AV-LAB CYBERSECURITY FOUNDATION

Transparency First Then Trust

CYBER TRANSPARENCY AUDIT OF XCITIUM BACKEND DATA

Q4 24

Cyber Transparency Audit – a review of cybersecurity vendor Xcitium and their endpoint workstations protection

Audit scope: October – December 2024 (Q4 2024)

2024

Q4 24

Table of contents

Transparency First

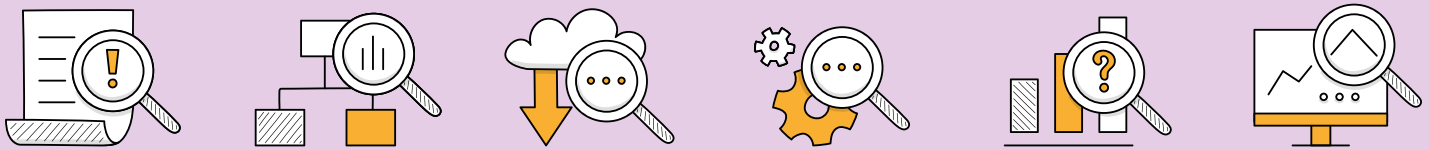
Then Trust

The world needs **more transparency** in the cybersecurity

Ensuring the protection of data and systems from potential damage is a fundamental aspect of cybersecurity.
It is challenging for customers to select a product if they do not have the opportunity to verify whether the software aligns with specific standards. The multibillion-dollar endpoint cybersecurity industry is characterized by the absence of standardized policies, despite its global impact on businesses.

Endpoint security software is designed to minimize risk.
A beneficial approach to ensuring user understanding of a developer's role in mitigating risk is through transparency of the application's functionality and the developer's infrastructure processes. By disclosing certain statistical information, it is possible to identify and understand the strengths of a product. This strategy has the potential to address the underlying issue, leading to the elimination of all remaining gaps. Conversely, developers who opt for the more challenging approach of disclosing statistical data from end devices may encounter public criticism and oversight. However, this approach is ultimately beneficial for all companies and institutions.

In the context of business-to-business relationships, clear guidelines are essential for fostering mutual trust.
The cybersecurity industry should adopt a transparency approach to bolster the trust end customers place in those responsible for their brand's image. This approach is instrumental in fostering collective progress in the realm of cybersecurity.



1 What is this audit?

Definition of "Cyber Transparency Audit"

As part of the "Cyber Transparency Audit," the testing body, in the role of the Auditor, verifies data from a cybersecurity solution provider to ensure historical compliance.

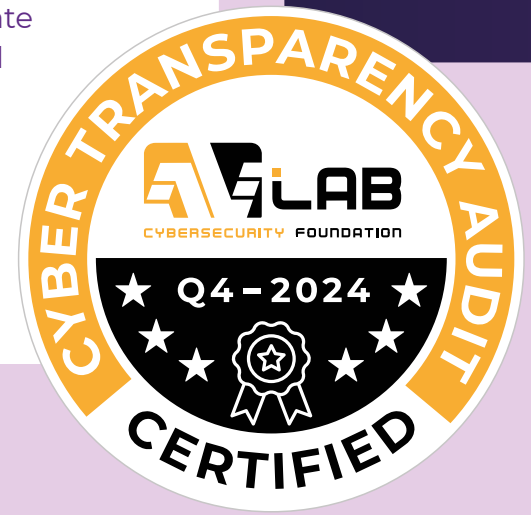
The audit is a formal evaluation of a system, organization, process, or project. The data is examined to ensure compliance with specific guidelines. The primary benefit of conducting the audit is the involvement of an external Auditor, who can meticulously assess and impartially identify areas that require enhancement.

Obtaining the "Cyber Transparency Audit – Certified" certificate by a provider means that its effectiveness regarding historical data is confirmed.

The methodology and policy are available to anyone who meets the specified criteria. Therefore, anyone is welcome to join the project as an auditor or developer.

Security incidents in telemetry data

This report contains analyzed and anonymized telemetry data from devices protected against malicious software by a product called Xcitium Advanced. The data show a correlation between potentially malicious activity on a Windows device and confirmed malware. This is significant because unknown files on employees' computers that have not yet been confirmed as malware can serve as a backdoor to serious threats, such as ransomware or spyware.



