

## VIRUS BULLETIN SPOTLIGHT: FRAME4: IN THE PICTURE

*Frame4 Security Services first became known to VB in November 2008 and after making a few enquiries it became clear that the company and, more pertinently, the services it provides have a somewhat cloudy reputation in the AV industry. VB decided to find out a little more about the company and discovered a small team attempting to provide a legitimate service for the fringes of the AV and mainstream security industry. Director and co-founder of the company, Anthony Aykut, tells the story.*

### START UP

Frame4 Security Services was set up by my business partner and me in 2006, operating from Alphen aan den Rijn, not far from Amsterdam, in The Netherlands. I handle the business side of things, while my partner is primarily involved in the technical aspects of the business, including the maintenance of the malware database.

There is a slightly Hitchcockian story behind the setting up of the business, as it all started with a discussion on a train. On the train I had met a technical rep from a company that was in the process of adding the finishing touches to a content-filtering device. The rep explained that they had experienced great problems testing the device – because they simply could not get their hands on enough malware. The developers had approached some AV companies, but had been stonewalled. After listening to the man's experiences I started thinking – what if we could develop a business model that would potentially give security researchers the room to concentrate on developing solutions, instead of spending valuable time trying to track down malware samples?

The result was the MD:Pro malware repository service. Criminals have had access to malware repositories for years,

whereas the mainstream security industry has never had a reputable research and development resource – and that is the niche we aimed to fill.

While the anti-virus industry has had file exchange mechanisms in place for many years, the exclusivity of this approach has meant that, for those security providers that fall outside of the core circle of anti-virus vendors, enormous amounts of time, money and effort have to be invested in order to gather resources for R&D and testing purposes.

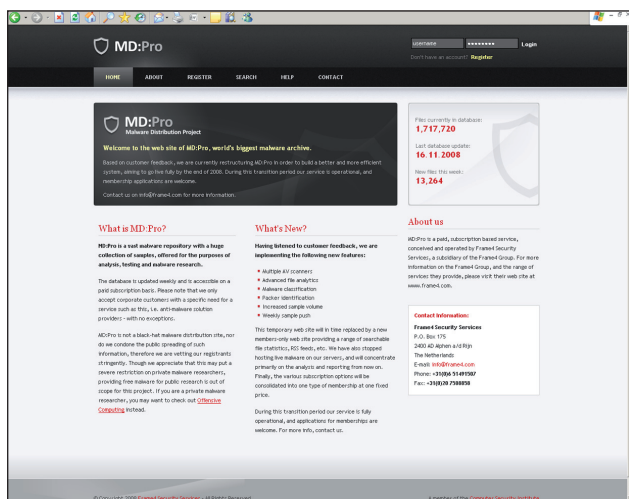
This is perfectly understandable, of course, as the AV industry invests huge amounts of time and resources in collecting malware – though I am puzzled and frustrated by the tendency for many members of the anti-virus community to look on our company and its services with suspicion and to doubt our ethics. For me it is simple: I believe that the security industry has long needed a service such as MD:Pro, and the amount of interest and positive feedback we have received from the mainstream security community affirms this belief.

### SERVICES

Initially, the company provided a multi-level pay-for-download service, starting off with around 270,000 malware samples. However, we quickly realized that this system would be unworkable as the number of samples in the database started increasing rapidly, with close to 100,000 new samples arriving per month. Realizing that it would be impossible to download such a large volume of samples from the website we went back to the drawing board to design a better system.

Frame4 currently delivers weekly samples via FTP and monthly samples on DVD, though MD:Pro is currently being re-structured in order to build a more efficient system. The new service will concentrate on collecting more samples and providing more information on those samples (for example: multiple AV scanning, advanced file analysis, malware classification, packer identification etc.), along with a secure FTP server from which the samples can be downloaded.

