# Learn About Advanced Threat Prevention

This *Learn About* examines advanced threat prevention (ATP) and an anti-malware solution from Juniper Networks called *Sky ATP*, both of which address vulnerabilities in today's networks.

## Overview

Malware is malicious software that disrupts network operations and gathers sensitive information on behalf of an unauthorized third party. While the majority of malware attacks are unfocused, new attacks are now using disguised threats that go after specific targets.

Targeted malware employs sophisticated methodology to evade traditional security defenses *in order to embed itself in the target's infrastructure*. Once attached, the malware can carry out a wide range of undetected malicious activities over months, or even years, including data theft, espionage, and disruption or destruction of network infrastructure and processes.

Unfortunately, there have been more than enough recent examples of malware attacks on major hotel chains, city infrastructures, and financial institutions. Examining some of these attacks in detail will illuminate the kind of advanced threats your network may be vulnerable to, and why technology like Sky ATP is so essential. (You can also learn more about each of these attacks, and Sky ATP, by using the links provided in the "*References and Resources*" section at the end of this *Learn About*.)

### Point of Sale (POS) Malware

In December of 2015 Hyatt Hotels disclosed that they had experienced unauthorized access to their credit card payment system at over 250 of their hotel sites between August and December of that year. Hyatt didn't disclose the type of malware that was used, but the breach spawned discussions about POS attacks and a long-standing weakness in the Payment Card Industry's Data Security Standard (PCI DSS).

This weakness has since been addressed by updated PCI DSS standards, but the standards are voluntary and not mandated by law. As of October 2015, all businesses are liable for credit card fraud that results from a transaction at any of their locations, unless an EMV chip-enabled reader is present. But the EMV chip is only used in brick-and-mortar stores and does not apply to online transactions. As it traverses various systems, POS malware searches for any weakness across the lifetime of a transaction. In the UK, where EMV chips have been used since 2003, in-person fraud has decreased but online fraud and other types of fraud have increased.

Eric Merritt, a researcher at Trustwave, discovered evidence of widespread malware targeting all sorts of POS retailers that may have existed undetected since 2011. It's called *Cherry Picker*. "Cherry Picker knows what it wants – and if it can't find it on the system, it simply exits," Merritt wrote of the technique in a blog entry referenced by Chris Brook in a *Threat Post* article posted on November 13, 2015: "This implies that the malware author *already scouted the system* and knows exactly what process they are targeting." See https://threatpost.com/researchers-discover-two-new-strains-of-pos-malware/115350/.

According to an article written by Eduard Kovacs, "'Cherry Picker' – PoS Malware Cleans Up After Itself" in *SecurityWeek*, dated November 12, 2015 (see http://www.securityweek.com/cherry-picker-pos-malware-cleans-after-itself), Cherry Picker not only knows what it wants, it knows how to cover its tracks. "Cherry Picker relies on a new memory scraping algorithm," the article states. "It uses a file infector for persistence, and it comes with a cleaner component that removes all traces of the infection from the system."

## Malware Targeting City Infrastructure

In December of 2015, just before the holidays, 80,000 customers in Ukraine experienced a 6-hour power outage. Experts widely describe the incident as the first known power outage caused by a cyberattack. "It's the major scenario we've all been concerned about for so long," said John Hultquist, head of iSIGHT's Cyber Espionage Intelligence Practice, in an article written by Dan Goodin in *Ars Technica* on January 6, 2016. See http://arstechnica.com/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/.

The outage is still being investigated, but a variant of a well-known Trojan horse called *Black Energy* was found on computers at the power the plant. "The Black Energy trojan, together with an SSH backdoor and the destructive KillDisk component, which were all detected in several electricity distribution companies in Ukraine, are a dangerous set of malicious tools theoretically capable of giving attackers remote access to a company's network, shutting down critical systems and, by wiping their data, making it harder to get them up and running again," said Robert Lipovsky, a senior malware researcher at ESET, in an article posted on January 11, 2016 on the *welivesecurity* website. See http://www.welivesecurity.com/2016/01/11/blackenergy-and-the-ukrainian-power-outage-what-we-really-know/.

As security experts continue to investigate, most agree that malware may not have directly caused the outage, but it was involved. "A new study of a cyberattack last month against Ukrainian power companies suggests malware didn't directly cause the outages that affected at least 80,000 customers. Instead, the malware provided a foothold for key access to networks that allowed the hackers to then open circuit breakers that cut power," wrote Jeremy Kirk from IDG News Service, in *PCWorld* on January 10, 2016 in the article Malware alone did not cause Ukraine power station outage; "They also conducted denial-of-service attacks on the utilities' phone systems to block complaints from affected customers." See http://www.pcworld.com/article/3020631/malware-alone-didnt-cause-ukraine-power-station-outage.html.

