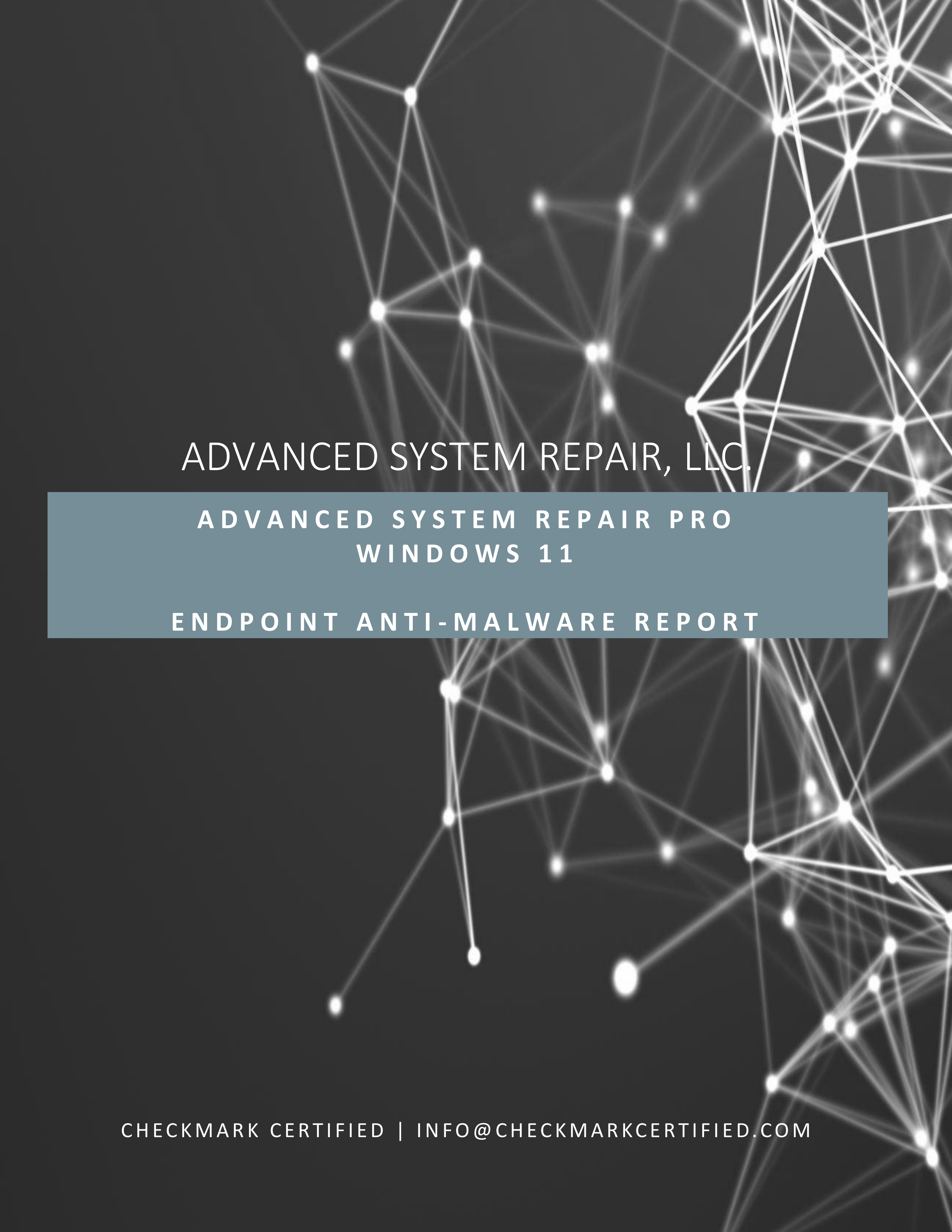


ADVANCED SYSTEM REPAIR, LLC.

