METAFORIC

MetaFortress DS Case History

including Efficacy Comparison to other AP Systems

METAFORTRESS

keeping software safe

The Only Proven Protection System for DS/DSi

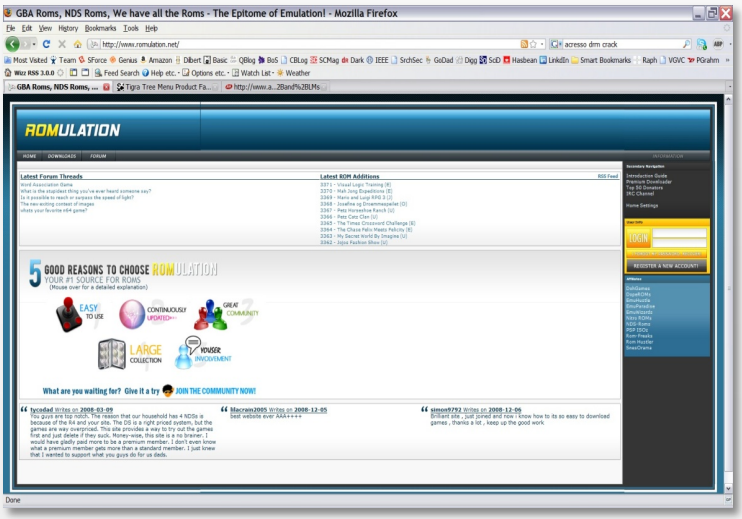
Introduction

For the past three years there has been no effective protection against ROM ripping and pirate play on "R4 style" adaptor cards for Nintendo DS and DSi games. These cards dynamically patch ripped ROMs to allow games to be played on DS & DSi, allowing easy piracy of any game for even the least technical of users.

To combat this threat, Metaforic has released a new copy protection system for DS & DSi – MetaFortress. MetaFortress adds a unique defensive system to each protected DS game, allowing it to protect itself by detecting the use of R4 style cards.

Metaforic has worked with a number of major publishers to utilise MetaFortress on their DS & DSi titles. This document reports the initial success of MetaFortress in "the wild".

Pirate Download Ecosystem



There are a large number of well known sites on the internet allowing the sharing of posted files, perhaps the most famous being BitTorrent and The Pirate Bay.

In addition there are many specific download and torrent sites designed to distribute pirate DS & DSi games, such as Romulation and GBATemp. These sites include a forum and tech support area that allows hackers and their "customers" to feedback issues with any particular game. Manufacturers of the adaptor cards are also keen followers of these forums - given the speed of reaction in creating new firmware patches for specific reported issues with games - as they wish to maintain ongoing sales of their cards to new users.

These sites serve as the distribution medium for a vast range of content, including games ripped from Nintendo DS & DSi retail cartridges. However, in most cases they do not actually create the files themselves. Individuals rip the game code from retail cartridges as soon as possible, often before retail release, and then make the resulting files available for others to download, via PC, to MicroSD flash memory cards. The process of ripping is straightforward requiring nothing more than a retail DS, a cable, and PC ripping software easily downloaded from numerous sites on-line.

This process is so widespread and easy that it results in games usually being available on the Internet before retail release, typically the day they ship to distribution.

The prevalence of piracy of DS & DSi games has resulted in several geographies becoming uneconomic areas for producers of retail DS cartridges, with consequent financial loss at all stages of the supply chain. It is this business reason alone that has resulted in the development of MetaFortress for DS & DSi.

MetaFortress Performance

Metaforic's engineering team directly engaged with the initial DS customer's development studio in order that MetaFortress could be incorporated into the production environment allowing automated protection of all games. At the same time, the developers were trained in the use of MetaFortress as an integral part of their release procedures. MetaFortress was configured to stop the game if a pirate copy was run on an R4 style adaptor card.

It should be noted that MetaFortress *does not* prevent the ripping of the game code from the cartridge, there is no mechanism to adequately prevent this, and therefore the aim is to ensure that once a game has been removed it will fail once play begins on the console. This failure may not be immediate, giving a false feeling of security to player and hacker/ card manufacture alike, however the game will fail at some stage and progress will be impossible beyond that point.

