

Norman Green Book on Analyzing Malware

Executive White Paper, 2009



NORMAN[®]

SAFETY FIRST



SAFETY FIRST

Malware – Abundant & Complex

Malicious threats assessed by security organizations have grown to tens of thousands every day. This flood of complex threats, often complicated by self-defending code techniques, has led to bottlenecks in security analysis labs. The volume and complexity of continuously emerging threats simply cannot be addressed appropriately by the same human resources as in the past.

Norman has built a foundation as one of the world's leading data security companies under the expertise of the world's top security researchers. Sustaining and expanding Norman's position as a data security leader has required the transfer of those expert skills and knowledge to artificially intelligent systems.

The time factor can be quantified as high as hundreds of thousands of dollars per hour and much higher when factoring in data loss and possible litigation costs.



SandBox emulates all hardware and software used in a real Windows environment, as well as necessary network services.

As a proprietary technology, Norman has full control to tailor the environment to current and future forensic needs and adapt to emerging threats.

Outpacing Traditional Methods

Organizations using traditional means cannot cost effectively respond to the daily swarm of threats in a timely manner. Analyzing such threats is a cumbersome and time consuming task, involving multiple applications for code analysis, as well as a network of computers. Most of the time, the analyzers must combine results of several applications to reveal the true actions and objectives of the malicious threats. For normal executables in low impact incidents, traditional methods will allow the analyst to gather the necessary forensic information. However, the commitment to bring human expertise in-house to accomplish these tasks involves a significant financial investment. Managers must also consider how the cost of time will impact their organization, considering a well-trained analyst spends at least 20 minutes per sample. Typically, time consumed by traditional analysis is sufficient to bring down a corporate network and compromise a significant amount of data. In many cases, the time factor can be quantified as high as hundreds of thousands of dollars per hour and much higher when factoring in data loss and possible litigation costs.

Keeping Pace – Security Intelligence

While the quantity of malware in the wild has grown exponentially, Norman's reverse engineering analysis team growth has remained linear. With larger organizations subject to more and more targeted attacks, the same pressure is on security managers outside the security industry to quickly and cost-effectively analyze malicious threats. They need to see and monitor new malicious code and trends so preventive measures can be taken before an attack is out of control. Such organizations have realized they can no longer rely entirely on outside help to protect them and must take responsibility themselves.

What is SandBox?

Norman has pioneered new advancements in reverse engineering technologies over the past decade and antivirus enhancements for over two decades. Years of real world testing and enhancements in Norman's analysis labs have resulted in Norman's proactive SandBox technology. SandBox is now one of the main components used to process the multitude of samples Norman and many other organizations receive each day. SandBox provides for a full simulation of potentially malicious executable code in a safe environment. The underlying SandBox technology simulates a Windows based computer system. SandBox emulates all hardware and software used in a real Windows environment, as well as necessary network services. The file to be analyzed is loaded into the simulated hard disk and started in the simulated Windows environment. Inside the simulated environment, the file will behave as it would in a real computer system. This behavior is observed by the SandBox as the SandBox emulator itself is responsible for processing all the file code. As a proprietary technology, Norman has full control to tailor the environment to current and future forensic needs and adapt to emerging threats.

It's vital that SandBox development continues to ensure new self defending code techniques.

Complex targeted code

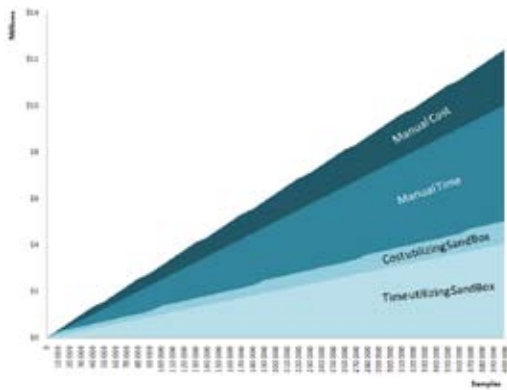
With higher frequency, more dangerous malicious executables are using complex self defense techniques, severely limiting the ability to respond efficiently and effectively. It's vital that SandBox development continues to reinsure new self defending code techniques. This will reinsure that the detection abilities of the SandBox analysis are unaffected. This is not only vital for our labs at Norman, but even more so for our SandBox customers who are often carrying out in-depth forensics investigations. While Norman simply needs to determine if a file is malicious or not in order to protect endpoints from infection, SandBox customers need much more detailed information before abandoning their analysis of the threat. These customers, often investigating and defending against targeted attacks directed at their organization and customers, must understand the full potential of each threat. They must know what information may be compromised, and where that information may be sent. The analysts also must identify the methods used in such attacks to prevent further and future compromise of their defenses and valuable assets.

