we estimated how effective each disguise was, and how succesful a bait each TV show was, as well as the overall potential of the setup as a source of spreading malware. To do that, we divided the total number of unique attacked users by the number of malicious files, and did the same for each TV series. This gave us the average number of users reached by at least one TV show-themed malicious file which, to some extent, allowed us to get at the TV show that worked best as a decoy.

Finally, we looked at what kind of threats are more likely to hit users under the cover of popular series.

These are our key findings:

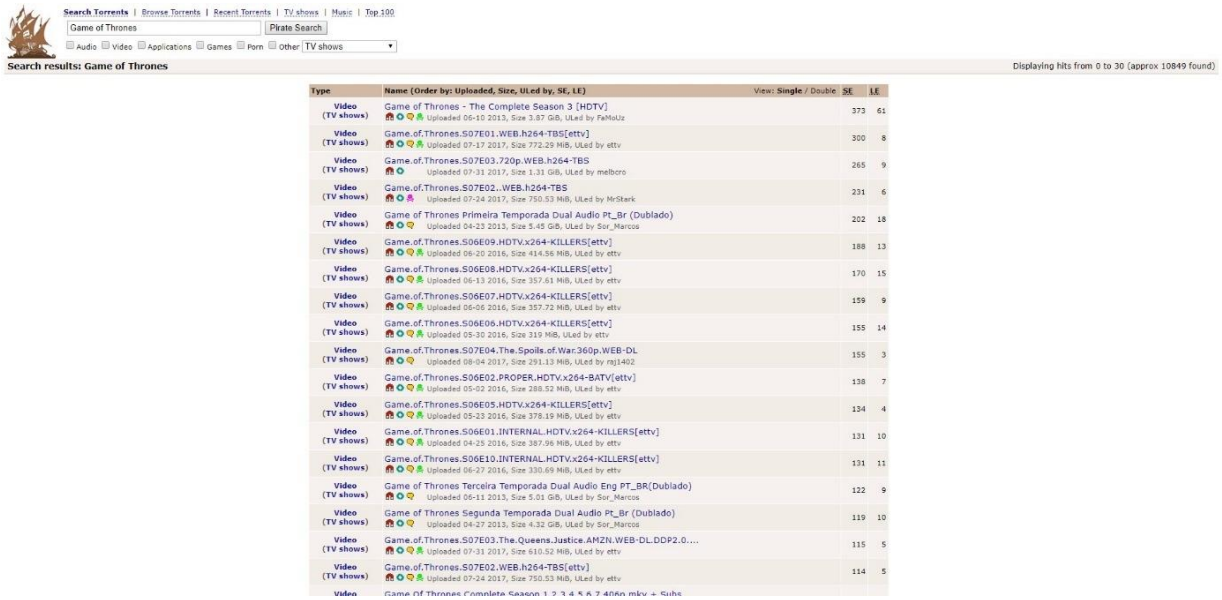
- The total number of **users** who encountered by TV-show-related malware in 2018 is **126,340 globally**, **one-third less**than in 2017. The number of **attacks** by such malware has seen a **decrease of 22% to 451,636** registered attempts
- The **top three** TV shows most often used for bait and used to attack the greatest number of users: **Game of Thrones, The Walking Dead and Arrow**
- **Game of Thrones** accounted for **17%** of all the infected pirated content in 2018, with **20,934 users attacked,** despite being **the only TV show in the list that didn't have new episodes released in 2018**
- **The first and the last episodes of each Game of Thrones season we analyzed turned out the most dangerous**, accounting for the greatest number of malicious files in Kaspersky Lab's collection and affecting the most users
- '**Winter Is Coming**' – the very first episode of the show – **was the one most actively used by cybercriminals**
- Within two years we detected **33 types** and **505 different families** of threats hiding behind the **Game of Thrones** title
- On average, 2.23 users **were attacked seven times** per each malware file guised as a TV show
- **American Horror Story proved to be the most effective malware cover** – each malicious file hidden behind the title has reached an average of three users
- **Not-a-virus:Downloader and Not-a-virus:AdWare** turned out to be two of the most popular threats delivered via TV show content, **the most popular one being the dangerous malware type called Trojan**

# General Overview: malware is coming

The analysis of malicious payloads guised as popular TV series names, and a comparison between the results for years 2017 and 2018, has demonstrated a **decrease in the numbers** of such malware files, attacks and affected users.

**A total of 126,340 users were attacked – one third less than in 2017 (188,769).** The decline is smaller than that seen elsewhere For example, a recent report showed that users affected by malware delivered via popular content, including porn, fell by 45% in 2018.

Same as user count, the malware count also declined: **in 2017, which was rich for malware, we added 82,091 samples to our database, yet in 2018 that number dropped 30% to 57,133**.




***Torrent website offering all sorts of pirated content***

The total number of **attacks** detected by our security solutions also dropped, but only by **22%, down to 451,636**.

Such a decline might be connected to some of this year's events potentially affecting the number of torrent file downloads. First, in 2018, Google downranked more than 65,000 torrent websites – major distributors of pirated TV shows – leaving great many users unable to find them when looking for TV series downloads. Active action against torrent websites does make a difference, more and more of them finding themselves blocked or troubled. For example, two major torrent trackers (Pirate Bay and Demonoid) have of late suffered functionality collapses, and one of the world's longest-standing ones, Leechers Paradise, was shut down for good.

In response, websites streaming pirated copies of movies and TV series are becoming more and more popular, draining the audience from the torrents.

Yet torrents are still running high and – based on our statistics – attempts to harm users are still registered. To measure how effective such malware is, we compared the overall number of unique users attacked with the number of malicious files detected. By dividing the number of users by the number of files we found that **every TV show malware file has infected an average of 2.23 users in 2018.**

Additionally, we compared the list of the most popular torrents in 2018 with the list of the most infected TV series.

| **The most popular TV show torrents** | **Top TV shows used to cover up malwa** |
|---|---|
| **The Walking Dead** | Game of Thrones |
| The Flash | **The Walking Dead** |
| **The Big Bang Theory** | **Arrow** |
| **Vikings** | **Suits** |
| Titans | **Vikings** |

| | |
|---|---|
| **Arrow** | **The Big Bang Theory** |
| **Supernatural** | **Supernatural** |
| Westworld | Grey's Anatomy |
| DC's Legends of Tomorrow | This Is Us |
| **Suits** | The Good Doctor |