Metaforic monitors torrent and game download sites for weeks before each release. The reason for this is borne out by piracy figures; DS titles often appear for download between one and five days *before* the official release dates - sometimes even more for eagerly anticipated or leaked titles.

As expected, there was a first appearance online of one of the protected versions of the first game in advance of the launch date. This was the European version which appeared on download sites four days before the European game was due to be placed on sale[1].

However, almost immediately, posts were placed on various online forums that the uploaded ROM did not work and that no one could understand what was wrong. Posters were asking about various brands of adaptor cards, which brands worked and whether patches were available.

Initially the reaction among the posters was that the original dump from the Nintendo Cartridge was at fault, though the originators hotly disputed this. Several other ROMs were posted through the balance of the first day on a range of sites in an attempt to make sure the ripped ROM was viable. These too failed.

Across all the forums and torrent sites on which the various ripped versions appeared, individuals claimed that they had patches that would cure the problem on specific cards. Once other forum users downloaded these, the feedback came quickly that they too still failed.

It became clear to the elite hackers in the community that there was a major new protection system in place and that it had some form of checking code as the "active ingredient".

One hacker thought there might be as many as 18 checks in the code, but another, who is a leading light in the DS hacker community and creator of a DS PC emulator, reported that he had counted a huge number of checks (81) and none of them "nice". In fact this first title had a very "light" version of MetaFortress due to memory constraints and in reality there were 114 checks injected into this version of the game.

This failure to count the correct number of checks is a fundamental and very deliberate function of MetaFortress protection and results from the hackers' inability to use tools to automatically identify checks. This means that the hacker has to attempt to manually remove the checks, but in order to do so he must also first identify each check individually. Subsequent DS titles MetaFortress can have over 600 interlocking and interrelated checks.

The reaction of the hackers themselves has been interesting; the level of consternation, concern and above all confusion has validated the Metaforic's approach to DS games anti piracy. Below are some quotations from the leading providers of firmware upgrades and patches for several of the adaptor cards.

[1] It is beyond the scope of this document but this may illustrate that some of the sources of pirate ROMS may be found within the publishers' and retailers' supply chains. It only takes one retail pack to be opened for a ROM to be distributed to the world.

- Normatt (on complexity) *"I hate this might and magic game - far too many ****ing checks"*
- Normatt (on check removal) "*They all differ in different ways, and no it cannot be automated*"
- CycloDS Team (giving up on Ubisoft compatibility) *"Regarding recent Ubisoft releases - these games incorporate a whole new form of protection and we are currently working on a generic fix"*

Recently the team behind the CycloDS card have claimed "fixes" for Metaforic protected games. They point out that manual hacks are required, which is exactly as intended, and they have been working on a new "stealth mode" for their cards.

However, this mode does not work on the latest protected titles now in LotCheck and there is come debate as to the extent of their capability on the initial protected titles from last year. Their "stealth mode" seems to have a partial effect, in testing; downloaded games are still seen to fail on the card under this mode. This may be a function of the many various beta versions of their firmware, which adds to the end-user's confusion- a reasonable aim in itself.

Their claimed "success" has taken them several months from the appearance of the first title to achieve but they are obviously still very confused as they list 14 games specifically as successfully playable on their cards even though *none* of them are MF protected. They make *no* mention of the Ubisoft titles actually protected.

This confusion demonstrates their actual knowledge and capability gaps in combating even the earliest versions of MetaFortress on DS.

The efforts of the hacker community have not only validated the original principles under which MetaFortress has been developed, but have also provided a new series of protection vectors and check processes which have now been incorporated into future protection builds.

Finally, as all games have a unique version of MetaFortress, the effort expended by the hackers will have to start all over again when the next game is released. As we will see below, this performance compared favourably to other anti-piracy attempts in the market and shows MetaFortress to be the *only* proven long term protection system for Nintendo DS & DSi games.

Anti-Piracy Performance Comparison

During Metaforic's active monitoring of numerous game piracy websites and forums it was noticed from the growth in chat traffic that new games, rumoured to be protected with some form of Anti-Piracy technology, had appeared. On deeper investigation it became clear that there was a new protection API and it had been added to several releases in late 2009. These have been identified from online comments requesting patches and fixes for playability problems and the resultant patches for the cards.