The average cost savings starts at USD 67,000 for the first analyst using SandBox Analyzer compared to utilizing a second analyst to process increased workloads.

SAFETY FIRST



"A current SandBox customer has dropped average response times from 3 days to an average of 3 hours as a direct result of adding the SandBox Analyzer Pro to their laboratory toolset."



*Fig.1 Time and Cost
This illustration shows average cost and time variances users can expect when using manual analysis methods as compared to integrating SandBox Analyzer into their analysis processes.*

Fig. 1 shows average cost and time variances users can expect when using manual analysis methods as compared to integrating SandBox Analyzer into their analysis processes. As with any software adoption, SandBox Analyzer complements human experts by automating and speeding up high level behavioral analysis, allowing analysts to focus on deeper and more technical information gathering with advanced methods like those provided by SandBox Analyzer Pro.

From a financial point of view, the average breakeven point based on sample volume will be about 3800 samples per year for SandBox Analyzer customers. This point also happens to represent the estimated point at which an additional malware analyst is required. The average cost savings starts at USD 67,000 for the first analyst using SandBox Analyzer compared to utilizing a second analyst to process increased workloads. For companies like Norman's telecom customers who are scanning up to more than 100,000 samples per day, at an average of 13 seconds per sample, significant cost savings quickly add up.

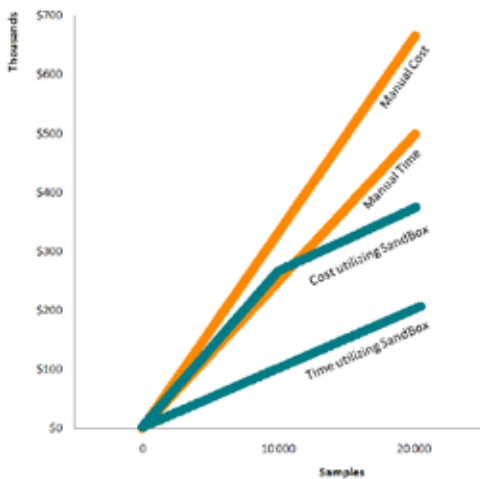


Fig. 2: The breakeven point for time savings using SanBox products is immediate. The financial breakeven point becomes irrelevant when response times can result in severe financial consequences.



The SandBox Analyzer is a tool designed primarily for automation of malware analysis.

The breakeven point for time savings using SandBox products is immediate (fig. 2). The financial breakeven point becomes irrelevant when response times can result in severe financial consequences. Often SandBox customers estimate the time savings pays for the software expenditure in one incident. For example, a current SandBox customer has dropped average response times from an average of 3 days to an average of 3 hours as a direct result of adding the SandBox Analyzer Pro to their laboratory toolset. This has enabled this multibillion dollar company to increase efficiency throughout the entire organization.

Automated Analysis

The SandBox Analyzer is a tool designed primarily for automation of malware analysis. Several different analysis output formats are available from both the command line and graphical interface versions of this tool. The most useful outputs are the SandBox summary, available in both text or XML formats, and the API log of system calls. The Analyzer also offers the ability to extract dropped files, memory dumps, and URL content from the SandBox environment. The graphical interface, used for help desk and quick behavioral analysis situations, provides other information windows including antivirus engine signature scanning, statistics, lists of dropped files, network connections, and IRC servers found in the batch of suspicious files analyzed.

In automated environments, once the files have been processed by the Analyzer by scripting or some other method of submission, the information output may be stored in a database. Once in the database, the information can be processed further to create signatures, cleaning scripts, send alerts, generate reports, or whatever the customer needs may be.

The Norman SandBox Information Center, at SandBox.Norman.com, is a simple example of how this tool can be used to do automated analysis on thousands of new files every day. Though limited compared to the full version of the SandBox, this service is a free service on Norman's website where suspicious samples can be uploaded and SandBox summary responses will be sent back to the analyst via email.