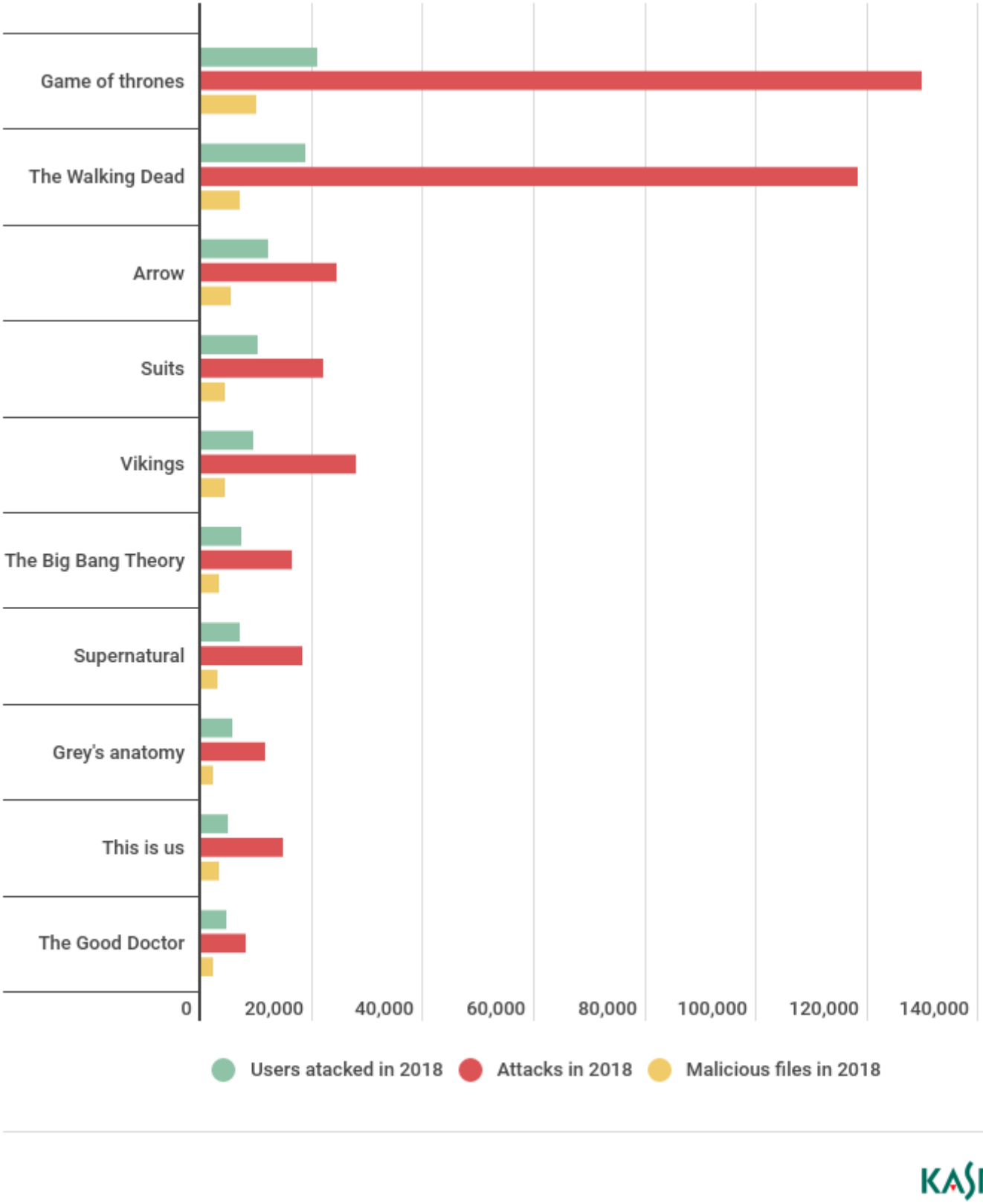
***The most popular torrents of 2018 as reported by TorrentFreak versus the most popular malware-decoy TV series titles***

As seen from the table above, **six out of 10 TV series are featured on both lists**, which we would expect: the more popular a TV show is, the more likely it is to be used by cybercriminals. At the same time, several shows that had been heavily promoted by their makers and were considered to be at the top in terms of popularity – Westworld, DC's Legends of Tomorrow and a few more – didn't make it to the top of disguised infections. This, in a way, may reflect the real popularity of these titles.

## The M-files: most often infected series

Of course, some TV series are more popular among cybercriminals than others – and threat statistics proves that. To understand which of them attract threat actors the most, we reviewed the number of malware files hidden behind the popular TV show title, the number of times they have attacked users and the number of users affected by such attacks. The leaders turned out to be Game of Thrones, The Walking Dead, Arrow, Suits, Vikings, The Big Bang Theory, Supernatural, Grey's Anatomy, This Is Us, and The Good Doctor. The latter has replaced House of Cards, which rounded out the top 10 in 2017.

'Malicious files' represents the number of unique samples of malware encountered by our users; 'Attacks' stands for the number of times our security solutions reported detects, and 'Users attacked' means users attacked by TV-series-related malware at least once.

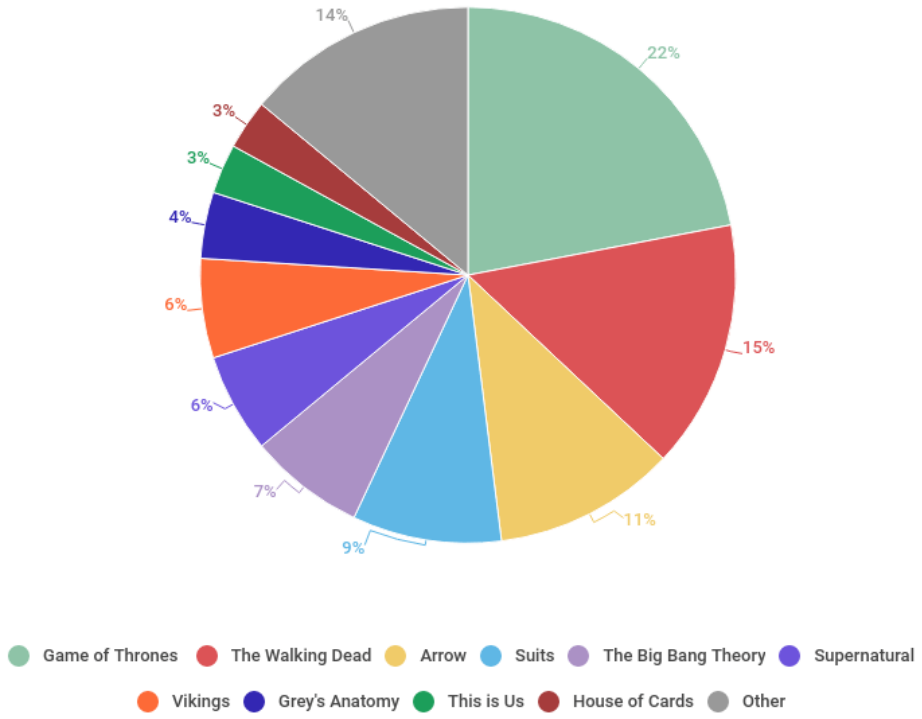



***Top 10 TV shows used as a disguise for malware in 2018***

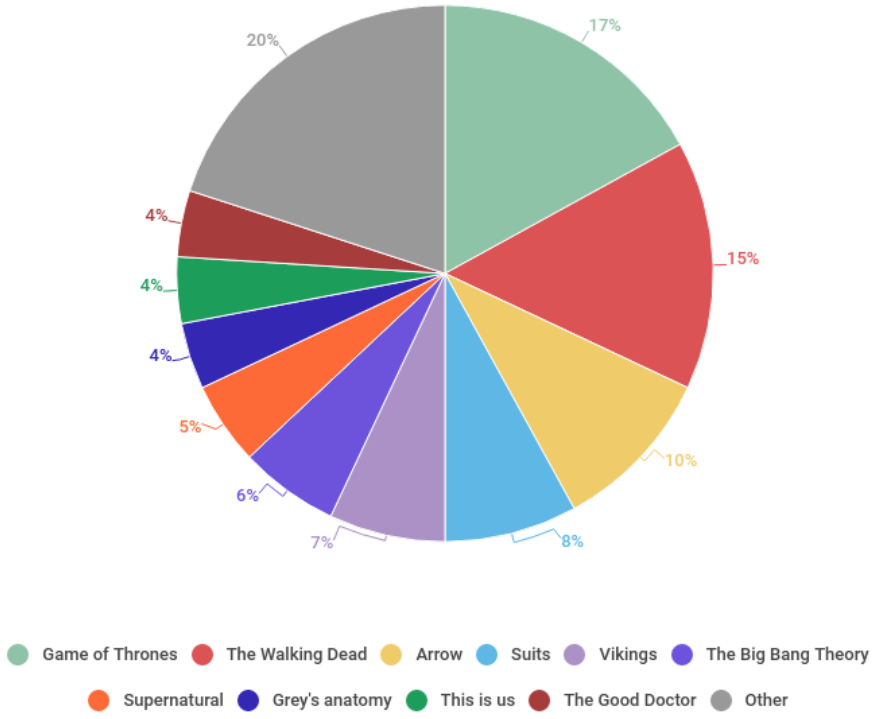
Of all the TV series analysed, Game of Thrones had the greatest number of **users** attacked by malware of the same name – **20,934**. It tried to infect users **129,819** times, and the total number

of Game of Thrones-themed malware files in our threat collection is **9,986.** This makes the show an unmatched leader in popularity not just among users but also among cybercriminals looking for the most effective way to distribute malware.