# ADVANCED SYSTEM REPAIR PRO
# WINDOWS 11

# ENDPOINT ANTI-MALWARE REPORT

CHECKMARK CERTIFIED | INFO@CHECKMARKCERTIFIED.COM

# SUMMARY

With corporate networks and user data, both at home and in the workplace, being under constant attack, having security measures in place has never been more vital. But what security measures? And how do you know they will provide an adequate level of protection? Worse yet, will the selected solution itself be a threat to your data?

Checkmark Certified, for almost three decades, has conducted the testing and evaluation of security solutions of various types, uses, and functionality. From enterprise-level network AI to home computer anti-malware.

The following report has been put together using that experience and with the aim to provide you with a clear overview of the solution being considered.

# INTRODUCTION

## ABOUT THE REPORT

This document is designed to provide a high-level outline of the outcome from the latest round of testing conducted against the listed solution. Tests were conducted as per the testing requirements and procedures that form the Checkmark Certified accreditation.

All information contained within this document shall remain the property of Checkmark Certified

## ABOUT THE LAB

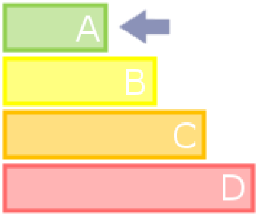
The Checkmark Certified (CC) business philosophy is founded on quality and excellence with all testing activities carried out in a secure, real-world test environment and within a framework of confidentiality that ensures integrity of information and test data.

CC prides itself on its open and proactive working relationship with all its clients through ongoing and meaningful communication.

The outcome is a sound technical working relationship, which ensures the client derives maximum benefit from engaging with an independent test facility that can also act as a conduit to a global buying market for security products and services

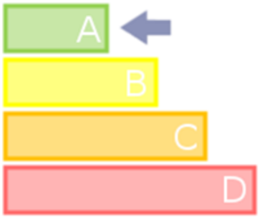
CHECKMARK CERTIFIED

# EXECUTIVE SUMMARY



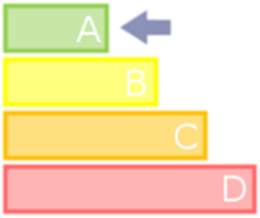
## TEST: THREAT

A report on the solution’s ability to mitigate the threat associated with the malware. Threat ratings are assigned based on the severity of the system interaction when the sample is executed or otherwise resident. The ratings range from 0 to 10+ and are categorized as PUP/Suspicious, Moderate, High, and Critical.



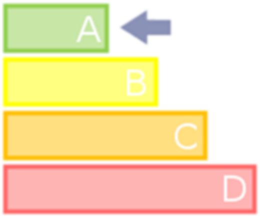
## TEST: SIGNATURE

Traditional testing that examines detection capability of isolated, static malware samples. Detection is recorded at either the transfer, scanning, or interaction stages. Samples are selected from a pre-existing suite and include a variety of malware “types” not limited to trojans, spyware, data extraction, and droppers.



