Efficacy Assessment of Datto RMM Ransomware Detection

December 2020

MRG Effitas
EFFICACY ASSESSMENT & ASSURANCE

+44 (0)20 3239 9289
www.mrg-effitas.com
@mrgeffitas

Copyright © 2021 MRG Effitas Ltd.

MRG Effitas Ltd.

Effitas is a world-leading, independent IT security efficacy testing & assurance company. We are trusted by antimalware vendors across the world.

WEBSITE:
www.mrg-effitas.com
TEL:
+44 (0)20 3239 9289
EMAIL:
contact@mrg-effitas.com
TWITTER:
@mrgeffitas

Contents

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Introduction

MRG Effitas is a world-leader in independent IT security efficacy testing, research and expertise.

In the drive to protect businesses and home users from ever more advanced malicious threats, malware and viruses, our innovative research and testing helps IT security vendors to be the best they can be.

Our technical competence and insight into future trends and challenges is trusted by IT security vendors across the world.

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

About this test

Ransomware-based attacks are one of the most prevalent threat factors for all companies. As recent examples show, even the most thriving organisations can be brought to a halt with a well-planned ransomware attack (for a famous example, recall the 2017 WannaCry campaign, which brought serious disruptions to the UK health service and several other entities worldwide). With a proper behaviour-based detection and protection framework in place, such attacks can be prevented.

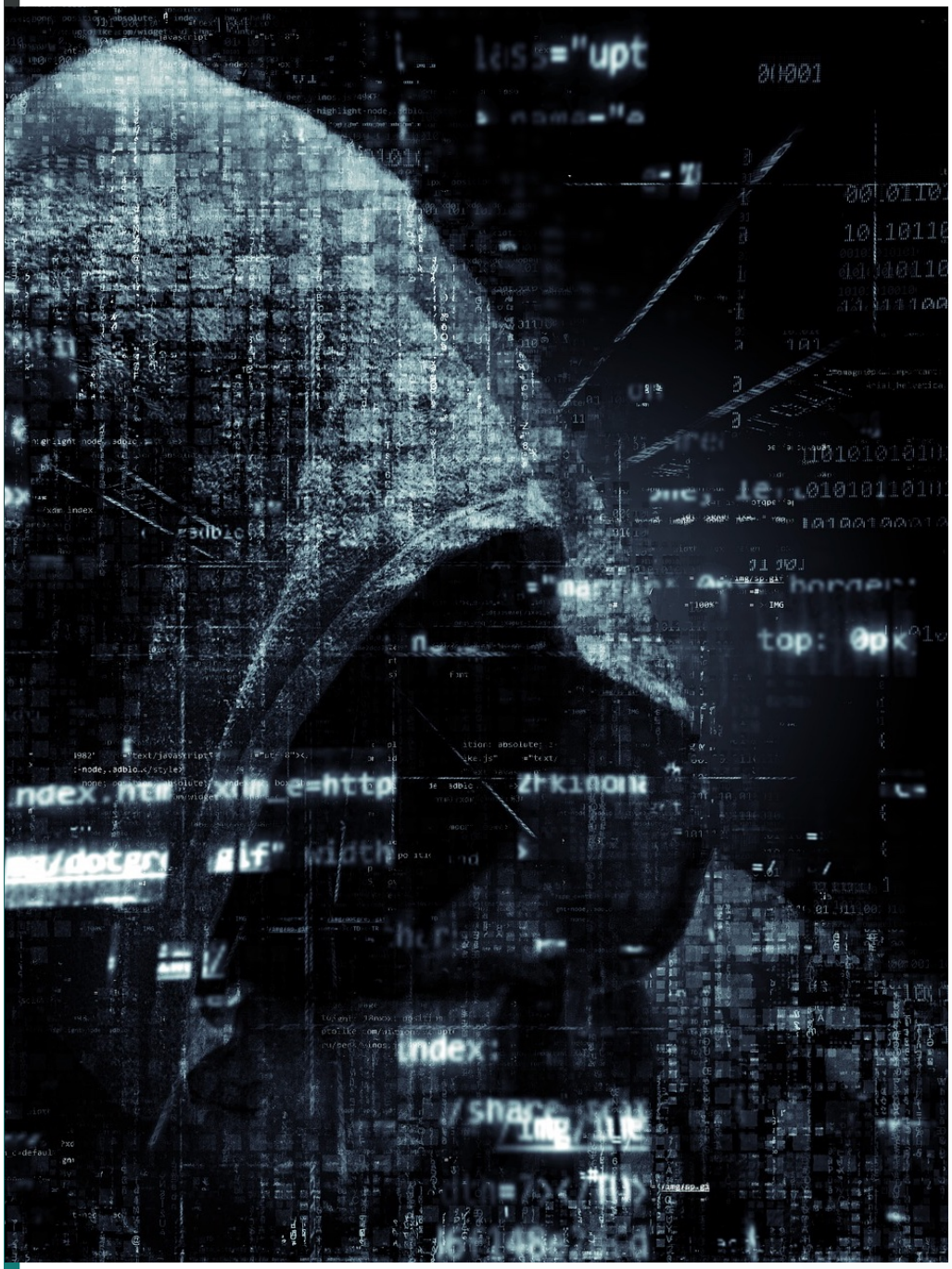
Datto approached us with the idea of a test that puts Datto's ransomware detection capabilities to the test in several respects. Besides in-the-wild ransomware samples, we carried out standard performance testing and created custom simulators to assess detection and prevention capabilities in real-life scenarios against unknown (0-hour) samples.

