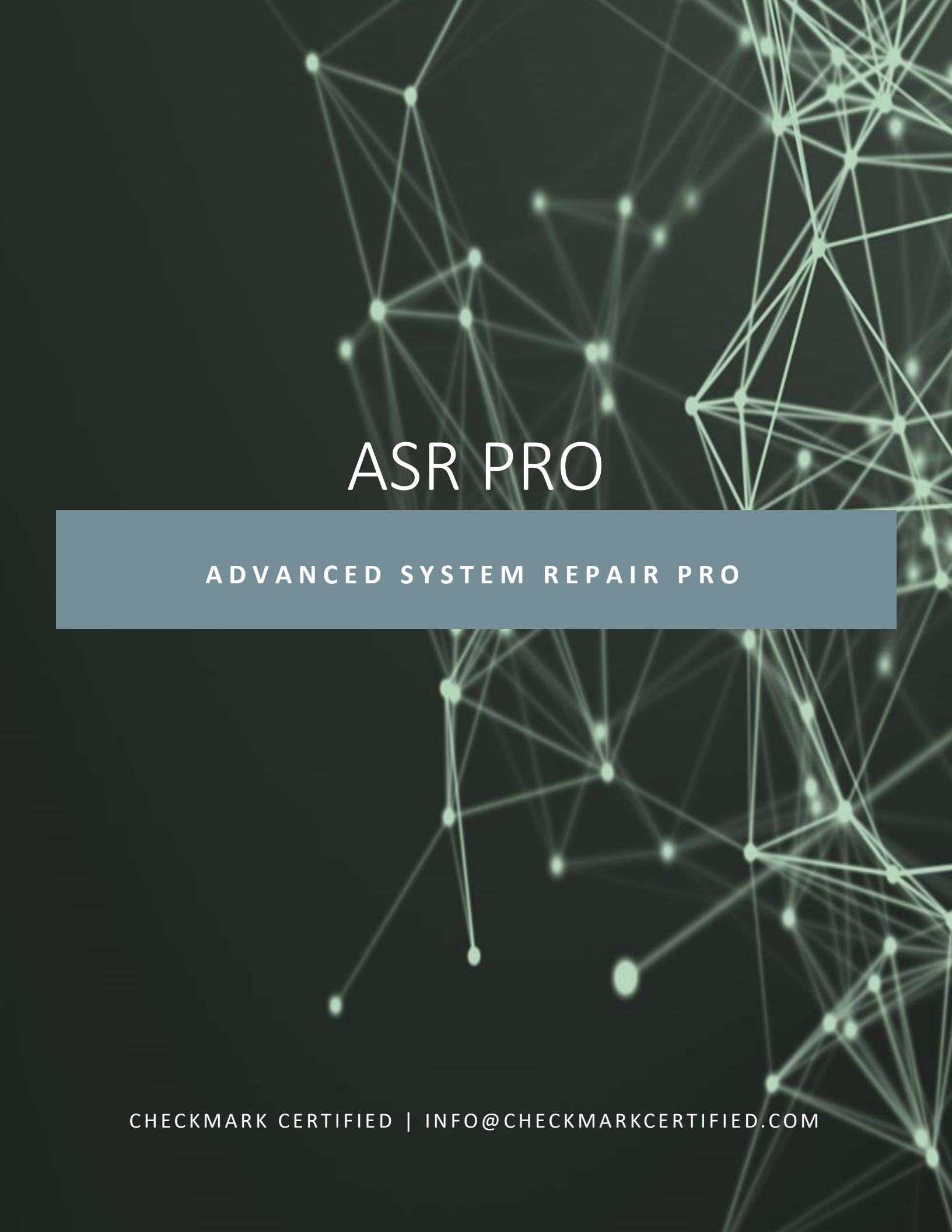


ASR PRO

ADVANCED SYSTEM REPAIR PRO

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

EXECUTIVE SUMMARY

Signature Based

- Overall Detection: 100%

Behaviour Based

- Overall Detection: 100%

SIGNATURE TESTING

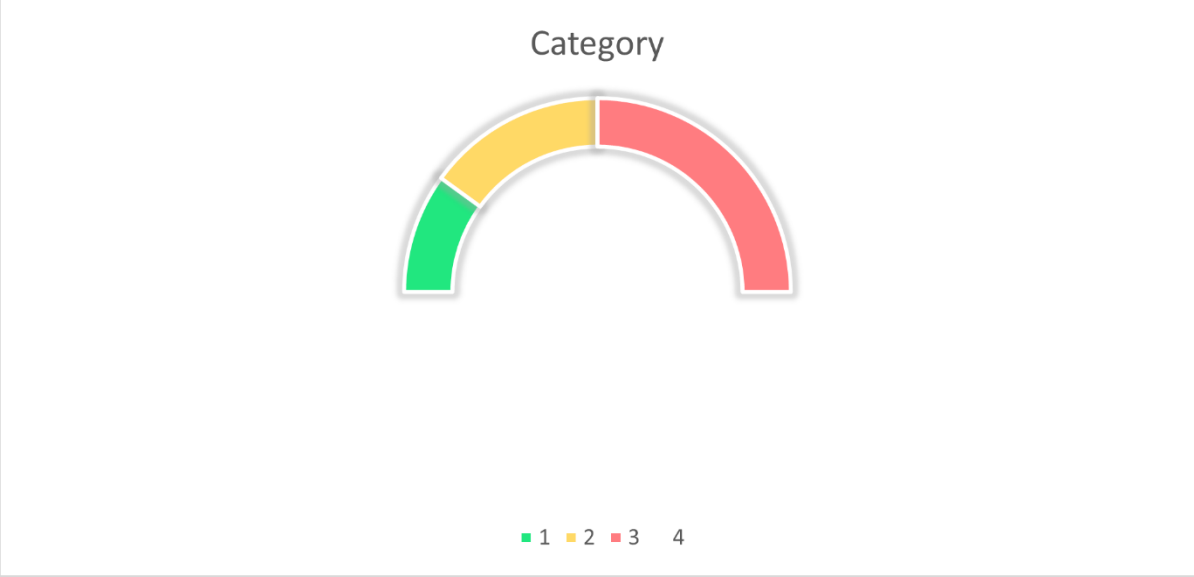
Traditional testing that examines detection capability of isolated, static malware samples. Detection is recorded at either the transfer, scanning, or interaction stages. Samples are selected from a pre-existing suite and include a variety