New standards for the endpoint protection industry

One of the current challenges facing the cybersecurity industry is the development of standards that will ultimately measure the effectiveness of modern security products installed on end devices. Transparency regarding statistics, malware data, and information about cyberattacks is essential for building trust. After fulfilling this condition, we, as the Auditor of historical data in the Xcitium infrastructure, can confirm that at the end of this chain there is an effective protection of the end customer's work environment. This protection undoubtedly inspires trust and builds a good opinion about a developer and its solutions.

Nowadays transparency means more

The primary objective of Endpoint Protection software is to mitigate risk by preventing incidents. Achieving this objective is contingent upon the public's awareness of the software's operational mechanisms. When implemented effectively, real-time protection can alleviate administrators' workload by enabling them to address vulnerabilities promptly, thereby enhancing the protection of systems and data. Therefore, making incidents and threats publicly available (or lack thereof) from the point of view of fairness and transparency allows for a better assessment of the developer's technologies – whether they work well in real scenarios or not. Additionally, auditing this statistical data enables a practical evaluation of whether the applied configuration of protection settings meets the needs of the majority of end customers.

The myth of closed source code

Open-source solutions for endpoint protection are not commonly used in this industry. However, developers can utilize certain libraries or frameworks, or even share their code. Contrary to popular belief, the security of closed source code has been proven to be no higher than that of open source. Numerous incidents have demonstrated that the same level of vulnerability exists in both types of code. Hackers do not require access to source code in order to comprehend its functionality. Through a process of trial and error, they are able to identify weaknesses and vulnerabilities in the application that were not discovered during the development process. Additionally, the disclosure of the source code may result from a cyberattack on the developer's servers or one of its partners (supply-chain attack). The unavailability of the code does not mean that we will not hear about incidents of critical vulnerabilities of the RCE (Remote Command Execution) class.

After reviewing the historical data, we can confirm that from September 30, 2024, to December 29, 2024, among 1,051,109 unknown 0-day files, no malware infection was recorded on systems protected by Xcitium software.

Key audit insights

- **Audited period:** September 30, 2024 – December 29, 2024
- **Purpose of the audit:** Confirmation of compliance with data from the audited period, indication of key information about malware and data leaks.
- **Scope of the conducted audit:** Audit of telemetry data concerns devices protected by the developer's software and file metadata as part of access to its static threat infrastructure.
- **Name of the audited developer:** Xcitium
- **Data comes from software of the class:** EDR, XDR, MDR Xcitium. The developer did not disclose which operating systems the audited period covers. Based on the audited file extensions for malware and clean samples, we conclude that this is a Windows environment.
- Public Data:
  https://www.xcitium.com/resources/threat-labs/data-statistics/
  https://verdict.xcitium.com/

The audit was prepared taking into account the following data set

1. Devices with potentially malicious activity (virtualized files).
2. Devices with confirmed malware status (virtualized files).
3. The number of 0-day files classified as secure.
4. Number of 0-day files classified as PUAs.
5. Number of 0-day files classified as malware.
6. Potential data leaks and active infections.

We used several samples to determine the compliance and authenticity of the audited data. These were executed in the Auditor's network on a test machine with Windows 11 on the following days:

SHA1: F39549CA5E29F78E2CB8B297D2B75FB5055925B2 2024-11-11 14:14:09

https://verdict.xcitium.com/get_info?sha1=f39549ca5e29f78e2cb8b297d2b75fb5055925b2
Human Expert Analysis Result: **Malware**

SHA1: 6532D75F817BBEFB11E817CFF6A729912BE162C9 2024-10-31 11:54:46

https://verdict.xcitium.com/get_info?sha1=6532d75f817bbefb11e817cff6a729912be162c9
Human Expert Analysis Result: **PUA**

SHA1: 744F9E241070E7AB43F6CB834420D2BA763A405A 2024-09-30 14:22:17

https://verdict.xcitium.com/get_info?sha1=744f9e241070e7ab43f6cb834420d2ba763a405a
Human Expert Analysis Result: **Clean**

The file checksums, along with machine and expert analysis, were included in the audited data, which we treat as confirmation of the data's authenticity.

