Adaptive Defense 360

&

Adaptive Defense

What's new in version 2.4?

Contents

1. Summary of news in version 2.4

Version 2.4 of the Adaptive Defense product and service family has the following aims:

1. **Detection/mitigation at the exploit stage of the cyber-attack life cycle – Dynamic anti-exploit technology**
   Adaptive Defense and Adaptive Defense 360 incorporate a new dynamic anti-exploit technology that prevents exploit attempts through continuous monitoring of the activity of devices, and identification of both known and unknown/zero-day exploits.

2. **Detection of malwareless/fileless attacks, and monitoring through the management console**
   Panda Adaptive Defense and Panda Adaptive Defense 360 incorporate techniques that detect malwareless attacks through process monitoring, action correlation and the solution's ability to identify malicious behaviors of legitimate applications.

   These techniques are further strengthened in version 2.4. From this version on, these attacks will be managed just as any other detection, that is, they will be shown in the console's dashboard and reports as malware detections. This will allow administrators to monitor their life cycle and receive email alerts whenever this type of attack is detected.

3. **Identification of computers used to propagate attacks throughout the network**
   From version 2.4 on, whenever a malware/PUP is detected or an unknown item is blocked, the solution will display the network computer that the infection originated from, its IP address and even the logged-in user. All this information will be part of the item's life cycle.

4. **Export of workstation and server status details for integration into operational applications**
   Version 2.4 incorporates a new type of report (in CSV format) with information about the status of all protected workstations and servers. This report can be exported by administrators and scheduled for sending.

5. **Greater flexibility for integration with the customer's on-premise SIEM tool**
   From version 2.4 on, logs can be sent using Syslog. Also, they can be encrypted using SSL/TLS. Additionally, this version includes a VPN service for greater security when sending logs via FTP/sFTP.

6. **Enhanced forensic analysis capabilities: Ability to export the life cycle details of one or multiple detections as well as command-line parameter information (version 2.4.1)**
   Version 2.4.1 provides the ability to export the life cycle details of one or multiple detections (or blocked items) to CSV format.

   Also, the console will display information about the command-line parameters used by attackers employing PowerShell scripts.

2. Detection and mitigation at the exploit stage of the cyber-attack life cycle – Dynamic anti-exploit technology

An exploit is a sequence of commands that takes advantage of a bug or vulnerability in a legitimate software application. Today's attackers make use of executable and non-executable files (or scripting-based fileless attacks), to access and exploit the systems installed on workstations and servers in order to perpetrate their attacks.

In a typical attack scenario, an attacker manipulates a legitimate program to run code while attempting to avoid detection. This code then downloads malware, that is, a malicious PE (portable executable) file, or uses a legitimate system tool to perform malicious actions without using any executable file (malwareless or fileless attack).

In the latter case, and in order to take full control of the target computer, the attacker must carry out a series of actions triggered or made possible by the exploitation of a software vulnerability.
In such a scenario, blocking the vulnerability exploit attempt will stop the attack altogether.

Adaptive Defense and Adaptive Defense 360 incorporate a new dynamic anti-exploit technology that prevents exploit attempts through continuous monitoring of the activity of devices, and identification of both known and unknown/zero-day exploits.

2.1. Why is it important to stop attacks at the exploit stage?

A cyber-attack consists of a chain of actions or movements that make use of different techniques to penetrate systems and bypass the detection mechanisms in place.

Many malicious attacks involve exploiting vulnerabilities found in trusted applications, and take place under the radar without raising suspicion. Attackers take advantage of software vulnerabilities to exploit the targeted application and from there, compromise the entire system. These vulnerabilities can therefore give attackers full access to the targeted device and to every other computer on the network.

The purpose of an advanced protection system such as Panda Adaptive Defense is to identify and stop this string of actions to prevent malicious code from running and compromising the targeted application, the system and any workstation or server.

The actions or stages that comprise a cyber-attack are known as the "Cyber Kill Chain" (CKC), whereas their expansion from the perimeter to the target workstations and servers is known as the "Expanded Cyber Kill Chain"[1].

[1] [1] If you want to know more about the Cyber-Kill Chain, we recommend reading this document "Understanding Cyber-Attacks. Part I. "The Cyber-Kill Chain""

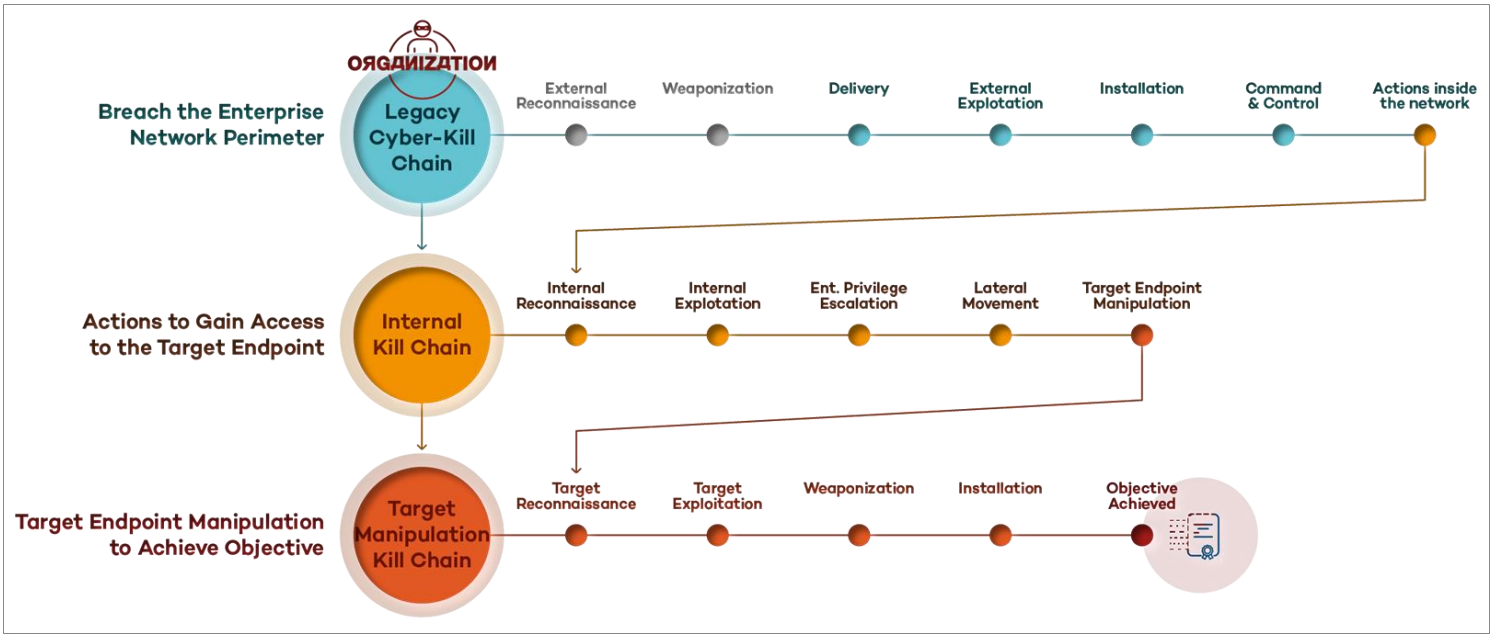


Figure 1. The Expanded Cyber Kill Chain model. Actions aimed at accessing the target servers and devices and their manipulation by the attacker

While attackers must successfully execute every phase in the expanded Cyber Kill Chain to reach their objective, we, in our role as protectors of our customers' networks, must be able to stop attacks at any phase, before the attacker manages to access their target's assets. Therefore, we must deploy technologies during each and every phase of an attack life cycle, in order to stop threats as soon as possible.

