TRUST IN
GERMAN
SICHERHEIT

G DATA SECURITYLABS MALWARE REPORT

HALF-YEAR REPORT
JULY – DECEMBER 2013

CONTENTS

AT A GLANCE

- In the 2nd half of 2013 the number of new malware programs increased by 24% to 1,874,141.
- Compared to 2012, the number of new malware strains rose by 28% in 2013. The 3,384,075 detected significantly exceeded the forecast milestone of 3 million. As an average over the year, 9,271 new malware types were identified every day.
- Adware is on the increase. It is not just the number of malware types that is increasing. Instances of individual adware families are also spreading fast and account for the Top 10 of most common malware types.
- Exploits are not very numerous. However they play a significant role in automated attacks.
- 99.9% of all malware runs under Windows. The proportion of .NET malware has increased to 5.2%.

- Malicious websites are only spread across marginally more categories than in the last half year (2.6%).
- New in the Top 10 of dangerous websites is the gambling category.
- Websites in the education category are no longer in the Top 10.

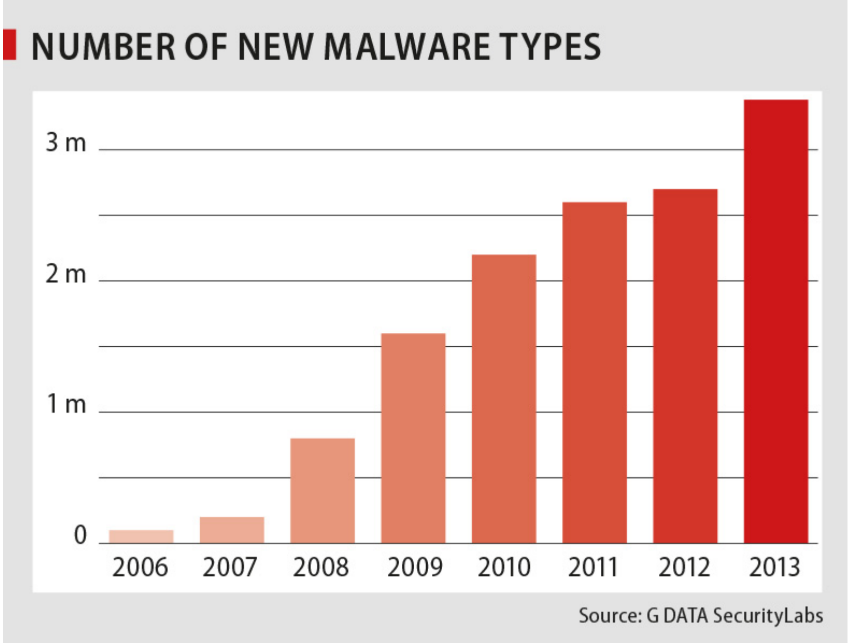
- The effect of a botnet server takedown initiated by Microsoft fizzled out quite quickly.
- The arrest of the developer of the Blackhole exploit kit had more effect, especially on the ZeuS clone Citadel.
- The Bebloh family of banking Trojans held onto its market share and actually increased it. The Bankpatch family is no longer a factor.
- Cridex (alias Feodo) achieved huge infection numbers via spam campaigns.

Forecasts and trends

- Once again, the number of malware categories will increase in the coming year. We expect that the milestone of 10,000 new malware types per day will be surpassed.
- Adware and encryption Trojans will increase.
- Hosting will continue to be carried out in high-tech countries.
- As a result of major sporting events, we expect that attacks on gambling and sport websites will occupy a greater share.
- Banking Trojans will become even more refined.

MALWARE STATISTICS

2013 broke all previous records once again in terms of the number of new types of malware program[1], ending the year with a total of 3,384,075. In the second half of 2013, G DATA SecurityLabs experts registered a new high: 1,874,141 new malware types.


NUMBER OF NEW MALWARE TYPES

Source: G DATA SecurityLabs

The second half of the year saw an increase of 364,207 compared to the first half of the year, representing an increase of 24%. A comparison of the total numbers in 2012 and 2013 shows an increase of around 28%. The anticipated breakthrough of the three million mark for new types of malware was not only achieved, but significantly exceeded. Based on these figures, almost 9,271 new types of malware were produced every day on average in H2 2013.