Using identical methodology to monitoring our own protected titles, Metaforic has been watching and analysing the performance of these protected titles: Pokemon Soul Silver, Mario & Luigi Bowser's Inside Story, Style Boutique and Rockman.

Metaforic's methodology tracks the titles announced by the manufacturer; identifies the date upon which they are first uploaded on the internet and then tracks the known ROM and Torrent sites & forums for the first identifiable "good" crack. A good crack is defined by positive feedback on the playability and features set available to Pirate ROM down-loaders. Each good crack is then tested on the relevant card to ensure it works.

It should be stressed that the appearance online of a crack and even some initial playability does not necessarily mean that a protection system has been compromised, careful analysis is needed to determine if a game is, in reality, fully compromised.

This gathered comparison data has been used to examine the anti-piracy efficacy in the wild of a MetaFortress protected DS title alongside these three others that have a form of anti-piracy protection.

From the data gathered it became clear that Pokemon Soul Silver had remained protected for around 16 days on a single card. However, across all card types it showed average protection strength of 4.6 days. It should also be noted that Pokemon Soul Silver was translated from Japanese to English, level by level, during the time span, which may contribute to its apparently longer safe period.

Mario & Luigi: Bowser's Inside Story showed similar performance on a single card at 14 days. However, across all card types it showed average protection strength of just 4.5 days with many more cards showing cracks on day zero.

The third title, Style Boutique, showed much weaker performance. Style Boutique was cracked across all card types in just three days. The average protection strength was only 1.1 days. The later game, Rockman, appeared to be 100% compromised from launch, the protection system affording no greater safety than if the game had been released unprotected as normal

In all cases the games were cracked on all cards and are fully playable on all cards.

This explains why Style Boutique had such limited success in protection. As the technique had been seen before it took no more than an identical 2 byte patch to remove it. Unfortunately this is a common weakness in most protection systems and generally leads to a class break within 2-3 titles. As there is already a dramatic reduction in protection strength being exhibited already in this protection technique it is likely that this scheme is now effectively redundant, and that any future games protected with it will be immediately available for piracy.

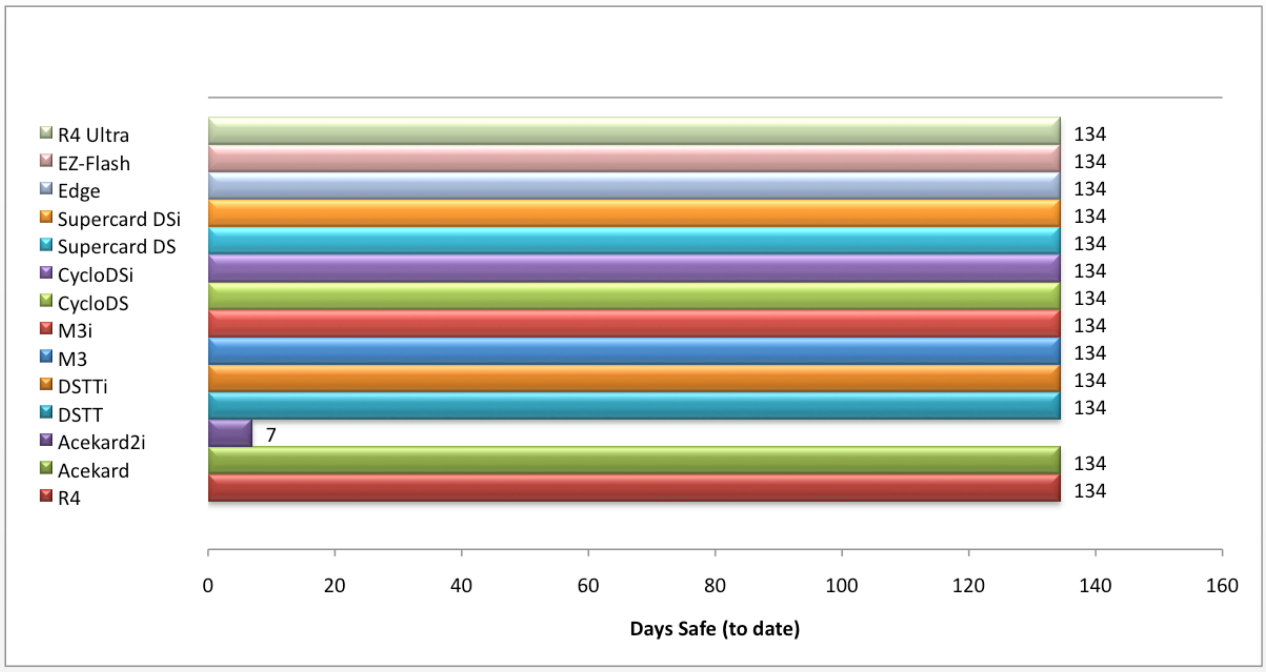
In comparison, quite deliberately, MetaFortress uses a different scheme on every protected title. Thus this kind of class break cannot be replicated on MetaFortress protected titles – they must always be hacked individually – maximising protection and days safe. The analysis data is graphed and presented below.