The dynamic anti-exploit technologies incorporated into version 2.4 are precisely designed to detect and abort attacks before trusted applications are compromised.

2.2. What does the anti-exploit technology included in Adaptive Defense provide?

Adaptive Defense incorporates new anti-exploit technologies developed by our **cyber-security experts** at Panda Security's laboratory. These technologies are based on **Panda Security's ever-evolving knowledge** (fed by real-time information generated by sensors installed on millions of devices), and the **continuous monitoring of processes and their activities on endpoints**.

The **key benefits** of this technology are:

- Provides an **extra layer of protection to block exploits in real time**. If an exploit takes place, the technology will prevent the malicious code from running, infecting the computer and spreading to other devices in the organization.
- **Monitors** the internal behavior of compromised processes, searching for anomalies that may indicate a known or zero-day exploit.
- **Detects threats regardless of the exploit** used in the attack. Adaptive Defense provides effective protection against **all types of exploits, especially zero-day exploits** that take advantage of:
    - **Web browser** vulnerabilities in Internet Explorer, Firefox, Chrome, Opera and others.
    - Commonly-targeted application families: Java, Adobe Reader, Adobe Flash, Microsoft Office, multimedia players...
    - Vulnerabilities in unsupported operating systems such as Microsoft XP and others.
- Provides end users with **seamless** protection and doesn't slow down systems.

Unlike other products on the market today, Adaptive Defense provides a **global** solution capable of neutralizing both known vulnerabilities and the most dangerous of threats: unknown or zero-day vulnerabilities.

Its global nature is the result of Panda Security's investment in developing proactive technologies that offer general solutions to problems. Thus, these technologies are heavily oriented towards detecting all sorts of anomalies and unusual behaviors in their execution context.

Adaptive Defense's unique technologies provide the solution with the necessary mechanisms to detect and block attacks designed to use **exploit techniques at any stage of their life cycle**.

Its detection capabilities are based on the **continuous monitoring** of all actions taken by the processes run by files as well as in memory.

As a result, our technology stops exploits and **prevents trusted applications from being compromised** at the early stages of vulnerability attacks, all **seamlessly** to the user of the protected device.

2.3. Key differentiators of Adaptive Defense's anti-exploit technologies

Most anti-exploit solutions on the market today either rely on performing a **morphological** analysis of files and/or their execution **context**, or implement various protection features **absent in Windows** (ASR, DEP, EAF, as well as specific detections of known vulnerabilities (Common Vulnerabilities and Exposures, CVE)).

These techniques, however, are not sufficient to stop the security attacks designed to take advantage of the entry points created by all types of vulnerabilities, including zero-day ones.

Adaptive Defense is the only solution on the market that is capable of stopping cyber-attacks **before or during an exploit** through the **continuous monitoring of all processes**: compromised ones and other system processes.

Considering all of these factors, the **key differentiators of the anti-exploit technology** now incorporated into our **Adaptive Defense** product family are:

- It is **global**: Detects exploits for both known and unknown **(zero-day) vulnerabilities**.
- Unlike other solutions on the market, our new anti-exploit technology is not designed to simply patch security flaws on Windows systems, but is **based on the continuous monitoring of all processes** running on devices and cloud-based correlation of the data gathered through machine learning algorithms.
- The **efficiency** of Adaptive Defense's new anti-exploit technology is due to the **thorough synchronization** of the following components:
    - **Anti-exploit protection on workstations and servers** fully integrated with the advanced protection. No updates or extra processing capabilities are required, as the model relies entirely on the monitoring of all actions carried out by any process and application running on the endpoint.
    - **Specialized machine learning algorithms run in cloud-based environments**. These algorithms are an integral part of the managed service and as such are always adapted to the new systems, applications and advanced evasion techniques used in exploit attacks.
    - **The managed service run by our expert team of threat hunters**, specialized in detecting advanced exploit techniques.

2.5. Implementation of the new anti-exploit technology in Panda Adaptive Defense

From version 2.4 of Panda Adaptive Defense, which includes a new version of the protection for workstations and servers (v7.70), you will benefit from the aforementioned new anti-exploit technology based on continuous network monitoring (when the technology is active).

1. Anti-exploit technology settings. Operational modes

From version 2.4, the Web management console allows you to configure this technology at security profile level. The anti-exploit technology is **enabled and disabled** independently from any other protection module in Adaptive Defense, including the Advanced Protection.
This technology is disabled by default in this version, although Panda Security strongly advises you to enable it gradually in all security profiles across the network.

When the anti-exploit protection is enabled, its default behavior is to **notify** all detections **in the console** and optionally via email. That is, the default behavior doesn't block detected exploits, and is therefore not recommended for normal situations.

These settings can be modified at any time to allow the anti-exploit protection to **notify detections in the console and act** against these attacks. More specifically, the protection will block the attack and implement remediation measures to stop attackers from continuing to compromise the target application, the endpoints and your network.

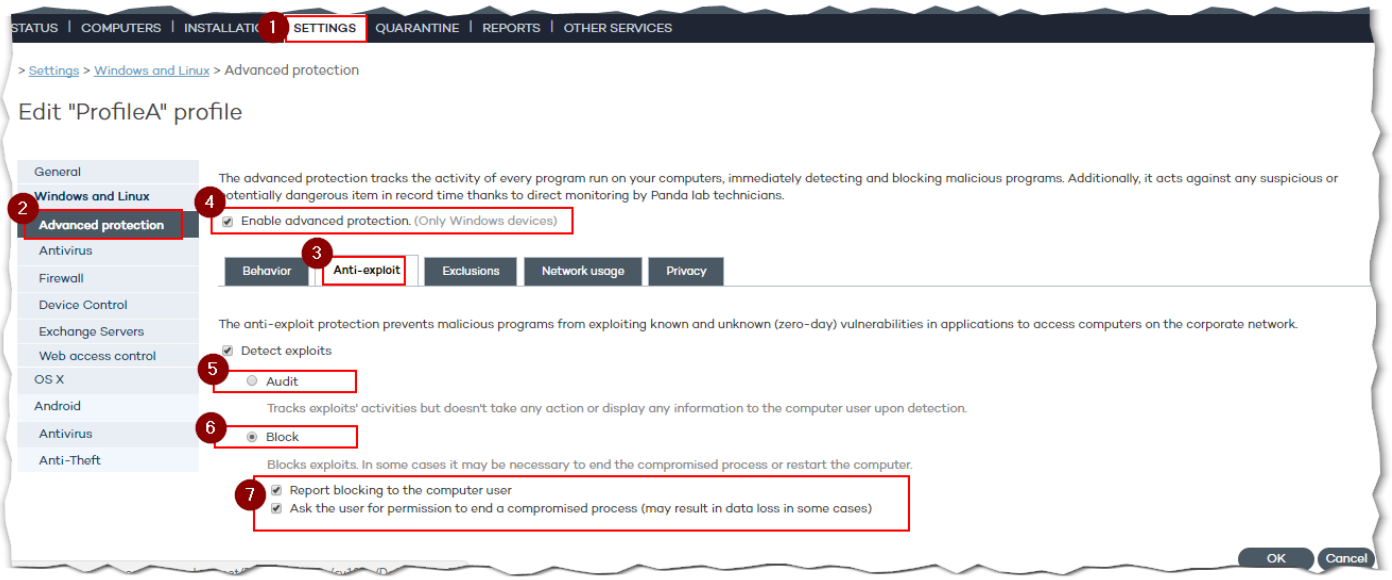


Figure 2. Setting of anti-exploit technology in security profiles

Mode 1: Only notify exploit detections in the console

In this operational mode, the solution won't take any actions when detecting an exploit attempt. It will just log the event in the Web management console, in the information displayed in the Advanced Reporting Tool (ART) module, and/or the logs sent as part of the SIEMFeeder service.