A year before, in 2017, the wave of Fire and Ice-themed malware was even bigger with almost twice as many users affected and malware files: **42,330 and 19,180, respectively. The number of attacks in 2017 exceeds the 2018 figure by 22% with 167,691 detects.**



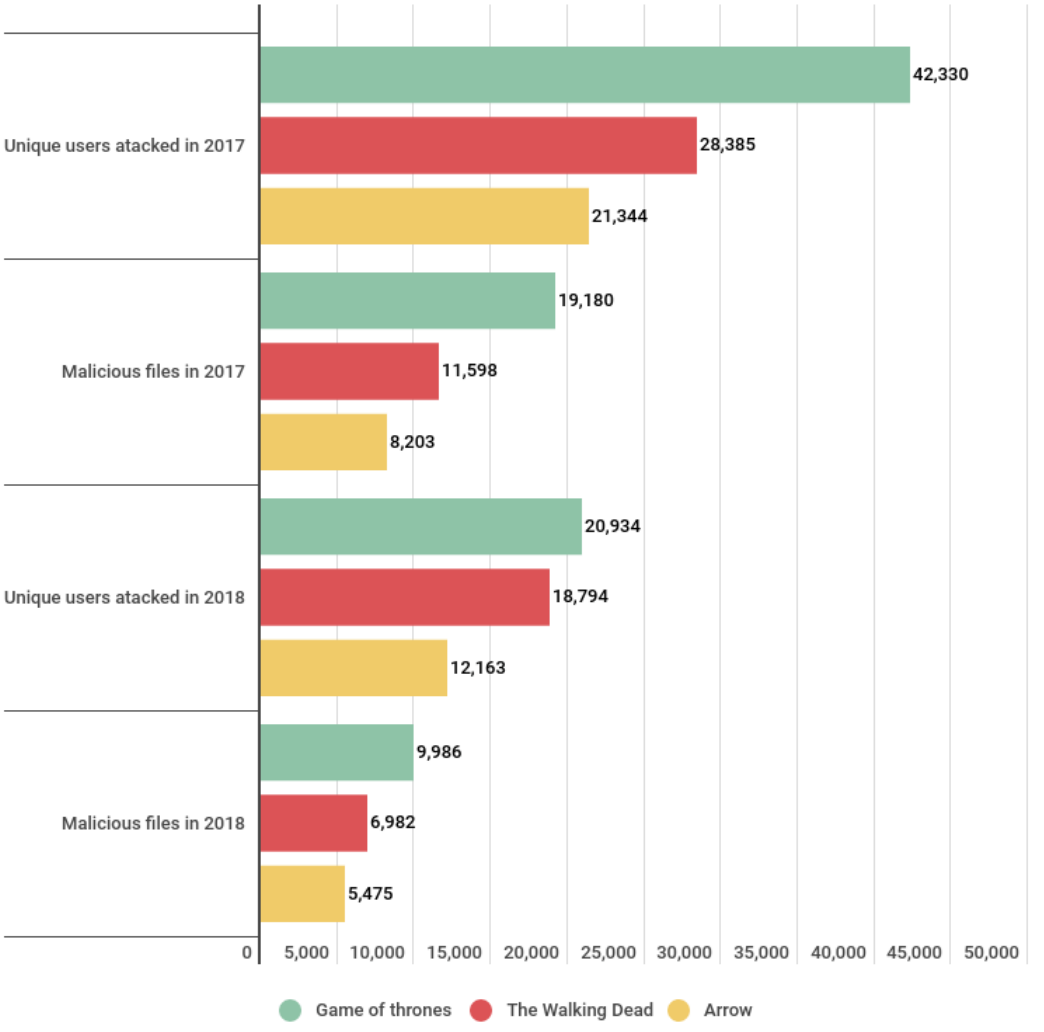

***Top 10 malware disguised as a TV show by the share of users attacked in 2017***




***Top 10 malware disguised as a TV show by the share of users attacked in 2018***

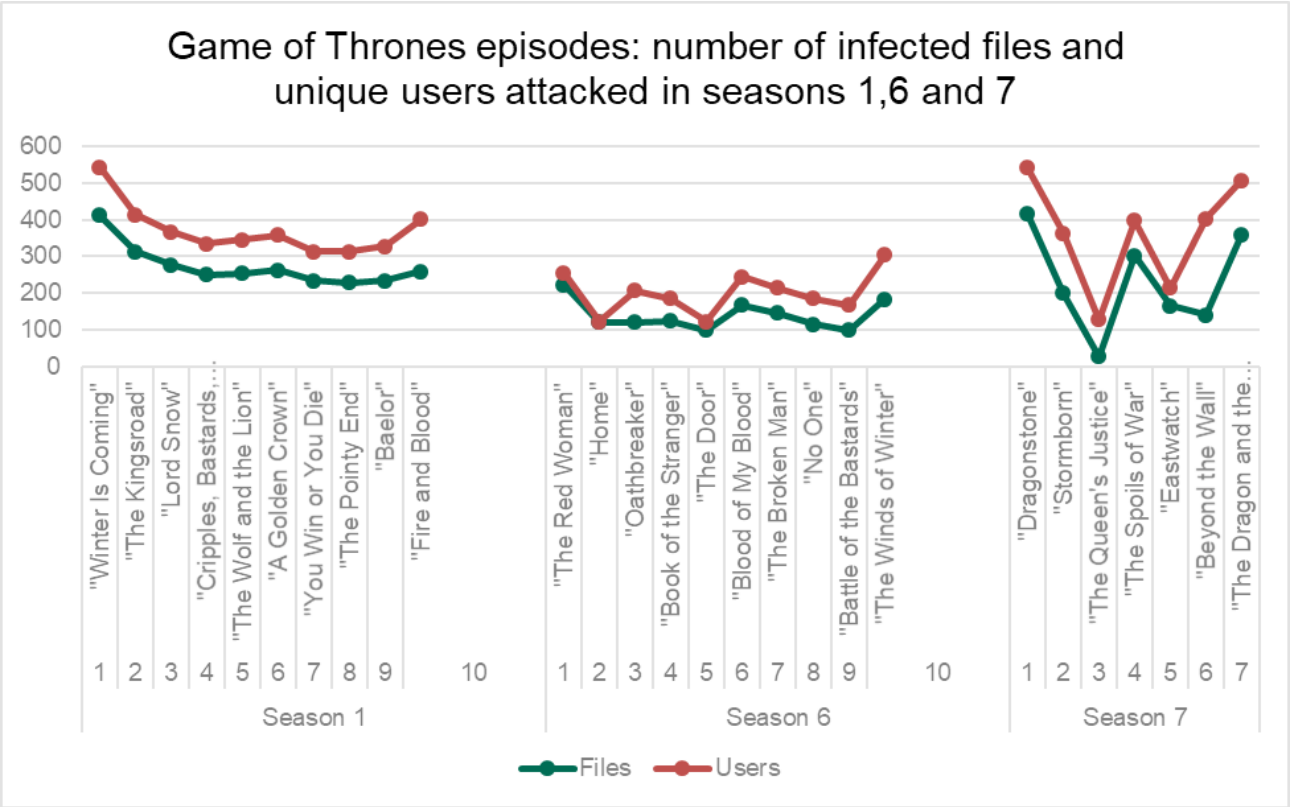
**The second place, both in 2017 and 2018,** was occupied by The Walking Dead, with 18,794 users attacked, and the third by Arrow (12,163 users). The gap of 380 between the number of users attacked by malware disguised as The Walking Dead versus Game of Thrones seems insignificant. However, we need to remember that Game of Thrones is the only TV series in the top 10 that was not even broadcast during 2018 – the period for which the statistics were gathered.