By comparison, the first release featuring MetaFortress has only been cracked on a single card, and is still protected on all other cards. The second release has not been cracked on any cards to date. As of this date (10th February 2010) majority protection of the first release is at 134 days, with the second fully protected for 83 days so far.

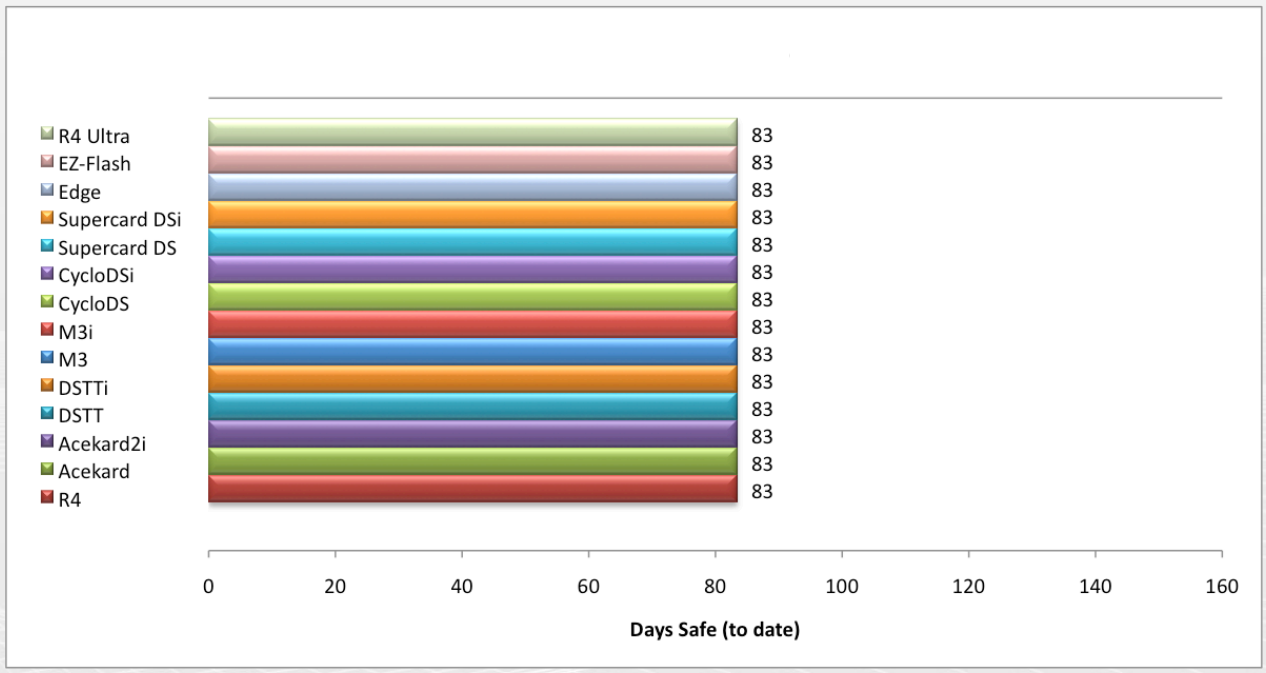
After examining the data we were able to determine that anti-piracy techniques had been used on these other titles, and that at two of them showed exactly the same technique.