Deep forensic analysis

SandBox Analyzer Pro provides deep forensic analysis. Analyzer Pro is a complete reverse engineering environment built on top of the stability of the SandBox technology. Analyzer Pro combines the capabilities of many other reverse engineering tools into one product. The user has full control over the SandBox environment and the execution of the sample being analyzed. Registers, memory, disassembled code, virtual hard disk, and network activity can all be closely monitored and manipulated in order to understand the full potential of the suspicious code. Analyzer Pro includes many advanced debugging features like the ability to take snapshots, simulate execution in reverse, search and dump memory contents, log and save network packets, and many others. The user is able

Responding to Threats: A Financial Approach

Analysis costs are a measurable variable of computer security incidents. Human resources, overhead, and laboratory costs are all components that can be quantified financially. Variables affecting these costs include the types of samples that threat the organization and the required technical depth of investigation, as well as the proficiency and efficiency of the analysis staff and the toolsets they're using. Using past financial cost basis for these activities, future costs can be computed with relative accuracy.

Tens of thousands of malicious samples from various avenues are submitted to Norman daily. This number will likely continue to increase exponentially. With slowing revenue growth in the antimalware industry, most anti-malware engine providers would not be able to continue operations if associated costs kept pace with this growth.

Like most in the industry, Norman has kept analysis costs at linear growth rate almost entirely based upon the increasing effec-

tiveness of automated analysis systems enabled by technologies like SandBox.

Unfortunately, the financial scope of security incidents is not limited to operations. Security compromises often produce major economic consequences. Numerous reports estimate breach costs broken down per minute, per incident, and in various other representations. Like the operational security lab costs, many variables will determine the actual cost of security compromises.

Every organization has different values associated with the assets being protected by computer security initiatives. The fact that every incident and threat is unique is the biggest factor making financial consequences unpredictable. For example, a worm propagating in a network may vary in consequence from minor network congestion to severe leakage of proprietary and customer data. Often the variability in these

"The fact that every incident and threat is unique is the biggest factor making financial consequences unpredictable."

consequences is directly related to the response time. Security teams can usually identify some basic behavior quite quickly, but it's often challenging to understand the full potential, due to the increasing obfuscation malware authors incorporate into their code. To mitigate security threats, the response team must understand the full potential of the threat. Getting to the bottom of these threats depends on the proficiency and speed of the software tools being utilized.

consequences is directly related to the response time. Security teams can usually identify some basic behavior quite quickly, but it's often challenging to understand the full potential, due to the increasing obfuscation malware authors incorporate into their code. To mitigate security threats, the response team must understand the full potential of the threat. Getting to the bottom of these threats depends on the proficiency and speed of the software tools being utilized.

The Norman SandBox product line focuses product development on the root of incident response problems. SandBox products benefit greatly from letting the market as a whole drive product development, consulting

"The Norman SandBox product line focuses product development on the root of incident response problems."

closely with customers, partners, and peers to constantly improve security team response. The combination of SandBox Analyzer quickly automating analysis of many files, and SandBox Analyzer Pro allowing quick deep forensic analysis, significantly reduces the financial impact of security incidents.

to see and work with code both at the application and kernel levels to see rootkit and exploit code behavior. The ability to connect to the live Internet allows analysts to quickly analyze and monitor botnets, network worms, downloaders, and other network reliant code.

“The SandBox technology can easily be built into commercial products.”

Other applications

The SandBox technology can easily be built into commercial products, including antivirus scanner engines, various forensic tools, threat management products, honeypots, firewalls, intrusion detection systems, and various other applications. Norman Network Protection (NNP) is an example of a product that uses these technologies. NNP scans your network traffic protocols in real time for malicious activity. This product has the SandBox technology built in to detect proactively any new threats that might be passing in or out of the network segment.

The SandBox Reporter data feed of threats Norman sees in its analysis labs, provides lists of new URLs and IRC servers that new malware is contacting. This information can be built into firewalls and other intrusion products. The behavior from the full SandBox summary reports included in the Reporter feed can be used for signatures to detect various other indications of malware in your network.