of malware "types" not limited to trojans, spyware, data extraction,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

BEHAVIOUR TESTING

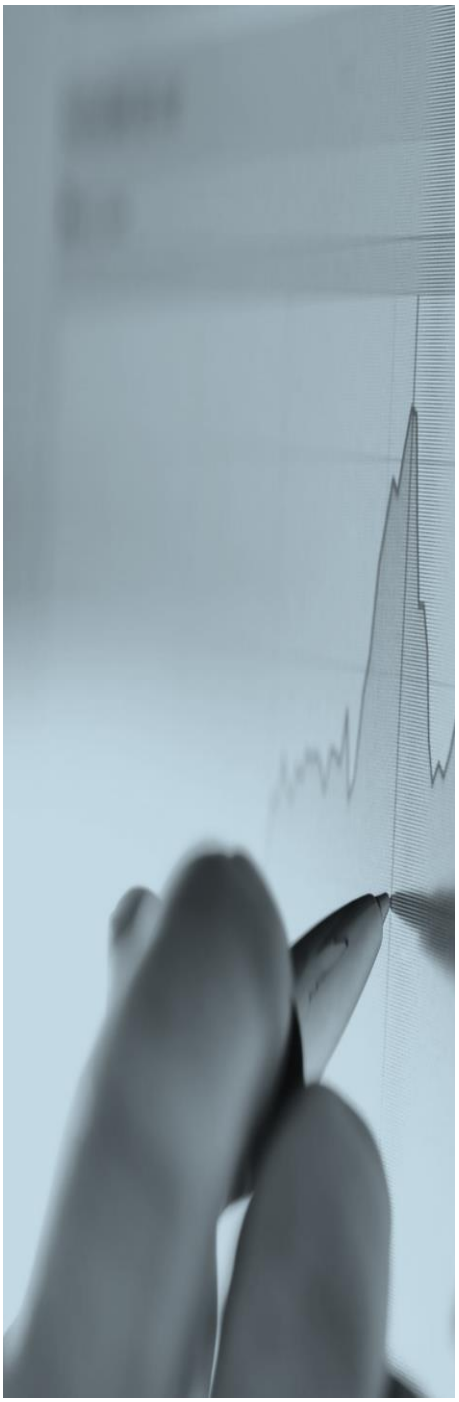
Testing focused on the isolated, individual behaviours associated with various categories of malware. Detection results are based solely on the correct identification and nullification of these behaviours and is designed to identify areas of weakness in the tested solution. Modified variations of the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