Protection Effectiveness Graphs

The graphs below shows MetaFortress' "days safe" across all current R4 style cards as of the 10th February 2010.

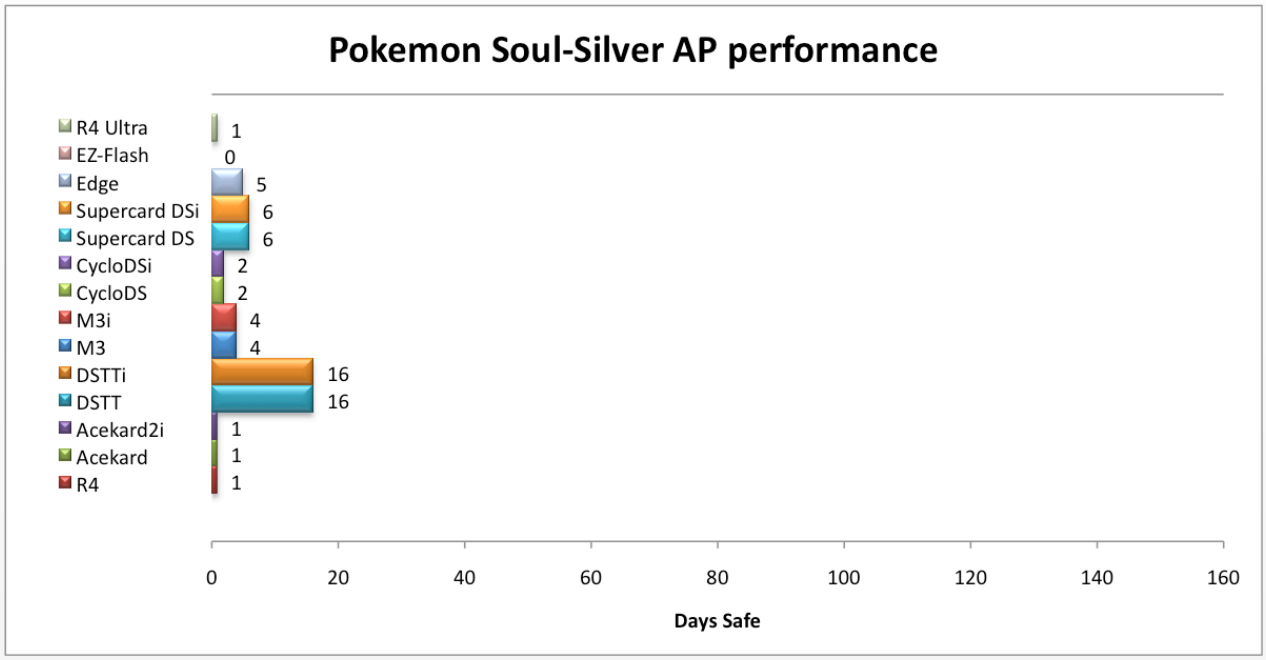


A further title below shows 100% protection so far. To our knowledge this has never before been demonstrated by any Nintendo DS or DSi Anti-Piracy protection system.

