Independent Tests of
Anti-Virus Software

Anti-Tampering Certification

Palo Alto Networks Cortex XDR Prevent

TEST PERIOD: APRIL 2023

LAST REVISION: 20TH MAY 2023

WWW.AV-COMPARATIVES.ORG

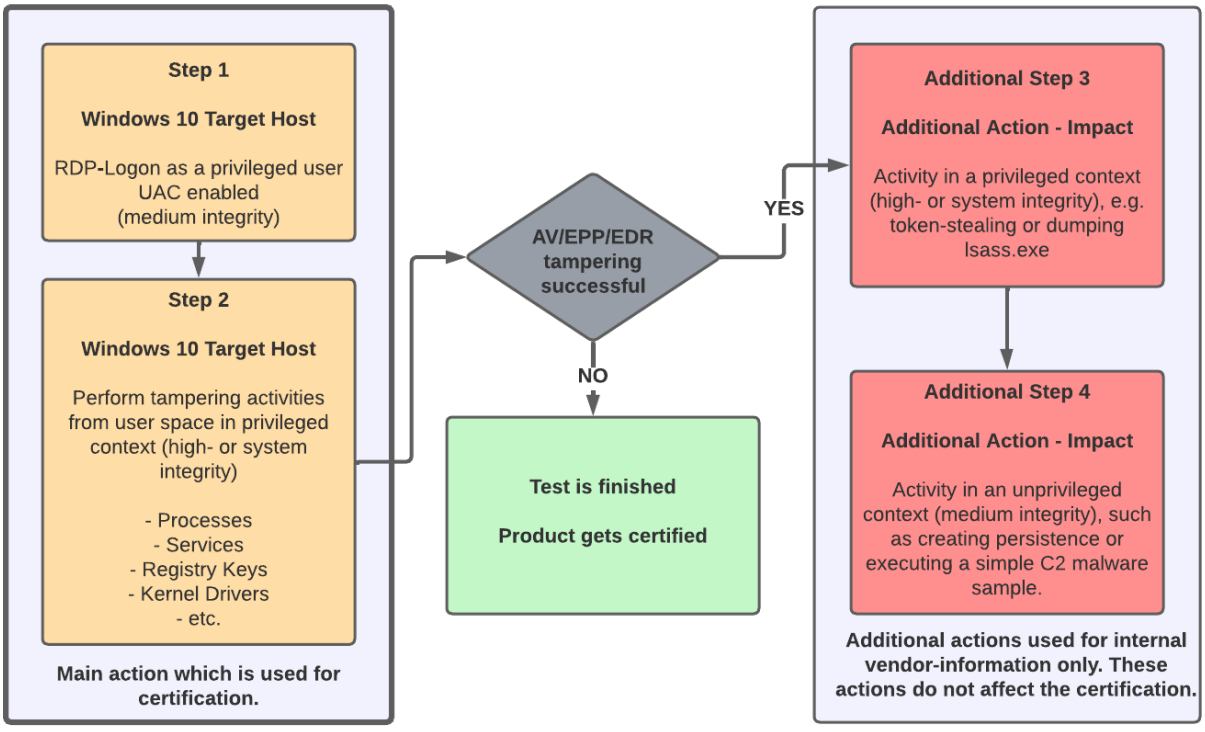
Introduction

Every year, AV-Comparatives provides a focus pen-test, to which vendors can apply to get certified. This year we focus on "Defense Evasion" (Anti-Tampering). Certification reports are published only for vendors who achieved the certification. Non-certified vendors received feedback on how the products were successfully tampered in order to improve their product.

After compromising a system in the targeted network, attackers have often to deal with endpoint security products like a classic anti-virus or a next generation anti-virus and endpoint detection and response (EDR) product. EDR products can be especially annoying in case of TTPs like credential dumping, lateral movement etc. Even if an attacker has already gained privileged user access (for example, local admin) most endpoint security products can still be very annoying to attackers. Therefore, attackers try to disable or modify tools[1] and get rid of the main capabilities from endpoint security products to permanently avoid the risk getting prevented or detect.

Test Procedure

In this test, which is done under Windows 10, we focus on evaluating whether it is possible to disable or modify AV/EPP/EDR components or capabilities through tampering. By penetrating the product, we attempt to disable or modify components of the product. All tampering activities are performed in the Windows user space as a high integrity or system integrity privileged user. We do not attempt to gain write access to the Windows kernel, although we do attempt to tamper with components in the kernel by remaining in user space. We do not perform any tampering activities in an unprivileged user context (low or medium integrity), as we are interested in evaluating the anti-tampering properties, not in finding exploits. If it were possible to disable key functionality from an AV/EPP/EDR as an unprivileged user, this would be an exploit. The purpose of this test is to evaluate the quality of the anti-tampering features of AV/EPP/EDR products. We will attempt to break into each product based on a list of checks and attempt to disable or modify the security solution by tampering with specific components.