## TEST: TYPE

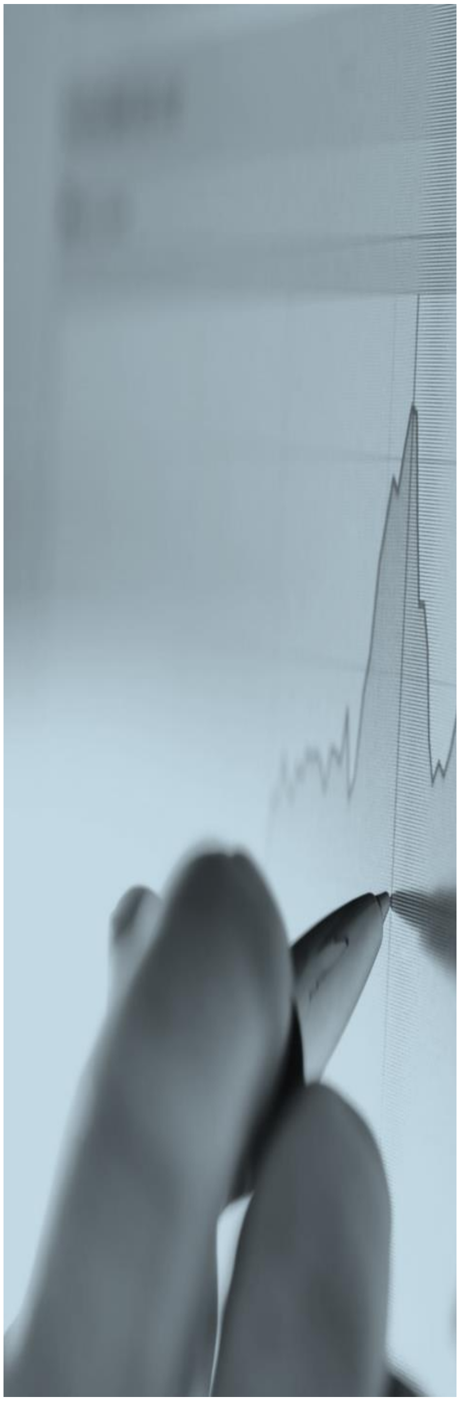
Solution detection capability against malware by group or type. Malware categories may be subject to change but will reflect those amongst the common type at the time of testing. Trojan, Spyware, and Ransomware will always be included.



## TEST: BEHAVIOR

Testing focused on the isolated, individual behaviors associated with various categories of malware. Detection results are based solely on the correct identification and nullification of these behaviors and is designed to identify areas of weakness in the tested solution. Modified variations of the behaviors are used where required.

# TEST APPROACH



**Principal**

When testing any form of software, steps should always be taken to guarantee that the testing is fair and representative of not just the product's intended use but also the environment to which it is designed to be deployed.

This approach remains true when addressing the testing of security solutions. In this case, the often-repeated mistake is the creation of a test that is designed to fit the features and functionality of the Solution Under Test (SUT), resulting in an outcome that will often favor the solution; but not one that represents the SUT's mitigative effects on a real-world threat.

So how do you assess the effectiveness of the SUT without directly testing the SUT? The approach taken by Checkmark Certified, during the certification process, is to test the threat, not the solution.

How does this work in the real world? The recreation and repetition of the behavior associated with the threat is always the goal, regardless of whether the SUT is in place or not. The attack is broken down into whatever constituent parts can be accurately measured; this is done prior to deployment of the SUT and then again after.

There are obvious caveats to this approach, such as where the SUT contains a feature designed to be initiated by the end user. However, the overall principal of not modifying the test to suit the product remains.

**Endpoint Anti-malware**

When considering an endpoint solution, the test is broken down into three phases: exposure, scanning, and execution. The exposure phase involves the initial transfer of files from source to the endpoint, with the source being direct web download, transfer from a localized source, and FTP.

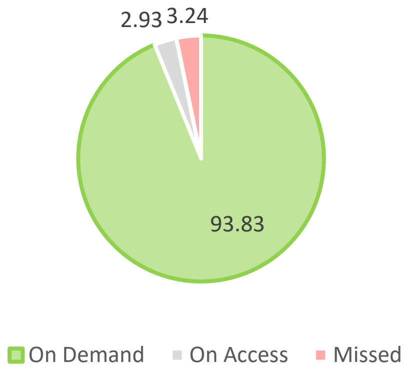
The second phase, scanning, focuses on any on-demand functionality provided within the SUT. Once the first phase is complete, remaining files are then directly scanned. As with the exposure test, the threat is considered mitigated by the file's removal, disinfection, or by alerting the end user.

The final phase assumes that either the SUT has so far failed to detect the threat or that the SUT is only intended to detect the threat on execution. Each file is executed, in turn, on the endpoint which is monitored for the known system interactions associated with the specific threat.