Testing was focused on how Datto's ransomware detection software performs in small to medium sized business (SMB) environments as managed by IT Managed Service Providers (MSPs). We evaluated several factors such as detection performance and the web console from a security analyst's perspective. The latter's aim is to detect and identify threats as soon as possible to prevent threat actors creating a scenario where their ransomware attack succeeds.

Datto does not rely on traditional signature-based detection methods, instead, the ransomware monitor product evaluates file system operations and this approach provides a platform and language-independent detection capability. In order to put this feature to the test, simulators have been created using multiple programming languages (python, C++, etc.) This approach also provides protection against unknown threats.

This report summarizes our test methodology, the samples used and our findings and insights.

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder



Executive Summary

Datto aims to provide an additional layer of protection for MSPs and SMB that may or may not have Security Operations Centre (SOC) capabilities. In its philosophy, the ransomware monitor does not attempt to be a direct competition of traditional Antivirus vendors; the monitor product is positioned complementary defense, should the AV engine fail in its detection. The capability utilises behaviour-based detection methods to prevent large-scale destruction of valuable data. As such, a small number of encrypted files is acceptable.

In order to help Datto in its efforts to provide valuable services to its clients, we performed a series of tests on several images having the latest version of Datto RW monitor. For several tests, we used traditional AV products with a significant market share alongside Datto's product – as is the expected use-case in a typical environment. Test cases have been used to find compatibility and interoperability issues of the RW monitor with common AV products, as well as to determine testing results in their own right.

1. **ITW tests.** We tested the detection capabilities using 15 in-the-wild (ITW) ransomware samples from recent campaigns.
2. **False positive tests**. We tested benign scenarios with carefully selected, benign software, which resembles ransomware activity.
3. **RW Simulator tests**. We used custom simulator samples to put detection capabilities to the test.
4. **Performance test**. We used medium-spec physical notebooks to measure any performance overhead of the RW monitor on a typical Windows 10 system.

The following report contains a detailed description of the tests, the samples and the results of our testing efforts. As we have spent considerable time with the product, we summarize our insights in terms of how the overall experience can be improved.

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Tests Employed

Throughout the test process, the following tests have been performed.

In-the-Wild Real Ransomware Test

In total, 15 live ITW ransomware attacks were used. The tests were performed using samples from families like Dharma, Ryuk, GandCrab, WannaCry, TeslaCrypt, etc.

False Positive Test

In order to test how the product handles benign, mass-file modification processes we used some common tools, such as Total Commander, photo editing software, file optimizer and disk/file encrypting applications. These applications have similar characteristics to ransomware (namely, they open a large number of files in quick succession, perform some kind of modification, and close the handles).

Ransomware Simulator Test

For the ransomware simulator test we developed in-house samples which contained valid attack methods commonly used by ransomware, implementing common evasion techniques. From a basic operation perspective, two basic kinds of ransomware are known; our tests aimed to cover them both.