For comparison, we looked at a similar rankings in 2017 when all three TV shows were releasing episodes live. As seen from the graph below, the difference between Game of Thrones and The Walking Dead was more pronounced, with the number of users attacked by Game of Thrones malware exceeding The Walking Dead and The Arrow figures by 33% and 50%, respectively.




***Top three TV shows used as a disguise for online threats***

We also took a closer look at sample episodes from the two latest seasons (six and seven) of Games of Thrones and the original first season. The results revealed that the number of infected files spotted by our protection technologies differed significantly from episode to episode. The common theme we were able to spot was that the first and last episodes were used as a disguise for malware each season. Also, the titles of the opening and closing episodes of each season were used the most actively to hide malware compared to other episodes.




***Game of Thrones episodes: number of infected files and unique users attacked in seasons 1, 6 and 7***

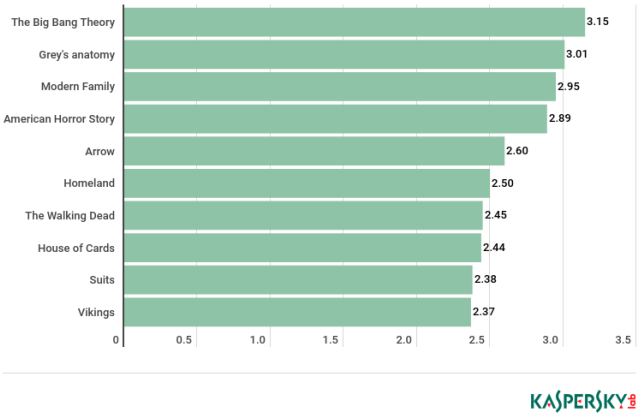
Due to huge time and resource requirements for such an analysis, we did not do any other series. But based on what we have on these three different seasons of GoT, an assumption that other series would be exploited in much the same way would be a safe bet.

But what we can't assume is that, while the malware disguise reached a significant number of users, it is the most effective method of distribution. As we mentioned earlier, malware files disguised to appear as TV show episodes (no matter which) have hit an average of 2.23 users in 2018. Out of the top 10 TV shows used for cyberattacks, Game of Thrones was only seventh in terms of the proportion of malicious files to the number of affected users. Moreover, it proved to be less effective as an average bait, there being one malicious file disguised as Game of Thrones per every 2.1 users attacked.

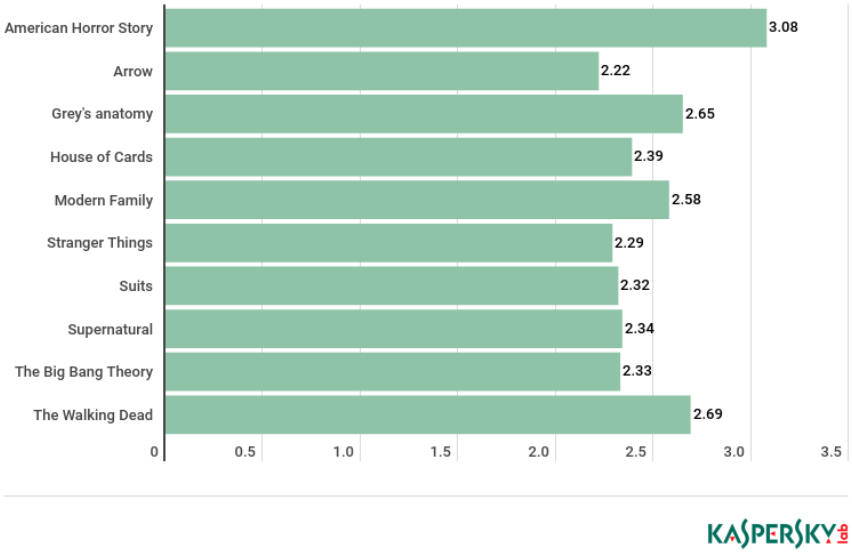
We looked at the files to users ratio when analyzing each TV series from the top 10. The files named after The Walking Dead proved to be the most successful, with 2.69 users attacked on average. Second place went to Grey's Anatomy with 2.65, and third to Supernatural with 2.34.

Later we also checked the remaining TV shows that were analyzed by us but did not make it to the top 10.

Surprisingly, it turned out that **the most successful and productive files were hiding behind TV shows that did not make it to the top 10. Each malicious file of the American Horror Story blood line has reached an average of three users in 2018,**lifting itself from the fourth place in the 2017 ratings. Back then the top three most effective malware files pretending to be TV shows looked different. Modern Family occupied the third position with 2.95, and Grey's Anatomy was second with three. **Each file of the Big Bang Theory line was able to reach 3.15 users and was topping the list, yet in 2018 it dramatically fell to the eighth position**.