Transparency of statistical data is a key argument in favor of the honesty of the developer for the end customer. This approach enables customers to make informed decisions by providing a comprehensive view of available products and competitive alternatives.

1. Without access to certain telemetry data, end customers are unable to assess the effectiveness of endpoint device security in practice.
2. Closed source code does not inherently guarantee superior protection against malware and hacker attacks.
3. Regular monitoring and auditing of statistical information about incidents from endpoint devices by external auditors can improve trust in the developer.
4. Early identification of problems in the audited project and neutralization of potential risk increases the effectiveness of security measures.

II Audit Summary

This section of the report offers a summary of the statistics collected from devices protected by Xcitium where potentially malicious activity has been detected in relation to confirmed malware.

The presence of unknown files on employees' computers can pose a significant security risk, potentially leading to infections with ransomware, spyware, or other malicious software. These files may be unintentionally downloaded from the Internet, brought to the company on mobile devices, or downloaded from emails. These files can cause damage to operating systems, resulting in data loss and potential infrastructure encryption or backup deletion.

From September 30, 2024, to December 29, 2024, a total of 1,051,109 unknown 0-day files were analyzed. Not a single system infection with malware or potentially unwanted software (PUA) was detected, which could have potentially led to data leakage.

Q4 2024 audit summary in numbers

Total audited devices	Devices with potential malicious activity	Devices with malware (API virtualization)
5,327,440	671,397	18,381

Total unknown files	Total clean files
1,051,109	1,011,839

Number of files with malware status	Number of files with PUA, PUP status
38,241	6,899

Number of unresolved malware issues	Number of infected systems	Number of data leaks
0 unresolved	0 infected	0 data leaks

Devices with potentially malicious activity (virtualized files)

This segment of telemetry is intended for devices running zero-day software that has not yet been identified by the system. This software may have exhibited indications of potential malicious activity during the preliminary machine analysis, thereby significantly increasing the risk of an incident.

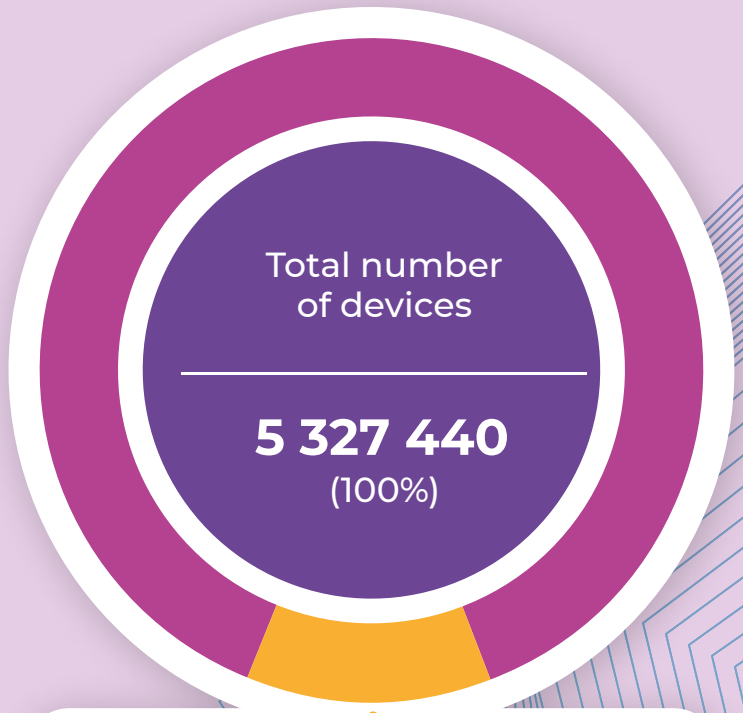
This is the first and most critical stage for protecting the entire organization when an unknown file is injected into one of the systems. Given the limitations of detecting up to 100% of zero-day threats, Xcitium employs virtualization of system resources to identify and isolate any malicious activity from the main operating system at the earliest stage. This patented technology involves virtualizing a file on an employee's device and then analyzing it automatically and manually by a Xcitium Threat Lab* employee.