And in January 2016 a new wave of malware, similar to BlackEnergy, continued to target Ukraine's power grid, reinforcing the fact that as governmental infrastructures become more connected to the Internet, they also become more vulnerable.

## Malware Targeting the Banking Sector

Malware has sometimes been stopped, only to evolve and reappear again. For example, a malware program called *Dridex* targeted the banking industry throughout 2015. Dridex would arrive on a system as an email with a Word attachment. When the user opened the attachment, a macro embedded in the document executed and triggered the download of Dridex onto the system.

Once the malware had infected an unsuspecting host, it would direct the victim's HTTP requests to a fake bank URL watching for authentication information that could be used on the real bank website.

"The technique, known as DNS cache poisoning, involves changing DNS settings to direct someone asking for a legitimate banking website to a fake site. DNS cache poisoning is a powerful attack. Even if a person types in the correct domain name for a bank, the fake website is still shown in the browser," writes Jeremy Kirk in *PCWorld* on January 19, 2016 in the article "Dridex banking malware adds a new trick." See http://www.pcworld.com/article/3024247/dridex-banking-malware-adds-a-new-trick.html.

Dridex spread quickly and managed to achieve a high infection rate. But even after its discovery, Dridex still continues to evolve using its botnets to spread even further into networks of compromised hosts.

## Ransomware – Malware Used in Extortion Schemes

In a paper entitled "2016 Threats Predictions," (http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf) McAfee Labs stated the following: "Ransomware will remain a major and rapidly growing threat in 2016. With upcoming new variants and the success of the *ransomware-as-a-service* business model, we predict that the rise of ransomware that started in the third quarter of 2014 will continue in 2016."

"On Monday, Nov. 24 (2014), a crushing cyberattack was launched on Sony Pictures. Employees logging on to its network were met with the sound of gunfire, scrolling threats, and the menacing image of a fiery skeleton looming over the tiny zombified heads of the studio's top two executives. Before Sony's IT staff could pull the plug, the hackers' malware had leaped from machine to machine throughout the lot and across continents, wiping out half of Sony's global network," writes Peter Elkind in the July 1, 2015 issue of *Fortune* in the article "Inside the Hack of the Century." See http://fortune.com/sony-hack-part-1/ for details on the hackers suspected of launching the attack and what their demands included.

At the RSA Conference in 2015, Stuart McClure, CEO of the computer security firm Cylance, spoke about how the Sony hack took place, explaining it as a combination of phishing emails, weak passwords, and a lack of server hardening.

The initial email, received by several Sony executives, contained fake Apple ID verification requests with a link to a fake domain that prompted them to enter their Apple ID and password information. Once entered, the attackers took these credentials and coded them into a strain of malware known as *Wiper* in hopes

that the Sony executives were using the same verification information on their corporate accounts. Apparently, some of them were; the attackers eventually crippled Sony's networks. The breach is estimated to have cost Sony upward of $171 million.

And, in February of 2016, Hollywood Presbyterian Medical Center paid a $17,000 Bitcoin ransom to hackers who used similar malware to take control of the medical center's computer systems and would not relinquish control until they were paid.

"The malware locks systems by encrypting files and demanding ransom to obtain the decryption key. The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key," said hospital Chief Executive Allen Stefanek, in a *Los Angeles Times* article published on February 18, 2016. See http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html.

The FBI is investigating the attack.

## The Juniper Networks Solution to Advanced Threat Prevention

As malware evolves and its attacks become more specialized and highly targeted, a new category of advanced security has also emerged that can detect, analyze, and prevent these advanced threats, which are able to bypass traditional security methods.

Juniper Networks' solution for preventing advanced and emerging threats is Sky Advanced Threat Prevention (ATP), a cloud-based anti-malware solution coupled with the SRX Series firewall. Let's drill down and see how this unique combination makes Sky ATP so effective.

### Sky ATP

Sky ATP is an add-on for the SRX Series. It provides anti-malware prevention for existing and new SRX Series customers. In addition to the SRX Series device, Sky ATP includes malware detection and analysis, host analyzer, and command and control feeds. Each component in the solution has a role in detecting, analyzing, and blocking malware, but only the actual SRX Series device has a footprint in your network. All other components act as cloud-based services.