THREAT LEVEL REDUCTION

Testing that accounts for the threat level introduced by the malware and the associated threat mitigation provided by the SUT.



TEST METHODOLOGY



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

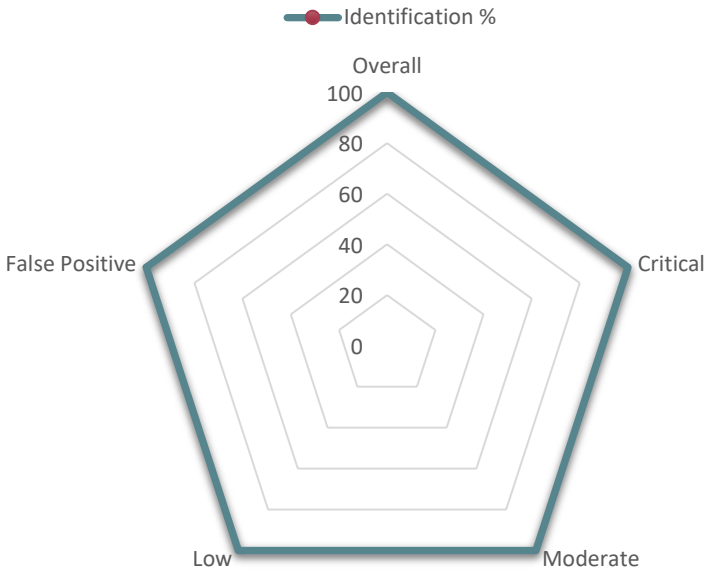
When considering an endpoint solution, the test is broken down into three phases: exposure, scanning, and execution. The exposure phase involves the initial transfer of files from source to the endpoint, with the source being direct web download, transfer from a localized source, and FTP.

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: THREAT

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?



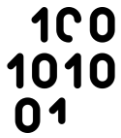
Critical	**Moderate**	**Low/PUP**	**False Positive**
Active threats that present a direct risk to the integrity of the system and user information. These will include ransomware, destructive malware, and data theft.	Malware used to create further vulnerabilities on the system or attempt to interfere with system operations.	Binaries and applications that interact with system registry and local files but that do not present a definitive risk either through design or error.	Known-good system and application files taken from genuine update and installation sources.
Result: 100%	Result: 100%	Result: 99%	Result: 100%

PROTECTION: TYPE

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?

Trojan
As used in testing, malware in this category is designated as trojan primarily by its appearance and behaviour 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.

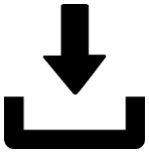


Fileless/Memory
Malware that is designed to leave no definitive trace on the system. These threats execute by the appropriation of vulnerable application access or by their exploitation.

Data Theft
Applications whose sole design is the theft of either user information or data. While similar, these threats are not limited to spyware. This category can also include file extraction.?

