EXHIBIT 4

HIGHLY CONFIDENTIAL – ATTORNEYS EYES' ONLY

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

FINJAN LLC., a Delaware Limited Liability Company, Plaintiff, v. QUALYS INC., a Delaware Corporation, Defendant.	Case No. 4:18-cv-07229-YGR (TSH) Hon. Yvonne Gonzalez Rogers **EXPERT REPORT OF NENAD MEDVIDOVIĆ, PH.D.** **[HC-AEO]**

Nenad Medvidovic, PH.D.
December 1, 2020

E. Viruses and Malware

73. Viruses and malware are harmful programs (or program fragments) that are downloaded or transferred by recordable media (i.e., floppy disk or USB flash drive) and installed on a user computer, often without their knowledge. The behavior of a virus or malware ranges from simply making a copy of itself, to annoying the user with strange computer problems, to invading the user's privacy by stealing sensitive personal or private information, to using the user's computer as a platform to attack other computers (as in denial-of-service attacks).

74. Once successfully installed on a target system, many viruses and malware programs will attempt to communicate with the person who deployed them by sending messages to that person indicating that they have been successfully deployed. Such messages come in many forms, and are often referred to as a "beacon." The messages may also be inserted into messages that a server sends out. Some viruses and malware, once deployed, will "exfiltrate" data from the targeted system to their user. Others all the user to gain access to the infected system, such as through a remote command shell interface that allows the user to perform actions within the system and to "pivot" to gain access to other servers and computers within the network.

75. To prevent these harmful programs from infecting a user's computer, anti-malware tools can be installed and executed on a security gateway. For example, a security tool in a security gateway may intercept a virus or malware before it reaches the user's computer.

76. Traditionally, an anti-virus software program compares a representation of the malware to the malware itself. This representation is often formed based on a pattern of bytes in the computer code that is unique to the virus program, and is called a "signature." For example, a signature could be the bytes "08 201 251 A T M." This six-byte sequence (three integers and three ASCII characters) may be present in a virus program but not observed in any other benign program (such as

Microsoft Word). Therefore, by looking for this string, one might identify the malware, without the risk of flagging benign programs as malicious.

77. A traditional anti-virus software program maintains a list of such signatures, one for each malicious program that it can detect, and may be installed on the security gateway. In this case, the anti-virus program looks for a particular set of bytes in the representation of the code, and takes action based on whether or not a match has been found. For example, a security gateway that identifies a mail attachment as a virus may discard the message and notify the client that the message was designed to damage the computer.

78. These signature-based approaches suffer from a number of problems. First, the approaches only detect malware after the fact. These approaches do not identify or block the vulnerabilities that were exploited to introduce the malware into the system in the first place. Such vulnerabilities can often be exploited to introduce any number of malware programs into a system until they are remediated.

79. Additionally, if a new malware threat is created, the anti-virus program will not have a signature that detects this new malware until its list of signatures is updated to include an identification of the new malware threat. During the period between updates, the user is vulnerable to an infection until a signature is created and distributed to the anti-virus tool. Therefore, this approach can only identify previously known malware samples for which a signature has been developed and added to the list of signatures. As the number of malware programs grows, the list of signatures will also grow. Therefore, signature-based approaches are difficult to manage (e.g., distributing large lists of signatures becomes complicated) and slow (looking for all the signatures in every file downloaded can take a long time). In the computer industry, using virus signatures to check files for viruses is called a reactive technology, because the system has to be informed of a new malware program in order to protect against a virus program infection. The bottom line is that

signature-based anti-virus tools are only effective after a virus has been identified and, therefore, after it has done its harm.

80. An alternative, more proactive, approach is to identify and close vulnerabilities before malware is event introduced into a system. Because a large, complex system often has many potential points of access it can have a large number of potential vulnerabilities. It is important then to prioritize which potential vulnerabilities are most likely to actually permit malware into the system, so that the network operator can prioritize using the limited available resources to remediating the most pressing vulnerabilities. One way to prioritize potential vulnerabilities is to use a penetration testing tool that attempts to exploit potential vulnerabilities. When a potential vulnerability is successfully exploited by the penetration testing tool, then the vulnerability is validated and can be prioritized.

81. To understand how behavior might be leveraged in order to detect viruses and malware, consider a scenario where a user inadvertently attempts to download a malware program via an HTTP request. The security gateway intercepts the program or webpage before it reaches the user's computer. The content of this malware program is then analyzed to determine which operations might be performed. This analysis can be performed by analyzing the file itself to look at operations within the file. These operations can then compared to a security policy to determine whether the operations might signal malicious behavior. If the malware program is detected, the security gateway can block the program from ever reaching the user's computer.

F. Vulnerability Management

82. Vulnerability management refers to the concept within the computer security field of identifying and remediating vulnerabilities. A vulnerability is a weakness in security that is subject to being exploited, which is when malicious software or a bad actor uses to vulnerability to harm or attack a computer or network. To illustrate the concept by analogy to a non-computer context, a

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.