- **Overwrite method**. The sample opens a file (gets a file handler pointer) and overwrites the actual content of the file. After the encryption is done, the handle is closed. In this case, the file metadata (its entry in the Master File Table NTFS metadata store[1]) remains.
- **New file creation method**. The sample opens a file (gets a file handler), reads its contents and creates a new file for the encrypted content. After the encrypted content is flushed, the original file gets deleted, its entry is removed from the MFT.

As for encryption methods, we created samples using traditional encryption methods, seen in the vast majority of ransomware incidents, as well as experimental samples using uncommon methods (such as block ciphers using 6-bytes block size).

Performance Test

During performance testing we used traditional medium-spec notebooks to measure any effect on boot-up time, browser operations, file system operations time, etc. The hardware inventory of the test notebooks reflects the capabilities of a common office workstation.

[1] For more information on how MFT works, refer to the official Microsoft documentation. A good starting point can be found on the following link. https://docs.microsoft.com/en-us/windows/win32/fileio/master-file-table

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Security Applications Tested

Throughout the test process we utilised virtualised images, equipped with the latest available version of Windows 10 and the AV software, where applicable.

Performance testing has been performed on physical laptops.

Cooperative images

Cooperative images were equipped with more than one security product.

- Datto RMM 4.4.2120.2120
- All other tested AVs were the latest versions with up to date definitions.

Standalone images

Standalone images were equipped with one single security product.

- Datto RMM 4.4.2120.2120
- All other tested AVs were the latest versions with up to date definitions.

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Test Samples

Samples used in the In-the-Wild Ransomware malware test

In total, 15 live ITW samples were used. The tests were conducted using samples from the following families.

Dharma

Once Dharma has infected a system, it creates registry entries to maintain persistence and encrypts practically every file type, while skipping system and malware files. It performs the encryption routine using a strong encryption algorithm (AES-256 combined with RSA-1024 asymmetric encryption), which is applied to fixed, removable and network drives.

Before the encryption routine, Dharma deletes all the Windows Restore Points by running the '*vssadmin delete shadows /all /quiet'* command.

On some Windows versions, it also attempts to run itself with administrator privileges, thus extending the list of files that can be encrypted.

After a successful RDP-based attack, it has been observed that before executing the ransomware payload, Dharma uninstalls security software installed on the system.

Ryuk

The sample starts by unpacking its actual payload in-memory. Once the unpacking process is done, the sample creates a copy of itself that it names with a 7-letter random name, and then places it in the same directory from which it was executed. It then invokes the new executable using "8 LAN" as the command line argument.

The initial execution of the sample focuses on encrypting files on the local machine and mapped drives, while the second invocation focuses on the encryption of network drives. This second invocation also attempts to wake machines on the network. Both invocations carry out the same steps as part of the attack, except that the original invocation also injects itself into multiple legitimate processes to run the encryption process in order to increase the chances of a successful attack.

GandCrab

The authors of this ransomware are very active and have released at least five versions of GandCrab to date. While there are no major differences between any two versions of this malware, the frequent changes show the time attackers are investing in maintaining and developing it.

GandCrab is also the first ransomware that demands payment in DASH cryptocurrency and utilizes the ".bit" top level domain (TLD). This TLD is not sanctioned by ICANN and it therefore provides an extra level of secrecy to the attackers.

During this reconnaissance, if GandCrab identifies a keyboard layout to be RUSSIAN it will terminate the execution immediately. GandCrab generates a unique Ransom-ID for each victim by calculating a CRC32 hash of the string formed by concatenating the volume serial number, processor name and processor identifier.

Buran

Buran is a new version of the Vega ransomware strain (a.k.a. Jamper, Ghost, Buhtrap) that attacked accountants from February through April 2019.

A specific trait of this ransomware is that the cryptolockers' code was written in Object Pascal in Delphi IDE. That's a programming language that was popular – mostly in Latin American and former Soviet Union countries – around two decades ago when it was being taught in colleges and technical

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

universities.

The ransomware code contains a homemade RSA algorithm implementation that does not use Fermat primes (such as 65537, the largest Fermat prime) for public exponent e.

Amnesia

Amnesia Ransomware was originally thought to be a variant of the infamous Globe Ransomware family. However, it seems it is an isolated ransomware Trojan, not based directly on an existing ransomware platform (although the code is often recycled in these attacks).

Like other ransomware Trojans, the Amnesia Ransomware uses a strong encryption algorithm to make the victim's files inaccessible. A combination of the AES and RSA encryption is used to take over the victims' files.