# PROTECTION: SIGNATURE

The following results are based on traditional signature-based malware testing. Malware samples are transferred to the system and tested by exposure type; including the file download, transfer, and on-demand scanning. Files are considered missed if allowed to execute on the protected system.

## DETECTION RATES

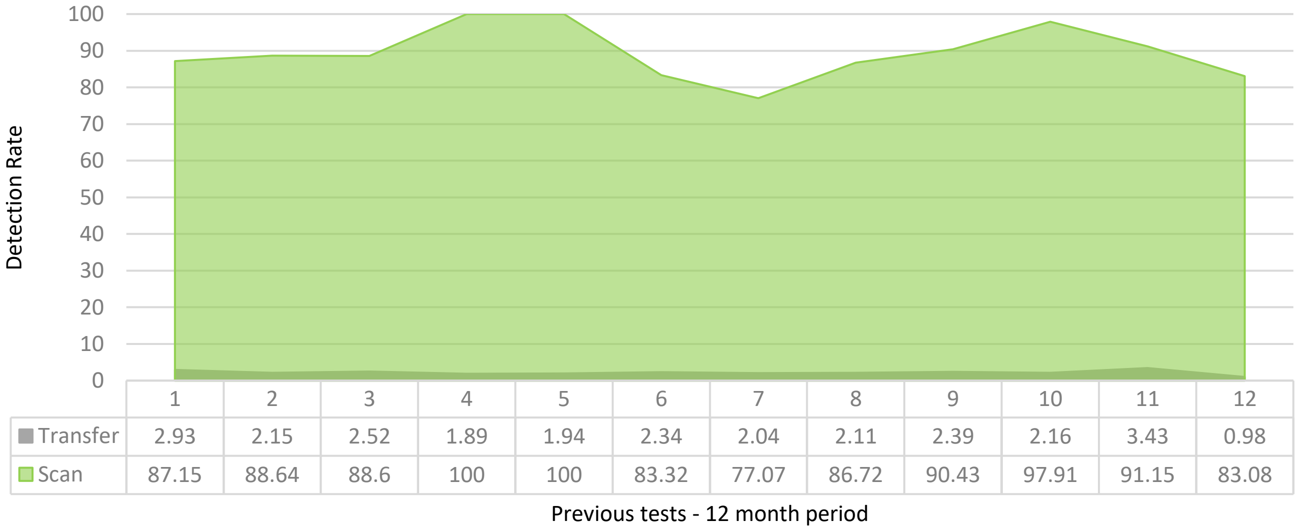


The following is a breakdown of detection rates recorded during testing over the previous 12 months. Current month percentage point change on previous test is indicated underneath.

| | *Current Month* | *Year Average* | *Year High* |
|---|---|---|---|
| *Transfer* | 2.93% | 41.52% | 100% |
| *Scan* | 87.15% | 90.88% | 100% |
| | ⌄ 1.49 | | |

## DETECTION OVER TIME

A record of the recorded detection rates over the past 12 months. Detection result is based on the final rate recorded after the transfer and scanning tests have been completed.