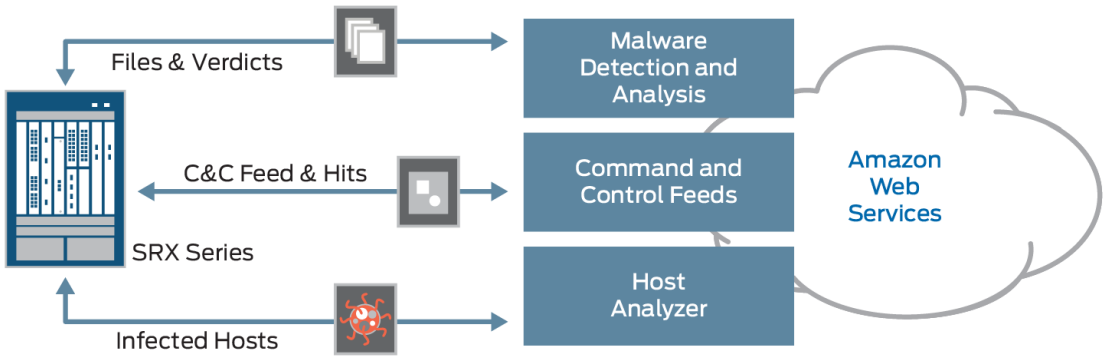



Figure 1 *Sky ATP Solution, Overview*

Sky ATP's cloud-based design delivers protection against Day Zero threats as it analyzes ingress and egress traffic for malware and indicators of compromise. It can instantly provide deep inspection, actionable reporting, and inline malware blocking. Sky ATP's solution components are listed in Table 1.

Table 1 *Sky ATP Solution Components:*

| | |
|---|---|
| Malware Detection and Analysis | Deployed in the cloud. |
| | Serves as the inspection pipeline, performs malware detonation, and provides the logging infrastructure. |
| | Returns verdicts and provides analytics. |
| Command and Control Feeds | Provides cloud-delivered security intelligence, specifically Juniper's command and control (C&C) feed. |
| | Accepts C&C detections. |
| Host Analyzer | Correlates C&C detections with malware detections to identify compromised hosts. |
| | Provides a feed of compromised hosts to the SRX Series for quarantine. |
| SRX Series Firewall | Extracts suspicious content and sends samples to the Sky ATP service for analysis. |
| | Performs inline blocking based on verdicts from the Sky ATP service. |
| | Leverages C&C feeds and sends detections to the Sky ATP service. |
| | Sends collected data to the Sky ATP service for reporting and telemetry purposes. |

## Analyzing and Detecting Malware

Sky ATP detects malware by using an *analysis pipeline*, as shown in Figure 2, when files are sent to the Sky ATP service by the SRX Series device:

- Cache lookup: Determines if the file in question is a known bad file.
- Anti-virus scanning: Runs the file through several well-known AV scanners.
- Static analysis: checks the file for suspicious signs such as unusual instructions or structure.
- Dynamic analysis: Executes the file in a real environment to see what it does in a secure test bed. This is the most thorough method of analysis, and it is used when the other methods have flagged a file as suspicious.

The analysis pipelines assigns values to each step of the process: these values are combined to provide a progressively more accurate verdict.