Once again, the number of new malware types will continue to increase in the coming year. It is possible that the milestone of 10,000 new types of malware per day will be exceeded.

Categories

Analysis of the categories of new malware program types allows several conclusions to be drawn as to the aims of cyber criminals. Malware programs are classified on the basis of the malicious actions that they execute in an infected system. The most important categories are shown in Figure 1.

The dominant categories in the last year, **Trojan horses, downloaders, backdoors** and **spyware**, continue to be found at the top of the ranking in 2013.

Downloaders are very frequently used by attackers to load the actual malware onto the system. How the victim's computer will be misused is not determined until the second step. This makes attacks on computer users more variable. Quite often they will then smuggle **backdoors** onto the system to control computers remotely and

[1] The figures in this report are based on the identification of malware using virus signatures. They are based on similarities in the code of harmful files. Much malware code is similar and is gathered together into families, in which minor deviations are referred to as variants. Fundamentally different files form the foundation for their own families. The count is based on new signature variants, also called malware types, created in the second half of 2013.

secure permanent access to the infected computer. **Trojan horses** remained the cyber criminals' most popular weapon, being valued for their variability and broad scope of malicious functions.

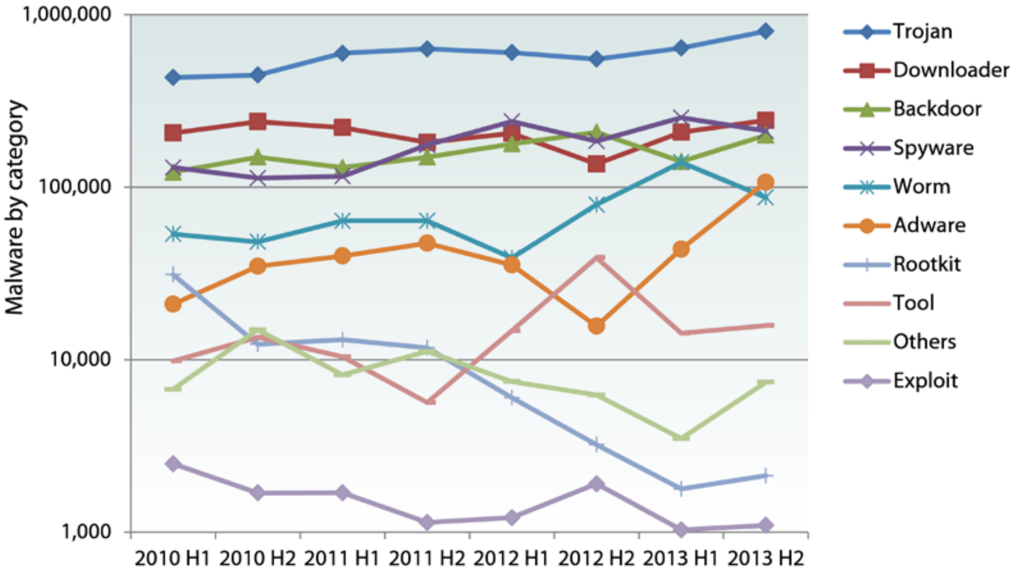


***Figure 1:** Number of new malware instances by category in the last six-month period*

The recent large increase in the number of new malware types in the **adware** category is notable. The distribution of generally unwanted browser enhancements and software add-ons, which then display unsolicited advertising or offers to the user, is a very lucrative business for attackers. They have a very good effort-to-reward ratio, which is also reflected in the actual number of attacks against computer users that were fended off, as reported in the RISK MONITOR section.

The number of exploits increased slightly, but is nevertheless low overall. However, this does not mean that exploits pose no threat. They are a key component of automated attacks, being used for example in drive-by infections when visiting websites. Web exploit kits are important goods in the black market. They enable even inexperienced users to exploit websites for the purpose of distributing malware without the need for any special knowledge.

Platforms – Windows still the focus

The vast majority of the new types of malware continue to target the Microsoft Windows operating system. Consequently, the proportion of **.NET developments (MSIL)** once again showed a significant increase, their share rising to 5.2%, which represents a doubling of the share in H2 2013 (2.6%) and a tripling of the share in H2 2011 (1.4%). Not only does this demonstrate an increase in the proportion of **MSIL** - the number of new malware types also more than doubled in the second half of last year and almost tripled overall in last year.