The final determination regarding a file is made through a combination of machine and human analysis. Once a file is deemed safe and trusted, it is classified as malware or potentially unwanted software (PUP). Interestingly, 18,92% of all files were immediately classified by machine learning, while 77,72% of files were verified again by a human to minimize the occurrence of false positives.

From September 30, 2024, to December 29, 2024 (the last day of the audit), the number of safe devices in relation to the number of devices with potentially suspicious activity (virtualization) is presented in the chart.

*https://enterprise.xcitium.com/what-we-do-for-detection-in-the-cloud/

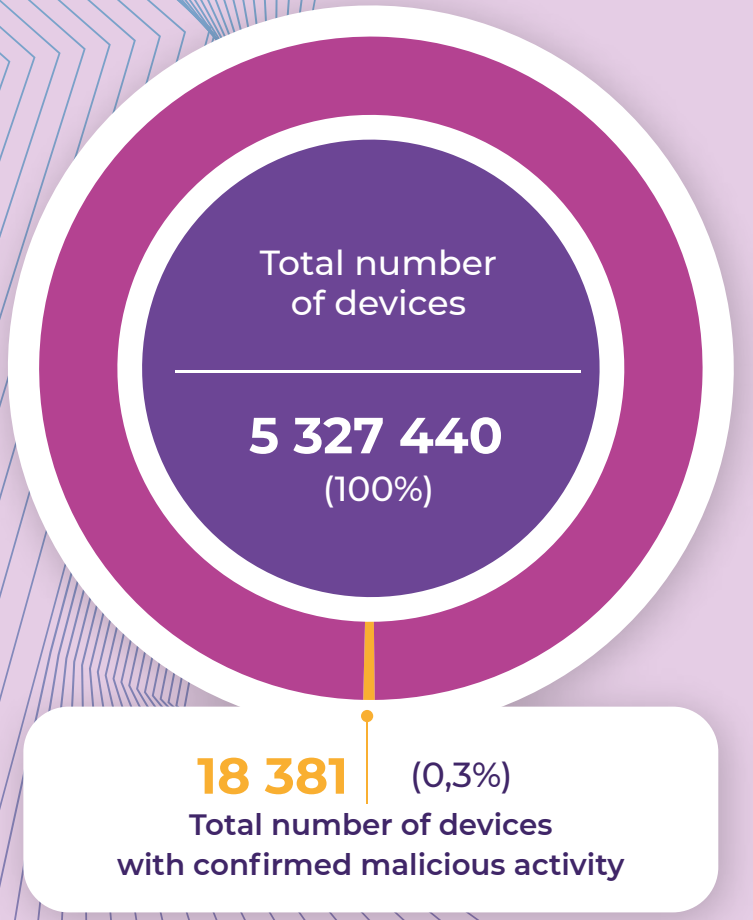
Number of devices without security incidents as a percentage of devices with 0-day files



671 397 (12,6%)

Total number of deviceswith potentially malicious activity (virtualization)

Devices with confirmed malware (virtualized files)



This component of the telemetry data concerns Windows devices in which the 0-day file is initially identified as a potential security incident during the preliminary analysis phase. Subsequently, a combination of machine and expert analysis is conducted to determine the definitive nature of the file, i.e., whether it is confirmed as malware or deemed to be safe. This process is seamless to the end user, ensuring their workstation remains secure throughout the analysis and post-analysis periods.

Regardless of the analysis outcome, a potentially unknown file has no way of infecting the operating system. From the perspective of the organization's security officer, this incident information is revealed in the admin console. Detailed logs are available for review to gain further insight into the verdict through file analysis in Xcitium Verdict Cloud.