WannaCry

WannaCry (also known as WCry or WannaCryptor) malware is a self-propagating (worm-like) ransomware that spreads through internal networks and over the public internet by exploiting a vulnerability in Microsoft's Server Message Block (SMB) protocol, MS17-010.

The authors did not appear to be concerned with thwarting analysis, as the samples analysed have contained little if any obfuscation, anti-debugging, or VM-aware code. The malware consists of two distinct components, one that provides ransomware functionality and a component used for propagation, which contains functionality to enable SMB exploitation capabilities.

TeslaCrypt

After encrypting popular file types with the AES-256 encryption algorithm, TeslaCrypt holds the files for a ransom of $250 to $1000. The malware uses the Tor anonymity network for command and control (C2) and does not require network connectivity to encrypt files, which complicates detection, prevention, and remediation. TeslaCrypt immediately copies itself into %AppData% using a random string of seven lowercase alphabetical characters (e.g., smshdff.exe). The original copy executes this new copy and then terminates.

To ensure persistence across reboots, the malware adds a Run key to the registry.

Cerber

Cerber is one of the most widely spread ransomware families, consisting of many different variants, most of them still active to date. Its damage capabilities are extensive, targeting files and databases, and its reach is wide, as this family is part of the most important ransomware-as-a-service platforms.

Sodinokibi

Sodinokibi ransomware, also known as REvil or Sodin, has been responsible for a series of high-profile attacks since April 2019.

The ransomware will then proceed to encrypt all files on local drives, skipping files and folders included on the config's exception list. Unless the executable was run with -nolan command line parameter, the malware will also attempt to encrypt files on network shares.

Each encrypted file will be renamed by adding a previously generated pseudo-random extension, which is stored in the rnd_ext value in the registry. A README file will be dropped in each directory and the background wallpaper will be set to a ransom message.

Fonix

FONIX is a newly-observed RaaS tool created by an unnamed threat actor previously involved in selling dark web malware packers. It uses a complicated four-fold implementation to encrypt files.

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Once delivered, FONIX will attempt to encrypt all non-system files using a combination of AES, Salsa20, ChaCha, and RSA algorithms. As a result, this unusual implementation appears to function far slower than equivalent RaaS tools.

Encrypted files are appended with the XONIF extension, and a ransom note is then displayed as the desktop background.

Neshta

Neshta is an older file infector that is still prevalent in the wild. The name of the virus comes from the Belarusian word "nesta" meaning "something." The program is a written in Delphi. To achieve persistence Neshta renames itself to svchost.com then modifies the registry so it runs each time an .exe file is launched.

This threat is commonly introduced into an environment through unintentional downloading or by other malware. It infects Windows executable files and may attack network shares and removable storage devices.

Predator

The Predator Ransomware is typically delivered to the victim's computer through the use of corrupted email attachments, which use embedded macro scripts in DOCX or PDF files to download and install the Predator Ransomware onto the victim's computer. Once installed, the Predator Ransomware will use the AES encryption to make the victim's files inaccessible, marking each compromised file with the new extension '.predator.'

The Predator Ransomware's attacks have the purpose of demanding ransom payments from the victims. The Predator Ransomware delivers its ransom note in a text file named 'README.txt,' which demands a ransom payment of 100 USD in Bitcoin to a specific Bitcoin Wallet.

FTCode

FTCode is a strain of ransomware, designed to encrypt data and force victims to pay a ransom to release it. It is fully written in PowerShell, meaning that it can encrypt files on a Windows device without downloading any other components. FTCode loads its executable code only into memory, without saving it to disk, to prevent detection by antivirus.

It triggers the DownloadString function, which loads the PowerShell code into memory, without saving it to disk. It uses the PowerShell invoke expression command to execute the malicious code.

It generates a globally unique identifier and a password with 50 characters including at least four non-alphanumeric characters. A hardcoded RSA public key is used to encrypt the password, and it can be deciphered only with the attacker’s private key. However, when communicating with the command-and-control server, FTCode sends an unencrypted version of the password in base64 encoding.

HiddenTear

Hidden Tear is the first open-source ransomware trojan that targets computers running Microsoft Windows. The original sample was posted in August 2015 to GitHub.

When Hidden Tear is activated, it encrypts certain types of files using a symmetric AES algorithm, then sends the symmetric key to the malware's control servers.