***Average number of users dealing with TV series-disguised malware files in 2017***

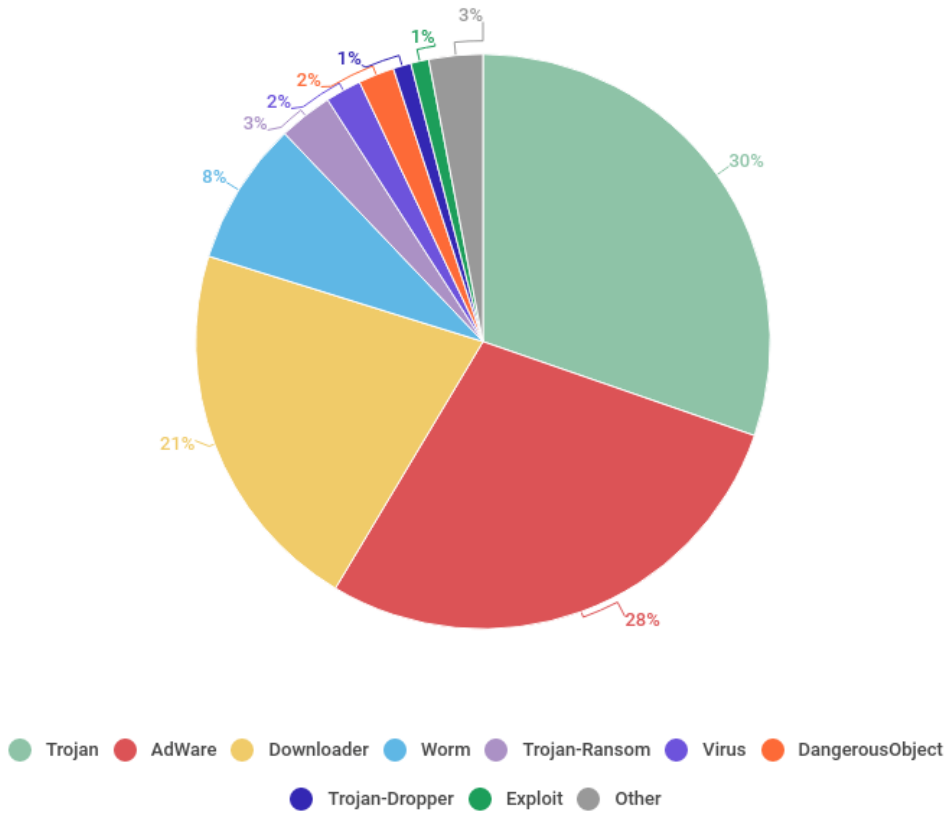



***Average number of users dealing with TV series-disguised malware files in 2018***

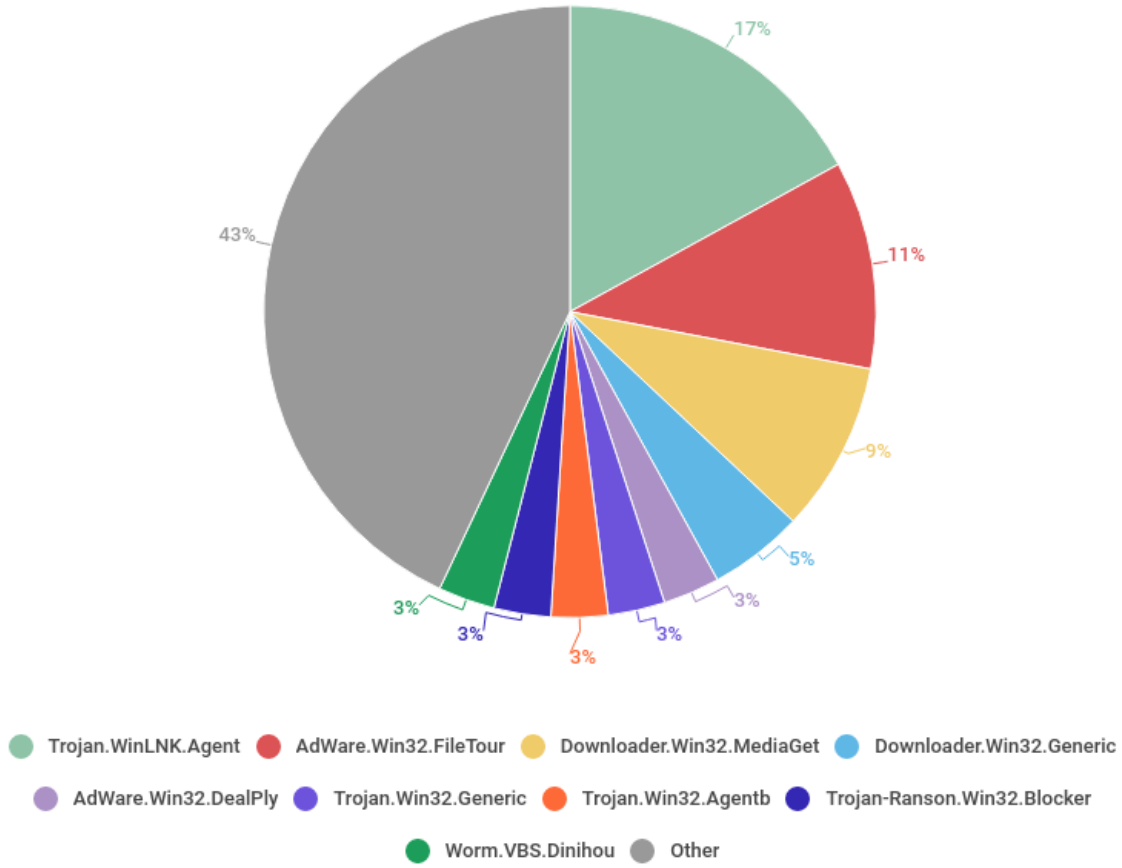
# Threat Anatomy: attack vectors and types of threats

To investigate what type of TV show-disguised threats are more likely to infect the users' computers, we extracted infected samples of the most popular TV shows in 2017 and 2018 and counted the different types and families of threats.

We detected a total of 33 threat types and 505 different families hiding behind the Game of Thrones TV show title. The top three most popular threat categories among these were: **Trojan, accounting for almost one third of all threats; not-a-virus:Downloader with 21%; and not-a-virus:AdWare with 28%.** The 'not-a-virus' type of threats are usually not classified as malware, yet such programs may interfere with users' sessions causing unwanted actions to be performed. AdWare, for instance, can show unsolicited ads, alter search results and collect user data to deliver targeted, contextual advertising.




***Top 10 most popular malware types by the share of unique users attacked in 2017-2018***

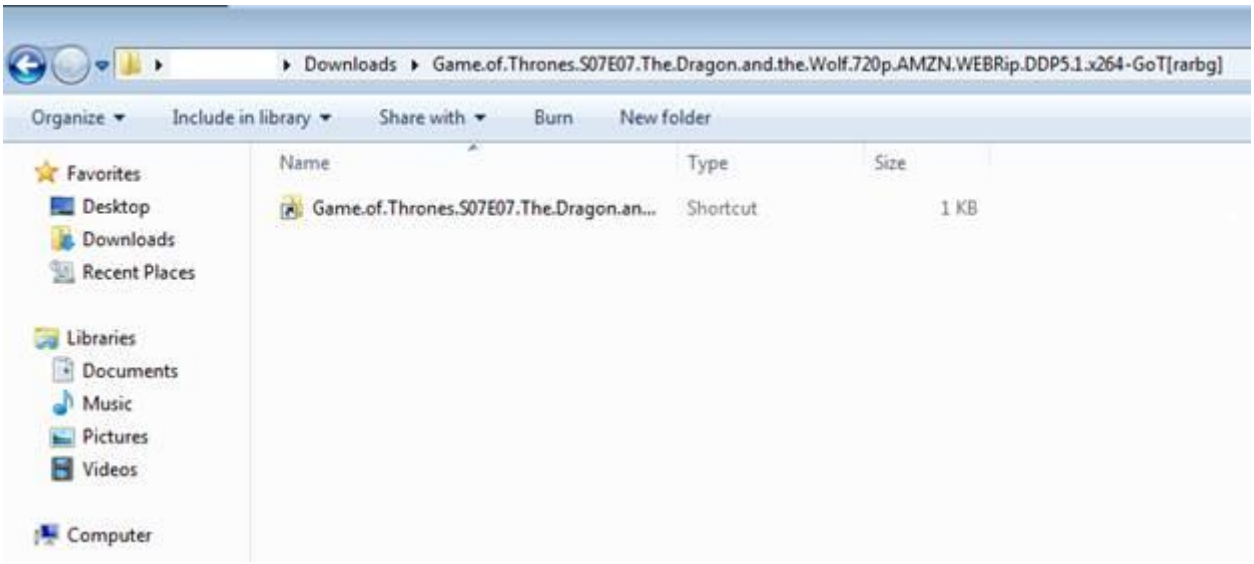



***Top 10 most popular malware families by the share of unique users attacked in 2017-2018***

As we looked at the statistics of threat types and threat families, we realized that the top-three most popular families represented the three most popular types of threats.