The SandBox tools delivered by Norman have become the primary analysis tools for some of the world's largest companies, trusted security organizations, and government security labs.

Self-defending code techniques are used to hinder analysis and detection.

Leading forensics into the future

The SandBox tools delivered by Norman have become the primary analysis tools for some of the world's largest companies, trusted security organizations, and government security labs. These organizations rely on SandBox tools to deliver virtually instant intelligence to protect customers and sensitive data. Norman continues to pioneer advancements in reverse engineering and forensic technologies for future threats and exploits. With the assistance of customer and industry security teams, Norman diligently monitors the threat landscape for means of performing more effective detection and analysis in the modern computer security environment.

Malware Playing Dead – Malware Self-Defense techniques

Malware often “plays dead” or modifies its behavior in response to reverse engineering activities. Such self-defending code techniques are used to hinder analysis and detection. Complex threats can slow down response times considerably, exposing organizations to potentially significant data compromise and loss. It is vital when analyzing these threats to understand the problem, how to resolve the problem, and ensure future threats do not compromise efficient and proficient response.

Self defense techniques can be categorized in different ways. Anti-environment, anti-emulation, and anti-analysis are some of the common sub-categories. Anti-environment code tries to detect virtual environments such as VMWare or Virtual PC based solutions. The anti-environment code uses various methods, from simply looking for registry keys to hooks into the real system software and hardware.

Since these virtualization solutions use a graphical interface that looks to the human eye like a separate safe computer environment, it's sometimes hard to remember that everything done in this piece of software is processed by the real system resources. It's quite easy and well documented how to detect and even jump out of these environments popular with analysts. In addition to these drawbacks, these environments also have numerous code and behavioral analysis tools installed in the environment. These tools are also vulnerable and easily detected by the malware, further compounding analysts abilities to effectively utilize such analysis methods. With more frequency, analysts must infect real computer systems and networks in order to analyze the malware, while using time-consuming patching techniques to avoid the detection of their analysis toolsets. In the case of virtualized and real environments, the time spent reverting to a clean state is extremely costly when dealing with large volumes of suspicious code.

Anti-emulation tricks try detecting if the code is being simulated in an emulator. These tricks are quite useful for malware writers because emulators are used by many antivirus engines for heuristic detection. Some

"Code might drop its own libraries to hide things so the analyst won't actually see it in the executable's code."

analysts also use more robust emulators for analysis activities. Emulators can be detected by malware writers by simply looking for some characteristic of a real system not emulated, or emulated incorrectly within the simulated environment. Emulators are difficult to develop to undetectable levels because the Windows kernel and operating system software code must be completely reverse engineered and converted to run inside the emulator. In a truly emulated system, you must also complete this process for all the hardware components as well. SandBox is a completely emulated environment with all hardware, software and operating system components rewritten specifically for the SandBox environment.

Anti-analysis code looks for the presence of debuggers and other analysis tools, often by simply observing tools active on the computers desktop. The code will also look for installed or running services associated with such tools. With more complex techniques, the code will identify strange registers and memory space used by the analyst's toolset. Code might also drop its own libraries to hide things so the analyst won't actually see it in the executable's code. When analyzing a file, the analyst must be aware of many different anti-analysis techniques. For example, code may only be malicious if it is able to download a particular file, and therefore the analyst must retrieve that file in order to see how the file would behave on the average users PC.

```
Anti debug/emulation code present.
--Locates window "SHELL: C:\Users\Kegnan\Class1" on desktop.
--Locates window "SHELL: C:\Users\Filipson\Class1" on desktop.
--Locates window "SHELL: C:\Users\SuckPee8C\Class1" on desktop.
--Locates window "SHELL: C:\Users\@P!Mantoo By Rohitab1" on desktop.
--Locates window "SHELL: C:\Users\TDDeHaHa\Class1" on desktop.
--Locates window "SHELL: C:\Users\T!de@!ndou1" on desktop.
```

Self defending code functionality is often built into many forms of protection commonly generalized into what the security industry calls packers. Techniques can be as simple as common compression software. These compression layers can of course use more complex compression layers using encryption layers the analyst may need to work through. Techniques advance further into advanced protection technologies such as those used by Slovak Protector and Themida, which hide and obfuscate code in a way that makes analysis almost completely impossible using traditional methods.