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Samples used in the False Positive test

The below applications are legitimate utilities with completely benign use cases. We carefully collected them to mimic malicious ransomware behaviour as closely as possible, just to see how AV apps and Datto in conjunction with AV apps, handle them.

Windows 10 PowerToys - Batch image resize

The Image Resizer Windows 10 PowerToys adds additional functionality to File Explorer by allowing users to apply bulk image resizing.

Eraser - Erase file on disk

Eraser is an advanced security tool for Windows, which allows users to completely remove sensitive data from the hard drive by overwriting it several times with carefully selected patterns.

IrfanView - Batch image resize

Using IrfanView batch image resize functionality is a pretty straightforward way to mass modify image files, simulating false ransomware activity.

IrfanView - Batch image resize with rename

Like the batch image resize scenario, IrfanView has a batch image resize and rename functionality, which is also an excellent procedure to simulate false ransomware action.

FastStone Photo Resizer - Batch image resize

FastStone Photo Resizer is an image converter and renaming tool that intends to enable users to convert, rename, resize, etc. to images in a quick and easy batch mode. Hence, it is suitable for testing anti-ransomware tools.

FastStone Photo Resizer - Batch image resize with rename

In addition to the previous test case, FastStone Photo Resizer has the ability to resize and rename files with batch processing.

XnResize - Batch image resize

XnResize can resize many images easily with a couple of clicks in a mass modification manner, which can be interpreted by an anti-ransomware product as malicious activity.

XnResize - Batch image resize with rename

Just like the previous test case, XnResize has the ability to resize and rename files with batch processing.

Total Commander - Batch file extension change

Total Commander is one of the most common tools on Windows; most workstations have it in one version or another.

Amongst many of its features, it has a mass file modification feature, allowing batch file extension change. This can easily be interpreted as an unfortunate ransomware activity.

Total Commander - Batch file rename

Such as the former test case, batch filename modification can be an indicator of ransomware activity.

Total Commander - Batch file hash calculation then write to disk

Total Commander's batch file hash calculation method with result writing to the filename itself is another method to mass modify files which can falsely be recognized as malicious behaviour.

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

FileOptimizer - Batch file optimalization

FileOptimizer compresses files without changing any of the file's significant characteristics. Its behaviour can deceive anti-ransomware software to identify the behaviour as malicious.

CryptoForge - Batch file encryption

CryptoForge, from Ranquel Technologies, is designed to encrypt files and folders for their protection. Its behaviour strongly suggests that a cryptographic process is happening, which qualifies this test false positive case for a difficult procedure to distinguish from a valid ransomware attack.

Jetico BestCrypt - Batch file encryption

Jetico BestCrypt can use a wide variety of block cipher algorithms including AES, Serpent, Blowfish, etc. to encrypt files on the user's demand to protect one's privacy. These ciphers are also used by ransomware to perform undesired activities. These characteristics make this test case one of the hardest to distinguish from valid ransomware behaviour.

Jetico BestCrypt - Batch file wiping

File wiping function of Jetico BestCrypt is designed to selectively remove all traces of any file beyond recovery. This behaviour can easily be mistaken with any wiper or ransomware behaviour.

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Samples used in the Ransomware Simulator test

Test case “ransomware_onyx_newfile.mrg”

SHA256: 13376f9911d9d83921501bfd33ec83854014d11f9bc3441f717616a5bd8e574c

OnyxLocker is a proof-of-concept ransomware written in the C# language using the .NET framework.

The test malware encrypts the user documents by creating a new encrypted file and deleting the original. Newly created filenames will have additional extensions like .onyx, .locked, .crypted.

Test case “ransomware_onyx_rename.mrg”

SHA256: d8dcedd0390c5af156e15ade36506244f0ba78986671ea407230052560396296

Just like the previous test case, OnyxLocker is a proof-of-concept ransomware written in the C# language using the .NET framework.

The test malware first encrypts the victim's file in place then appends the extensions like .onyx, .locked, .crypted.

Test case “ransomware_hiddentear_rename.exe”

SHA256: 6cd56746be90d78472f67a86a4de2347270ff243f76d4e0af44a3de4dc362dce

HiddenTear is a proof-of-concept ransomware written in the C# language using the .NET framework.

