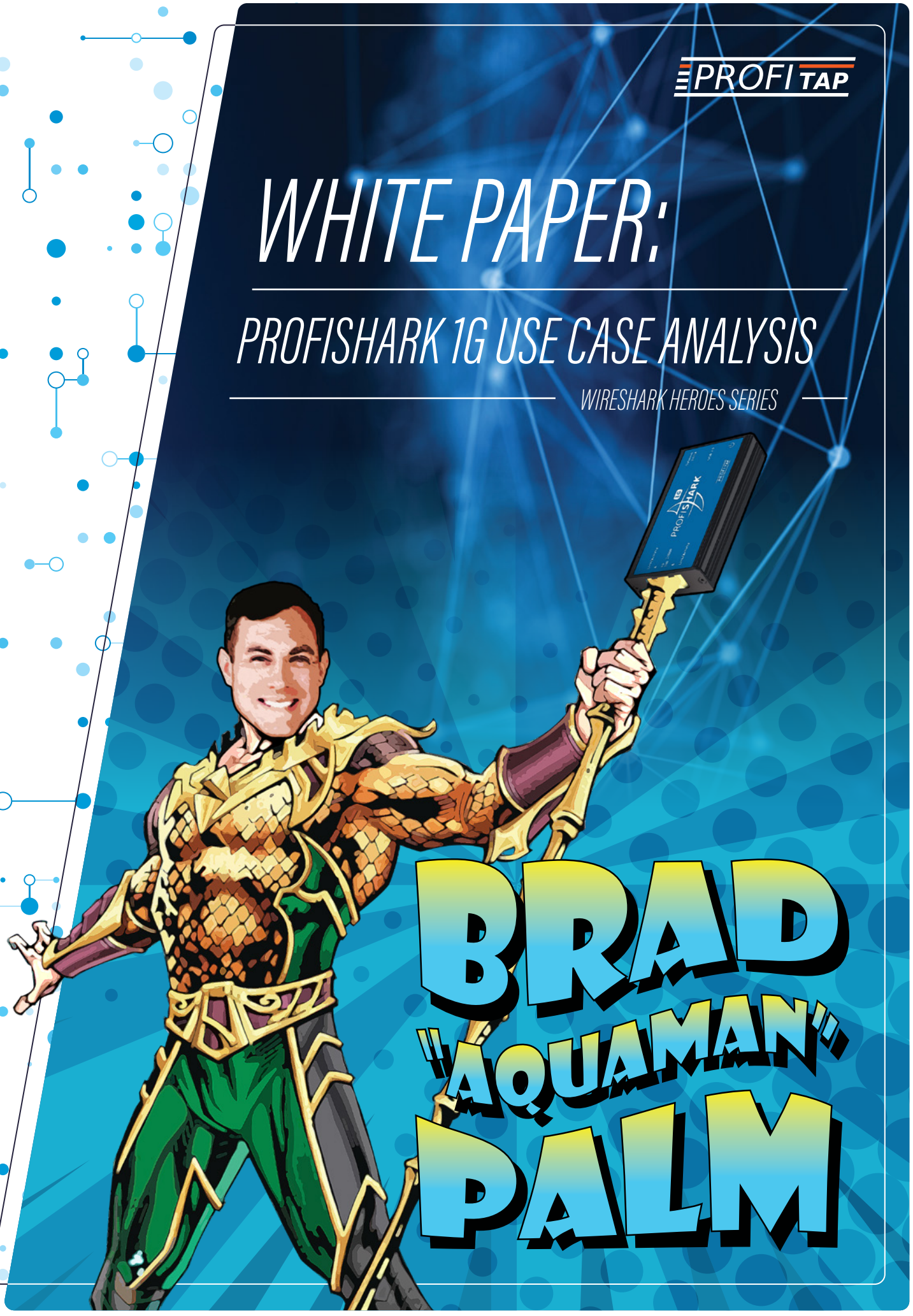
PROFITAP

# WHITE PAPER:

## PROFISHARK 1G USE CASE ANALYSIS

WIRESHARK HEROES SERIES




VISIT WWW.PROFITAP.COM

# BRAD PALM

## OPERATOR AT BRUTEFORCE LLC

*Brad is a problem solver and a convergent thinker that looks forward to challenges in bridging the physical and virtual worlds. Highly skilled at analyzing and navigating the IT risks that are inherent when adopting technologies, he is motivated to work with dynamic, fast-paced, high-performing teams. Brad is operating BruteForce, a digital security and network analysis consulting firm. Their solution stack consists of building resilient architectures with DevOps principles, pressure testing and breaking those designs to constantly improve and harden them, and then actively defending and hunting their environments for continued mission accomplishment.*

## EXPERTISE:

- *DevOps/Security Engineer focused on IT solutions enabling resiliency.*
- *Passionate about build, break, hunt!*


BRAD@BRUTEFORCE.IO

LINKEDIN.COM/IN/BRADPALM/


# BACKGROUND

The importance of having a quality network test access port (TAP) when conducting Digital Forensics and Incident Response (DFIR) has been covered in a white paper by Profitap, titled "Special Tool for Special Forces: Tapping into real-time threats in the cyberspace". In addition to the points presented in the white paper, I would like to provide a recent use case where the ProfiShark 1G was pivotal in determining the compromise of a system.