Destructive
Malware designed to overtly disrupt, and to cause damage to, the affected system or installed software.

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



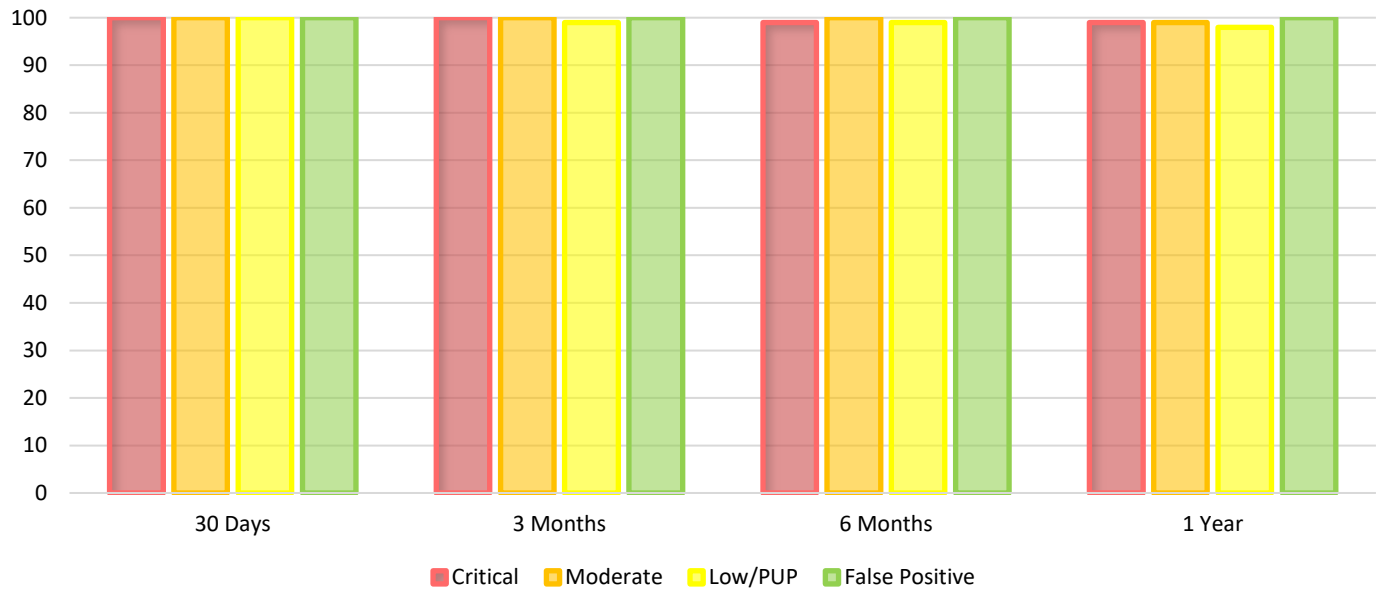
Dropper
Any threat that places new files or code on the target system that is either a threat itself or allows for further corruption of system integrity.

CHECKMARK CERTIFIED

PROTECTION: OVER TIME

Overall detection rate for the following categories over the specified period of time. Malware trends may be reflected in the detection rates, including the reclassification of one or more malware categories into a different threat level if appropriate.

Threat	30 Days	3 Months	6 Months	1 Year
Critical	100%	100%	99%	99%
Moderate	100%	100%	100%	99%
Low/PUP	100%	99%	99%	98%
False Positive	100%	100%	100%	100%



PROTECTION: BEHAVIOUR

CODE INJECTION

Behaviour	Count	Block Rate	Threat Level
Powershell Downloader DFSP	213	94%	
Potential heapspray	65	92%	
Heapspray attack on powershell	22	88%	
Code injection	123	91%	
Process searches	42	89%	
Process memory code injection	106	97%	
Buffer exploits (code injection)	94	93%	
Buffer exploits (PE file)	84	94%	
Corrupted files - services.exe	132	89%	
Corrupted files - csrss.exe	114	94%	
Process injection	206	98%	
Code injection to executed	187	86%	
Existing process memory/code	221	92%	
Modification of read-write memory	246	97%	
Read-write-execute memory	176	93%	