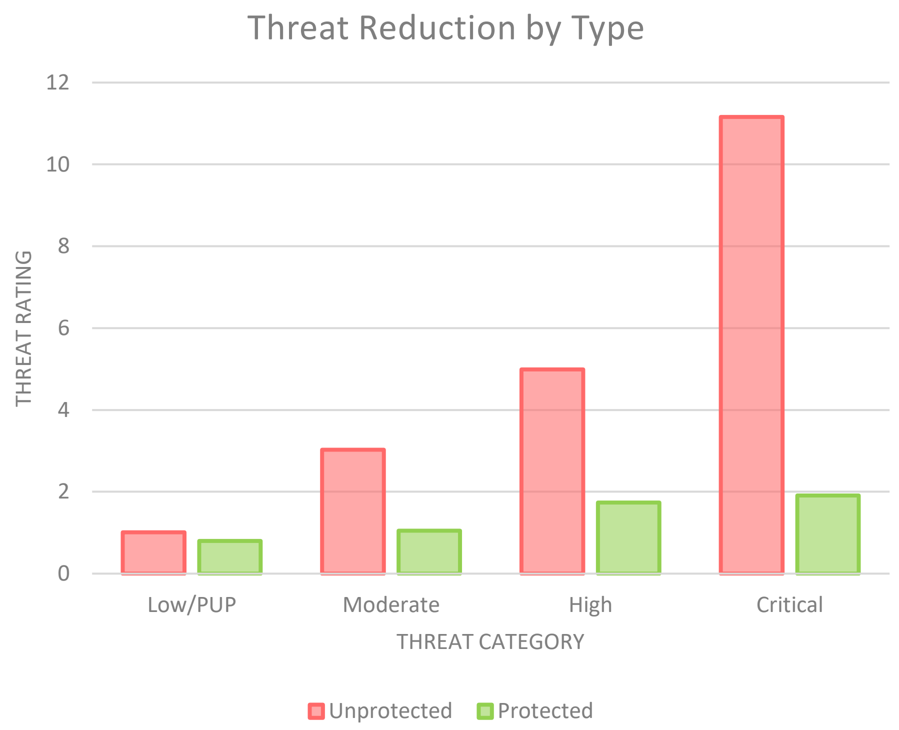


| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ▨ Transfer | 2.93 | 2.15 | 2.52 | 1.89 | 1.94 | 2.34 | 2.04 | 2.11 | 2.39 | 2.16 | 3.43 | 0.98 |
| 🟩 Scan | 87.15 | 88.64 | 88.6 | 100 | 100 | 83.32 | 77.07 | 86.72 | 90.43 | 97.91 | 91.15 | 83.08 |

Previous tests - 12 month period

# PROTECTION: THREAT

The following results indicate the solution’s ability to mitigate threats based on the associated risk. While traditional signature testing can indicate a product’s effectiveness, it is often built on the assumption that all included binaries represent an equal threat. This can lead to an incorrect rating of that solution’s effectiveness.



## RATINGS

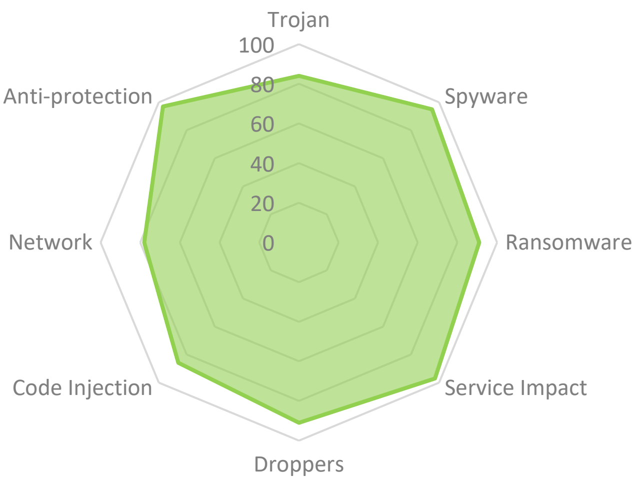
All tested binaries are assigned an associated threat rating based on their monitored behavior under analysis.

Any binary with a threat rating above 10 is automatically categorized as Critical. Associated ratings may be the result of a high number of lower impact system interactions or those that are  individual yet high impact.

| **Low/PUP** | **Moderate** | **High** | **Critical** |
|---|---|---|---|
| Binaries and applications that interact with system registry and local files but that do not present a definitive risk either through design or error. | Malware used to create further vulnerabilities on the system or attempt to interfere with system operations. | Malware that presents a definitive risk to the user’s data/information, or that may facilitate further security breaches. | Active threats that present a direct risk to the integrity of the system and user information. These will include ransomware, destructive malware, and data theft. |
| Range: 0.5 - 2.0<br>Unprotected: 1.01<br>Protected: 0.8 | Range: 2.1 - 4.0<br>Unprotected: 3.03<br>Protected : 1.05 | Range: 4.1 – 10.0<br>Unprotected: 4.99<br>Protected : 1.74 | Range: 10.1 +<br>Unprotected: 11.16<br>Protected : 1.91 |