In total, more than 99.9% of all new malware programs in H2 2013 were targeting **Windows**.[2] The proportion did not change compared to the previous half year.

[2] For us, malware for Windows means executable files in PE format that are declared there for Windows or executed files created in Microsoft Intermediate Language (MSIL). MSIL is the intermediate format that is used in the .NET environment. Most .NET applications are platform independent but they are used almost exclusively on Windows computers.

	Platform	#2013 H2	Share	#2013 H1	Share	Difference #2013 H2 #2013 H1	Difference #2013 H2 #2012 H2
1	Win	1,774,287	94.7%	1,462,527	96.9%	+21.3%	+45.0%
2	MSIL	97,686	5.2%	46,448	3.1%	+110.3%	+195.8%
3	WebScripts	720	<0.1%	540	<0.1%	+33.3%	-33.8%
4	Java	154	<0.1%	163	<0.1%	-5.6%	-63.9%
5	Scripts[3]	642	<0.1%	146	<0.1%	+333.9%	+63.8%

Table 1: *Top 5 platforms in the last two six-month periods*

A glance at the next section, RISK MONITOR, shows which attacks were actually executed against computer users in the past half year, irrespective of the changes in new malware program types.

RISK MONITOR

The risk monitor shows the Top 10 defeated attacks against computer users[4] involving G DATA security solutions and activated MII.[5] The most frequently averted attacks in the second half of 2013 are shown below. A permanently updated list for individual months can be found on the G DATA SecurityLabs website.[6]

Rank	Name	Percent
1	Gen:Variant.Adware.BHO.Bprotector.1	5.75%
2	JS:AddLyrics-B [Adw]	2.33%
3	Trojan.Downloader.JQAC	1.61%
4	Gen:Variant.Graftor.10487	1.50%
5	JS:AddLyrics-D [Adw]	0.92%
6	Gen:Adware.MPlug.1	0.86%
7	Win32:DNSChanger-VJ [Trj]	0.76%
8	Adware.DealPly.B	0.60%
9	Adware.WebCake.C	0.60%
10	Adware.BHO.BProtector.A	0.58%

Table 2: *The Top 10 attacks registered by the MII in H2 2013*

The observed trend of more and more new malware being added to the **adware** category is also reflected in the registered attacks on G DATA users. The Top 10 is filled with attacks experienced by most users as very inconvenient, very troublesome changes to their system. In the past two half years, the **Sirefef** malware family (also called **ZeroAccess**) has dominated the rankings. This family also included widely distributed components

[3] "Scripts" are batch or shell scripts or programs that have been written e.g. in the scripting languages VBS, Perl, Python or Ruby.

[4] The way of counting in this section differs from the preceding section because the number of actual attacks is evaluated rather than the number of new malware types. A single malware program can have a massive effect when the attacks are counted, even if the family has produced few (new) variants (for example: Adware.BHO.BProtector.A)

[5] The Malware Information Initiative (MII) relies on the power of the online community and any customer that purchases a G DATA security solution can take part in this initiative. The prerequisite for this is that customers must activate this function in their G DATA security solution. If a computer malware attack is fended off, a completely anonymous report of this event is sent to G DATA SecurityLabs. G DATA SecurityLabs then collects and statistically assesses data on the malware.

[6] https://www.gdatasoftware.co.uk/securitylabs/top10-malware.html

ready-made for click fraud. Yet the actual change observed can no longer be ascribed to just one particular malware family.

Adware.BHO.BProtector.A, a method of detecting potentially unwanted browser toolbars, earns money for attackers under the pay-per-install principle. In this particular case, the Babylon tool bar is involved. Even though this malware only ranks tenth in the current Top 10, it is nevertheless an indicator of an ongoing trend marked by the quest for direct monetary profits, without going through data theft or similar scenarios. **Gen:Variant.Adware.BHO.Bprotector.1**, in 1st place in the half year assessment, is the re-engineering of the identifier just mentioned. Numerous other adware instances relating to the Babylon toolbar have been generically associated with it.

The malware variants in the **Addlyrics family** also fall into the adware category. As the family name suggests, this involves song lyrics that can be overlaid onto streamed videos. Yet besides the official function sought by the user, the detected variants also include functions for displaying unwanted advertising.

