toolsmith #107

There Is No Privacy: Hook Analyser vs. Hacking Team

By Russ McRee – ISSA Senior Member, Puget Sound (Seattle) Chapter

Prerequisites

Hook Analyser

As we explore privacy in this month's *ISSA Journal*, timing couldn't be better. Since last we convened, the Hacking Team breach has informed us all that privacy literally is for sale. Hacking Team's primary product is Remote Control System (RCS), "a solution designed to evade encryption by means of an agent directly installed on the device to monitor. Evidence collection on monitored devices is stealth and transmission of collected data from the device to the RCS server is encrypted and untraceable."[1] While Hacking Team initially claimed their products are not sold to "governments or to countries blacklisted by the US, EU, UN, NATO, or ASEAN,"[2] the data dump made public as result of their breach indicated otherwise. In fact, their customers include major players in finance, energy, and telecommunications. Among all the 0-days and exploits in the Hacking Team dump, it was even discovered that they offered UEFI BIOS rootkit to ensure "that it silently reinstalls its surveillance tool even if the hard drive is wiped clean or replaced."[3] With industry giants willing to seemingly utilize the likes of RCS, we're left to wonder where the line will be drawn. I long ago assumed there is no line and therefore assume there is no privacy. May I recommend you join me in this gloomy outlook?

Perhaps a little proof may help you come to terms with this simple rule: don't store or transmit via digital media that what which you don't want read by anyone and everyone.

To get to the heart of the matter, we'll assess some Hacking Team "products" pulled from the public dump with Beenu Arora's Hook Analyser.[4] Beenu just celebrated the release of Hook Analyser 3.2 as of 19 JUL. You may recall that I mentioned Hook Analyser via the Internet Storm Center Diary for the Keeping the RATs Out series[5]; we'll put it through its paces here. Per Beenu, Hook Analyser is a freeware project that brings malware (static and dynamic) analysis and cyber-threat intelligence capabilities together. It can perform analysis on suspicious or malware files and can analyze software for crash-points or security bugs. The malware analysis module can perform the following actions:

- Spawn and hook to application
- Hook to a specific running process
- Static malware analysis
  - Scans PE/Windows executables to identify potential malware traces
- Application crash analysis
  - Allows you to analyze memory content when an application crashes
- Exe extractor
  - Extracts executables from running process/s

The Cyber Threat Intelligence module provides open source intelligence where you can search for IP addresses, hashes, or keywords. It will collect relevant information from various sources, analyze the information to eliminate false-positives, correlate the various datasets, and visualize the results.

What better to run Hacking Team binaries through. Let's begin.

Hacking Team samples

I pulled four random binaries out of the Hacking Team dump for analysis, sticking exclusively to EXEs. There are numerous weaponized document and media files, but I was most interested in getting to the heart of the matter with Hook Analyser. Details for the four samples follow:

1. agent 222.exe
   a. MD5: fea2b67d59b0af196273fb204fd039a2
   b. VT: 36/55
2. agent 1154.exe
   a. MD5: c1c99e0014c6d067a6b1092f2860df4a
   b. VT: 31/55

1 http://www.hackingteam.it/index.php/remote-control-system.

2 http://www.hackingteam.it/index.php/customer-policy.

3 http://www.pcworld.com/article/2948092/security/hacking-teams-malware-uses-uefi-rootkit-to-survive-os-reinstalls.html.

4 http://www.hookanalyser.com/.

5 https://isc.sans.edu/forums/diary/Keeping+the+RATs+out+the+trap+is+sprung+Part+3/18415/.

3. Microsoft Word 2010 2.exe
   a. MD5: 1ea8826eeabfce348864f147e0a5648d
   b. VT: 0/55
4. my_photo_holiday_my_ass_7786868767878 19.exe
   a. MD5: e36ff18f794ff51c15c08bac37d4c431
   b. VT: 48/55

I found it interesting that one of the four (Microsoft Word 2010 2.exe) exhibited no anti-malware detection via Virus Total as this was written, so I started there.

Hook Analyser

Hook Analyser is stand-alone and runs in console mode on contemporary Windows systems. For this effort I ran it on Windows 7 x32 & x64 virtual machines. The initial UI as seen in figure 1 is basic and straightforward.

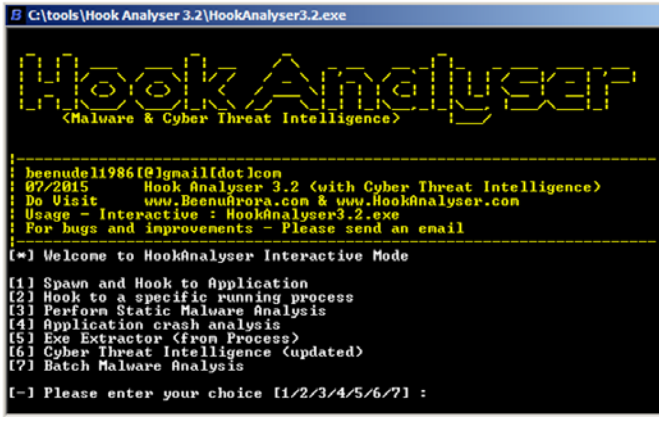

Figure 1 – Hook Analyser UI

For Microsoft Word 2010 2.exe, I opted to use *Spawn and Hook to Application* and provided the full path to the sample. Hook Analyser exited quickly but spawned C:\tools\Hook Analyser 3.2\QR7C8A.exe, with which I repeated the process. The result was a robust output log to a text file named by date and time of the analysis, an XML report, named identically, of the high-level behaviors of the sample.