## The most widespread threat: Trojans

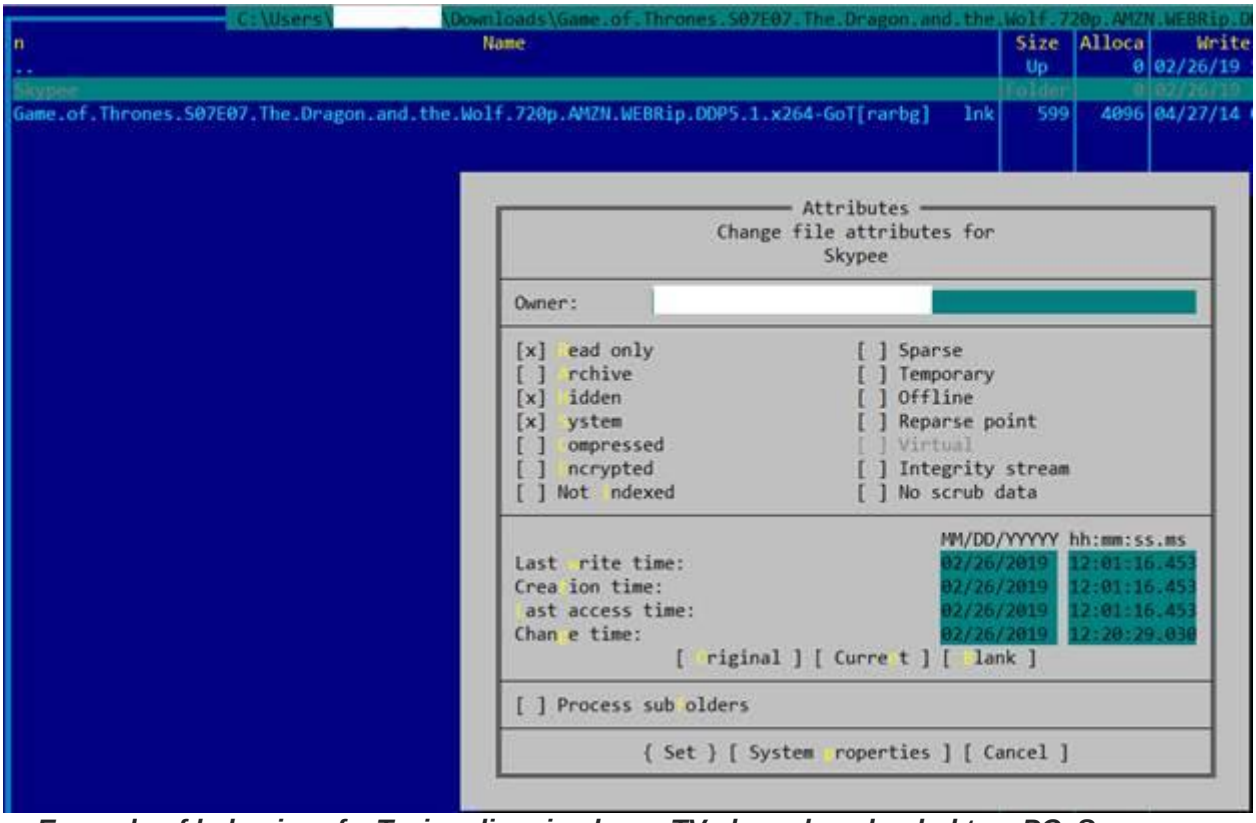
According to the statistics, the most common **type of threat was Trojan. And in 17%** of all cases pirated TV shows users had to deal with worms of the **Trojan.WinLNK.Agent** family. A Trojan is a dangerous type of malware able to cause much harm, from information theft to gaining control of the infected system. The Trojan family pretending to be Game of Thrones that most actively attacked users usually looks like a shortcut to the file and is distributed very differently – usually through emails or questionable websites.




***Example of a Trojan disguised as a TV show downloaded to a PC***

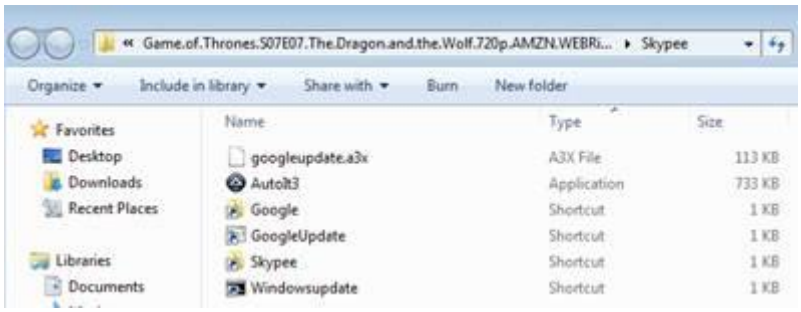
The common scenario is this: the user downloads a torrent file or receives an archive with a shortcut by email. At first glance the package contains a copy of the long-awaited episode.

Yet, apart from the shortcut, the archive will also contain a hidden folder with the 'system' attribute on, making it invisible even if Windows Explorer is configured to display hidden files.




***Example of behavior of a Trojan disguised as a TV show downloaded to a PC. Source: Kaspersky Lab***

By clicking on the shortcut in hope to watch the video, the user will launch the AutoIt script sitting in the hidden folder along with its interpreter and several other .lnk files.




***Example of behavior of a Trojan disguised as a TV show downloaded to a PC. Source: Kaspersky Lab***

```
C:\WINDOWS\system32\cmd.exe /c start ..\Skypee\AutoIt3.exe  /AutoIt3ExecuteScript
..\Skypee\googleupdate.a3x explorer "%CD%" & exit
```

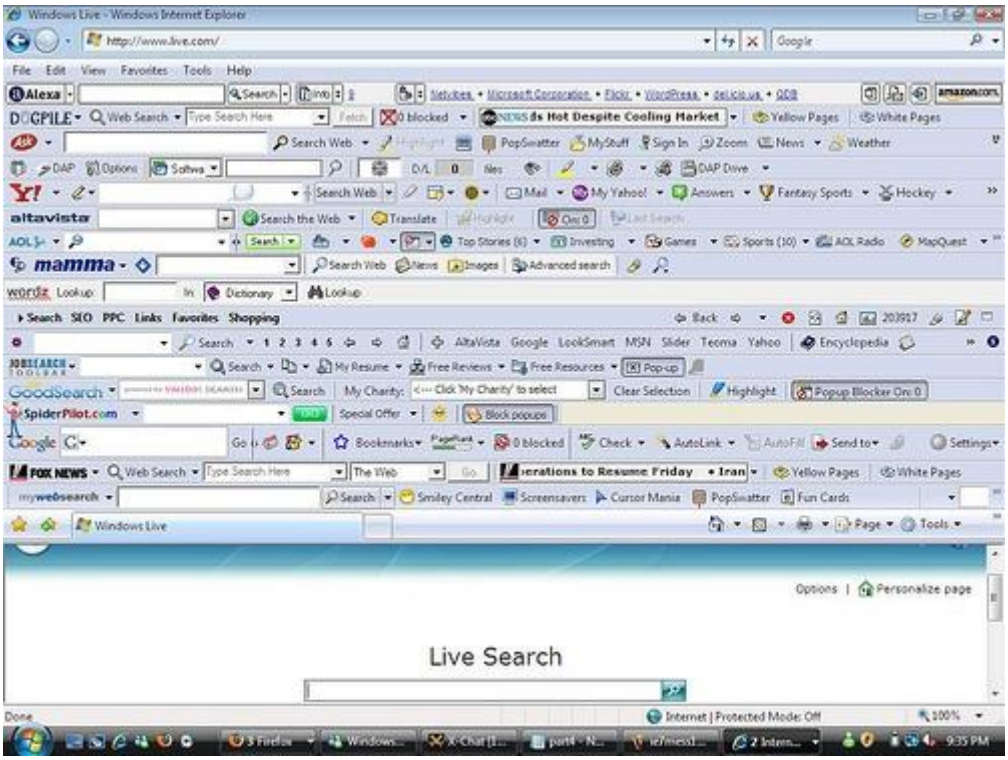
***Example of behavior of a Trojan disguised as a TV show downloaded to a PC. Source: Kaspersky Lab***

AutoIt is a worm that spreads through removable disks and runs a backdoor, which is then added to autorun (writing paths to the .lnk files from the hidden folder) and used to accomplish the following actions:

1. Display a specified message
2. Execute commands in cmd.exe
3. Download and launch to% Temp% files
4. Shutdown/restart computer
5. Go to a specified URL
6. Auto-click various webpage items
7. Terminate, restart, update itself