DNSChangers change the computer's Internet settings. The contact on the Internet is generated via servers that can display fake content. Here again cash is frequently earned through advertising.

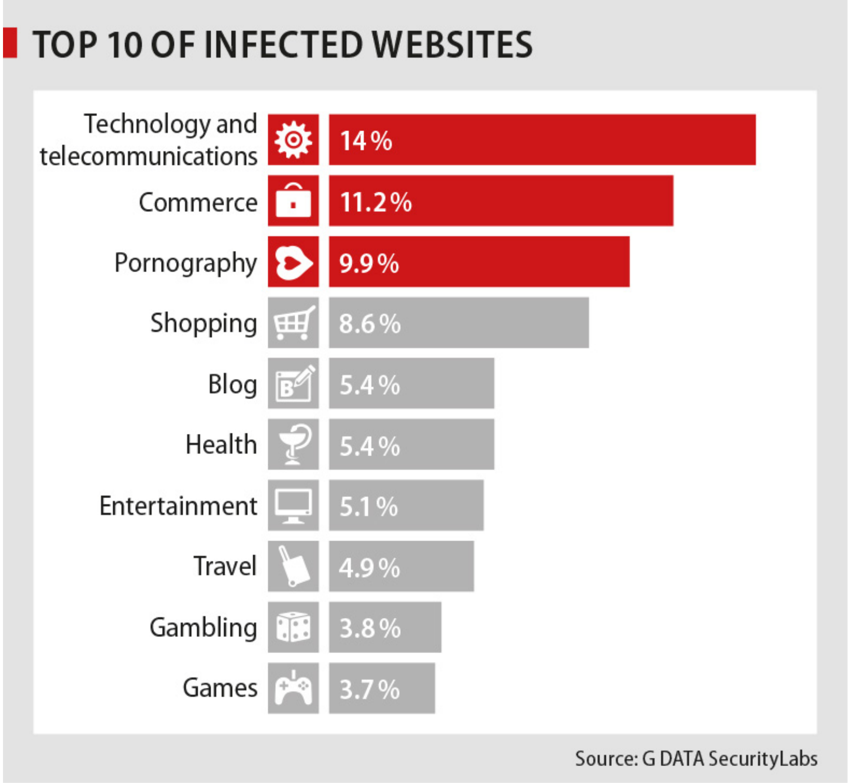
WEBSITE ANALYSES

Categorisation by topic

In the second half of 2013, experts at G DATA SecurityLabs recorded a new entrant in the Top 10 categories of malicious websites.[7]

Gambling is the new thematic category that has never previously made the leap into the Top 10 rankings in the analyses. The new entrant climbed to **9th place** with 3.8%. Prominent representatives of this category are online casinos, online betting shops and lotteries.

If the thematically similar categories of **games** and **entertainment** are taken into consideration, these three taken together make up 12.6%.
The ten most dangerous categories make up exactly 72% of the total. That is a drop of 2.6% compared to H1 2013; however, the level remains high. It means that almost one in three dangerous websites comes from one of these thematic areas. The Top 5 categories add up to almost 50% - which is around 5% less than in the first half of the year.



TOP 10 OF INFECTED WEBSITES

Source: G DATA SecurityLabs

As a result, the **education** category has dropped out of the top rankings, ending up in 11th place in the second half of the year.

[7] In this context, malicious websites include phishing sites as well as malware sites. The count also does not distinguish between domains set up specifically for this purpose and legitimate sites that have been manipulated.

Categorisation by server location

The local distribution of malicious websites indicates which countries malicious websites are predominantly hosted in. In this analysis, pages containing malware and phishing sites are once again taken together. Figure 2 shows that, when selecting host countries, cyber criminals mostly look to countries where they can find good infrastructure and cheap prices for making websites available.