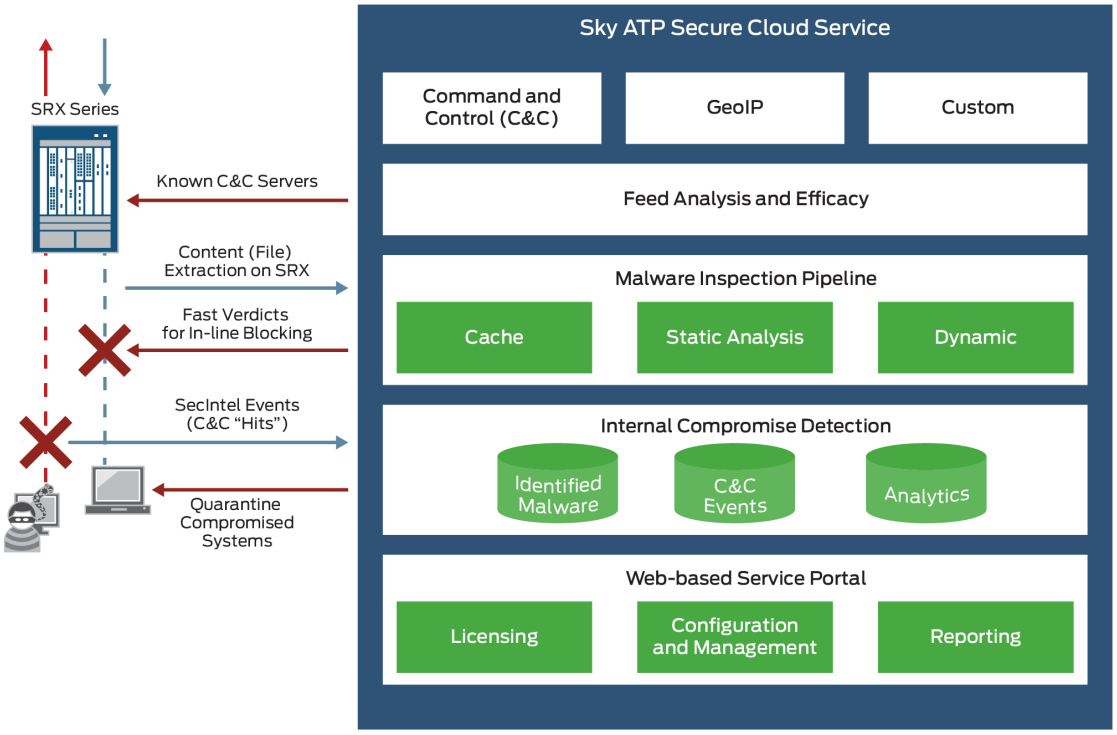



Figure 2 *The Sky ATP Analysis Pipeline*

## Methods of Detection

*Third-Party Anti-Virus Scanners*

Anti-virus (AV) scanners continue to play a role in detecting known viruses and malware. Although their reliance on signature matching provides a low Day Zero detection rate, by day one of a virus's appearance that detection rate increases to 55 percent. For viruses that have been in the wild for at least 3 months, the successful detection rate averages 75 percent. In order to improve the results of AV analysis, Sky ATP combines multiple AV scanners, and users can change which scanners they use at any time.

*Machine Learning*

Sky ATP uses a proprietary implementation of machine learning as another method of analysis that recognizes patterns and then correlates the information. The machine-learning algorithm is trained with features from thousands of malware samples as well as thousands of samples. Sky ATP learns how malware acts and is regularly retrained to get smarter as threats evolve.

*Static Analysis*

Static analysis investigates suspect files for known information about their type or source. For example, the source URL from which the file originates will be investigated along with the file itself, which is broken down into specific features such as file structure, meta information, category of instruction used, and file entropy. Then each feature is fed into the Sky ATP's machine-learning algorithm and the technology improves itself.

*Using Dynamic Analysis*

Dynamic analysis sandboxes suspect files and executes them in a real environment where they can run uninterrupted for minutes. During that time, active deception encourages the malware to show itself, and a record of its activity is kept. The file is then fed into the Sky ATP machine-learning algorithms.

### Dynamic Analysis Deception Techniques

Within the Sky ATP sandbox environment, various methods are used to draw out the malware and provoke it into action. So, for example, the sandbox must emulate a user environment with realistic patterns of user interaction, and high-value targets must appear with vulnerabilities so that the malware is sufficiently provoked. These targets could be stored credentials, vulnerable software, or tempting user files.

Because some malware is not so easily fooled, and will wait for specific signs that a real user is sitting at a computer before it shows itself, it's especially important that effective and realistic user actions, such as the following, are simulated within the sandbox:

- Faking a webcam feed
- Faking a microphone feed
- Moving the mouse
- Simulating key strokes
- Operating dialog boxes
- Installing and launching software
- Adding and removing USB sources

Once the malware exercises its payload, all actions taken by it are detected, analyzed, and documented.

## The Sky ATP Dashboard and Web UI

The Web-based user interface for Sky ATP includes a dashboard that provides a visual summary of all information gathered on compromised content and hosts in real time (see Figure 3). The Web UI for Sky ATP cloud-based services (see Figure 4) allows you to customize information in various filtered windows, and track the devices in your network, as well as create specialized white lists and black lists, among many other features. For a complete list of features, visit the links at the end of this *Learn About*.

As shown in Figures 3 and 4, the Sky ATP dashboard can display, among other features:

- The top infected hosts, including IP address, domain, and threat level.
- A file scanning summary with percentages of blocked malware, Day Zero malware, unknown files, and clean files for a chosen amount of time (for example, one week).
- A summary of top users downloading malware, which provides a list of those users, including the number of downloads they make and their email addresses.
- A list of infected file types (for example, PDF, XLS, DOC, CSV, RTF, and others) with a graphical comparison of the number of downloaded files for each type that was blocked.
- A map of the world with shaded areas displaying countries with the highest number of C&C servers and malware sources.