A few key items jumped right out in the reports. First, the sample is debug aware. Second, it spawns a new process. Third, Hook Analyser found one trace of a potential PDB/Project at offset 00007F0. When I ran strings against the sample, I found c:\users\guido\documents\visual studio 2012\Projects\fake_office\Release\fake_office.pdb, confirming the project and even the developer. I'd have to err on the side of threat related in this scenario, just on project name alone. Further analysis by Microsoft's Malware Protection Center revealed that it checks for the presence of a legitimate instance of winword.exe on C: or D:, then executes C:\a.exe. As a results, this sample has been classified "threat related." Based on naming conventions followed by Hacking Team, one can reasonably conclude that C:\a.exe is likely an RCS agent. By the way, Guido, in this case, is probably Guido Landi, a former senior Hacking Team software developer.

You can see the overall output from both reports in a combined figure 2.

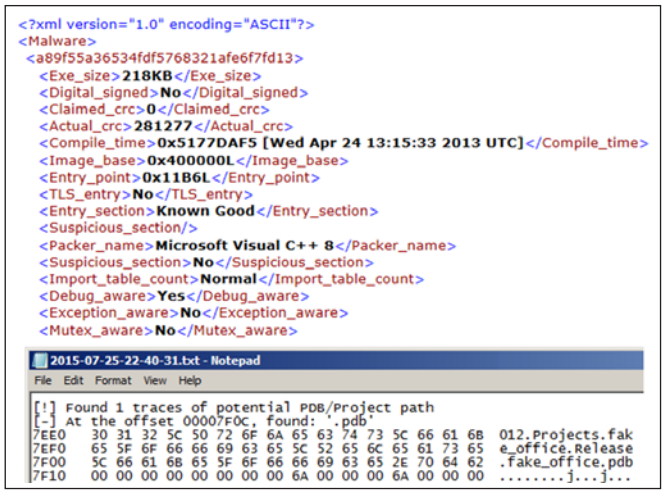

Figure 2 – Hook Analyser results

I took a different approach with the next sample analysis, specifically agent 222.exe. I first executed the sample, then chose *Hook to a specific running process*. Hook Analyser then provides a listing of all active processes. Agent 222.exe showed itself with process ID 3376. I entered 3376 and Hook Analyser executed a quick run and spawned GVNTDQ.exe. I reran Hook Analyser, selected 3 for *Perform Static Malware Analysis*, and provided C:\tools\Hook Analyser 3.2\GVNTDQ.exe. GVNTDQ.exe is simply a new instance of Agent 222.exe. This time another slew of very interesting artifacts revealed themselves. The "agent" process runs as TreeSizeFree.exe, an alleged hard disk space manager from JAM Software, and runs as trusted given that it is signed by a Certum/Unizeto cert. It also appears to be anti-debugging aware and packed using an unknown packer. The sample manipulates GDI32.dll, the OS's graphic device interface and WINHTTP.dll (mapped in memory) with a `WinHttpGetIEProxyConfigForCurrentUser` call, which provides the Internet Explorer proxy settings for the current active network connection. Remember that privacy you were so interested in maintaining?

Let's say you're asked to investigate a suspect system, and you have no prior knowledge or IOCs. You do discover a suspicious process running and you'd like to dump it. Choose *Exe Extractor* (from Process), reply *no* when it asks if you'd like to dump all processes, then provide the process ID you'd like extracted. It will write an EXE named for the process ID to your Hook Analyser working directory.

You can also run batch jobs against a directory of samples by choosing *Batch Malware Analysis*, then providing the path to the sample set.

I'd be remiss if I didn't use the Threat Intelligence module with some of the indicators discovered with Hook Analyser. To use it, you really want to prep it first. The Threat Intelligence module includes:

