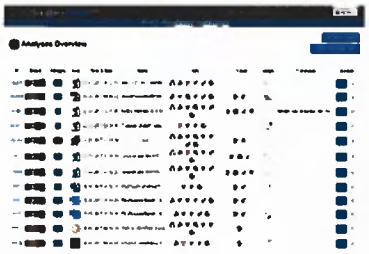
May 1, 2017

# First Look: Joe Security Joe Sandbox Cloud

Peter Stephenson



From time to time we run across a product or service, purely serendipitously, that knocks our virtual socks off. Joe Sandbox Cloud is one such product. It happened this way: We have a suite of sites that we use for information for the Threat Hunter blog. These include open source threat feeds, threat intelligence and a bunch of other functions that we need to do a credible analysis for our readers. Among those was malwr.com. At the time, we were needing some reversing on a malware sample and, as was our habit, we went to malwr.com only to find it down. It stayed down for quite a while (it's back online) so we went searching for an alternative.

We found a site for a company called Joe Security. With a name like that we almost didn't take it seriously. That would have been a huge mistake. The company has a web-based sandbox similar to, but far more complete, than what we were using. Joe Sandbox is the most complete reversing and malware analysis tool we have ever seen. It predates Cuckoo (malwr.com is Cuckoo and we have a Cuckoo instance in our lab), goes to a lot more depth and its display is far more complete and detailed. Joe Sandbox can put malware reversing and analysis within the reach of just about any organization, especially those which do not have the skills in-house to do full reversing.

Reversing is not just for geeks who like to attack a malware with virtual tweezers to dissect it and marvel at its innards. There is a lot of very useful information – indicators of compromise, for example – available when the malware detonates. We also use it on files that we suspect may be malicious, but are not certain.

Knowing how a piece of malware works is useful. For example, does it use a dropper or a downloader? What IPs or URLs does it visit that you should block? All of this is available with a little reversing.

"A little reversing" was an oxymoron until we found Joe Sandbox. Now, in a matter of minutes, we have the information we need and can move on with our investigation, defenses or whatever else is appropriate to the situation.

To use Joe Sandbox, you simply upload the sample and wait. It creates a whole collection of specialized reports from a plain vanilla pdf file to yara rules – it creates them from your sample – xml files and a whole slew of others. For the impatient, there is a lucid classification chart that shows the types of activities that the malware performs, such as ransomware, spyware, exploiter, etc.

Joe Sandbox uses "cookbooks" that let you apply special conditions. For example, an analysis of a Cerber ransomware shows that it sleeps a long time, so you should re-analyze your sample with the "Bypass long sleeps" cookbook. The second graphic is a circle graph of the overview of the sample's signature containing such things as Cryptography, Networking, Persistence and Installation Behavior, Data Obfuscation and lots of others. Clicking on one of these section takes you to the details farther on in the report.

Clicking on "Change of System Appearance," for example, takes us to a detail that tells us that Cerber can change the wallpaper and it gives us the specific code segments. Joe Sandbox can log into email servers and check all the emails for malicious attachments. It analyzes the attachments for malicious content and issues alerts as necessary. All this is based on over 1,300 specific signatures handwritten by experts at the vendor. Another unique capability is decompilation back to C code. While reversing usually goes to Assembly, it is not so easy to craft C code listings. However, far more programmers can handle C and its progeny than can handle Assembler.

The networking section of the report is especially useful for SOC and NOC personnel. Here we can see the external IPs, URLs and domains with which the malware communicates. This leads to blocking and threat hunting on the network. For example, if you have a product such as WebSense running you can cross-correlate its results with Joe's to determine what device was infected first and what other devices have been infected, as well as whether any data might have been exfiltrated or downloaders used successfully. In other words, the whole enterprise threat hunting process can start with these two tools.

In short, this is a must-have tool. We have found it so valuable that we are naming it as part of our SC Lab Approved tool set.

**Product** Joe Sandbox Cloud

**Company** Joe Security

**Price** Contact vendor for details.

**What it does** Malware reversing/analysis in the cloud with extensive report generation.

**What we liked** The capabilities of this tool are beyond any single tool set we've seen. This is a malware reversing/forensics lab in the cloud with all of the bells and whistles you'd expect, plus a fistfull of ones you wouldn't. So much functionality there isn't room in this review to cover it all.

**The bottom line** This is a must-have tool for IT security shops in organizations of just about any size. We could not get along as well without it.

From the May 01, 2017 Issue of SC Media

TOPICS: CLOUD SECURITY



Back to Top ↑