

available at www.sciencedirect.comjournal homepage: www.elsevier.com/locate/diin
**Digital
Investigation**

Anti-forensics with a small army of exploits

S. Hilley

Anti-forensics (AF) is a multi-headed demon with a range of weapons in its arsenal. Sarah Hilley looks at a set of hell-raising attacks directed at prominent forensic tools. Major forensic programs have started to attract unwanted attention from hackers aka security researchers of a type that have plagued mainstream software developers for years. This report focuses on the development of the Metasploit Anti-Forensic Investigation Arsenal (MAFIA).

1. Mainstream

Digital forensics is hitting the mainstream – the signs are everywhere. Home grown firm – Guidance Software, has gone public, firms are amalgamating, and the field is getting international acclaim for its role in high profile cases. But not all of the attention on digital forensic techniques is obviously helpful. So-called security researchers, dubbed Metasploit, are starting to pick holes in digital forensics programs creating more weaponry for the cause of anti-forensics. Of course software makers have been plagued by researchers finding holes in their products for years, and digital forensic vendors are now taking the brunt.

Forensic tool developers cannot ignore the anti-forensic exploits and Guidance Software has even made friends with Metasploit developers by inviting them to attend its conference as speakers. The Californian-based company's reaction is mirroring the example set by Microsoft and Oracle who have befriended hackers in the past to try and quash a flurry of exploits.

2. Interfering with investigations

[Metasploit Project](#) anti-forensic wares get very personal with investigative software as they do more than just corrupt it to gain access to a user's computer. They interfere with the software's results for use in investigating a crime. The Timestamp exploit, for example, interferes with the Timestamping capability in Guidance Software's Encase program and FTK from Access Data – potentially upsetting evidence collection. And

the Metasploit Anti-Forensic Investigation Arsenal (MAFIA) is not the only slew of AF exploits out there. Other documented attacks have targeted iLook, WinHex, TCT and Sleuthkit.

3. AF categories

But Metasploit exploits are only one of a variety of approaches to subverting evidence.

Criminals can choose from a bunch of ways to cover up crimes on digital devices. Steganography, data wiping programs and encryption all make life more complicated for investigators.

With the variety of anti-forensics approaches come numerous attempts by academics and practitioners to define AF. [Ryan Harris](#) at Purdue University presented a definition at the DFRWS conference in August which attempts to take all types of anti-forensics techniques into account. He classifies anti-forensics as “any attempts to compromise the availability or usefulness of evidence to the forensics process.”

[Dr. Marcus Rogers](#), also at Purdue University, breaks anti-forensics into four categories: data wiping, artifact wiping, trail obfuscation and attacks against the latest CF processes and tools. MAFIA fits into the latter category. See [Fig. 1](#) for a breakdown of specific examples of Rogers' categories.

4. Benefits?

MAFIA exploits do not have clear beneficial applications like other anti-forensic techniques. Data wiping, for instance, has legitimate as well as nefarious purposes as it is good PC house-keeping practice. Likewise encryption is useful for secret communications between the security services. But finding a useful reason for subverting flaws in forensic tools is more taxing.

5. Motivation

The Metasploit group has come up with its own justification for its actions on the group's website. Its “goal is to provide

E-mail address: sorchahilley@hotmail.com

Anti-forensic categories	
Datahiding <ul style="list-style-type: none"> • Rootkits • Encryption • Steganography 	Artifact wiping <ul style="list-style-type: none"> • Disk cleaner • Free space and memory cleaners • Prophylactic
Trial obfuscation <ul style="list-style-type: none"> • Log cleaners • Spoofing • Misinformation • Zombied accounts • Trojan commands 	Attacks against the CF process/tools <ul style="list-style-type: none"> • File signature altering • Hash fooling • Nested directories

Fig. 1 – Anti-forensic categories – source Dr. Marcus Rogers, purdue.

useful information to people who perform penetration testing, IDS signature development, and exploit research. This site was created to fill the gaps in the information publicly available on various exploitation techniques and to create a useful resource for exploit developers.”

The Project was founded by HD Moore – a well known vulnerability researcher who concentrates on revealing embarrassing vulnerabilities in popular programs from giants like Microsoft and Apple. Moore launched a month of browser bugs campaign last year where he revealed a number of Internet Explorer holes in one month. Imagine if there was a month dedicated to forensic tool bugs? So far the group’s website has around 156 exploits and more than 70 payloads available for download.

In October 2005 while presenting at the Bluehat Microsoft conference, Metasploit member Vincent Liu, said there were a number of reasons why the group decided to expose weaknesses in digital forensics programs. His presentation cited there was “no pressure to innovate in the forensics community” and “too much dependence on forensic tools.”

6. AF tools

So far, Metasploit has developed four tools focusing on anti-forensics: Timestomp, Slacker, Transmogify and SAM Juicer. The group’s website says Timestomp, Slacker and Transmogify are the first tools of their kind.

Timestomp allows all four NTFS timestamp values to be changed. Slacker allows files to be hidden within the slack space of the NTFS file system. The SAM Juicer tool allows hashes to be dumped from SAM without hitting the disk. Finally, Transmogify, which has yet to be released, is said to defeat EnCase’s file signaturing capabilities.