# PROTECTION: TYPE

Protection capability when malware is classified by type or category. Categories may differ between tests depending on trends at the time of testing. Categorization is based on observed behaviors during initial analysis against an unprotected system.



| *Category* | *Reduction* | *Threat Before* | *Threat After* |
|---|---|---|---|
| *Trojan* | 84% | 7.9 | 1.3 |
| *Spyware* | 95% | 11.91 | 0.6 |
| *Ransomware* | 91% | 11.94 | 1.1 |
| *Service Impact* | 97% | 7.22 | 0.2 |
| *Droppers* | 91% | 6.88 | 0.6 |
| *Code Injection* | 86% | 7.68 | 1.1 |
| *Network* | 78% | 8.8 | 1.9 |
| *Anti-protection* | 97% | 10.98 | 0.3 |

TROJAN
As used in testing, malware in this category is designated as trojan primarily by its authentic appearance and behavior but where it also presents a threat to the user/system.

SPYWARE
Applications that are designed to remain hidden on the affected system and present a threat to the user by the theft and use of their information or data.

RANSOMWARE
Applications designed to perform the unauthorized encryption, or by action enable the encryption, of system or user’s files and data.

SERVICE IMPACT
Malware that attempts to interrupt, disable, or otherwise corrupt authentic services running on the target system. Includes the running of malicious/mimic services.

DROPPERS
Any threat that places new files or code on the target system that is either a threat itself or allows for further corruption of system integrity.

CODE INJECTION
Malware that is designed to leave no definitive trace on the system. These threats execute by the appropriation of vulnerable application access or by their exploitation.

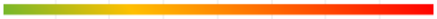
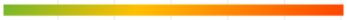
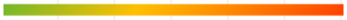
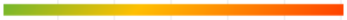
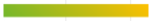
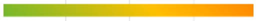
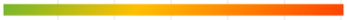
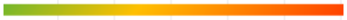
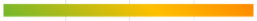
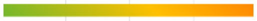
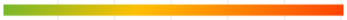
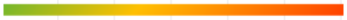
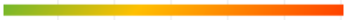
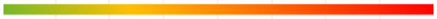
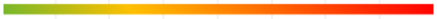
NETWORK
Traffic associated with malware that is either directly related to the exfiltration of data of for the transfer of data or further malicious files. Includes interaction with C&C servers.

ANTI-PROTECTION
Malware that exhibits behavior designed to either interfere with the correct operation of malware/threat protection applications or that contain detection avoidance mechanisms.

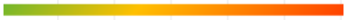
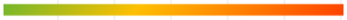
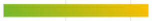
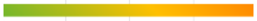
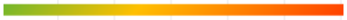
# PROTECTION: BEHAVIOUR

The following is a breakdown of the solution’s ability to identify and, where necessary, block or disrupt isolated behaviour. Each behaviour is assigned a threat level appropriate to the disruption or damage that may be caused. Behaviours are grouped by approximate category.

CODE INJECTION

| Behaviour | Count | Block Rate | Threat Level |
|---|---|---|---|
| Powershell Downloader DFSP | 0 | 0% |  |
| Potential heapspray | 0 | 0% |  |
| Heapspray attack on powershell | 0 | 0% |  |
| Code injection - CreateRemoteThread | 25 | 96% |  |
| Process searches | 2787 | 100% |  |
| Process memory code injection | 53 | 94% |  |
| Buffer exploits (code injection) | 0 | 0% |  |
| Buffer exploits (embeds PE file) | 17 | 100% |  |
| Corrupted files - services.exe | 0 | 0% |  |
| Corrupted files - csrss.exe | 0 | 0% |  |
| Process injection | 215 | 93% |  |
| Code injection to executed process | 198 | 96% |  |
| Existing process memory/code injection | 6 | 100% |  |
| Modification of read-write memory | 17 | 100% |  |
| Read-write-execute memory injection | 136 | 100% |  |