Mode 2: Notify exploit detections in the console and act against them

In this operational mode, the solution not only notifies the administrator of every exploit attempt through the console and by email, it also acts on the compromised workstation and server, **blocking the attack without end user intervention**.

Nevertheless, since most exploits reside in the memory of the compromised application, it will often be necessary to **end the process** and clean its memory.

Under those circumstances, if the compromised process is a **critical system process**, stopping the attack may require restarting the target computer.

Notifying the compromised computer's user when action is required

Due to the inconvenience that inadvertently stopping a trusted application or restarting the system may cause to the computer's user, the solution provides administrators with tools to give end users the option to voluntarily stop the compromised process or restart the computer. This will give them time to save their work, for example.

Figure 3. Exploit detected and blocked

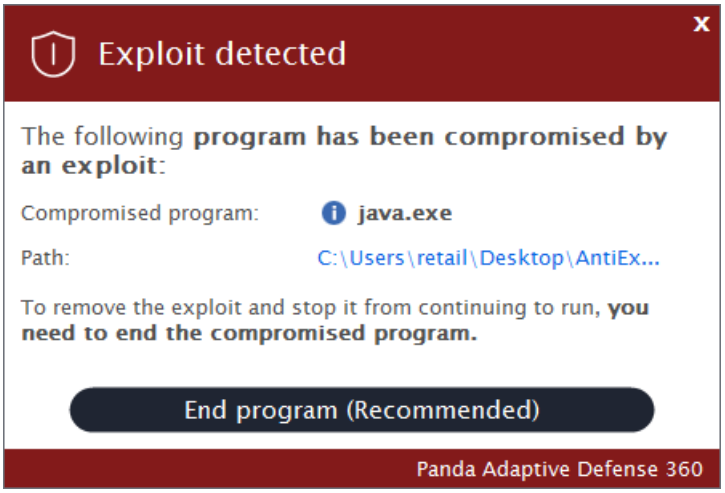


Figure 4. Detected Exploit that requires to end the compromised program

Figure 5. Exploit removed after ending the compromised program

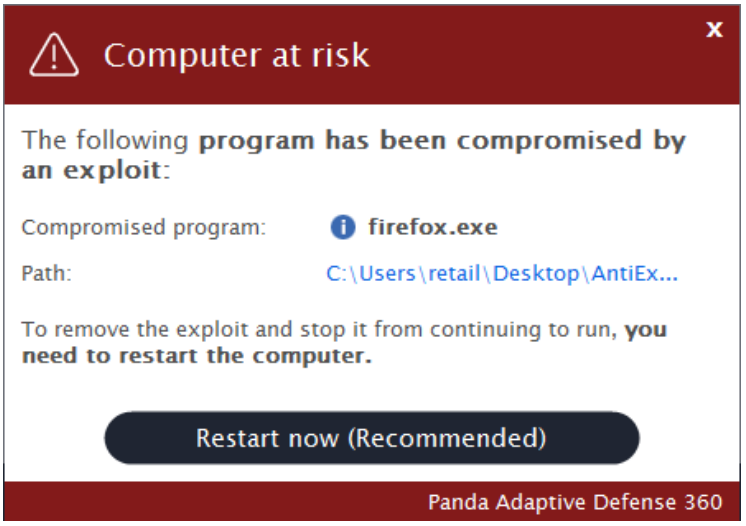


Figure 6. Detected Exploit that requires to restart the computer. This notification will be shown periodically until the endpoint is restarted.

However, it is **worth noting** that **from the time a compromised process is detected until it is ended or the computer is restarted, the exploit attempt remains loaded in memory running malicious code**. To remind users of this potentially dangerous situation, the local console will display a warning prompting users to end the compromised application or restart the computer until they do so.

2. Monitoring anti-exploit detections

Exploit detections are notified by the solution in the following ways:

In the Adaptive Defense console

'Activity' section. 'Classification of all programs run and scanned' panel
The number of detected exploits is added to the total number of programs classified as malware and exploits.

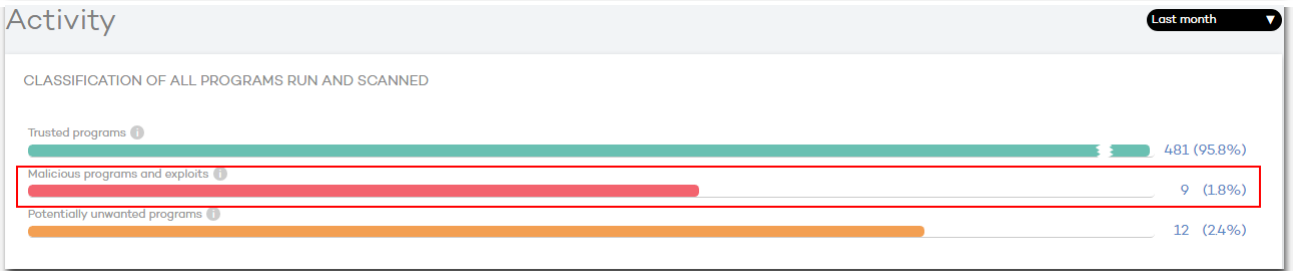


Figure 7. Activity Dashboard with malicious programs and exploits

'Activity' section. 'Malicious programs and exploits' panel
Detected exploits are displayed in real time in the management console (in a new section called 'Exploits' on the 'Malicious programs and exploits' screen).

Figure 8. Malicious programs and exploits Dashboard

Detected exploit details:

The 'Exploits' screen displays the following information:

- **Computer name**
- **Path of the compromised program**
- Action taken on the exploit. This column can have the following values:
  - **Allowed by the administrator**: In 'Notify only ' mode.
  - **Blocked (immediately)**: In 'Notify and block' mode. The exploit was immediately blocked without requiring user intervention.
  - **Blocked (not immediately)**: In 'Notify and block' mode. The exploit was neutralized after the user ended the application.
  - **Allowed by the user**. In 'Notify and block' mode. The user has been prompted to end the application, but they haven't done so yet.
  - **Detected. Pending restart**. In 'Notify and block' mode. This action appears under the following circumstances:
    - When it is necessary to restart the system to block and remedy the exploit, since it affects system processes.
    - If the user is prompted to end the compromised application but doesn't do it after a certain period of time. The computer's status will change and it will be necessary to restart the system.
- **Risk**. If the exploit was not blocked immediately, the 'Risk' column will indicate that the computer was at risk from the time the exploit was detected until it was blocked (if it has been actually blocked).
- **Detection Date.**