The test malware first encrypts the victim's file in place then appends the extensions like .onyx, .locked, .crypted.

Test case “ransomware_hiddentear_newfile_2.mrg”

SHA256: 828923e86fdf43811e35e9040d03aa6cf8913ed91c5ffbb9daad906edc4af733

HiddenTear is a proof-of-concept ransomware written in the C# language using the .NET framework.

The test malware encrypts the user documents by creating a new encrypted file and deleting the original. Newly created filenames will have additional extensions like .onyx, .locked, .crypted.

Test case “ransomware_powershell_newfile.zip”

SHA256: fd61bf34451024daaa290bae3893313a944d49bda00fa837fc2662bc3ee87317

We created a proof-of-concept test PowerShell script to simulate ransomware activities. The product should have to block the application before it finishes its activities.

The test malware encrypts the user documents by creating a new encrypted file and deleting the original. Newly created filenames will have additional extensions like .onyx, .locked, .crypted.

Test case “ransomware_powershell_rename.zip”

SHA256: 6b200fd7934b2e730e0ee450ca8de77058149869c5e077eb7bf3c353ab1245b7

Based on the previous test case. We created a proof-of-concept test PowerShell script to simulate ransomware activities. The product should have to block the application before it finishes its activities.

The test malware first encrypts the victim's file in place then appends the extensions like .onyx, .locked, .crypted.

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Experimental Ransomware Simulator tests

Test case “ransomware_python_newfile.mrg”

SHA256: ec4ab943cea6c987774629535b18685a9c065a704713973a83d674e2216d0d61

We created a proof-of-concept test application based on python and pyinstaller to simulate ransomware activity. The product has to block the application before it finishes its activities.

The test malware encrypts the user documents by creating a new encrypted file and deleting the original. Newly created filenames will have additional extensions like .onyx, .locked, .crypted. Note that this simulator utilises unconventional cryptographic primitives.

Test case “ransomware_python_rename.mrg”

SHA256: dcdfb49aabf5bbf622a13f2282e526aa1344d02bf76e5518df56a6fe400d1487

We created a proof-of-concept test application based on python and pyinstaller to simulate ransomware activities. The product should have to block the application before it finishes its activities.

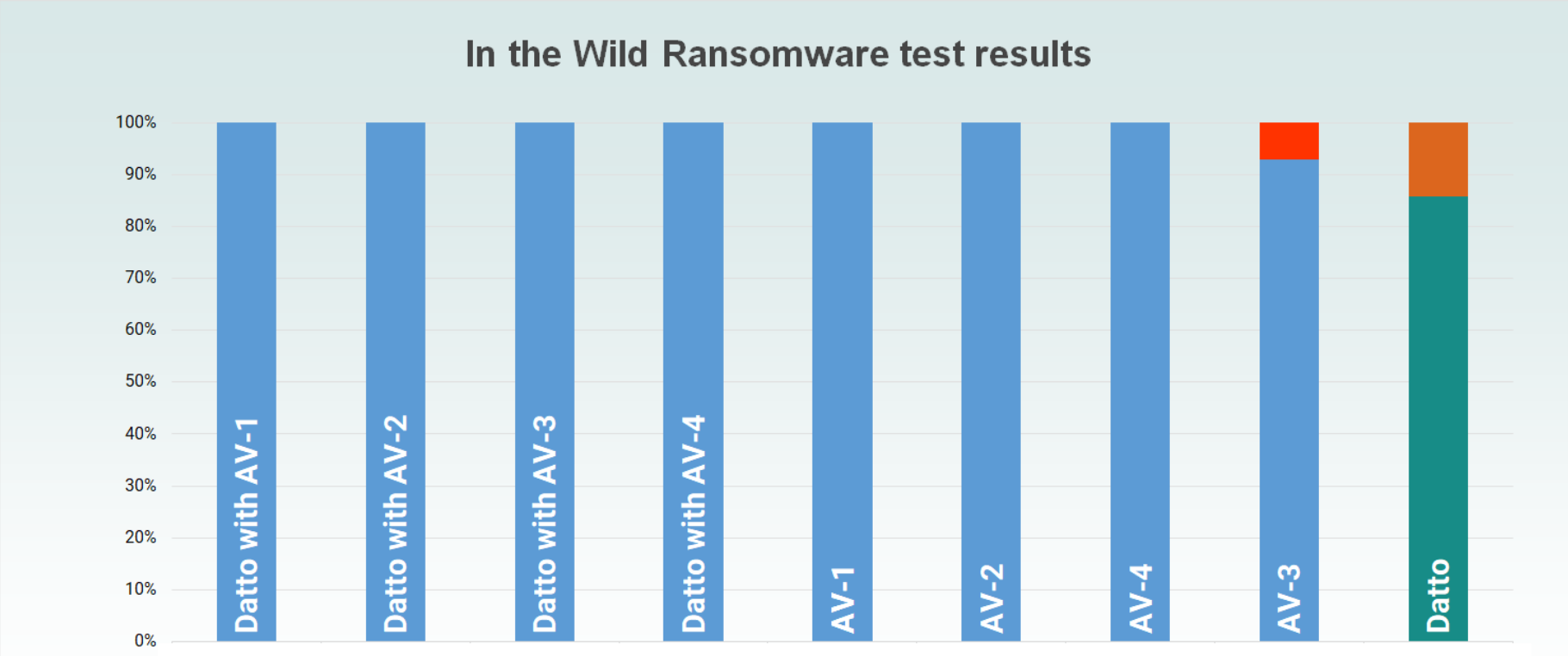
The test malware first encrypts the victim's file in place then appends the extensions like .onyx, .locked, .crypted. Note that this simulator utilises unconventional cryptographic primitives.