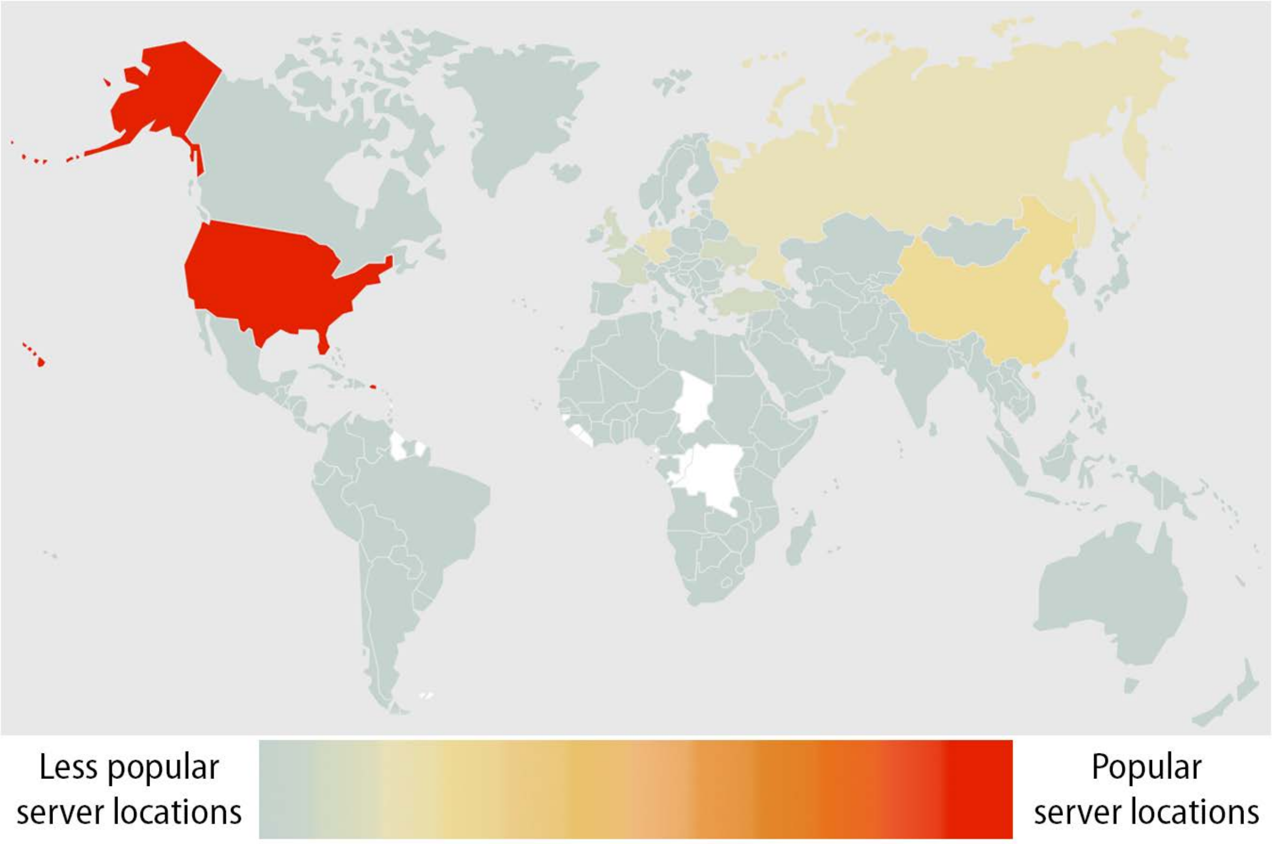


Figure 2: *Choropleth map showing how many hosted, malicious websites there are in different countries*

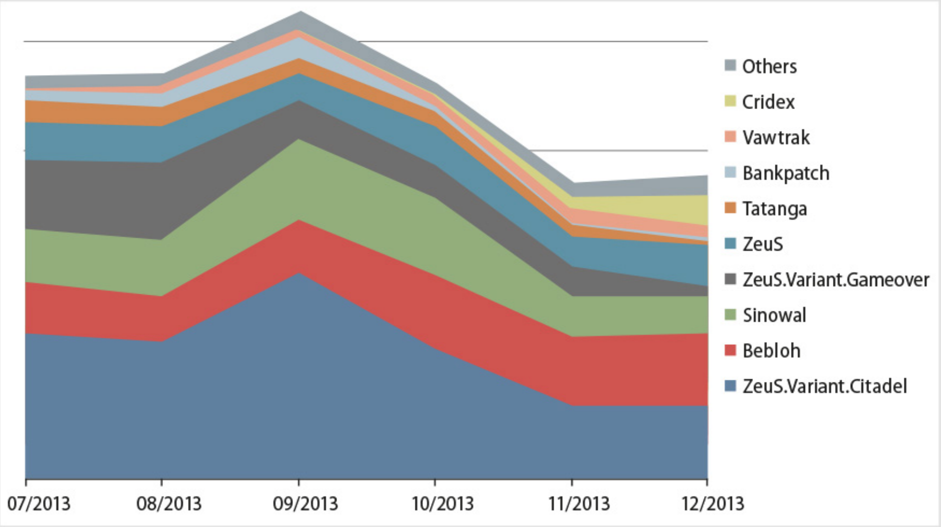
In the second half of 2013 more malicious websites were noted in **China** compared to the previous half year. This means that China has recorded an increase in this analysis since H1 2012 and in H2 2013 is the country with the second most malicious websites, after the **USA**. **Russia** has given up this second spot and now sits on a par with **Germany** in the list of displayed frequency distribution.