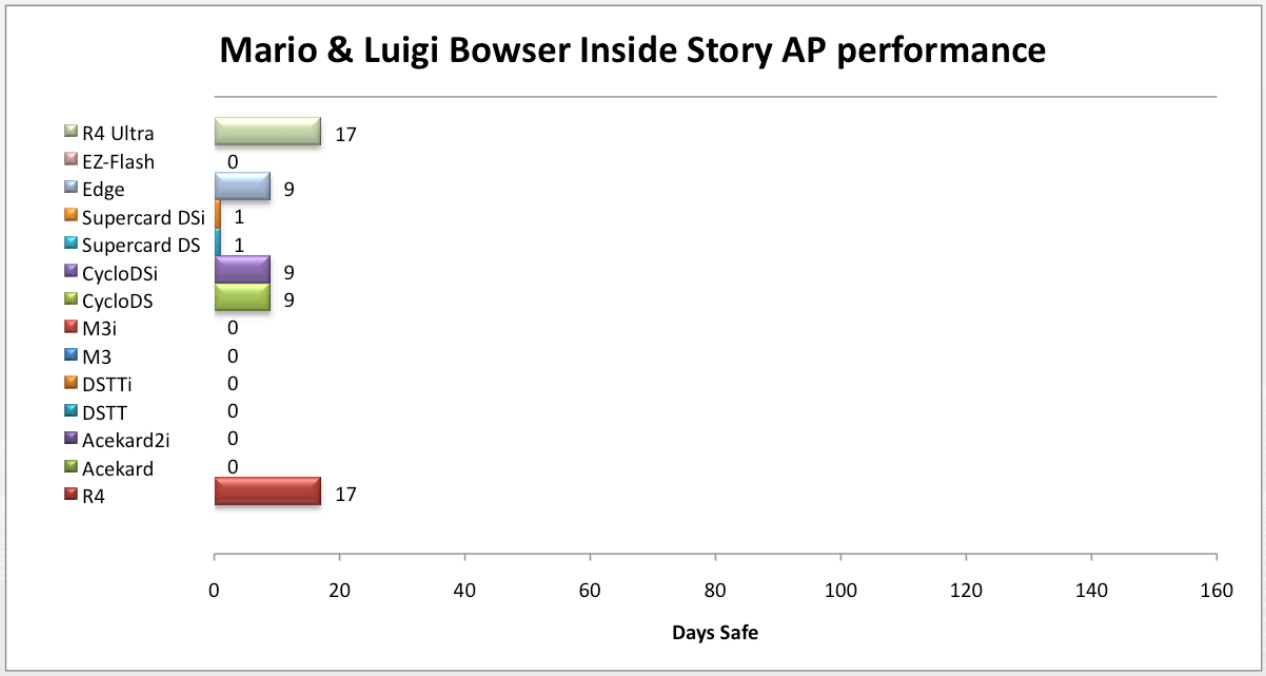


It should be noted that MetaFortress is applied to the game source code and as such does not interfere with any user's legitimate use of these cards to create their own "home-brew" software.

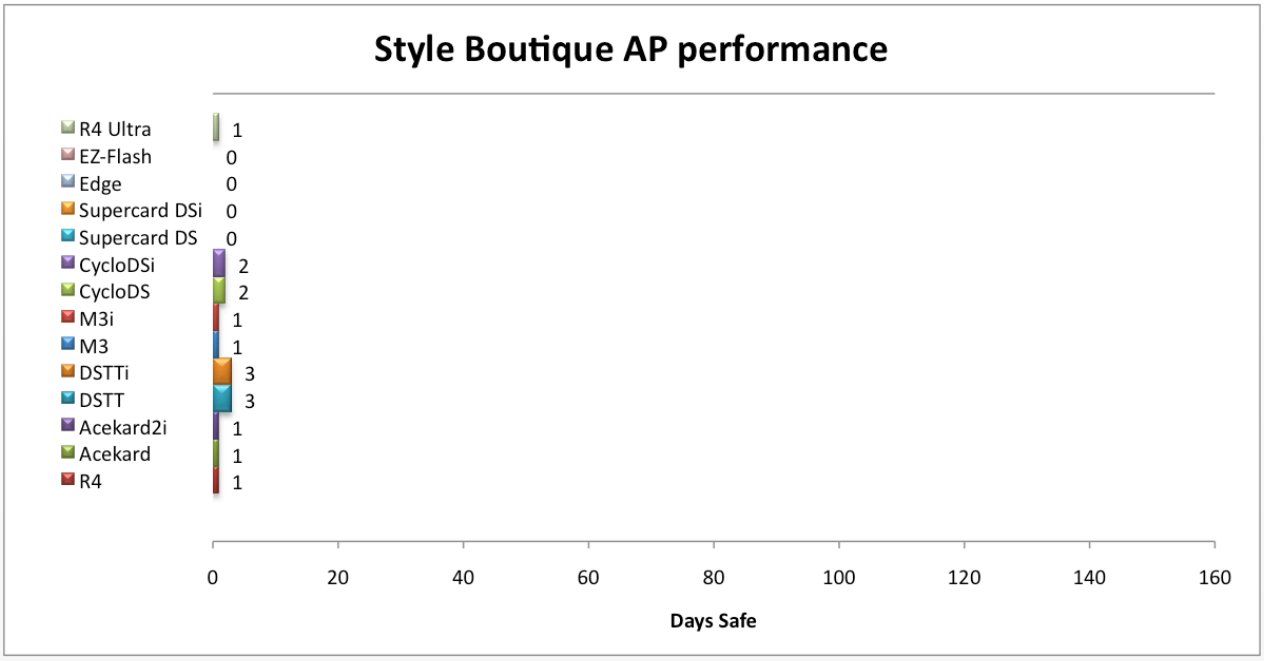
The graphs below shows “days safe” of the three titles mentioned in the body text across all current R4 style cards as of 10th February 2010.