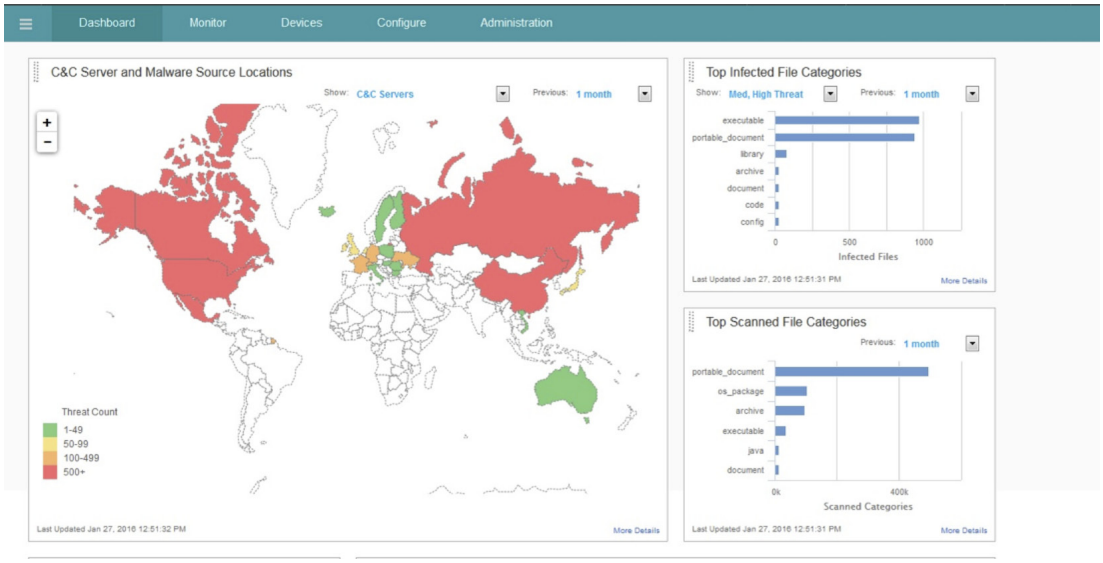



Figure 3 *Sky ATP Dashboard*

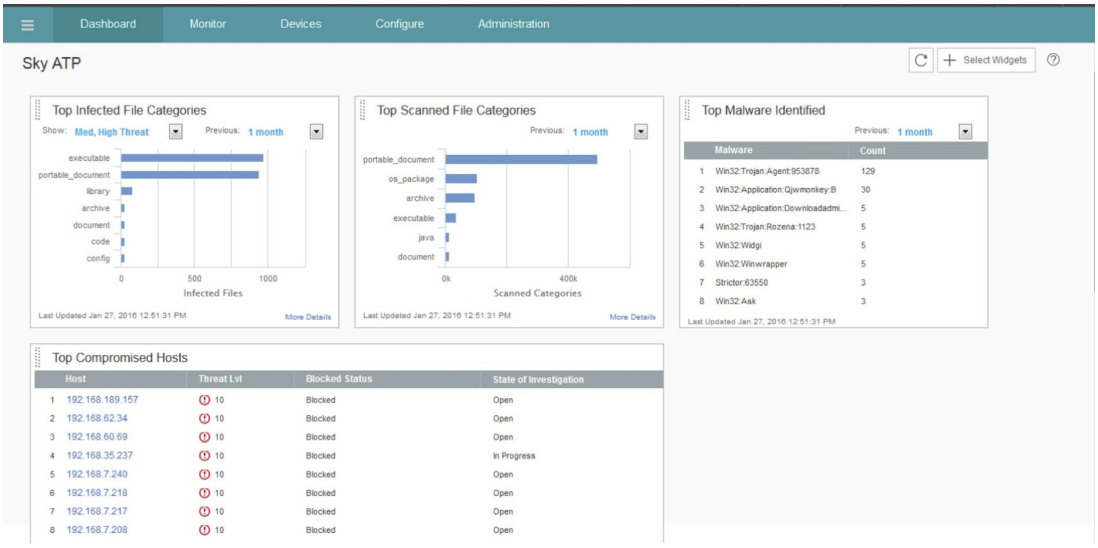



Figure 4 *Sky Web UI*

# References and Resources

## Sky ATP

Start here at the Sky ATP product page on the Juniper Networks website:
http://www.juniper.net/us/en/products-services/security/sky-advanced-threat-prevention/