Recently while threat hunting an environment, I came across a host system that presented an indicator of compromise (IOC) that was extremely convincing. Upon running a battery of tests against the host (e.g. chkrootkit, lynis, rkhunter), all tools came back reporting that the system was clean and not compromised. At this point you are faced with the decision to rule out the compromise of the host system or develop a follow-on test which will allow a more fine-grained view of the system.

The following use case analysis dives into how the ProfiShark 1G provides you the desired fine-grained view to inspect network traffic and provides you the ability to determine if a system is compromised. I have approached this analysis in the manner of describing a value proposition for a product. I use this approach since this is how I compare and evaluate products to include in my personal DFIR go-bag or include in my technology "solution stack" for solving problems; and it allows me to get down to the basic facts quickly. For the purposes of this use case, I have found that both the ProfiShark 1G and the ProfiShark 1G+, shown in Figure 1, are equally suited for DFIR work and when I refer to the ProfiShark 1G it can also be read as the "ProfiShark family of products".

Figure 1: ProfiShark 1G and 1G+ Comparison

# WHAT PROBLEM DOES PROFISHARK 1G SOLVE?

At a high level overview, the ProfiShark 1G enables you to conduct network analysis which consists of three big buckets - troubleshooting, optimization, and forensics. All three of these disciplines rely heavily upon having a baseline of your network traffic, to then determine what is suspect or "interesting" traffic. The ProfiShark removes the barriers to conducting these baselines, since it has been specifically crafted with the network engineer/security engineer in mind.

With regard to the use case presented, the ProfiShark 1G allows you to achieve a fine-grained view of the host system by assisting in network based "cross-view" rootkit analysis. Network based cross-view analysis consists of looking at network connections from two different vantage points. One vantage point is from the user space perspective on the host system. The other vantage point is from an unbiased perspective, where a rootkit can not manipulate the information being presented to the analyst. You then compare the results gathered from these two vantage points and if there are any network connection discrepancies you can conclude that a rootkit is present (this is a simplified heuristic, since the logic required to address all the edge cases is beyond the scope of this paper). ProfiShark 1G provides the unbiased vantage point when it is inserted into the network path, adjacent to the host system's network interface controller (NIC), and captures packets to/from the host system.

When I first began interrogating the host system, I uploaded two popular rootkit checking tools and ran them. The results from a portion of the rkhunter scan are shown in Figure 2 and a portion of the results from the chkrootkit scan are shown in Figure 3. Both these tools concluded that no rootkit was present.

```
[13:48:57] System checks summary
[13:48:57] ====================
[13:48:57]
[13:48:57] File properties checks...
[13:48:57] Required commands check failed
[13:48:57] Files checked: 124
[13:48:57] Suspect files: 5
[13:48:57]
[13:48:57] Rootkit checks...
[13:48:57] Rootkits checked : 431
[13:48:57] Possible rootkits: 0
[13:48:57]
[13:48:57] Applications checks...
[13:48:57] All checks skipped
[13:48:58]
[13:48:58] The system checks took: 1 minute and 42 seconds
```

Figure 2: Output from the Conclusion of the rkhunter Scan

```
ROOTDIR is `/'
Checking `amd'... not found
Checking `basename'... not infected
Checking `biff'... not found
Checking `chfn'... not found
Checking `chsh'... not found
Checking `cron'... not infected
Checking `crontab'... not infected
Checking `date'... not infected
Checking `du'... not infected
Checking `dirname'... not infected
Checking `echo'... not infected
Checking `egrep'... not infected
Checking `env'... not infected
Checking `find'... not infected
Checking `fingerd'... not found
Checking `gpm'... not found
Checking `grep'... not infected
Checking `hdparm'... not found
Checking `su'... not infected
Checking `ifconfig'... not infected
Checking `inetd'... not tested
Checking `inetdconf'... not found
Checking `identd'... not found
Checking `init'... not infected
Checking `killall'... not infected
Checking `ldsopreload'... can't exec ./strings-static, not tested
Checking `login'... not infected
Checking `ls'... not infected
Checking `lsof'... not infected
Checking `mail'... not found
Checking `mingetty'... not found
Checking `netstat'... not infected
Checking `named'... not found
Checking `passwd'... not infected
Checking `pidof'... not infected
Checking `pop2'... not found
Checking `pop3'... not found
Checking `ps'... not infected
```

Figure 3: Output from a Portion of the chkrootkit Scan

I was not comfortable with the conclusion these tools provided and felt the need to do further analysis on the host system. Now begins the cross-view analytic technique that was described previously. For the user space vantage point, I used the netstat tool which prints out network connections to the command-line. I used the following flags $ netstat -plant to check active TCP sockets. This command output only one active session and that was my SSH session, used for remotely connecting to the host system.

