

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 Junos Space Security Director. The interface includes a sidebar with navigation options (Hosts, C&C Servers, File Scanning) and a main content area. At the top, there are filters for 'Export' and 'Threat level' (High, Medium, Low, None/clean). A table lists scanned files with the following columns: File Signature, Threat Level, Filename, Last Submitted, URL, Malware Name, Category, and Status. A red circle highlights the 'threat_level' column header.

File Signature	Threat Level	Filename	Last Submitted	URL	Malware Name	Category	Status
eg. 123, 456							
714cDec6aef294bc4...	9	unoriwik.dll	Dec 11, 2016 2:23 AM	http://notrutkonuto.org/uno...	Win32:Trojandownloader...	other	Blocked
714cDec6aef294bc4...	9	unoriwik.dll	Dec 9, 2016 10:36 PM	http://notrutkonuto.org/uno...	Win32:Trojandownloader...	other	Blocked
714cDec6aef294bc4...	9	unoriwik.dll	Dec 9, 2016 10:19 PM	http://notrutkonuto.org/uno...	Win32:Trojandownloader...	other	Blocked
f10f6986bd852e5ecc...	5	odaronipbat	Dec 9, 2016 10:19 PM	http://kodurkor.com/odaro...	Root:Constructor.AJ	other	Allowed
815a3b0e794e06b4...	5	alo/c/ulini	Nov 30, 2016 11:42 PM	http://nopurot.edu/alo/c/u...	ChromeOS:Trojandownlo...	other	Blocked
a33f63426101cc96a...	5	ii/unuxiso	Nov 30, 2016 11:42 PM	http://kunatro.ru/ii/unuxiso	HTML:Constructor:Pascal...	other	Allowed
112427f025939b687...	7	ipovono.bat	Nov 30, 2016 11:42 PM	http://rorororo.gov/ipovon...	HTML:Python:Milky:Smal...	other	Blocked
8261d0f82df924f11...	8	ukunamac.bat	Nov 21, 2016 12:33 PM	http://badware.com/ukuna...	Unix:Python:Rastluby:Mo...	unknown	Blocked
6d3762b62e957783...	7	acusapoc.zip	Nov 21, 2016 12:33 PM	http://badware.com/acusa...	Trojandownloader:Conferi...	unknown	Allowed
316737c6601505a6...	8	avesobax.ini	Nov 21, 2016 12:33 PM	http://badware.com/avoso...	Linux:MultiPacked:A	unknown	Blocked
54b98dae3055bb12...	4	obitowax.tar.gz	Nov 21, 2016 12:33 PM	http://badware.com/obitow...	Spyware:Downloadadmin...	unknown	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 of a scanned file in Junos Space Security Director. The interface includes a sidebar with navigation options (Hosts, C&C Servers, File Scanning) and a main content area. The file signature '714c0ec6aef294bc4077...' is highlighted. The details are organized into several sections:

- Threat Level:** 9. File name: unoriwik.dll. Category: other (Extension: dll, MIME ty... Action taken: Blocked.
- Top Indicators:** Malware Name: Win32:Tr:Golroted:Denqs; Signature Match: Golroted (Tr); Networking: 152.19.134.46, http://8.8.8.8.in-addr.arpa
- Prevalence:** Global prevalence: High; Unique users: 3; Protocols seen: HTTP
- GENERAL:** NETWORK ACTIVITY
- Status:** Threat Level: 9; Action Taken: Blocked; Global Prevalence: High; Last Scanned: Dec 9, 2016 10:36 PM
- File Information:** File Name: unoriwik.dll; Category: other (Extension: dll, MIME type: application/octet-stream); Size: 1KB; Platform: Win32; Malware Name: Win32:Tr:Golroted:Denqs; Type: Tr; Strain: Golroted:Denqs
- Other Details:** sha256: 714c0ec6aef294bc40773d5b4e8e2c68691c6412b7bb2b6119e1b7411cb1b2; md5: fc24687e644d2b4a6bb48e36527abb8
- HTTP Downloads:** Table with columns: Client Host, Client IP Address, File Name, Date/Time Submitted, Device, URL, Destination IP, User Name. One entry is visible: Client Host: 212.90., Client IP Address: unoriwik.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