The datasheet for Sky ATP provides a great product overview:
http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000549-en.pdf

Sky ATP is an add-on service to the SRX Series:
http://www.juniper.net/us/en/products-services/security/srx-series/

Learn more about security intelligence feeds used by Sky ATP:
http://www.juniper.net/us/en/products-services/security/spotlight/

## Malware Examples and Industry Reaction

Read about the Hyatt breach in detail:
http://www.esecurityplanet.com/network-security/hyatt-breach-affected-250-hotels-worldwide.html

Read why consumers should be angry at negligent retailers:
https://www.securestate.com/blog/2014/01/14/why-chip-and-pin-isnt-the-answer-to-retailers-problems

Read about Cherry Picker malware in detail:

- http://www.securityweek.com/cherry-picker-pos-malware-cleans-after-itself
- https://threatpost.com/researchers-discover-two-new-strains-of-pos-malware/115350/

Read about the first power outage caused by a cyberattack:

- http://www.welivesecurity.com/2016/01/20/new-wave-attacks-ukrainian-power-industry/
- http://www.pcworld.com/article/3020631/malware-alone-didnt-cause-ukraine-power-station-outage.html
- http://www.welivesecurity.com/2016/01/11/blackenergy-and-the-ukrainian-power-outage-what-we-really-know/
- http://arstechnica.com/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/
- http://www.pcworld.com/article/3024918/ukrainian-power-companies-are-getting-hit-with-more-cyberattacks.html

Learn how Dridex was discovered and the damage it can cause:

- https://www.fireeye.com/blog/threat-research/2015/06/evolution_of_dridex.html
- http://www.pcworld.com/article/3024247/dridex-banking-malware-adds-a-new-trick.html

Learn more about the alleged hackers behind the Sony Pictures attack:

- http://fortune.com/sony-hack-part-1/
- http://www.engadget.com/2014/12/10/sony-pictures-hack-the-whole-story/
- http://www.theguardian.com/film/2014/dec/16/employees-sue-failure-guard-personal-data-leaked-hackers

Read about the ransomware attack on Hollywood Presbyterian Medical Center:

http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

Read how hackers released sensitive data when a 3 million dollar ransom was not paid:

http://www.wired.com/2015/12/hacker-leaks-customer-data-after-a-united-arab-emirates-bank-fails-to-pay-ransom/

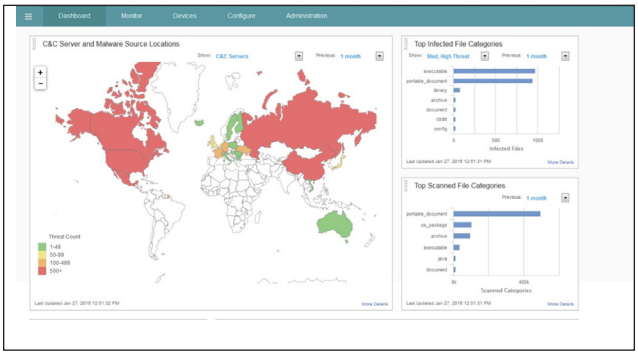
Read McAfee Labs' predictions about the most prevalent cyber attacks you'll see in 2016.

http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf

# Learn About Advanced Threat Prevention

**by Debra Malver**

*Malware is very malicious software, cleverly disguised to go after specific targets. Newer forms of malware can infiltrate your system and then wait for weeks, or even months, to strike. Sometimes the purpose of malware is to embed itself undetected into your infrastructure for future mayhem. In response to these threats, Juniper has developed Advanced Threat Prevention (ATP) to prevent malware from causing theft, espionage, and disruption. But only if you use it! Juniper's cloud-based* Sky ATP *is one security solution you really need to* Learn About.




About the Author:
Debra Malver is a Juniper Networks staff technical writer with over fifteen years in the industry. She has written networking and security documentation for many companies including Cisco Systems, Raptor Systems, and OKENA.

Author's Acknowledgments:
The author thanks the following for their engagement in this project: Patrick Ames, Editor in Chief; Karen Joice, illustrator; and project promoters Mindy Isham and Linnea Wickstrom.



Version History: First Edition, April 2016 2 3 4 5 6 7 8 9

For more information go to the TechLibrary at: www.juniper.net/documentation