For the unbiased vantage point, I unplugged the Cat5e Ethernet cable from the host, inserted a ProfiShark 1G TAP into the network equipment string, and then reconnected the Cat5e cable back into the host. This provided me the vantage point that would be able to verify if the user space netstat command was giving me an accurate portrayal of the network connections on the host system.

After starting a network capture in Wireshark and letting it run for a few minutes, the live capture portrayed a different story and showed that there was an additional SSH session to a foreign IP address that the system had no business talking to. I confirmed that this session was not being shown in the user space vantage point by running the netstat command again. Now that I was armed with this information I could confidently pull this system offline and begin the incident response steps necessary to bring it back to a known good state.

# WHAT VALUE IS CREATED BY PROFISHARK 1G?

If you had accepted the output of the rootkit checking tools, you would have allowed a compromised system to persist on your network. Now, the motives of an attacker are extremely challenging to determine especially when your goal is to reduce the time to detection of the IOC and the response time to mitigate it. However, I don't recommend you allow your network to be a petri dish where you can watch the latest adversary move through your network so you can conduct motive and behavioral analysis on them (this interesting work is being done by researchers with fascinating honeypot/active defense environments). Instead, by looking at the latest trends in adversarial activity one can conclude that had you allowed a threat to persist in your environment they may have been looking to make a quick payday (e.g., ransomware), harvest your host system's resources to mine cryptocurrency (e.g., cryptojacking), or maybe dig in for the long haul if you are an organization with some interesting research or intellectual property (e.g., advanced persistent threat).

By taking the thorough approach and conducting a network based cross-view analysis with the ProfiShark 1G, you can answer the critical question that begs to be answered - *am I compromised?*

# WHAT'S THE IMPACT OF THE PROFISHARK 1G SOLUTION?

As previously discussed, the ProfiShark 1G removes the barriers to conducting baselines. It accomplishes this by being cross-platform, small form factor, and doesn't have the bottleneck considerations that other RJ-45 aggregation TAPs have. Case in point - I have installed and used the ProfiShark 1G on Windows and Linux operating systems, the ProfiShark is smaller than my iPhone 6, and I have stress tested the capture capabilities of the ProfiShark by sending full line rate traffic in both directions without dropping packets.

Earlier, I mentioned that the ProfiShark 1G and 1G+ were interchangeable with regards to the use case I presented and I'd like to retract that. The one case where they are not so easily interchangeable is when considering time stamping. The ProfiShark 1G+, shown in Figure 4, adds the additional capability of pulling time from a precise time server in the sky, also known as the Global Positioning System (GPS). This feature is especially interesting when you have to take captures at geographically dispersed sites and want to merge or cross-reference those

captures to do in-depth analysis. It is also compelling that you can use this precise third-party time sync as a way of adding validity to the network capture should it have to be used as direct evidence, as part of a legal proceeding. Now you don't have to rely on time shifts or trying to sync multiple capture boxes, before deploying to those various capture sites.


Figure 4: ProfiShark 1G+ with GPS Antenna

# CONCLUSION

It was through the use of a ProfiShark 1G network TAP that I was able to confirm that a rootkit was indeed on the system and it was obfuscating the network socket that was being used for malicious communications. The packets never lie and they showed that there was malicious activity being masked, when a one-to-one comparison was conducted between the captured traffic from a TAP (external to the host's NIC) and the host system's built-in network tools. When a scenario like this occurs and you can no longer trust the host operating system, you have to leverage a trusted third-party tool to interrogate the infected system.

Bottom line - as an IT professional charged with keeping networks operational and secure, I am highly selective in the tools that go into my network troubleshooting/network forensics go-bag. ProfiShark 1G or 1G+ has absolutely earned its place in my go-bag, or pocket for that matter!

# IT ALL STARTS WITH VISIBILITY

PROFITAP

Profitap develops a wide range of state-of-the-art and user-friendly network monitoring tools for both SMEs and the enterprise sector. Our wide range of high-density network TAPs, field service troubleshooters and network packet brokers are extremely performant, providing complete visibility and access to your network, 24/7.

We've been creating monitoring solutions for network analysis and traffic acquisition for more than 33 years. Therefore, we are experts in our field and our award-winning ProfiShark® 1G stands to prove it. This lightweight, advanced and portable network TAP is one the most innovative products on the market.

With more than 1,000 clients from 55 countries, PROFITAP has become a must-have solution for many important businesses, many of which are among Fortune 500 companies.

PROFITAP HQ B.V.
HIGH TECH CAMPUS 9
5656 AE EINDHOVEN
THE NETHERLANDS

sales@profitap.com
www.profitap.com

Profitap

@Profitap

profitap-international