[1] https://attack.mitre.org/techniques/T1562/001/

How is tamper protection in general defined?
Tamper protection protects the product against end-user and third-party changes, and the services, processes, files, registry entries, etc. against any controlling attempts, even in context of a privileged user (high- or system integrity).

How is successful tampering (manipulation) defined for this test? Whether it is possible to:

- Disable or modify configuration files or registry keys related to the security solution, or to shut down the related services or processes, or to disable or modify components in kernel space
- Uninstall the respective product or change the product configuration
- Disabling the product in general or by using the product itself
- Modify or setting up exclusion or allowlisting
- Partially or completely disable a product e.g., user space component disabled

Importantly, this test really focuses on the quality of tamper resistance! This means that we do not evaluate any steps of impact after it has been possible to tamper with a particular component of the product. For example, if it was possible to kill a process related to the security solution permanently or temporarily from the product in the system session, then that is our result. For certification we do not evaluate the impact; information about possible impacts is for internal vendor use only and is not relevant for certification.

We understand that, for example, disabling or terminating a single process in the Windows user space does not always result in a complete disabling of the product, but because our focus in this test is on tampering, we must define this scope in this way.

Scope

For certification purposes, we assess whether it has been possible to disable or modify the product or product components through tampering. For example:

- The tester was able to kill the user space process in the system session or one of the processes in the system session. → **This is our result.**
- For certification we do not evaluate the impact on prevention, detection, and response capabilities. → **Out of Scope:** The results from Step 3 and Step 4 are for the vendor's internal use only and are not disclosed to the public.

Out of Scope

In this test, we make a clear distinction between endpoint security products and the Windows operating system. This means, we do not enable or evaluate Windows hardening measures like Virtual Based Security (VBS), Hyper Visor Code Integrity (HVCI) etc.

Also out of scope:

- Putting the system into a lockdown mode
- Allowlisting by using the AV/EPP/EDR or allowlisting by using AppLocker or similar
- Using the safe mode to tamper the product
- Physical access (therefore, we log on to the VM via RDP)
- Any tamper activities by using the web console from the product.

Tested Product

In this test, the following up-to-date and latest publicly available product was submitted by the vendor and tested in April 2023:

Palo Alto Networks Cortex XDR Prevent

Settings

In business environments, and with business products in general, it is usual for products to be configured by the system administrator in accordance with vendor's guidelines, and so we invited all vendors to configure their respective products. Each vendor had the opportunity to enable product-specific tamper protection settings (if not already activated by default), such as enabling uninstall protection, enabling tamper protection for settings, setting passwords, etc.

Below we have listed the product settings applied by the vendor. Setting changes that we consider were relevant for this test are highlighted in red.

Palo Alto Networks: "PE and DLL examination" turned on and set to "Quarantine Wildfire and local analysis malware verdicts"; "Treat Greyware as Malware" turned on; "Quarantine" enabled for "Global Behavior Threat Protection Rules", "Credential gathering protections", "Anti-Webshell Protection", "Financial Malware Threat Protection", "Cryptominers Protection", "In-Process Shellcode Protection" and "Ransomware Protection". In "Password protection", the password was changed[2].

Please note that the results reached are valid only for the products tested with their respective settings. With other settings the anti-tampering certification might not have been reached. Therefore, we urge readers to make sure that at least the settings marked in red are enabled/configured properly if they want to increase the tampering protection of the product. We would also kindly ask vendors to consider applying such settings by default or at least to clearly recommend them to the users.

[2] **Note:** Cortex XDR has password-protection enabled by default, but uses a default password which is publicly known. Therefore, it is essential that a strong password is set by the users.

AV-Comparatives Anti-Tampering Certification

To be approved by AV-Comparatives for Anti-Tampering protection, all tampering attempts undergone during the test must be hindered.

Using various tests, tools and procedures, we attempt to penetrate/test the tamper resistance of each product, thus attempting to disable the main functions in the context of prevention, by attempting to influence different components of the respective product.

Only products which were submitted for the Anti-Tampering Test, and which passed the test, are published. **Palo Alto Networks Cortex XDR Prevent** reached the certification requirements, i.e. successfully protected against the tampering attacks used in this test[3].

Successfully protected against tampering attack, i.e. manipulation or termination, which could lead to temporary or permanently and partial or complete disabling of the EDR's functionality, was not possible.	✓

The following components or categories have been tested against tampering attacks that could result in permanent, temporary, partial or complete loss of product functionality:

User-space processes, including threads and handles (terminate, suspend, etc.)	✓
User-space services (pause, stop, disable, uninstall, etc.)	✓
Registry keys (delete, remove, rename, add, etc.)	✓
DLLs (manipulation, modification, hijacking, etc.)	✓
Agent integrity (disable, modify, uninstall, etc.)	✓
File system (manipulation, modification, etc.)	✓
Kernel drivers (ELAM driver, Filter driver, Minifilter driver, etc.)	✓
Other components and functions (e.g. connection to update services, etc.)	✓

[3] Please note that the reached certification applies for the products tested with the settings specified on the previous page.

Copyright and Disclaimer

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives
(May 2023)