INSTALLERS

| Behaviour | Count | Block Rate | Threat Level |
|---|---|---|---|
| Suspicious reg entry length, possible binary | 14 | 93% |  |
| Installed hooks for mouse | 13 | 92% |  |
| Loaded drivers | 0 | 0% |  |
| Autorun installs | 755 | 96% |  |
| Browser corruption | 41 | 98% |  |

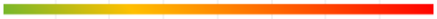
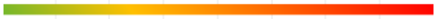
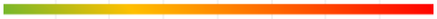
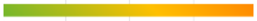
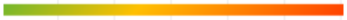
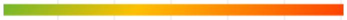
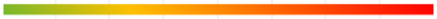
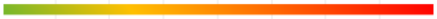
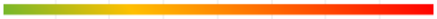
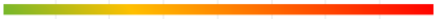
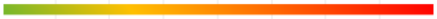
DATA THEFT

| Behaviour | Count | Block Rate | Threat Level |
|---|---|---|---|
| Browser data theft | 564 | 100% | 🟩🟨🟧🟥🟥 |
| Queries for the computername | 144 | 100% | 🟩🟨 |
| Keyloggers (Windows hook) | 4 | 100% | 🟩🟨🟧🟥🟥 |
| System fingerprint through data capture | 53 | 96% | 🟩🟨 |
| Data capture on installed applications | 9 | 100% | 🟩🟨🟧 |
| Checks for the Locally Unique Identifier | 55 | 93% | 🟩🟨 |
| Instant Messenger data miners | 0 | 0% | 🟩🟨🟧🟥 |
| FTP credential capture/theft | 0 | 0% | 🟩🟨🟧🟥🟥 |
| Data capture of specific processes | 12 | 83% | 🟩🟨🟧🟥🟥 |
| Theft attempts of email | 0 | 0% | 🟩🟨🟧🟥🟥 |
| WMI system queries | 9 | 89% | 🟩🟨 |
| Browser file searches | 4 | 75% | 🟩🟨 |

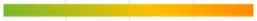
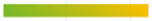
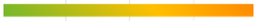
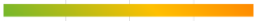
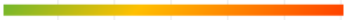
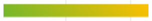
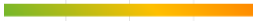
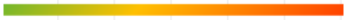
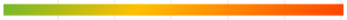
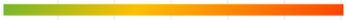
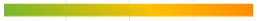
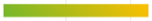
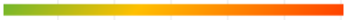
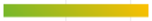
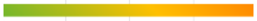
DROPPERS/DROPPED FILES

| Behaviour | Count | Block Rate | Threat Level |
|---|---|---|---|
| Executable file written to disk by process | 0 | 0% | 🟩🟨🟧🟥🟥 |
| Outlook.exe used to write files | 0 | 0% | 🟩🟨🟧🟥 |
| Mime files dropped | 0 | 0% | 🟩🟨🟧🟥🟥 |
| PE file foreign language | 0 | 0% | 🟩🟨 |
| Dropped and executed EXE files | 17 | 88% | 🟩🟨🟧🟥🟥 |
| Ransomware files | 0 | 0% | 🟩🟨🟧🟥🟥 |
| Deletes original binary | 1 | 100% | 🟩🟨 |
| Deletes executed files | 1 | 100% | 🟩🟨 |
| Dropped Office docs | 27 | 82% | 🟩🟨🟧 |
| Dropped hidden/system files | 262 | 96% | 🟩🟨🟧🟥🟥 |
| Dropped EXE shortcuts | 12 | 100% | 🟩🟨🟧🟥 |
| Autorun.inf file created | 2 | 100% | 🟩🟨🟧🟥 |