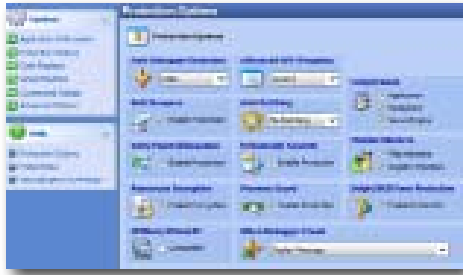


Fig. 3

"In general, packers and protectors are not a problem for SandBox."

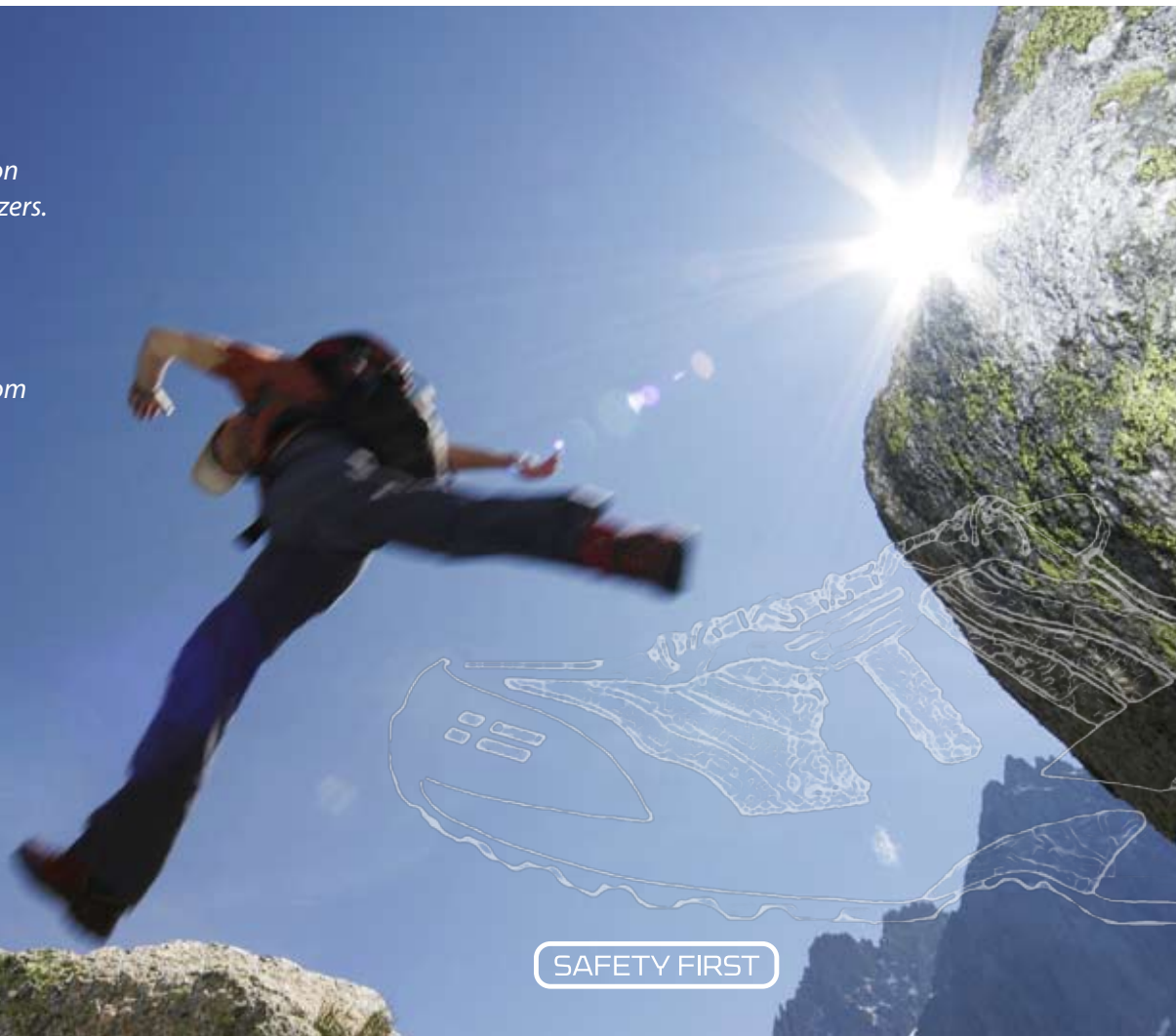
Fig. 3: Packers are increasing in use, with trends moving toward the more complex protectors. These technologies are readily available as both free and commercial applications, making it easy for any malware author not skilled enough to write self-defending code themselves, to build such functionality into their malicious applications. In general, packers and protectors are not a problem for SandBox. As a fully emulated Windows system, the executable will simply run through the protection mechanisms as it would on a real system.