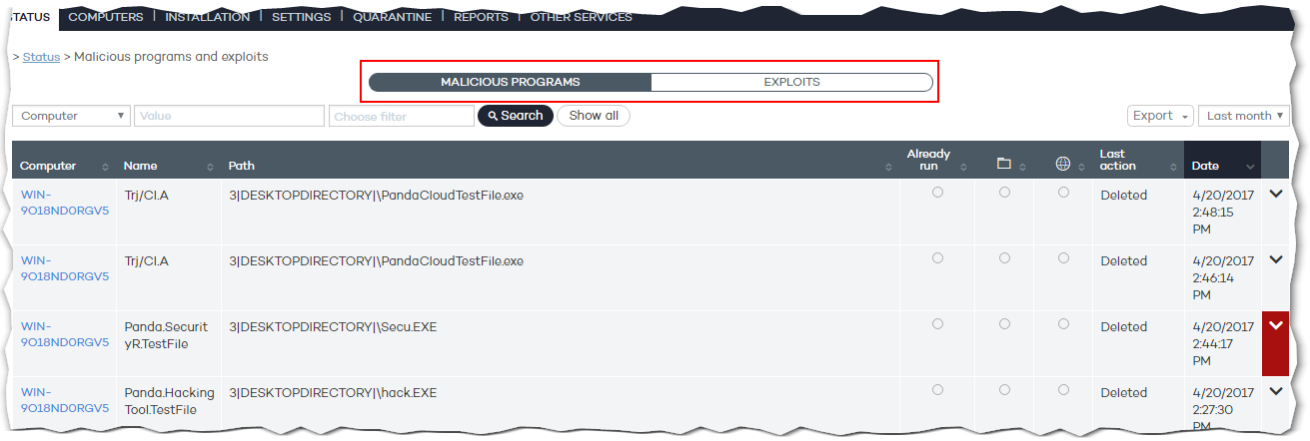


Figure 9. Malicious programs and detected exploits alerts

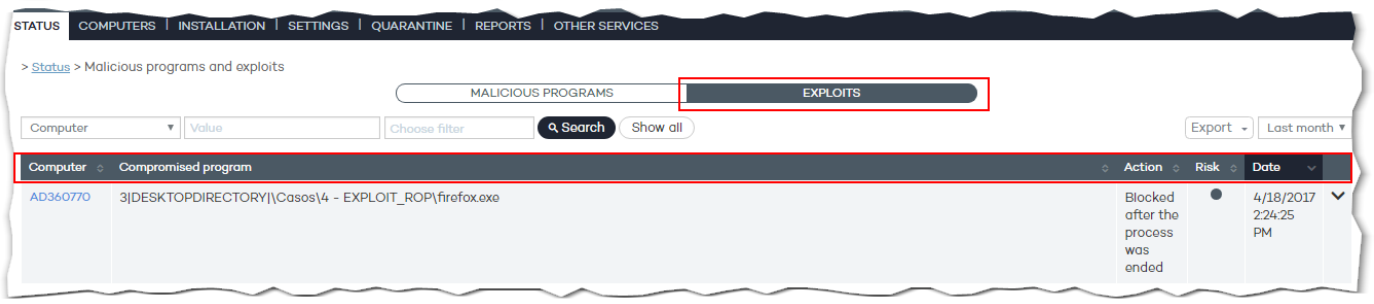


Figure 10Exploit alert details

The alert details show other relevant information for the **forensic analysis** of the attack: exploit life cycle and activity **graph** detailing the exploit's evolution until it was stopped (if it was stopped), as well as the **URLs accessed** before the attack was detected, as there is a high probability that some of those addresses are related to the attack.

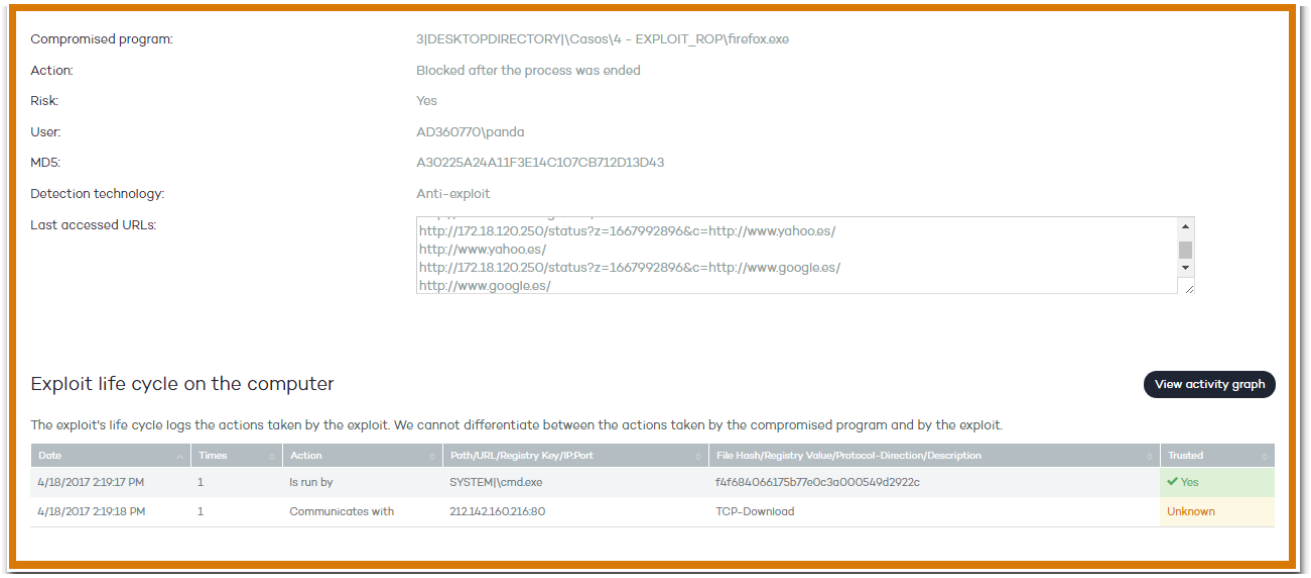


Figure 11. Detailed exploit information, including URLs visited before the detection and exploit lifecycle

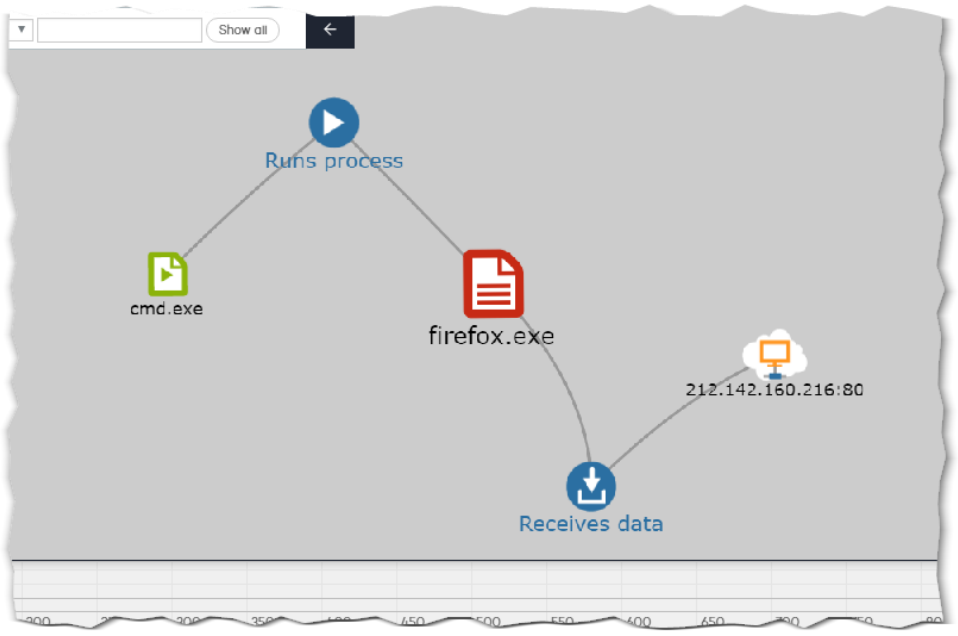


Figure 12. Exploit life cycle

The predefined filters for the exploits section allow you to search for specific computers, compromised applications, etc. in the same way as the predefined filters for the malware, PUP and blocked items sections.

Preconfigured reports

The executive reports, extended executive reports and threat reports will all include information about the exploits detected.

Email alerts

Additionally, should the option to **send email alerts** whenever malware is detected be enabled, the network administrator or head of security will receive an email immediately after an exploit is detected.