## Not-a-virus rounds up the top three

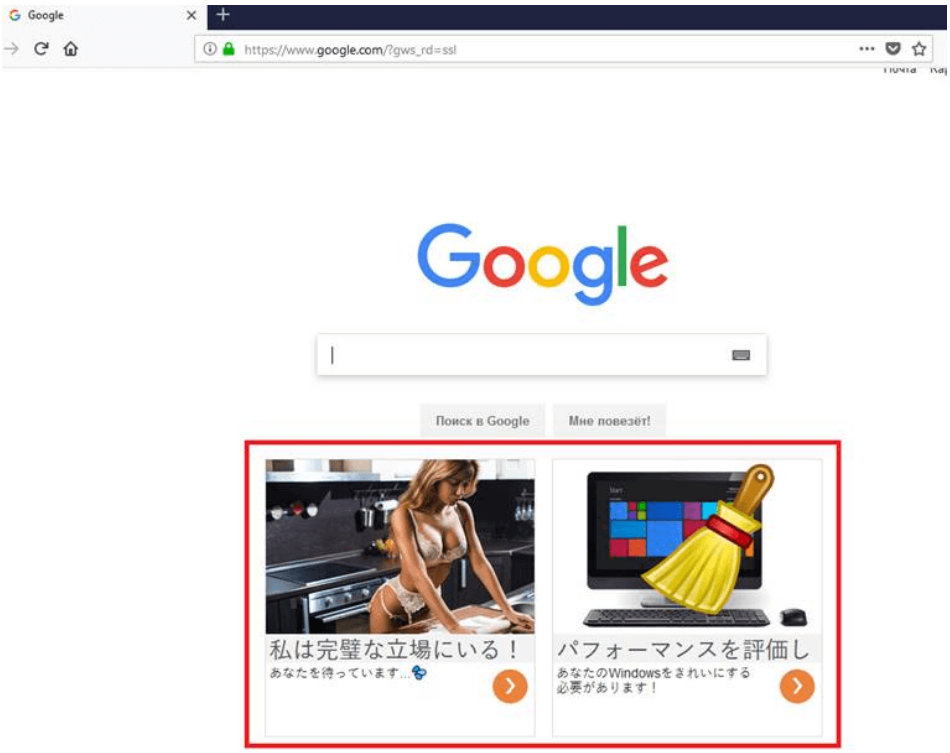
The second and third place in the rating list of the most popular types of threats and their families are occupied by the not-a-virus families, also known as potentially unwanted software: adware and downloaders.




***Example of a PC browser page with AdWare installed. Source: Kaspersky Lab***

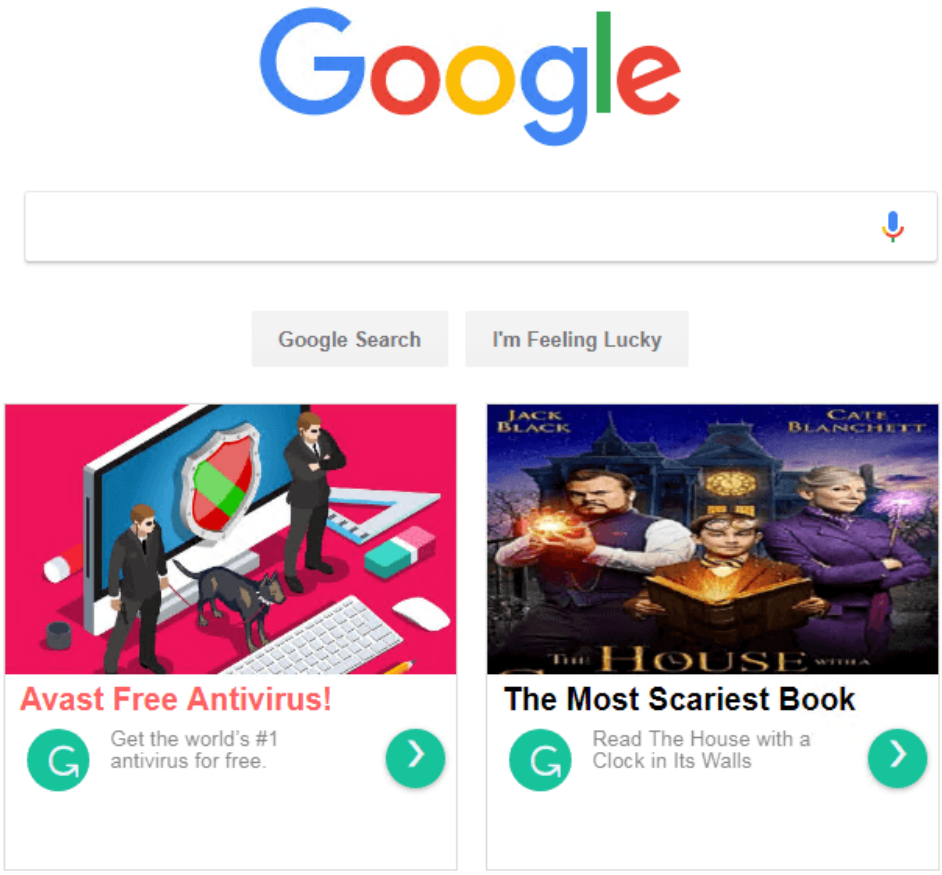
One of the most popular threat families is not-a-virus:**AdWare**.Win32.FileTour. Kaspersky Lab classifies it as a type of AdWare. While technically AdWare may represent legitimate software, in many cases users have to deal with file partner programs trying to install partner software and sometimes also download malware to their computers. Unlike not-a-viruses, these threats can vary in type and include malicious miners, password stealers, banking Trojans, and so forth. This happens because the owners of file partner programs often neither know, nor want to check what kind of software they distribute.

Just like not-a-virus:Downloader – another popular not-a-virus threat we will be describing in more detail later – it is distributed through download portals, yet unlike Downloaders it can also be spread through torrent trackers.




***Example of an internet page on a PC with adware installed. Source: Kaspersky Lab***

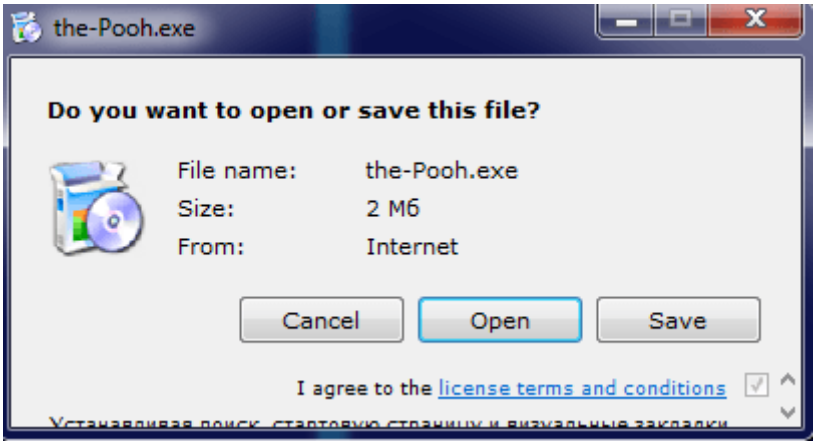
Another distinguishing feature of adware compared to the relatively innocent not-a-virus:Downloader is the use of more aggressive strategies. AdWare can trick its way into the users' devices and play dirty, for instance, by disguising executable files (.exe files) as media (for example, The.Walking.Dead.S06E04.FASTSUB.VOSTFR.HDTV.XviD-ZT.**avi.exe**).