Average days safe for Pokemon Soul Silver across all cards was only 4.6 days.

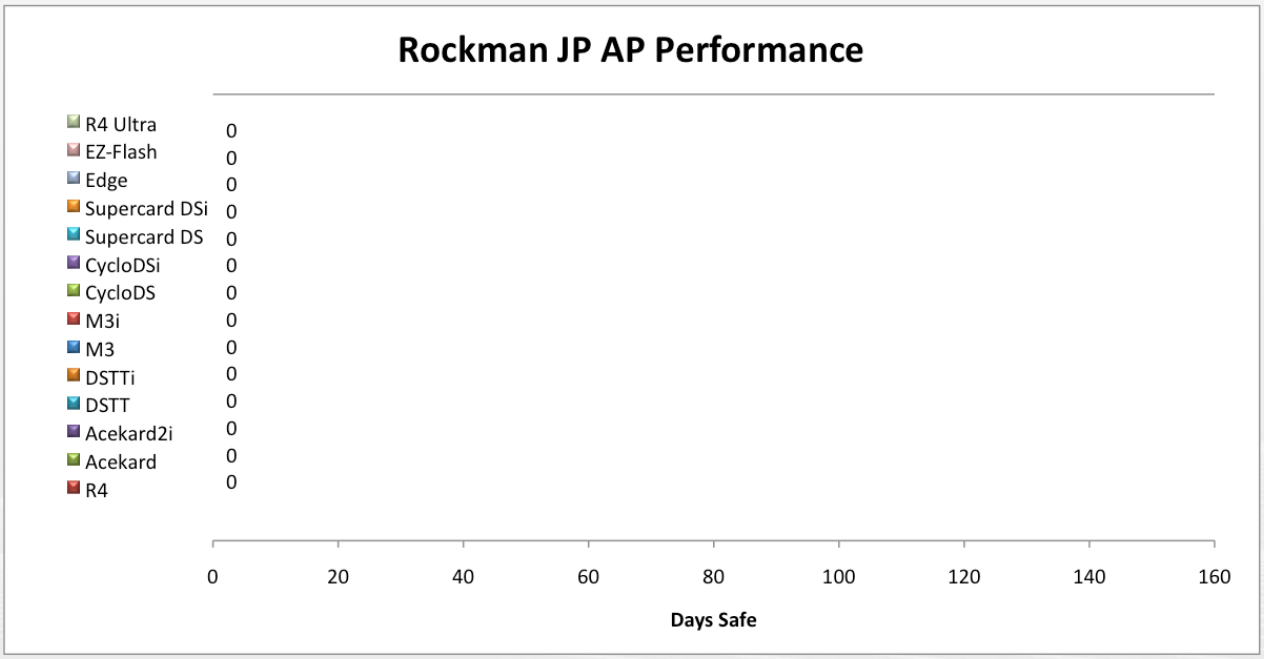


Average days safe for Mario & Bowser across all cards was only 4.5 days.



Average days safe for Style Boutique across all cards was only 1.1 days.

A fourth title was identified during a recent visit to Japan, this from a different publisher appears, on investigation to use the same methodology as the previous three.