INSTALLERS

Behaviour	Count	Block Rate	Threat Level
Suspicious registry entry length, possible binary	106	91%	
Installed hooks for mouse	94	89%	
Loaded drivers	84	97%	
Autorun installs	132	93%	
Browser corruption	114	94%	

DATA THEFT

Behaviour	Count	Block Rate	Threat Level
Browser data theft	123	91%	
Queries for the computername	42	89%	
Keyloggers (Windows hook)	106	97%	
System fingerprint through data	94	93%	
Data capture on installed	84	94%	
Checks for the Locally Unique	132	89%	
Instant Messenger data miners	114	94%	
FTP credential capture/theft	206	98%	
Data capture of specific	187	86%	
Theft attempts of email	221	92%	
WMI system queries	246	97%	
Browser file searches	176	93%	

DROPPERS/DROPPED FILES

Behaviour	Count	Block Rate	Threat Level
Executable file written to disk by process	123	91%	
Outlook.exe used to write files	42	89%	
Mime files dropped	106	97%	
PE file foreign language	94	93%	
Dropped and executed EXE files	84	94%	
Ransomware files	132	89%	
Deletes original binary	114	94%	
Deletes executed files	206	98%	
Dropped Office docs	187	86%	
Dropped hidden/system files	221	92%	
Dropped EXE shortcuts	246	97%	
Autorun.inf files	176	93%	

RANSOMWARE

Behaviour	Count	Block Rate	Threat Level
Cerber ransomware detection	106	91%	
File deletion and/or encryption	94	89%	
TOR ransomware URLs	84	97%	
Dropped ransomware message	132	93%	
Windows utility interactions	114	94%	
Windows API crypto key	206	89%	
Encrypted ransomware files	187	94%	
Removal of system recovery files	221	98%	
Ransomware file encryption and extension	246	86%	
Dropped ransomware files	176	92%	
Encrypted files written to disk	123	97%	

SERVICE INTERACTION

Behaviour	Count	Block Rate	Threat Level
Suspicious Powershell Process	106	91%	
Potentially unwanted processes	94	89%	
Suspicious OS Processes	84	97%	
Created services	132	93%	
System process mimic	114	94%	
Running of command console	206	89%	
Service created but not started	187	94%	
Launched server	221	98%	
Injected process creates hidden window	246	86%	
Disabled system restore	176	92%	
Terminated system processes	123	97%	
Disabled task manager	42	93%	
Windows services stopped	106	91%	
Crashed processes	94	89%	
Stopped Windows services	84	97%	

GENERIC BEHAVIOURS

Behaviour	Count	Block Rate	Threat Level
Behaviour detection (Dridex sig)	123	91%	
Trojan files (Upatre sig)	42	89%	
Botnet files (Nitol sig)	106	97%	
Backdoors (Fynloski sig)	94	93%	
Banking trojan files	84	94%	
Created batch file to remove original file	132	89%	
Trojan files (Redosru sig)	114	94%	
Created Alternate Data Streams	206	98%	
Spyware files found (SpyNet sig)	187	86%	
Putty files found	221	92%	
Trojan files dropped (Bublik sig)	246	97%	
Multiple user agents detected in traffic	176	93%	
Suspicious command line tools	123	91%	
Created malware files (Hupigon	42	89%	
XtremeRAT file drop	106	97%	
Known trojan files and registry	94	93%	
Created registry keys (NJRat sig)	84	94%	
Requests against User Agent	132	89%	
Trojan files (Zeus sig)	114	94%	
Explorer configuration for hidden files	206	98%	
PDB path detections	187	86%	
Known packers	221	92%	
UPX compressed files	246	97%	
Suspected packers	176	93%	
Suspected packers (encryption)	123	91%	