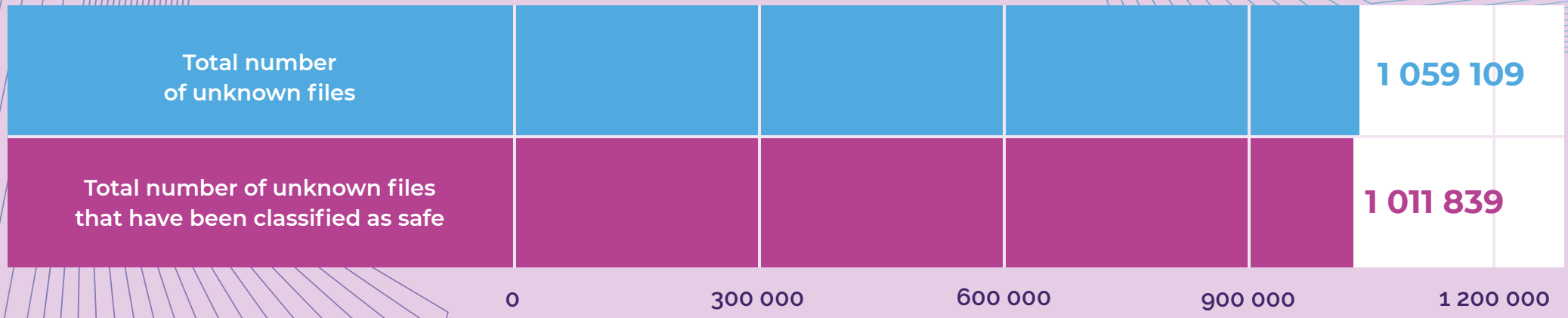
The machine analysis quickly classifies an unknown file as malware if it detects activity similar to that of malware using the Windows API. The file is then analyzed by a human expert in the Xcitium Threat Lab, providing a dual verification process. This additional layer of verification provides a valuable service to any organization looking to assess the security provided by human expertise.

0-day files classified as safe

This part of the telemetry data concerns files unknown (0-day) in the initial phase of intrusion into the system which after machine and human analysis turned out to be clean and safe.

Audited data demonstrated that, on average, 95,5% of unknown files were found to be safe. Xcitium's strategy regarding potential risks has proven effective, particularly in terms of preventing the infection of devices with malware through the execution of unknown files. Appropriate preventive measures have been implemented to minimize or eliminate human risk to a minimum.

Number of unknown files in relation to files classified as safe



0-day files classified as PUAs

This part of telemetry data concerns initially unknown files and later classified in the developer's infrastructure as potentially unwanted software (PUAs) installed on a computer, often without explicit user consent. Such software can run in the background, collecting data, or causing other damage.

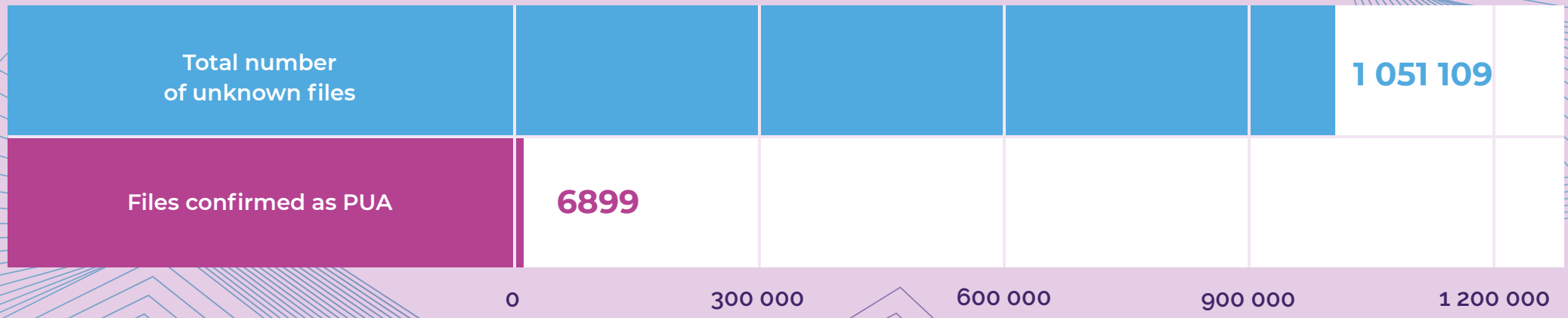
The audit has shown that PUA threats had a small share in the statistics as fake programs pretending to be antiviruses, applications supposedly cleaning the system, applications allegedly taking care of updating drivers. A large percentage of these types of applications have got advanced mechanisms that make it difficult to both detect and remove them from the system.