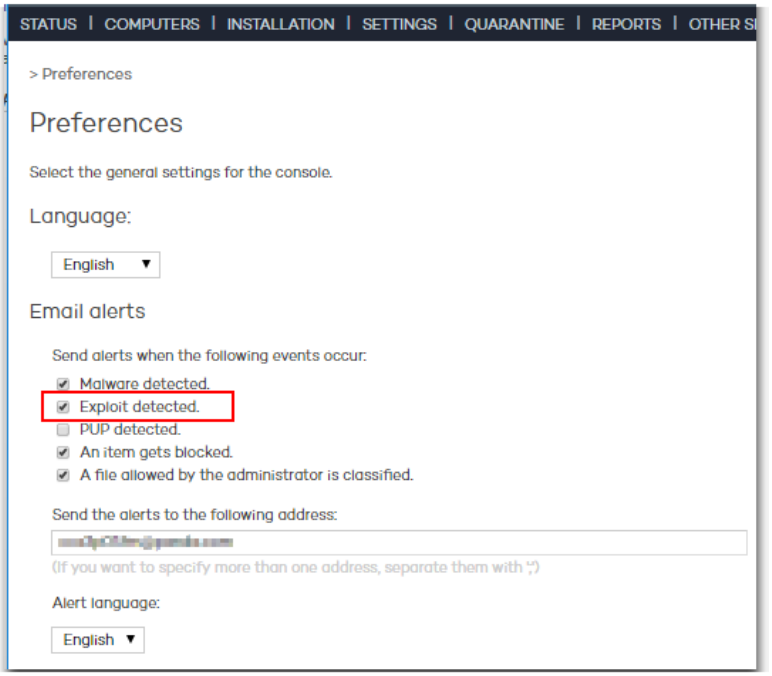
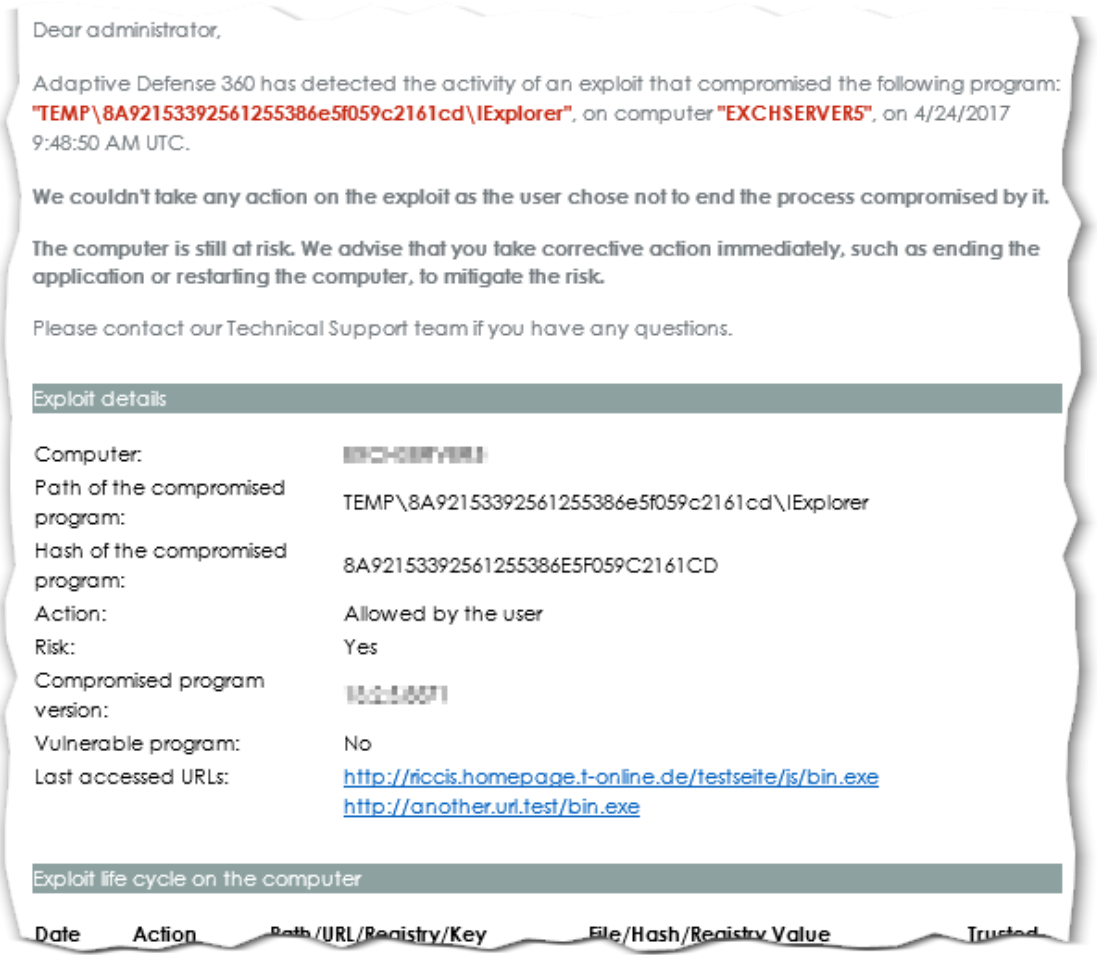


Figure 13. Email alerts in real time settings, including detected exploit alerts



Dear administrator,

Adaptive Defense 360 has detected the activity of an exploit that compromised the following program: **"TEMP\8A92153392561255386e5f059c2161cd\IExplorer"**, on computer **"EXCHSERVER5"**, on 4/24/2017 9:48:50 AM UTC.

We couldn't take any action on the exploit as the user chose not to end the process compromised by it.

The computer is still at risk. We advise that you take corrective action immediately, such as ending the application or restarting the computer, to mitigate the risk.

Please contact our Technical Support team if you have any questions.

Exploit details

Computer:	[redacted]
Path of the compromised program:	TEMP\8A92153392561255386e5f059c2161cd\IExplorer
Hash of the compromised program:	8A92153392561255386E5F059C2161CD
Action:	Allowed by the user
Risk:	Yes
Compromised program version:	[redacted]
Vulnerable program:	No
Last accessed URLs:	http://riccis.homepage.t-online.de/testseite/js/bin.exe http://another.url.test/bin.exe

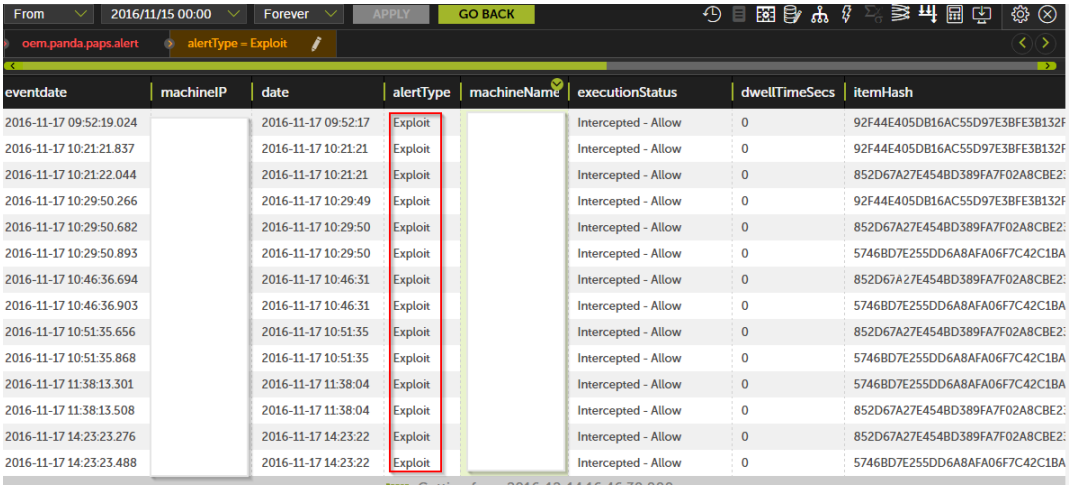
Exploit life cycle on the computer

Date	Action	Path/URL/Registry/Key	File/Hash/Registry Value	Trusted

Figure 14. Email alert for a detected exploit that compromised Internet Explorer. The end user did not end the application, therefore the risk status is high

Information available in Advanced Reporting Tool (Only for clients with the Advanced Reporting tool module)

Every time an attempt is detected to exploit a vulnerability on the customer's network, ART will receive an alert similar to those received whenever a malware item or PUP is detected, although in this case it will display 'Exploit' in the AlertType column.