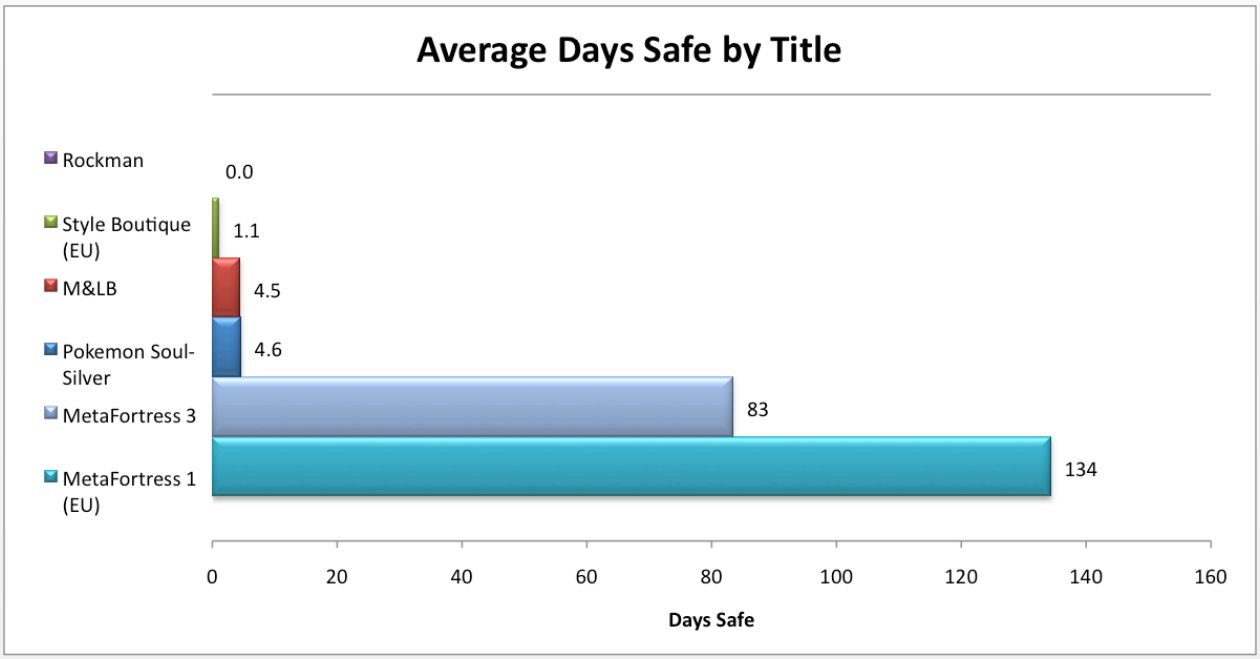
In this case the patches already developed to crack the others have been successful in ensuring that the anti-piracy measures are beaten from the game's release, thus rendering it payable from day one.

Results

The results of our analysis of the MetaFortress protected titles and the other releases show a stark contrast in the quality of protection.

MetaFortress protection is consistent, effective, and long lasting. The alternative protection is weak, patchy and degraded quickly; each patch used in cracking a title ensured a faster and more complete crack on all subsequent releases.

Simply examining the average of days safe to gain a measure of the effectiveness of the protection schemes against all cards on the market illustrates this clearly.



This ongoing performance demonstrates MetaFortress is the *only* viable long-term protection system for Nintendo DS & DSi games.

Conclusion

The first title release proved the efficacy of MetaFortress, subsequent releases have confirmed the principles followed by Metaforic in developing MetaFortress. Analysis of the ongoing, and ever more frantic, attacks on MetaFortress have allowed Metaforic to further enhance an already revolutionary protection system for Nintendo DS & DSi.

To date, the first title only operates on a single “R4” style card, out of the 15 or so on the market. This was a manual crack and was largely due to the light version of MetaFortress applied. However, even with this light version other cards are unable to play the title. This means that this game title is unavailable to more than 90% of the pirate community 134 days after first release and counting. Therefore the vast majority of pirates across the world have been unable to play the game and card vendors have been frustrated that their various firmware changes have not yielded results.

The second MetaFortress protected title is safe on all cards and has been for 83 days so far.

These “days-safe” figures represent a considerable improvement over the industry average; where viable downloads for all cards often appear days before retail versions are available to buy and is demonstrably better than the recently released anti-piracy tool seen on other games released the Autumn of 2009.

Contacts

For more information please contact:

North America	Europe & ROW
Metaforic Inc. Rockefeller Group Business Centre 560 S. Winchester Boulevard San Jose, CA95128 USA +1 408 236 7570	Metaforic Ltd. Regent Court 70 W. Regent Street Glasgow, G2 2QZ UK +44 141 333 6580
Web: www.metaforic.com	Email: sales@metaforic.com