Thanks to the triple verification of files (static, dynamic, and human analysis), it is possible to better understand the operation of an unknown file in its initial phase, and to classify it later.

PUAs usually come bundled with installers for main software, and thus users may not be aware of installing unwanted applications, potentially posing a greater risk to an organization's security.

The number of PUAs detected among unknown files is marginal, and it is only 0.4%.

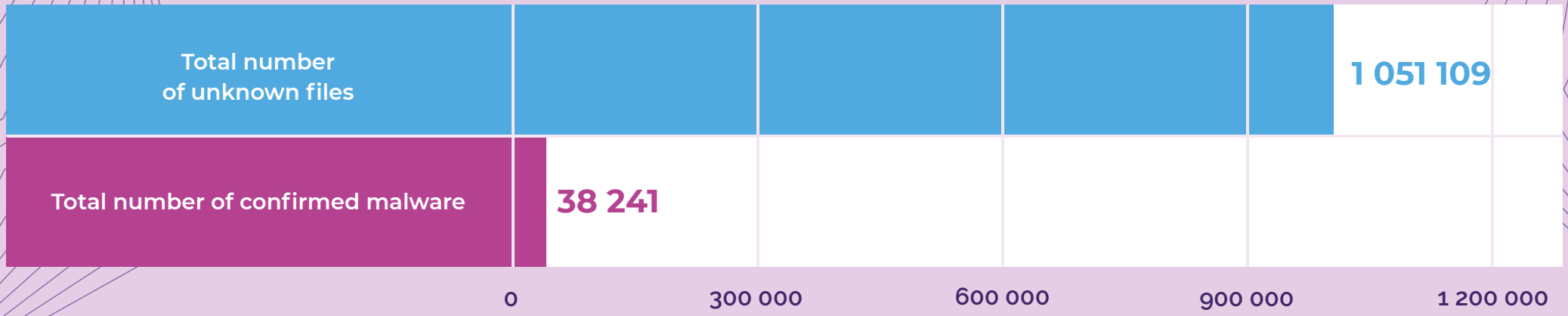
Number of unknown files in relation to files classified as PUA



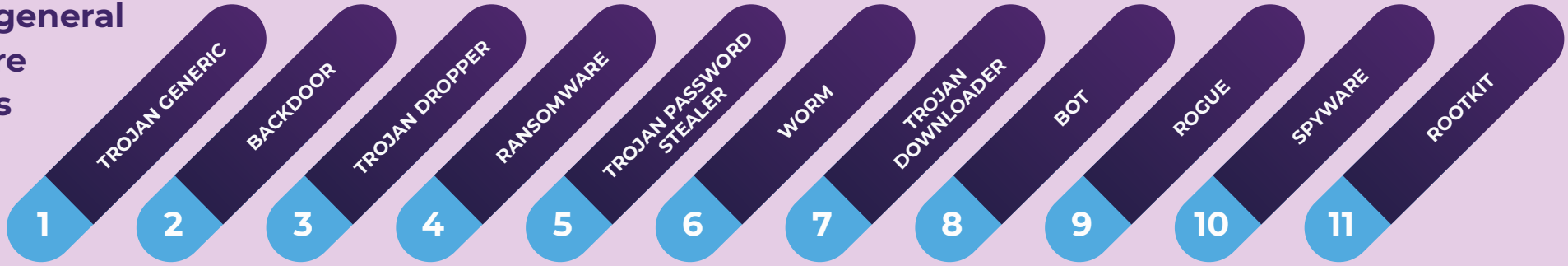
0-day files classified as malware

This is the final segment of the telemetry data that has been reviewed for historical compliance with the data provided by the developer. It concerns files initially unknown, and later confirmed as malware as a result of machine analysis, and the analysis by Xcitium Threat Lab experts.

Number of unknown files in relation to files with confirmed malware status



TOP 11 general malware families



It has been determined that, on average, 3,6% of unknown files are determined to be malware. In summary, for every 900 files examined in the developer's audited static infrastructure, one was identified as malware. When applied to third-party software, it can be theorized that 3,6% of unknown files could be allowed to run after the first contact with antivirus software, which drastically increases the risk of infecting the work environment. It is crucial to understand that a single malware file can have severe consequences for organizations, potentially leading to financial and reputational losses.