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Test Results[2]

In-the-Wild Ransomware test results

The table below shows the results of testing using In-the-Wild Ransomware.



	Datto with AV-1	Datto with AV-2	Datto with AV-3	Datto with AV-4	AV-1	AV-2	AV-4	AV-3	Datto
Missed	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	7.14%	0.00%
Detected	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	14.29%
Blocked by AV	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	92.86%	0.00%
Blocked by Datto	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	85.71%

[2] For a detailed explanation on what the individual categories mean, refer to Appendix A.

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Detailed results of the In-the-Wild Ransomware test

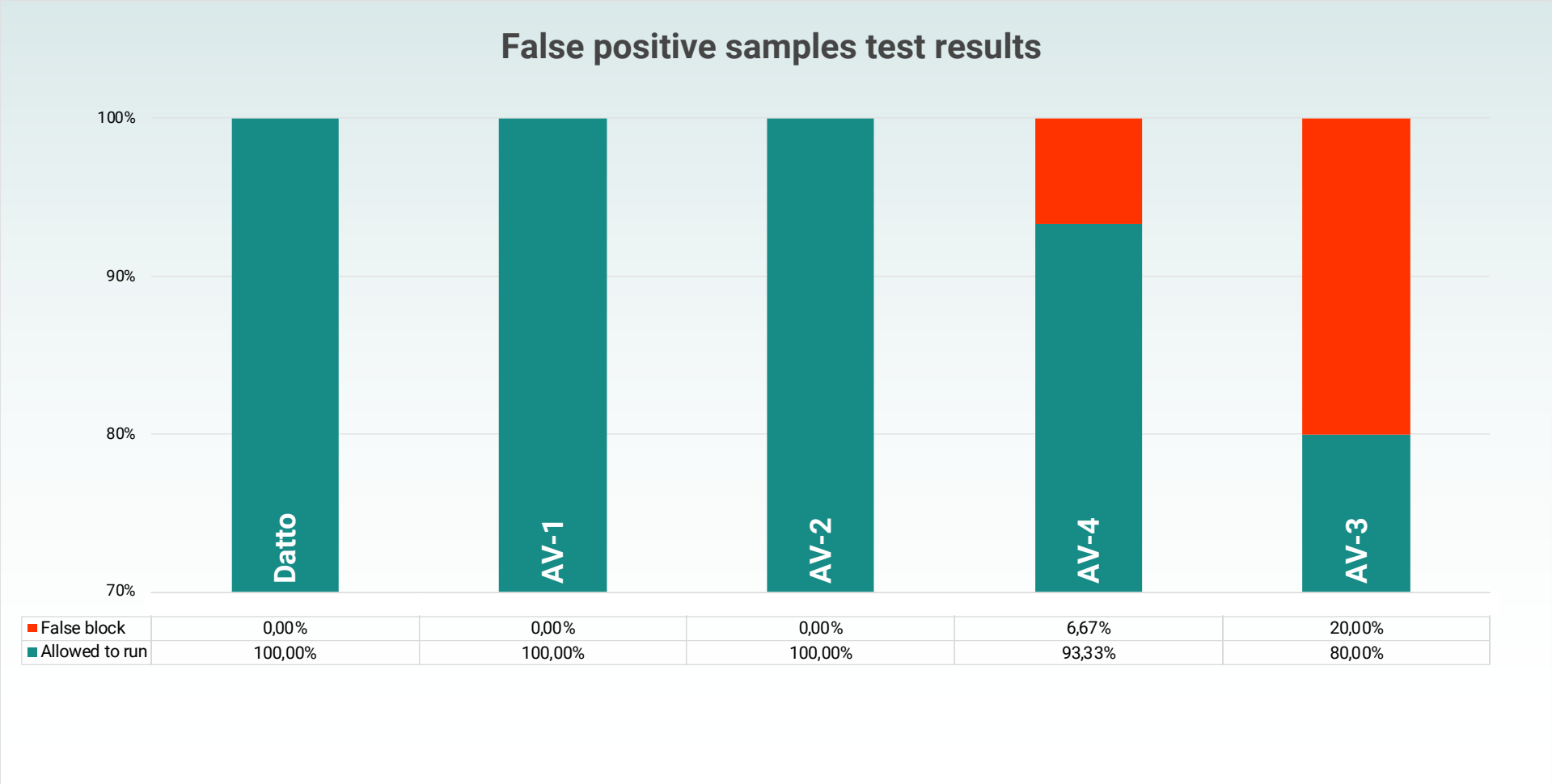
The table below shows the detailed results of the In-the-Wild Ransomware test. This table is sorted alphabetically.