BANKING

Changes in the banking Trojan market

The desired effect failed to materialise after Microsoft carried out an organised takedown of command & control servers at the end of the first half of 2013.[8] September saw the highest infection rate of the second half of the year, around 16% higher than in July. The effect of the takedown manifestly fizzled out.

FREQUENCY OF OCCURENCE OF BANKING TROJANS IN H2 2013



Source: G DATA SecurityLabs

However, another blow was delivered against the cyber criminals: the ringleader of the Blackhole exploit kit, who went under the pseudonym "Paunch", was arrested.[9] PCs have been contaminated en masse with malware by means of exploit kits. And the Blackhole exploit kit in particular was notorious for the broad distribution of banking Trojans. The drop-off in infections was particularly noticeable with the ZeuS clone Citadel. Bankpatch, the Trojan that implemented an innovative technique for gaining control via Jabber in the first half of 2013, almost completely disappeared from the picture.

With Exploit Protection in the new 2015 product generation, G DATA offers protection against attacks using exploit kits.

At the end of the year, the number of infections levelled out at around 3/4 of the volume in September.

However, the next wave soon rolled in: Cridex (alias Feodo) achieved significant infection numbers, with numerous infections via spam email.[10]

As far as infection numbers are concerned, Bebloh emerged out of nowhere at the end of the last half year. This effect was confirmed in the second half of the year, and Bebloh continued to be one of the four most common banking Trojans. Previously Bebloh was regarded as innovative because of its returns trick, for example, but it never attracted attention through especially high infection numbers.

[8] http://www.microsoft.com/en-us/news/Press/2013/Jun13/06-05DCUPR.aspx

[9] http://krebsonsecurity.com/2013/12/meet-paunch-the-accused-author-of-the-blackhole-exploit-kit/
http://www.bbc.co.uk/news/technology-24456988

[10] https://blog.gdatasoftware.com/blog/article/cridex-banking-trojan-on-the-rise.html

The returns trick involves the user being misleadingly told by the Trojan that he has wrongly received a transfer – which also seems to appear as a deposit in his account balance (also manipulated by the Trojan). This social engineering method leads to many honest victims transferring the money back without being asked. In this case, they are directed to a form to fill out to return the transfer. In fact the recipient's account is an attacker's account, to which the victim is almost voluntarily transferring the sum in question via any type of authentication method such as TAN numbers. However, there never was any wrongly made transfer, and the transfer is a loss to the victim of the infection.

Banking Trojan trends

One trend has long been anticipated by G DATA – increased use of the Tor anonymisation technique. In September 2012, G DATA discovered Skynet[11], the first Trojan to operate its control functions via Tor. A variant was subsequently noted where a variant of ZeuS is also controlled via the Tor network.[12] The brains behind Skynet were arrested in late 2013.[13] However, almost simultaneously another ZeuS variant with Tor functionality was discovered.[14]

A further diversification can essentially be identified as a trend. In recent years there have always been specific Trojans that have dominated the market. In late 2013, however, the field of banking Trojans was practically homogeneous. This does not make discovering and pursuing the perpetrators any easier.

[11] http://blog.gdatasoftware.com/blog/article/botnet-command-server-hidden-in-tor.html
[12] http://community.rapid7.com/community/infosec/blog/2012/12/06/skynet-a-tor-powered-botnet-straight-from-reddit
[13] http://thehackernews.com/2013/12/alleged-skynet-botnet-creator-arrested.html
[14] http://www.heise.de/security/meldung/Baukasten-Trojaner-Zeus-jetzt-in-64-Bit-und-mit-TOR-2064515.html