7. Welcome hackers

Many investigators may be worried by the publishing of such concepts, but Guidance Software had decided to stay on the good side of what most would consider ‘bad guys’ by liaising with the developers and inviting them to speak at its CEIC conference.

Director of Product Strategies Brian Karney says: “We think it’s a good thing. Computer forensics is an evolving field and

there will always be people finding new ways to complicate processes. We’ll always have communities doing research to bypass traditional methods,” he says.

He plays down the innovation of the timestamp altering program – Timestomp, saying it is merely based on a simpler principle, which criminals have been using for years.

“Child pornographers have been doing that by changing their clock on their computer for years. Timestomp glorifies time-changing,” he says.

8. Counter anti-forensics

Karney says Guidance is developing features to counter anti-forensic exploits such as Timestomp, although he cannot offer a timeline for them yet.

He says Timestomp only alters one set of attributes and if you look elsewhere you can retrieve the real times stored in the NTFS system. Guidance is working on a process that uses the filename attribute.

He also says the company has found a way to identify a meterpreter module that dumps the hashes from SAM without hitting the disk.

“We’ve developed code to identify that (meterpreter) running in memory,” he says.

He believes the Metasploit AF tools are not being widely yet used as very few people would have the skills and knowledge to do so.

“Computer forensics is a dark art. Those using advanced forensic techniques is a small subset,” he says. He adds that it is difficult to know for sure, however, as practitioners are guarded in discussing what they know.

Therefore, the company is taking precautions by briefly introducing the AF tools to customers when training on Encase.

Paul Henry, vice president of strategic accounts at Secure Computing, agrees it is unlikely the Metasploit armoury is widely used, but still feels it is unacceptable that forensic tools do not alert investigators to their use yet.

“Anti-forensic tools tend to leave known traces themselves yet commercial forensic tools do little to alert the investigator that a given tool has been run – this is inexcusable in today’s environment where being able to prove that a person had used a tool to hide his/her actions could be useful in court,” he says.

He also says lack of peer review makes forensics tools particularly vulnerable to attack.

There is “not enough peer review and not enough commercial pressure to drive better products,” he says.

And he believes Timestomp is the most worrying program from the Metasploit arsenal.

“In a forensics investigation “time” is critical – if a defendant is able to alter a timestamp to place the given evidence outside of a timeframe when he had computer access he wins,” he says.

He recommends investigators use multiple tools to reduce the potential risk of exploits interfering with a case.

“A forensics investigator has to realise that one size does not fit all when it comes to forensic tools when performing an investigation. Multiple tools should be used and then the results compared to see if anything is hidden. That is using SMART for data acquisition and then Encase can potentially

show different results in a partition table and should alert the investigator to an issue of a hidden partition and possibly hidden data. Beyond a good hex editor, tools like Autopsy, SMART, FTK and Encase should be in every forensic investigators tool kit."

Henry says it is unlikely that Metasploit-type attacks are in the wild as there are easier options for those wishing to hide their computer activities.

"I do not believe that they (MAFIA) are being actively used today – firstly, they are limited to a single function and require command line capabilities/knowledge. Secondly, there is no great need for these tools when there are so many easy to use multi function data hiding tools out there."

9. Unskilled

Robert Jones at Queen Mary University of London also says use of the data hiding technique – encryption – is set to increase.

"Encryption is going to be the next big problem as it is instantaneous these days due to faster machines," he says.

Jones says most people who use anti-forensic software skillfully do not get caught. "The top cyber villains stay in the background," he says.

The ones most often caught using AF tools are low-level cyber criminals.

Simon Janes founder of the Forensic Alliance says the use of artifact wiping tools by unskilled users is common.

"There are lots of tools out there for wiping hard drives. The first thing is don't be intimidated by the fact they've

been used. They are often used by people who don't understand how they work so you can normally find something."

Unlike artifact wiping tools, direct attacks on forensics tools seem to be considerably rare. But is it any comfort to think that only extremely skilled hackers can use them? – criminals so elusive they could be beyond reach.

And the fact there is no immediate fix to address such exploits means criminals could use them without much fear of being detected. The last anti-forensics tool release (Sam Juicer) from the Metasploit team was in 2005, but there are still no fixes available.

And it does not end there. The [Metasploit Project](#) website points to future work involving NTFS change journal modification, secure deletion, browser log manipulation and file meta-data modification.

With more demonic exploits on the way, it is clear to see the forensic community will be haunted for some time to come.

REFERENCES

- Dr. Marcus K Rogers. Lockheed presentation. In: Anti-forensics. Available from: <www.cyberforensics.purdue.edu>.
- Metasploit project. Available from: <<http://www.metasploit.com/>>.
- Paul Henry. Presentation. In: Anti-forensics, considering a career in computer forensics? Don't quit your day job... Available from: <http://www.layerone.info/2006/presentations/Anti-Forensics-LayerOne-Paul_Henry.pdf>.
- Ryan Harris. DFRWS 2006 conference proceedings. In: Arriving at an anti-forensics consensus. Available from: <<http://www.dfrws.org/2006/proceedings/6-Harris-pres.pdf>>.