

EXHIBIT 24

Sky Advanced Threat Prevention Scanned File Overview

Sky ATP keeps a record of all file metadata sent to the cloud for inspection. You can view the files sent from your network by selecting **Monitor > File Scanning** in the Web UI. See Figure 1. Your firewall policy determines what to do if a file is suspected of being malware. For example, block that file from being downloaded to the client.

Figure 1: List of Inspected Files and Their Results

The screenshot shows the 'File Scanning' page in the Junos Space Security Director. At the top, there's a navigation bar with 'Hosts', 'C&C Servers', and 'File Scanning'. Below that, a 'File Scanning' header includes an 'Export' button and a 'Threat level' filter set to '4'. A table lists scanned files with columns: File Signature, Threat Level, Filename, Last Submitted, URL, Malware Name, Category, and Status. The first three rows show files with a threat level of 9 and status 'Blocked'. The next three rows show files with a threat level of 5 and status 'Allowed'. The last four rows show files with threat levels of 7, 8, and 4, with statuses ranging from 'Allowed' to 'Blocked'.

By default, threat levels 4 and above are shown. Click the file's signature to view more information, such as file details, what other malware scanners say about this file, and a complete list of hosts that downloaded this file. See Figure 2.

Figure 2: Viewing Scanned File Details

The screenshot shows the detailed view for a scanned file with signature '714c0ec6aef294bc4077...'. The interface is divided into several sections:

- Threat Level:** A large '9' is displayed. Below it, the file name is 'unorwik.dll', the category is 'other (Extension: dll, MIME ty...', and the action taken is 'Blocked'.
- Top Indicators:** Shows 'Malware Name: Win32:Tr:Golroted.Denqs', 'Signature Match: Golroted (Tr)', and 'Networking: 152.19.134.46, http://8.8.8.8.in-addr.arpa'.
- Prevalence:** Shows 'Global prevalence: High', 'Unique users: 3', and 'Protocols seen: HTTP'.
- GENERAL NETWORK ACTIVITY:** A section header with a downward arrow.
- Status:** Lists 'Threat Level: 9', 'Action Taken: Blocked', 'Global Prevalence: High', and 'Last Scanned: Dec 9, 2016 10:36 PM'.
- File Information:** Lists 'File Name: unorwik.dll', 'Category: other (Extension: dll, MIME type: application/octet-stream)', 'Size: 1KB', 'Platform: Win32', 'Malware Name: Win32:Tr:Golroted.Denqs', 'Type: Tr', and 'Strain: Golroted.Denqs'.
- Other Details:** Lists 'sha256: 714c0ec6aef294bc40773d5b4e8e2c68691c6412b7bb2b6119e1b7411cb1b2' and 'md5: fc24687e644d2b4a6bb48e36527abb8'.
- HTTP Downloads:** A table with columns: Client Host, Client IP Address, File Name, Date/Time Submitted, Device, URL, Destination IP, and User Name. One entry is shown: Client Host '212.90.', File Name 'unorwik.dll', Date/Time Submitted 'Dec 11, 2016 2:23...', Device 'TU3814TE2916', URL 'http://notrutkonuto...', Destination IP '193.0.'.

For more information on the file scan details page, see the Web UI tooltips and online help.

If you suspect a file is suspicious, you can manually upload it for scanning and evaluation. Click **Monitor > File Scanning > Manual Upload** to browse to the file you want to upload. The file can be up to 32 MB.

There is a limit to the number of files administrators can upload for manual scanning. File uploads are limited by realm (across all users in a realm) in a 24-hour period. You can upload two files per each active device enrolled and 10 files per each premium-licensed device in your account. For example, if you have two Sky ATP premium-licensed SRX Series devices and one other SRX Series device, Sky ATP will allow a maximum of 22 files to be allowed in a 24-hour window.

For more information on scanning files, see the Web UI infotips and online help.

Modified: 2017-01-10