Potential Data Leaks and Active Infections

Initially, 0-day and later files classified as malware did not cause any harmful changes to devices with Xcitium protection installed due to the system resource access virtualization technology used.

The patented technology is designed to prevent any damage by detonating the file in a secure environment, eliminating the need for faulty static and partly dynamic threat detection.

Data Leaks	Potentially infected devices	Number of unresolved malware issues
0	0	0
(0%)	(0%)	(0%)

III Audit methodology in the Q4 2024

The testing organization connects to the static infrastructure of the cybersecurity solution provider. It carries out additional tasks and is granted authorization to verify the results.
The certificate it provides serves as a formal attestation of the congruence between the results and the methodology.

General description & requirements for joining the audit

The methodology will be updated as it becomes available to all participants in the discussion on its development. The methodology for the audited developer in the fourth quarter of 2024 has been prepared in cooperation with the Cyber Transparency Forum group, and it may be subject to change in the future with the participation of other developers, which will be communicated in subsequent audits.

These changes are necessary because, depending on the data that can be provided to us by developers, we want to adapt the methodology to all protective solutions as best as possible in order to extract the maximum benefit from the statistics for end customers and developers.

Requirements for Developers

The Cyber Transparency Forum invites any developer that has telemetry data from at least 100 000 (one hundred thousand) devices to participate.

The testing organization will require access to data that will match at least the recommended settings of the protection policy. They may include the so-called hardened settings. It is not allowed to audit data from devices with disabled security modules, for examples, antivirus, SSL scanning, unless it is a recommended policy.

It is allowed to participate in the audit of a device with the following settings:

1. **Recommended Policy:** These are the required settings for workstation protection to meet the minimum security measures proposed by the developer. The IT solution provider must recognize these settings in the provided static infrastructure so that the Auditor does not check data from devices with policy of key product features disabled.
2. **Hardened Policy:** Protection settings have been increased by the administrator, or have been switched on maximum security using a predefined hardened policy prepared by the developer.

The developer will create access to statistical data via API or graphic panel. Access to data should be possible in time intervals:

1. access to data from the last 1-3 hours,
2. last 24h,
3. last week,
4. last month,
5. last full quarter.

The developer agrees to publish the results online. Transparency enables a better understanding of the product's strengths, and the development of ways to detect and fix product weaknesses that may pose a high risk.

The developer must prepare the data in accordance with section "2A" below with at least the recommended telemetry data that will be part of the overall analysis performed by the Auditor.

Other requirements are listed in the rules of the Cyber Transparency Forum.

Requirements for Auditors

Any entity that tests IT solutions, the so-called test laboratory, can become an auditor.

Auditor at the auditing stage will communicate with the Developer and, if possible, will indicate errors that falsify or prevent performing a full audit.

Auditor may propose adding new feature and data to the static infrastructure, and using new data in the same or subsequent edition of the audit.

IV Audit Test Components

This is general information that must be met by the Developer, and the Auditor in order to effectively validate the data.

Minimum Requirements Data for Endpoint Security

To conduct a transparency audit, we have set ourselves the goal of validating data from at least 100 000 (one hundred thousand) end devices, regardless of the operating system. It is not required to include all devices in the statistics, as this may constitute a trade secret or may be technically difficult for the Auditor to isolate.

Therefore, in order to properly conduct the audit, we require:

1. Telemetry data from a minimum of 100 000 endpoints.
2. Taking into account only those endpoints that are secured by a security agent with at least a default (predefined by the Producer) or hardened (enhanced) security policy.

Developer should care about making its customers aware of the protection settings used. In specific situations, the system administrator can reduce the level of security, so we want to exclude devices with a reduced level of protection from the audit.

File information and metadata from endpoints

We include file telemetry in the audit. The data provided by the Developer should be anonymized to not reveal confidential information.

1. The total number of unknown files that were found to be clean.
2. The total number of unknown files that turned out to be malware.
3. Total number of unknown files that turned out to be PUAs/PUPs.