From | 2016/11/15 00:00 | Forever | APPLY | GO BACK

oem.panda.paps.alert | alertType = Exploit

eventdate	machineIP	date	alertType	machineName	executionStatus	dwellTimeSecs	itemHash
2016-11-17 09:52:19.024		2016-11-17 09:52:17	Exploit		Intercepted - Allow	0	92F44E405DB16AC55D97E3BFE3B132F
2016-11-17 10:21:21.837		2016-11-17 10:21:21	Exploit		Intercepted - Allow	0	92F44E405DB16AC55D97E3BFE3B132F
2016-11-17 10:21:22.044		2016-11-17 10:21:21	Exploit		Intercepted - Allow	0	852D67A27E454BD389FA7F02A8CBE2
2016-11-17 10:29:50.266		2016-11-17 10:29:49	Exploit		Intercepted - Allow	0	92F44E405DB16AC55D97E3BFE3B132F
2016-11-17 10:29:50.682		2016-11-17 10:29:50	Exploit		Intercepted - Allow	0	852D67A27E454BD389FA7F02A8CBE2
2016-11-17 10:29:50.893		2016-11-17 10:29:50	Exploit		Intercepted - Allow	0	5746BD7E255DD6A8AFA06F7C42C1BA
2016-11-17 10:46:36.694		2016-11-17 10:46:31	Exploit		Intercepted - Allow	0	852D67A27E454BD389FA7F02A8CBE2
2016-11-17 10:46:36.903		2016-11-17 10:46:31	Exploit		Intercepted - Allow	0	5746BD7E255DD6A8AFA06F7C42C1BA
2016-11-17 10:51:35.656		2016-11-17 10:51:35	Exploit		Intercepted - Allow	0	852D67A27E454BD389FA7F02A8CBE2
2016-11-17 10:51:35.868		2016-11-17 10:51:35	Exploit		Intercepted - Allow	0	5746BD7E255DD6A8AFA06F7C42C1BA
2016-11-17 11:38:13.301		2016-11-17 11:38:04	Exploit		Intercepted - Allow	0	5746BD7E255DD6A8AFA06F7C42C1BA
2016-11-17 11:38:13.508		2016-11-17 11:38:04	Exploit		Intercepted - Allow	0	852D67A27E454BD389FA7F02A8CBE2
2016-11-17 14:23:23.276		2016-11-17 14:23:22	Exploit		Intercepted - Allow	0	852D67A27E454BD389FA7F02A8CBE2
2016-11-17 14:23:23.488		2016-11-17 14:23:22	Exploit		Intercepted - Allow	0	5746BD7E255DD6A8AFA06F7C42C1BA

Figure 15. Alerts table with Exploit detections

Consequently, should detections of this type be confirmed, they will be shown in the 'Security Incidents' vertical application.

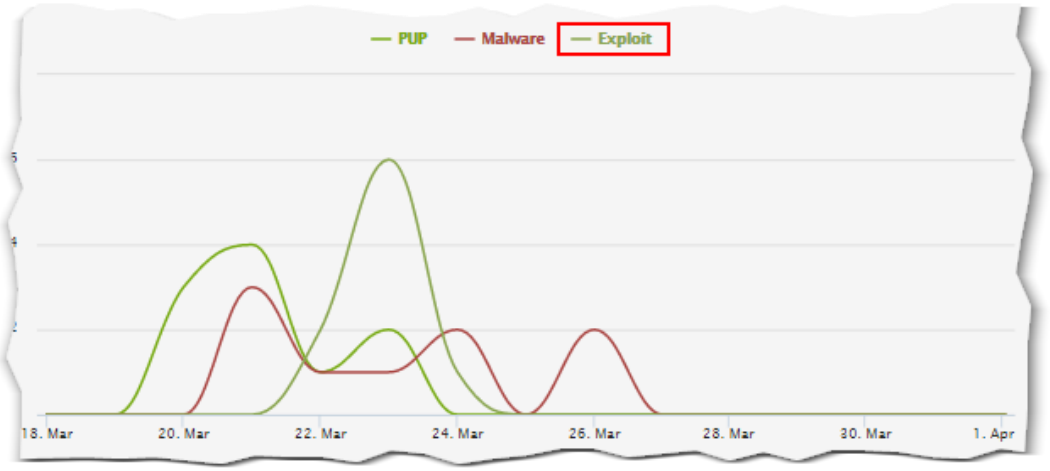


Figure 17. Vertical Application *Security Incidents* with exploit information

Refer to section **Improvements to the Advanced Reporting Tool service**

Information available in the SIEM tool (Only for clients with the SIEMFeeder tool module)

Every detection of a vulnerability exploit attempt, regardless of the technique used, will be reported to the SIEM tool in the form of an alert similar to malware and PUP alerts. More specifically, they will be reported as an 'Exploit' type event.

Refer to section **Improvements to the SIEMFeeder service**

3. Detection of malwareless or fileless attacks

Malwareless attacks make use of non-executable files, exploit vulnerabilities in legitimate applications such as Chrome, Firefox, Internet Explorer, Microsoft Office (Word, Excel, etc.), Java VM and Adobe products, and compromise workstations and servers through the distribution and execution of code in memory, when the target user opens files with macros, for example.
Attacks with non-executable files manipulate the memory stack of legitimate applications and achieve their objectives without downloading malicious executable files.

Additionally, fileless or script-based attacks are based on command sequences in scripting languages (such as Java or PowerShell). These malicious scripts are run without the need to write files to disk, hence the name fileless attack.

Finally, many attacks use a combination of macros and PowerShell command-line arguments. For example, we've seen attacks that opened a Word document with a macro that used evasion techniques to hide and launch an attack using PowerShell scripts from a remote Command & Control server.

Fileless and non-executable based attacks are nothing new, but they are becoming increasingly prevalent and go undetected by traditional anti-malware solutions,

Panda Adaptive Defense and Panda Adaptive Defense 360 incorporate techniques that detect this type of attack through process monitoring, action correlation and the solution's ability to identify malicious behaviors of legitimate applications.

These techniques are further strengthened in version 2.4. From this version on, these attacks will be managed just as any other detection, that is, they will be shown in the console's dashboard and reports as malware detections. This will allow administrators to monitor their life cycle and receive email alerts whenever this type of attack is detected.

4. Computers used as a launch pad for a network attack (source of infection)

It is a known fact that attackers get into corporate networks through their weak points and then use privilege escalation techniques, evasion techniques and lateral movements between computers and servers to get close to and reach their targets. On multiple occasions, some of the network's computers are turned into 'zombie' computers in the hands of external C&C servers that send commands to them. These 'zombie' computers can be used as launch pads to launch a cyber-attack on the other computers on the network.

In this and other scenarios, early detection of the workstations and servers that an infection originates from is extremely important.

From version 2.4 on, whenever a malware/PUP is detected or an unknown item is blocked, the solution will display the network computer that the infection originated from, its IP address and even the logged-in user. All this information will be part of the item's life cycle.

5. Computer status report

On multiple occasions, specially in mid-to-large companies, where endpoint security is managed, and which have systems, applications, processes and tools managed by the organization's CIT department or a third party, there is a need for the workstation and server status information to be integrated into those processes and tools. An example of this would be corporate ticketing tools.

