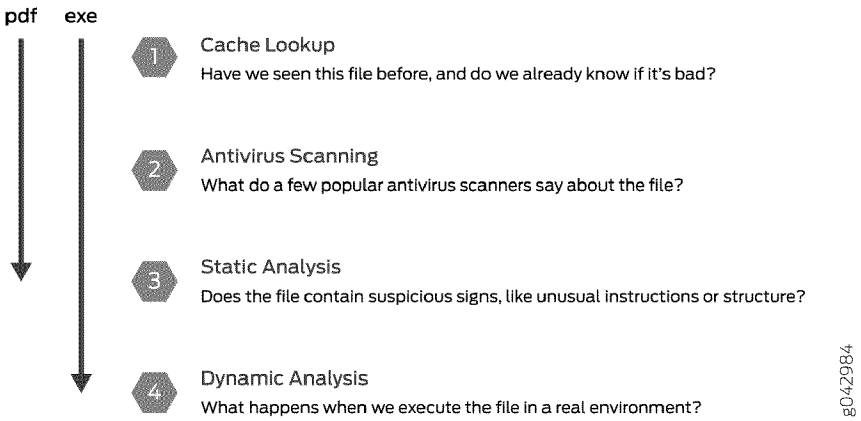
EXHIBIT 12

How is Malware Analyzed and Detected?

Sky ATP uses a pipeline approach to analyzing and detecting malware. If an analysis reveals that the file is absolutely malware, it is not necessary to continue the pipeline to further examine the malware. See Figure 1.

Figure 1: Example Sky ATP Pipeline Approach for Analyzing Malware



Each analysis technique creates a verdict number, which is combined to create a final verdict number between 1 and 10. A verdict number is a score or threat level. The higher the number, the higher the malware threat. The SRX Series device compares this verdict number to the policy settings and either permits or denies the session. If the session is denied, a reset packet is sent to the client and the packets are dropped from the server.

Cache Lookup

When a file is analyzed, a file hash is generated, and the results of the analysis are stored in a database. When a file is uploaded to the Sky ATP cloud, the first step is to check whether this file has been looked at before. If it has, the stored verdict is returned to the SRX Series device and there is no need to re-analyze the file. In addition to files scanned by Sky ATP, information about common malware files is also stored to provide faster response.

Cache lookup is performed in real time. All other techniques are done offline. This means that if the cache lookup does not return a verdict, the file is sent to the client system while the Sky ATP cloud continues to examine the file using the remaining pipeline techniques. If a later analysis returns a malware verdict, then the file and host are flagged.

Antivirus Scan

The advantage of antivirus software is its protection against a large number of potential threats, such as viruses, trojans, worms, spyware, and rootkits. The disadvantage of antivirus software is that it is always behind the malware. The virus comes first and the patch to the virus comes second. Antivirus is better at defending familiar threats and known malware than zero-day threats.

Sky ATP utilizes multiple antivirus software packages, not just one, to analyze a file. The results are then fed into the machine learning algorithm to overcome false positives and false negatives.

Static Analysis

Static analysis examines files without actually running them. Basic static analysis is straightforward and fast, typically around 30 seconds. The following are examples of areas static analysis inspects:

- Metadata information—Na[illegible] file was compiled on.
- Categories of instructions [illegible] APIs?.

- File entropy—How random is the file? A common technique for malware is to encrypt portions of the code and then decrypt it during runtime. A lot of encryption is a strong indication a this file is malware.

The output of the static analysis is fed into the machine learning algorithm to improve the verdict accuracy.

Dynamic Analysis

The majority of the time spent inspecting a file is in dynamic analysis. With dynamic analysis, often called *sandboxing*, a file is studied as it is executed in a secure environment. During this analysis, an operating system environment is set up, typically in a virtual machine, and tools are started to monitor all activity. The file is uploaded to this environment and is allowed to run for several minutes. Once the allotted time has passed, the record of activity is downloaded and passed to the machine learning algorithm to generate a verdict.

Sophisticated malware can detect a sandbox environment due to its lack of human interaction, such as mouse movement. Sky ATP uses a number of *deception techniques* to trick the malware into determining this is a real user environment. For example, Sky ATP can:

- Generate a realistic pattern of user interaction such as mouse movement, simulating keystrokes, and installing and launching common software packages.
- Create fake high-value targets in the client, such as stored credentials, user files, and a realistic network with Internet access.
- Create vulnerable areas in the operating system.

Deception techniques by themselves greatly boost the detection rate while reducing false positives. They also boosts the detection rate of the sandbox the file is running in because they get the malware to perform more activity. The more the file runs the more data is obtained to detect whether it is malware.

Machine Learning Algorithm

Sky ATP uses its own proprietary implementation of machine learning to assist in analysis. Machine learning recognizes patterns and correlates information for improved file analysis. The machine learning algorithm is programmed with features from thousands of malware samples and thousands of goodware samples. It learns what malware looks like, and is regularly re-programmed to get smarter as threats evolve.

Threat Levels

Sky ATP assigns a number between 0-10 to indicate the threat level of files scanned for malware and the threat level for infected hosts. See Table 1.

Table 1: Threat Level Definitions

Threat Level	Definition
0	Clean; no action is required.
1 - 3	Low threat level.
4 - 6	Medium threat level.
7 -10	High threat level.

For more information on threat levels, see the Sky ATP Web UI online help.

Modified: 2017-06-07