RANSOMWARE

| Behaviour | Count | Block Rate | Threat Level |
|---|---|---|---|
| Cerber ransomware detection | 0 | 0% |  |
| File deletion and/or encryption | 992 | 93% |  |
| TOR ransomware URLs | 0 | 0% |  |
| Dropped ransomware message | 69 | 85% |  |
| Windows utility interactions | 9 | 100% |  |
| Windows API crypto key use | 117 | 85% |  |
| Encrypted ransomware files | 0 | 0% |  |
| Removal of system recovery files | 0 | 0% |  |
| Ransomware file encryption and extension | 0 | 0% |  |
| Dropped ransomware files | 0 | 0% |  |
| Encrypted files written to disk | 52 | 100% |  |

SERVICE INTERACTION

| Behaviour | Count | Block Rate | Threat Level |
|---|---|---|---|
| Suspicious Powershell Process | 13 | 100% |  |
| Potentially unwanted processes | 10 | 90% |  |
| Suspicious OS Processes | 26 | 80% |  |
| Created services | 10 | 100% |  |
| System process mimic | 31 | 87% |  |
| Running of command console | 477 | 91% |  |
| Service created but not started | 35 | 94% |  |
| Launched server | 0 | 0% |  |
| Injected process creates hidden window | 18 | 90% |  |
| Disabled system restore | 0 | 0% |  |
| Terminated system processes | 19 | 100% |  |
| Disabled task manager | 42 | 90% |  |
| Windows services stopped | 0 | 0% |  |
| Crashed or disabled processes | 98 | 89% |  |
| Stopped Windows services | 32 | 84% |  |

GENERIC BEHAVIOURS

| Behaviour | Count | Block Rate | Threat Level |
|---|---|---|---|
| Behaviour detection (Dridex sig) | 0 | 0% | ▬▬▬▬▬▬ |
| Trojan files (Upatre sig) | 16 | 100% | ▬▬▬▬▬▬ |
| Botnet files (Nitol sig) | 21 | 100% | ▬▬▬▬▬▬ |
| Backdoor trojan files (Fynloski sig type) | 27 | 100% | ▬▬▬▬▬▬ |
| Banking trojan files (Dyreza sig type) | 22 | 100% | ▬▬▬▬▬▬ |
| Created batch file to remove original file | 32 | 84% | ▬▬ |
| Trojan files (Redosru sig) | 0 | 0% | ▬▬▬▬▬▬ |
| Created Alternate Data Streams | 0 | 0% | ▬▬▬▬▬▬ |
| Spyware files found (SpyNet sig) | 82 | 100% | ▬▬▬▬▬▬ |
| Putty files found | 0 | 0% | ▬▬ |
| Trojan files dropped (Bublik sig) | 0 | 0% | ▬▬▬▬▬▬ |
| Multiple user agents detected in traffic | 27 | 100% | ▬▬▬▬ |
| Suspicious command line tools | 31 | 100% | ▬▬▬▬ |
| Created malware files (Hupigon | 0 | 0% | ▬▬▬▬▬▬ |
| XtremeRAT file drop | 41 | 100% | ▬▬▬▬ |
| Known trojan files and registry | 0 | 0% | ▬▬▬▬▬▬ |
| Created registry keys (NJRat sig) | 0 | 0% | ▬▬▬▬▬▬ |
| Requests against User Agent | 0 | 0% | ▬▬ |
| Trojan files (Zeus sig) | 0 | 0% | ▬▬▬▬▬▬ |
| Explorer configuration for hidden files | 16 | 100% | ▬▬ |
| PDB path detections | 34 | 94% | ▬▬ |
| Known packers | 48 | 92% | ▬▬ |
| UPX compressed files | 59 | 98% | ▬▬ |
| Suspected packers | 184 | 93% | ▬▬ |
| Suspected packers (encryption) | 329 | 92% | ▬▬ |