Internet-type tricks are also increasing in usage. Malware will connect to various URLs to make sure it is receiving the real-world response from a legitimate site. It will check to see if something is returning a response from a site that does not exist on the real internet. Malware will also frequently authenticate itself with a commanding server to verify a connection to the real internet. Malware will look for applications such as antivirus software, MSN messenger, and other services that should be running on a normal system, but not in a reverse engineering environment. All these evolving techniques must be considered in any analysis environment whether the system is manual or automated.

Make a leap - contact us today for more information about our SandBox Analyzers.

Norman ASA
sandbox@norman.com

www.malwareanalyzer.com



SAFETY FIRST

Norway, headquarter

Norman ASA
Strandvn. 37, Postboks 43
1324 Lysaker, Norway
Tel: +47 67 10 97 00
email: norman@norman.no
www.norman.no

Denmark

Norman Data Defense Systems A/S
Blangstedgårdsvej 1
5220 Odense SØ, Denmark
Tel: +45 63 11 05 08
email: info@normandk.com
www.norman.com/dk

Sweden

Norman Data Defense Systems AB
Södra Grytsgatan 7, 2tr, Norrköping Science Park
602 33 Norrköping, Sweden
Tel: +46 011 - 230 330
email: sales.se@norman.no
www.norman.com/se

United Kingdom

Norman Data Defense Systems (UK) Ltd
Exchange House, 494 Midsummer Boulevard
Central Milton Keynes
MK9 2EA, UK
Tel: +44 - 08707 448044 / 01908 255990
email: norman@normanuk.com
www.normanuk.com

Germany

Norman Data Defense Systems GmbH
Gladbecker Strasse 3
40472 Düsseldorf, Germany
Tel: +49-211 / 5 86 99-0
email: info@norman.de
www.norman.de

Norman Data Defense Systems GmbH
Niederlassung München
Ludwigstr. 47
85399 Hallbergmoos, Germany
Tel: +49-811 / 5 41 84-0
email: info@norman.de
www.norman.de

Switzerland

Norman Data Defense Systems AG
Münchensteinerstrasse 43
4052 Basel, Switzerland
Tel: +41-61 317 25 25
email: norman@norman.ch
www.norman.ch

The Netherlands and Luxemburg

Norman/SHARK BV
Postbus 159
2130 AD Hoofddorp, The Netherlands
Tel: +31-23-7890222
email: info@norman.nl
www.norman.nl



Belgium

Norman/SHARK BV
Grote Baan 119/2
3511 Kuringen (Hasselt), Belgium
Tel: +32 11 32 30 22
email: belgium@norman.nl
www.norman.com/be

France

Norman France
8 rue de Berri
75008 Paris, France
Tel: + 33 1 42 99 94 14
email: info@norman.fr
www.norman.fr

Spain

Norman Data Defense Systems
Camino Cerro de los Gamos 1, Edif.1
28224 Pozuelo de Alarcón MADRID, Spain
Tel: +34 (0)91 790 11 31
email: norman@normandata.es
www.normandata.es

Italy

Norman Data Defense Systems
Centro Direzionale Lombardo
Via Roma, 108
20060 Cassina de'Pecchi (MI), Italy
Tel: +39 02 951 58 952
email: info@normanit.com
www.normanit.com

USA

Norman Data Defense Systems Inc
9302 Lee Highway, Suite 950A
Fairfax, VA 22031, USA
Tel: +1-703 267 6109
email: norman@norman.com
www.norman.com

Norman Data Defense Systems, Inc.
2603 Camino Ramon, Suite 200,
San Ramon, CA-94583, USA
Tel: +1 925 242 2000
email: sandbox@norman.com
www.norman.com

NORMAN®