Obtaining information about files and metadata will allow to better interpret the audited data, which can contribute to:

1. Search for trends over time to better understand whether a threat or cyberattack is growing or decreasing in statistics.
2. See the severity of threats over time, such as the type of malware detected or the number of malicious domains blocked.
3. Remediation so that the developer's end customers can receive recommendations to improve their security fundamentals, such as increasing the use of SSL certificates or strengthening email security.
4. Compare data with industry averages or other sources to see how the vendor and its customers are vulnerable to, and how they deal with them.

Required data from the Developer about devices

Endpoints secured with developer software must provide the following telemetry data to the central system to prepare for the audit:

1. Total number of devices.
2. The number of devices that contain potential malicious activity.
3. The number of devices with confirmed malicious activity.
4. The number of devices that meet ecurity standards (not infected).

V Audit Test Process – Step by step

01 A cybersecurity service provider provides an API or graphical interface with anonymized telemetry data for the testing organization.

02 The required data must have the option to be sorted according to a specific time schedule, for example, last hour, week, month, or quarter.

03 Telemetry data should include basic information about devices and files.

04 The developer will create a process that will allow testing organizations to access this data at any time during the audit. It is imperative that the data be updated on a regular basis, at least once a day. The auditor can use malware samples to verify the data's authenticity.

05 The developer will provide the same set of data through the software API or the proposed data format (JSON, XML, CSV, etc.), enabling the testing organization to connect to the developer's statistical infrastructure and download the data for further analysis.

06 The audit schedule is determined by the mutually agreed-upon schedule between the Developer and the Auditor. During this period, both parties are expected to cooperate, and any aspects requiring clarification are to be addressed promptly. There may be "spot checks" or additional questions regarding the data provided by the testing organization to the Developer.

07 The testing organization will publish an audit report. The report will be made available at the conclusion of the reporting period.

08 The testing organization will issue a certificate confirming the successful validation of the audited telemetry data.

VI FAQ - questions & answers

How do we collect data from a developer?

We obtain data from a developer's static infrastructure via API or graphical interface. The scope of this data and its detail is discussed during the initial audit preparation. The auditor can verify the percentage data using malware samples which should be included in a developer's telemetry data.

Why it is worth joining?

The Cyber Transparency Forum working group is comprised of leading security software vendors who collaborate to enhance transparency and share telemetry data with the broader Internet community. We work together to set new security standards for cybersecurity software vendors.

How long is the certificate valid and why?

The certificate's validity extends for a period of one year, commencing on the date of its issuance. Please note that historical telemetry data may differ significantly from the initial state after such a long time. Therefore, further use of the certificate will require data validation.

How to obtain the data compliance certificate?

To obtain the transparency certificate, it is necessary to meet all data compliance requirements in the audited period.
During the audit, a developer must cooperate with the Auditor and respond to all of his questions.

How to join the Cyber Transparency Audit program?

If you are a provider of security software, please contact the Cyber Transparency Forum group.
To be considered for onboarding, your company must meet specific criteria, including the protection of 100,000 devices and the submission of telemetry data.

AVLab
CYBERSECURITY FOUNDATION

The AVLab Cybersecurity Foundation is an independent organization dedicated to protecting privacy and security on the Internet. We are affiliated with the CTF (Cyber Transparency Forum) and provide independent assessments of cybersecurity vendors' systems. We are a member of AMTSO (Anti-Malware Testing Standards Organization), an organization dedicated to enhancing transparency, objectivity, and the quality of testing. We are also affiliated with the Microsoft Virus Initiative.

We build awareness of users in the field of digital protection. We issue opinions, technical analyzes and tests of IT solutions in the field of cybersecurity.
Our strongest assets include thorough and detailed reviews, preparation of reports related to privacy and endpoint protection, and in particular, security tests that make us recognizable all over the world as one of the most trusted and popular testing laboratories.

To learn more about other opportunities for cooperation, please refer to our full offer and contact us: **kontakt@avlab.pl**

CYBER TRANSPARENCY AUDIT FORUM MEMBER

amtso
The cybersecurity industry's testing standard community
MEMBER

www.avlab.pl