For this reason, version 2.4 incorporates a new type of report (in CSV format) with information about the status of all protected workstations and server. This report can be exported by administrators and scheduled for sending.

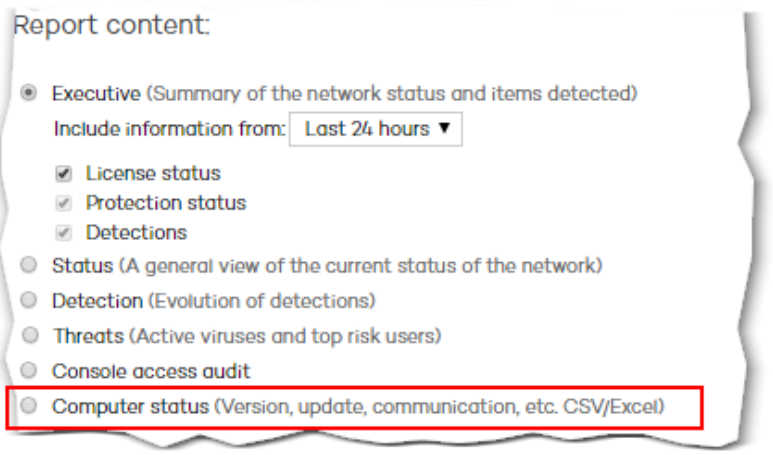


Figure 18. Computer Status report that allows to integrate that data into organization's operation software such as ticketing

6. Improvements to the Advanced Reporting Tool service

This functionality is only available to customers subscribing to Advanced Reporting Tool (ART)

6.1. New data in existing tables

- The **OPS** table will display now the command-line argument used to launch the application, including its parameters.

- **ALERTS** table:
  - This table will show now 'Exploit' type events as well as the last visited URLs (up to a maximum of 10 URLs, separated by "*" in the UrlList field).
  - In the case of malware detections, if the detection took place when the malware file was transferred from a computer on the network to another, the table will display the IP address and logged-in user of the source computer.

- Up to this version, the **SOCKETS** table only indicated network protocols (TCP, UDP, ICMP). This version, however, also displays information about application-level connections for RDP (Remote Desktop Protocol) traffic. This enables identification of RDP attacks (the 'Protocol' key will show the value 'TCP-RDP').

6.2. New widget in the Security Incidents vertical application

Two new widgets have been included with information about the source computer when malware is copied or transferred from one computer to another. One of the widgets is a node graph representing the relationship established between the two computers in the selected period.

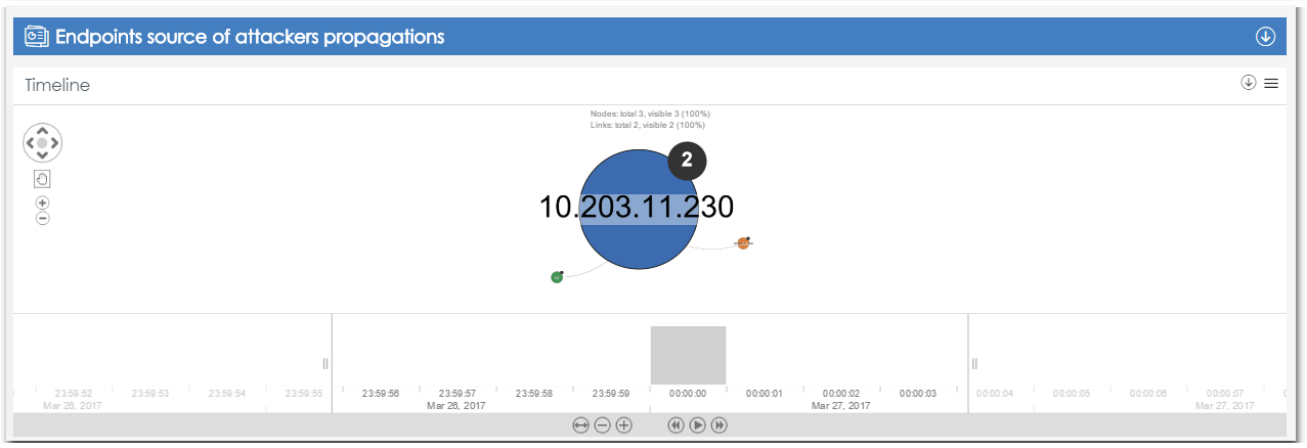


Figure 19. New widget in ART with the lifetime of endpoints originating infections and the endpoints affected

The second is an affinity graph relating the source and destination computers.

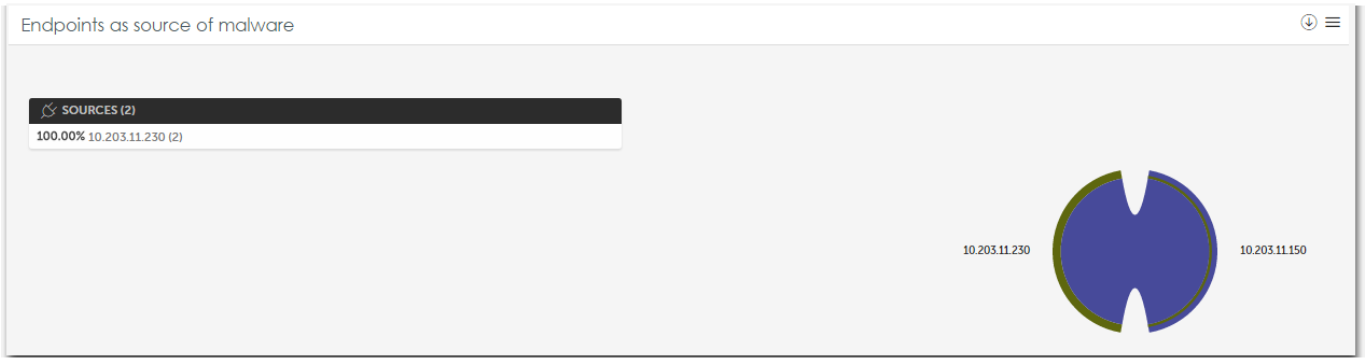


Figure 20. New widget in ART with endpoints originating infections and the endpoints affected

6.3. Information about the current category of hashes involved in events

All tables showing the category associated with the hash of the parent or child process will now display the category at the time when the event took place and the current category (with a maximum refreshment rate of 4 hours).

7. Improvements to the SIEMFeeder service

This functionality is only available to subscribers to SIEMFeeder.

7.1. More information in events

- **OPS** events display now the command-line argument used to launch the application, including its parameters.

- **ALERTS** events:
  - They show now 'Exploit' type events as well as the last visited URLs (up to a maximum of 10 URLs, separated by "*" in the UrlList field). In the case of exploits originated from a document, the Doclist field will be populated.

CEF:1|[redacted] Date=2017-02-21 15:16:49 HostIp=[redacted] HostName=[redacted] ThreatType=Exploit ExecutionStatus=Not Executed - Allow DwellTimeSecs=9608 ItemHash=6E3D7F11D087FE1AC7865F702665D768 ItemPath=3|\plugins\Universal Agent\Dev\Dev\Integration\Minerva\Tools\MinervaEventsCreator\Release\iexplore.exe ItemName=Exploit/Shellcode.Behaviour SourceIP= SourceMachineName= SourceUserName=
UrlList=http://www.stackoverflow.com/*http://www.codeproject.com/Questions*http://www.pandasecurity.com/*http://www.codeproject.com/Questions/427350/calling-a-website-from-cplusplus*http://www.stackoverflow.com/*http://www.codeproject.com/Questions*http://www.pandasecurity.com/*http://www.codeproject.com/Questions/427350/calling-a-website-from-cplusplus*http://www.stackoverflow.com/*http://www.codeproject.com/Questions DocList= Version=10.0.0.396 Vulnerable=True

Figure 21. *Alerts* event format in SIEMFeeder

- In the case of malware detections, if the detection took place when the malware file was transferred from a computer on the network to another, the event will display the IP address and logged-in user of the source computer.

