

# Autoreporter – Keeping the Finnish Network Space Secure<sup>1</sup>

*The idea in this article originally appeared in the ENISA Quarterly Review*

*Thomas Grenman / CERT-FI*

*Thomas.Grenman@ficora.fi*

## **Introduction**

Autoreporter is a fully automated service provided by CERT-FI for collecting and reporting information security incidents in the Finnish network space. The development started in late 2005 as an internal trial funded by an almost nonexistent budget. Back then, the service did not even have a name. Now, three years later, the name of the service has been branded, and some much needed functionality has been added. Safe to say, Autoreporter has become a vital part of the daily operations of CERT-FI.

## **Customer base**

Autoreporter's customers range from major Finnish Internet service providers (ISPs) to small domestic enterprises. If you administer your own network space and your business is concentrated in Finland, or if you have an Autonomous System (AS) registered under the Finnish country code, then you are probably a customer of Autoreporter. Currently, Autoreporter is continuously tracking and reporting incidents for roughly 170 Autonomous System Numbers.

## **Sharing information adds value**

It is tempting to quote the fictional Gordon Gekko from the 1980s film, *Wall Street*, who said, "The most valuable commodity I know of is information." A lack of information eventually led Mr. Gekko to his downfall. The same holds true for Autoreporter; without any information to process, Autoreporter would be blind and useless.

---

<sup>1</sup> This paper was chosen as a winner in the Best Practices Contest 2009, which was sponsored by the CERT® Coordination Center and the Forum of Incident Response and Security Teams (FIRST) in conjunction with the 2009 FIRST annual conference. CERT and FIRST make no warranties about the content of the paper.

A significant amount of data related to information security incidents is collected every day. Sadly, most of this data just ends up in a database somewhere, and only a fraction of it ever sees any serious post processing, let alone any concrete action. As the national computer security incident response team (CSIRT), we see it as our responsibility to take some of this data and feed it to our constituency for investigation and, if needed, swift action.

Currently, Autoreporter is fed with information from intrusion detection systems, honeynets, and sinkholes run by trusted third parties. The correctness of this information is evaluated on the basis of customer feedback and also, from time to time, internally.

As a bonus, using data supplied by third parties is very cost-effective. We do not, however, feel that we are living off these third parties in any way. Instead, we are working toward the same goal by helping them out. After all, we are the ones with the closest contacts and connections at a national level.

We do, however, recognise the risk of our service being solely dependent on information from external parties. To increase resilience, we have therefore started working on a sensor network of our own. This network will eventually serve Autoreporter as a localised source of information with information gathering parameters set internally. By operating a sensor network, we will also become data providers ourselves. This will allow us to feed incident-related data back to the international community and eventually achieve mutual symbiosis.

## **Technology in brief**

Autoreporter has undergone a few major development cycles. It is still just a collection of simple, but efficient, scripts. The system does not even boast a graphical user interface.

The underlying engine acts as a common framework. This framework is responsible for fetching, categorising, sorting, and formatting the reported incidents according to predefined templates. The engine also takes care of compiling the daily reports and emailing them out at predefined times to addresses found in our contact list.

Each data source is attached to the framework through a tailor-made plug-in. The flexibility provided by plug-ins has proved valuable, as it allows for virtually any type of data feed to be attached. Currently, Autoreporter is able to handle sources where data is either pushed (e.g., receiving data by email) or pulled (e.g., fetching the data from an external web server).

The daily reports that are emailed to customers follow strict formatting rules. By sticking to a predefined format, we have tried to make the post-processing of the incidents as easy as possible for the recipient. Based on feedback from our customers, we eventually included the data in several complementary formats.

For historical reasons, all reported data are included as plain text in the body of the email message. In addition to this, the same data are attached as an easily parsed, comma-separated text file. For heavy duty processing, the data are also formatted with Extensible Markup Language (XML). The mark-up elements are used in accordance with the Incident Object Description and Exchange Format (IODEF). IODEF is defined in RFC 5070 published by the Internet Engineering Task Force (IETF).

## **Some statistics**

In addition to forwarding incident-related data to network administrators, Autoreporter also feeds back much needed statistics for in-depth assessment. We have discovered that even the strongest peaks usually come with very short-lasting effect. Hence, it is not really useful to look at the statistics on a day-to-day basis.

The most interesting observations can be made by looking at the statistics over a longer period of time. Autoreporter has now been running for three years, and this timeframe is enough to draw some conclusions. In addition to looking at yearly trends and categories of incidents, we like to scale the total number of incidents against the number of existing broadband subscriptions. We reason that the number of incidents should correlate with the number of computers brought online. When looking at this scaled result, we are delighted to be able to say that the ratio of malware incidents to broadband subscriptions has dropped since Autoreporter was introduced.

In addition to making overall statistics public, Autoreporter makes it possible to create individual and tailor-made statistics; for example, for all major Internet service providers in Finland. These statistics can be valuable for the ISPs when benchmarking their ability to deal with incidents against other ISPs (without mentioning the names of their competitors, of course). These statistics also point out which particular IP addresses have triggered the most reports. We are currently defining a process which will allow us to track these “chronic” cases on a day-to-day basis.

## **Conclusions and further work**

The automated assistance provided by Autoreporter is invaluable when fighting malicious activities in the Finnish network space. The sheer volume of incidents that Autoreporter is able to handle annually is impressive. In 2008, Autoreporter outperformed the manual incident handling of CERT-FI’s duty-officers at a rate of nearly 20 to 1. In addition to this, Autoreporter provides us with much appreciated statistics. In a way, Autoreporter also forces us to track changes in both the regulatory landscape as well as in the structure of the Finnish network space.

A small-scale project that started out as a simple test has slowly evolved into a service CERT-FI can no longer do without. We have come to rely on Autoreporter in many different ways. Having become dependent on a system that was not initially designed for 24/7 operations has also forced us to evaluate the risks involved. It has become clear that the service must be moved out of the laboratory and into an environment where uninterrupted power can be guaranteed and redundant hardware and network connectivity is available.

In addition to all this, CERT-FI is constantly looking for new trustworthy partners willing to share incident-related data for further processing. The postgraduate students in our team are also considering whether comparing and cross-referencing the data from the different sources would make an interesting research topic.

Statistics generated by CERT-FI's Autoreporter are available at <http://www.cert.fi/en/reports/statistics/autoreporter.html>.