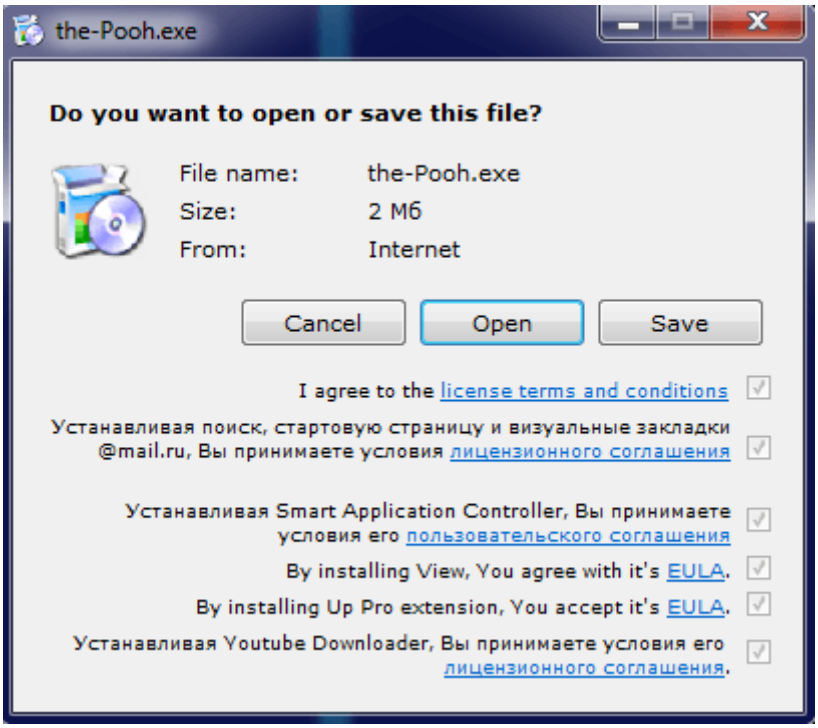



***Example of an internet page on a PC with adware installed. Source: Kaspersky Lab***

**The third place** is held by the not-a-virus:Downloader threat. This threat type can be completely innocent yet annoying as it will attempt to download utilities. Positioned as software made to simplify downloading files from the internet, the threat is used to distribute the leading malware family hiding behind the Game of Thrones title – MediaGet (we put it in the not-a-virus family: Downloader.Win32.MediaGet) – as well as many others such as uBar, AppDater, etc.

The typical not-a-virus:Downloader distribution scheme is quite simple – the user visits a website in search for a TV show or another media file and sees many different 'download' buttons.

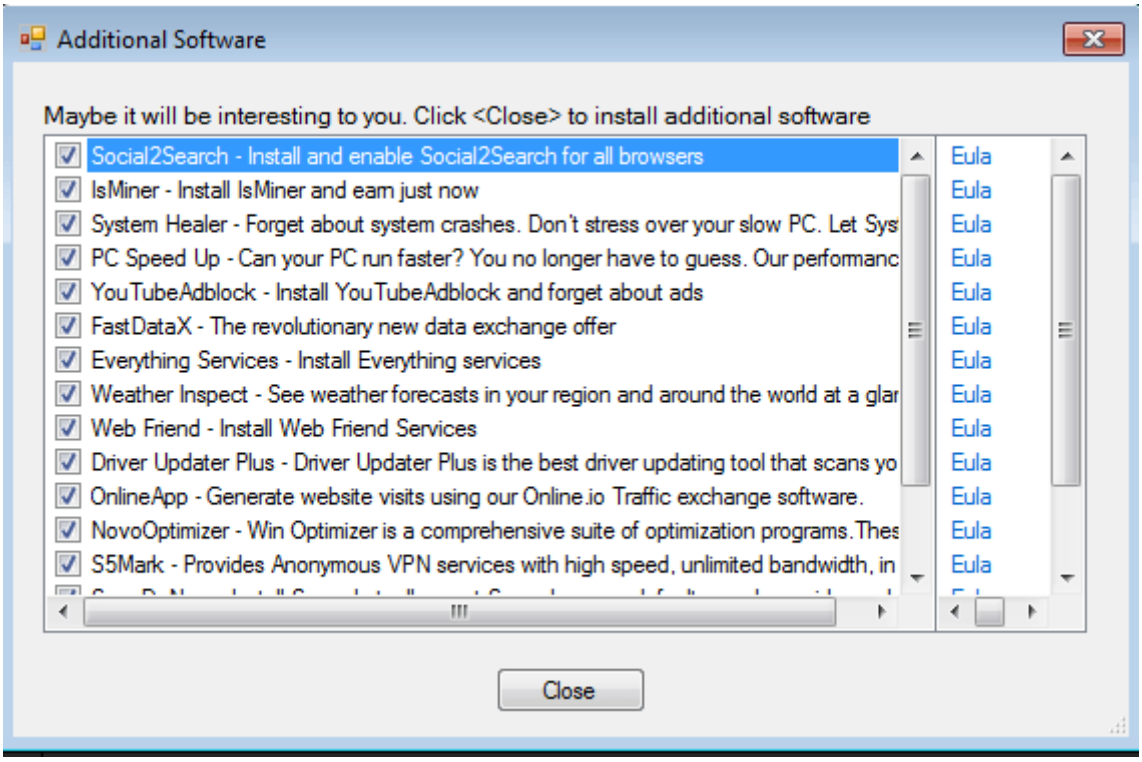





***Example of a hidden download agreement in not-a-virus:Downloader. Source: Kaspersky Lab***

It is very difficult to figure out which one leads to the desired TV episode, so the user often ignores or misses the information displayed like ‘download using the download manager’.

As a result, instead of the video the user gets nothing but a utility-loader through which the content can be potentially downloaded.




***Example of a not-a-virus:Downloader. Source: Kaspersky Lab***

Downloader utilities themselves are usually quite harmless, yet they are trying to cement themselves firmly into the system and may show unwanted ads or suggest additional unwanted software. This is not dangerous but rather annoying.

## Danger Things: how to stay safe

As the world tightens up policies regarding pirated content and treats intellectual property more like physical property, malware distributors seem to be leaving file hosting and torrent websites. But, as we said earlier, this might be due to increased popularity of streaming websites that do not require files to be downloaded, yet might be a source of different threats.

At the same time, we've seen that the number of users faced with TV-series-themed malware is still quite large and this threat is proving problematic to those who are looking for free content on the internet. Especially when it comes to extremely popular shows like Game of Thrones, The Walking Dead, Arrow and others. Game of Thrones deserves a special mention as it was one of the very few series which had no new episodes out last year but still topped the malware charts, according to Kaspersky Lab telemetry.

That said, it won't come as a big surprise to see a new wave of malicious activity accompanying the release of the final season of Game of Thrones in April 2019.

The best way to avoid falling victim of any hostile tactics and make sure you are not hit by a Trojan, which will to zombify your PC, but are going to safely enjoy yet another episode of your favorite TV series, is to use only legitimate sources of content. But even if you do follow that rule, stay alerted as it is quite possible to encounter malicious activity accidentally.

**To avoid threats coming from untrusted content distributing platforms, we recommend:**

- Pay close attention to website authenticity and do not visit them unless you are sure they are legitimate
- Always make sure the website is genuine by double-checking the URL format or company name spelling before you download. Fake websites may look just like the real thing, but there will be anomalies to help you spot the difference
- Pay attention to the extension of the downloaded file. If downloading TV show episodes, the file must not end in **.exe**
- Be careful about the torrents you use and do look up the comments about the downloadable files. If comments are unrelated to the content, you are probably looking at malware
- Don't click on suspicious links promising exclusive early premiere of the latest episodes; consult the TV show schedule and keep track of it
- Use reliable security solutions for comprehensive protection against a wide range of threats, such as Kaspersky Internet Security