- IP intelligence
- Keyword intelligence
- Network file analysis
  - PCAP

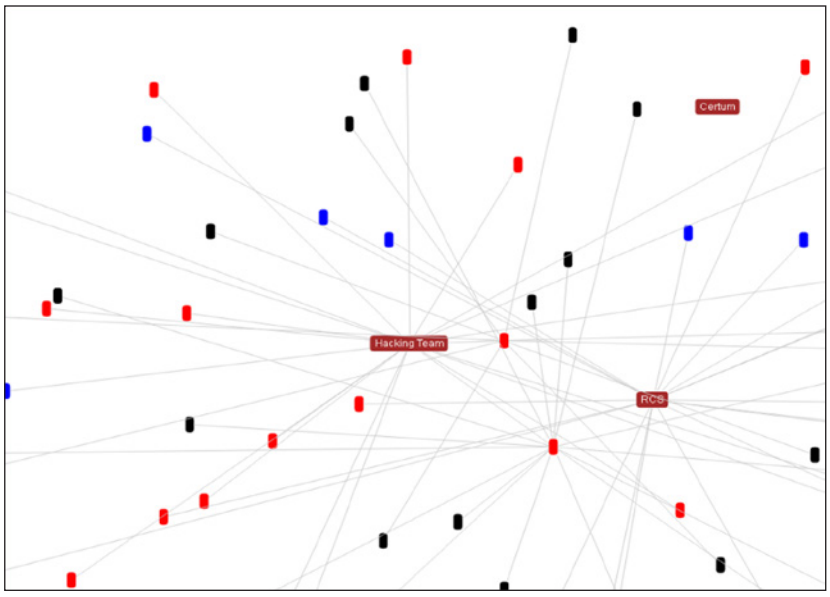

Figure 3 – A bird's eye view to related Hacking Team keywords

- Social intelligence
  - Pulls data from Twitter for user-defined keywords, performs network analysis

Each of these is managed by a flat text file as described in Beenu's recent post.[6] One note: don't get too extravagant with your keywords. Try to use unique terms that are tightly related to your investigation and avoid using broad terms such as *agent* in this case. I dropped a Hacking Team-related IP address in the intelligence-ipdb.txt file, the keywords *Certum, Unizeto, Hacking Team*, and *RCS* in keywords.txt, and *Hacking Team* in channels.txt. Tune these files to your liking and current relevance. As an example, URL.txt has some extremely dated resources from which it pulls IP information; there's no reason to waste cycles on all of the default list. I ran the Threat Intelligence module as a standalone feature as follows: `ThreatIntel.exe -auto`. Give it a bit of time, it checks against all the provided sources and against Twitter as well. Once complete it will pop a view open in your default browser. You'll note general information under Global Threat Landscape including suspicious IPs and ASNs, recent vulnerability data, as well as country and geo-specific threat visualizations. More interesting and related to your investigation will be the likes of *Keyword-based Cyber Intelligence*. The resulting co-relation (bird eye) view is pretty cool, as seen in figure 3.

Drill into the complete view for full keyword content results. I updated channels.txt to include only hackingteam and intelligence-ipdb.txt with related Hacking Team IP addresses. While I was unable to retrieve viable results for IP intelligence, the partial results under *Social Intelligence (Rececent Tweets)* were relavent and timely as seen in figure 4.

There are a few bugs that remain in the Threat Intelligence module, but it definitely does show promise; I'm sure they'll be worked out in later releases.

In conclusion

The updates to the Threat Intelligence are reasonable, potentially making for a useful aggregation of data related to your investigation, gleaned from your indicators and analysis. Couple that with run-time and static analysis of malicious binaries and you have quite a combination for your arsenal. Use it in good health, to you and your network!

Ping me via email or Twitter if you have questions (russ at holisticinfosec dot org or @holisticinfosec).

Cheers…until next month.

ACK

—Beenu Arora, @beenuar, Hook Analyser developer and project lead

About the Author

Russ McRee manages the Threat Intelligence & Engineering team for Microsoft's Online Services Security & Compliance organization. In addition to toolsmith, he's written for numerous other publications, speaks regularly at events such as DEFCON, Black Hat, and RSA, and is a SANS Internet Storm Center handler. As an advocate for a holistic approach to the practice of information assurance Russ maintains holisticinfosec.org. He serves in the Washington State Guard as the Cybersecurity Advisor to the Washington Military Department. Reach him at russ at holisticinfosec dot org or @holisticinfosec.

6 http://www.hookanalyser.com/2015/07/hook-analyser-32-major-release.html.

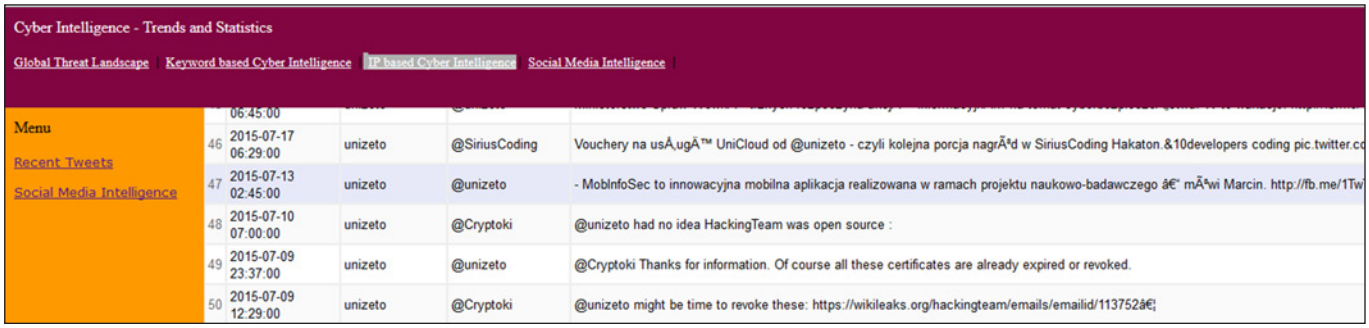

Figure 4 – Recent Hacking Team related tweets per the Threat Intelligence module