- Up to this version, **SOCKETS** events only indicated network protocols (TCP, UDP, ICMP). This version, however, also displays information about application-level connections for RDP (Remote Desktop Protocol) traffic. This enables identification of RDP attacks (the 'Protocol' key will show the value 'TCP-RDP').

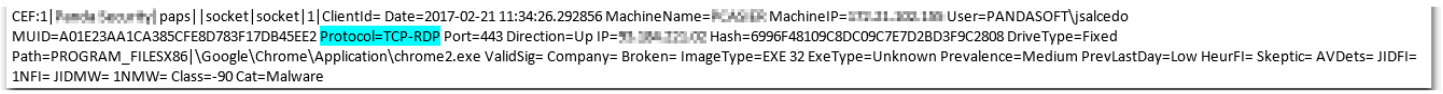


Figure 22. *Sockets* event format in SIEMFeeder

7.2. Greater flexibility for integration with your on-premise SIEM

In addition to the delivery of activity logs from workstation and servers via sFTP or FTP, version 2.4 also allows logs to be sent via the Syslog protocol. Optionally, the transmitted data can be encrypted with SSL/TLS encryption. To be able to use the Syslog protocol, there must be a Syslog server implementation in the network, ready to receive logs from our servers, which on many occasions is already incorporated into the SIEM tool.

Note that you will need prior configuration information and time to adjust the service parameters (number of simultaneous connections, retries (3 by default, etc.).

Finally, this version implements a VPN service for greater security when sending logs via FTP/sFTP.

8. Other improvements in version 2.4

Version 2.4 of Adaptive Defense and Adaptive Defense 360 with protection version 7.70 and agent version 7.71 incorporates the following additional improvements:

1. **Exclusion management:**
   - Profile-level exclusions will also affect the advanced protection.
   - Greater consistency between detection alerts and exclusions: If an item is excluded from the advanced protection, the solution won't send any more email alerts for that item until the exclusion is removed.

2. **Lock mode and advanced users**: If a user decides to run an application that is not yet classified as trusted, the solution will allow the execution of the application and any libraries it may need, even if they haven't been classified as trusted either. That is, priority will be given to the user's decision so as not to interrupt their work.

3. Fixed a bug that occurred when **detecting items in transit on Exchange Servers**, when there was no path to display in the console.

4. Bug fix: If a workstation or server's **anti-malware protection is disabled**, but the **advanced protection** is enabled, the information displayed in the notification area will now indicate that the advanced protection is enabled.

5. Improvement: The detection notifications displayed to workstation or server users **were visible for a few minutes only** and disappeared automatically. If the user missed them, they missed important information for their security. From this version on, however, these **notifications** are **periodic** and **are displayed until the user interacts with them.**

Figure 23. Endpoint notification that remains end-user an item was blocked.

Other improvements:

- Ability to enable **Panda's proprietary Remote Control** module, **integrated** with Adaptive Defense/Adaptive Defense 360's agent and protection.
- The Web console includes a shortcut to the **SIEMFeeder** service guide.

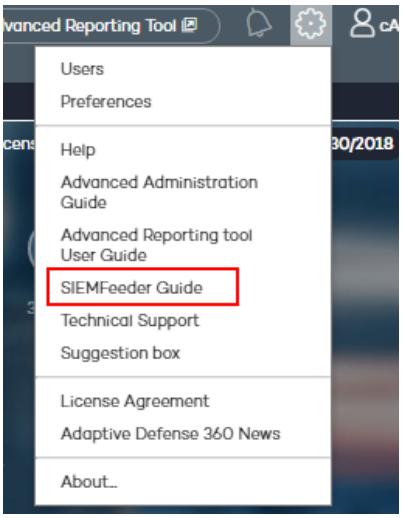


Figure 24. Direct access to SIEMFeeder Guide

Finally, we have modified the Software License Agreement to include:

- An adjustment for those environments where the service is run on a Windows Terminal Server.
- A new section to avoid inappropriate uses of the service. This aims at offering maximum protection guarantees to our customers and partners.
- Finally, it is informed that administrators could be contacted by us to conduct product surveys with the aim of improving this, there is also a mechanism to stop receiving such communications.

For that reason, the first time you access the management console after the update to version 2.4, you'll be asked to **accept the License Agreement again**.

9. New supported systems

Version 2.4 of Adaptive Defense and Adaptive Defense 360 with protection version 7.70 and agent version 7.71 supports the following systems:

- **Server Core 2008 (32-bit or 64-bit), 2008 R2 (64-bit), 2012 and 2012 R2, without a GUI.** As the server has no GUI, we recommend the following practices:
  - Carry the installation and update processes in a scheduled way as no messages will be displayed locally prompting to restart the server. Make sure that the server has been restarted appropriately by checking the Web management console.
  - Make sure you keep the proxy settings up-to-date in the profile since, should a problem occur, the server won't display any local messages asking for the proxy data.
- **Windows MultiPoint Server 2012**
- New version of the protection for **Mac** based on **Virus Barrier X9**

10. Exporting life cycle and command-line information (version 2.4.1)

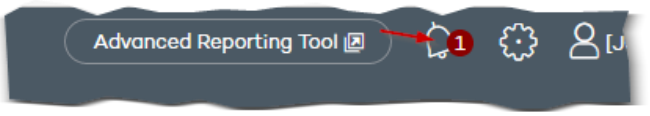
Version 2.4.1 provides the ability to export the life cycle details of one or multiple detections or blocked items to CSV format. This data can be easily imported and/or managed with applications such as Excel, allowing administrators to perform forensic analyses for the entire network with maximum granularity levels and correlating any item or entity.

For example, you'll be able to export all the detections that have taken place in the last 24 hours, and see how many computers have been affected by a particular malware attack.
You will also see which files have been accessed during the attack, in order to assess the impact on your organization.
You will also be able to correlate detections over time, and identify the lateral movements and entry points used by attackers.

Finally, the console will display information about the command-line parameters used by attackers employing PowerShell scripts.

11. When and how can you upgrade to v2.4?

The new version 2.4 will be available from May 8, 2017 by accessing the information published in the management console, in the notification area.



Please note that the version of the console will be 2.4, that of the protection is 7.70, and that of the agent 7.71.

- To update the version of the console to the version 2.4, you must, actively, press the button that you will find in the notification.

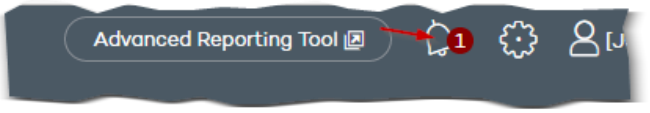
  Please note, that over the next few weeks we will update the console version automatically. This is the automatic update calendar.
  - Clientes de menos de 101 licencias: Miércoles 17/05
  - Clientes de entre 101 y 501 licencias: Miércoles 29/05
  - Clientes de más de 501 licencias: Lunes 12/06

- Once you have updated the version of the console to 2.4, the agents are automatically updated to version 7.71,

- The protection will be updated to 7.70 automatically only if it is configured in the security policies that apply to the endpoints. Please check the configuration in your security profiles.

12. When and how can you upgrade to v2.4.1?

The new version 2.4.1 will be available in June by accessing the information published in the management console, in the notification area.



Unlike version 2.4, version 2.4.1 only involves an update of console.