We are aiming to go fully live with the restructured service by the end of 2008/beginning of 2009. The new service will be complemented by a members-only website providing a range of searchable file statistics, RSS feeds, etc., though it will no longer be possible to download live samples from the website. We have also decided to get rid of the various different subscription options we started with and instead provide one type of membership at a fixed price.



## ETHICS

While we do not have an 'ethics statement' *per se*, we do have a strict set of rules and guidelines within which we operate, and we stick to them rigidly – for example, we only provide malware to corporate customers, and only to those in the IT security field. We made this decision on day one and we have stuck by it without exception. Since we began operating we have had many requests from individuals wanting to access the database – particularly in the early days – but we have always stuck to our guns and declined to do business with non-corporate customers.

We are lucky in that our customers are generally well-known anti-malware providers or respected players in the IT security field – and if we are dealing with specific individuals within these companies, their identity can easily be verified by contacting the company directly. However, if we are in any way in doubt about a company, its motives (what it is going to do with the malware) or the individual(s) we are dealing with within a company, we will not accept them as a customer – it is simply not worth running the risk of malware getting into the wrong hands. And, yes, we have had to turn away applicants (both individual and corporate) on a few occasions.

## TECHNICAL DETAILS

All matters pertaining to the technical side of the business are dealt with by my business partner. When I asked him to describe how our malware collections are maintained, he literally threw the book at me – according to him, *Analysis and Maintenance of a Clean Virus Library* by Vesselin Bontchev is a must-read.

Our collection currently exceeds 1.7 million malware samples, with between 20,000 and 100,000 new samples being added every month. Our samples come from various sources: our own honeypots, trading with other security providers, strategic alliances with security companies, donations and our own research. We are now even trading samples with an anti-virus company.

All samples that we receive are checked against our database; existing samples are discarded, and new samples are run through a set of tools (AV packages, *PEiD*, *TrID*, etc.) that collect various pieces of information about them. This information is written to our database and the identified samples are moved to the repository. Any unidentified and/or suspicious samples are moved to a holding area for further analysis.

Customer access to the collections is granted on a monthly subscription basis. Customers sign an agreement, pay a subscription fee and start receiving samples from us on a weekly or monthly basis.

The collection is currently divided into broad categories by type of malware: worms, viruses, trojans, backdoors and other files (jokes, hoaxes, adware), though we are working on a complete reclassification of the database, as part of the current system overhaul.

## CUSTOMERS

Our customer base consists almost entirely of anti-malware vendors – generally those that exist on the fringes of the traditional AV community and in the mainstream security industry. Our malware database is in use in various commercial anti-malware products around the world, ranging from various white and/or blacklisting applications to hardware-based security appliances. *DriveSentry*, for example, uses the samples and the report we provide along with the malware as the backbone of its innovative blacklisting products. There are also customers who use our samples purely for research purposes – such as the team from *Zynamics* (run by Halvar Flake), who use the samples to develop and fine-tune their *VxClass* software.

## THE FUTURE

Our hopes for the company and its services in the future are to gain the trust of the entire IT security community – to be acknowledged as a legitimate business and as individuals who are seriously dedicated to the cause and what we believe in. A different approach is not necessarily evil, but in some cases it is a necessary evil. And, of course, we would like *MD:Pro* eventually to become the world's biggest and most trusted malware repository.

We want to be able to provide information about malware to all IT security companies who need and want to have access to it. The knowledge about a specific piece of malware should not be exclusive to one company, or a group of companies – if anything, this is counterproductive. There are a lot of brilliant ideas out there about how malware should be tackled, some in development, some yet to be developed and some on the shelf; we believe that there is no reason why research should suffer due to competition or for the pursuit of exclusivity.



Frame4 Security Services

P.O. Box 175, 2400 AD Alphen a/d Rijn, The Netherlands

Phone: +31 (0)6 51491507, Fax: +31 (0)20 7508858

Email: [info@frame4.com](mailto:info@frame4.com), Web: <http://www.frame4.net/>