	Datto	Datto with AV-1	Datto with AV-2	Datto with AV-3	Datto with AV-4	AV-1	AV-2	AV-3	AV-4
Dharma (34c485ad11076ede709ff409c0e1867dc50fd40311ae6e7318ddf50679fa4049)	Blocked by Datto	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV
Neshta.a (afba1763b57889eaa1cd6fd35a34880cdeb25b7bd120a867e2bf79f0de18c560)	Detected	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV
Ryuk (102c242eafbbc9cbd29348814941310e39fa2f296c4f85827c13bda177de4db1)	Blocked by Datto	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV
HiddenTear (fe64d14dec32a2e5d48f0af40e74b1be744e781359429ab18066626947463adb)	Blocked by Datto but not alerted	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Missed	Blocked by AV
GandCrab (78ff7ca1dd8b2821ecc7d09cde5537a18d890d001300b7442eeb25fff204caf7)	Blocked by Datto	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV
Buran (29cdd5206422831334afa75c113b615bb8e0121254dd9a2196703ce6b1704ff8)	Blocked by Datto	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV
Amnesia (26690dae115f47a1e0167750209a30cc68f51c5090e3b908105c93967e5156fa)	Blocked by Datto	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV
WannaCry (149601e15002f78866ab73033eb8577f11bd489a4cea87b10c52a70fdf78d9ff)	Detected	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV
TeslaCrypt (9b462800f1bef019d7ec00098682d3ea7fc60e6721555f616399228e4e3ad122)	Blocked by Datto	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV
Cerber (272e46f6cb9c3045b19f956b77758f90ab69b420a1a2787438790d5d76d69a1a)	Blocked by Datto	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV
Sodinokibi (142d55646ed59b488eaf27b98d7cbbba1b97d07a954822ef02f66f563c60e311)	Blocked by Datto	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV
Predator (1e8d75a4728b7dfb07fe15971fb352ce1cfda32c3f9f055770a37bb49a1b3d8d)	Blocked by Datto	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV
Fonix (5263c485f21886aad8737183a71ddc1dc77a92f64c58657c0628374e09bb6899)	Blocked by Datto	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV
VBS.Vshell - FTCode (750d967eed9f13868d413444fd3176c904c0ab410c50bffc68ea568c00aa4ffb)	Blocked by Datto	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

False positive test results

The table below shows the results of testing using False positive methods.



	Datto	AV-1	AV-2	AV-4	AV-3
False block	0,00%	0,00%	0,00%	6,67%	20,00%
Allowed to run	100,00%	100,00%	100,00%	93,33%	80,00%

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Detailed results of the False Positive test

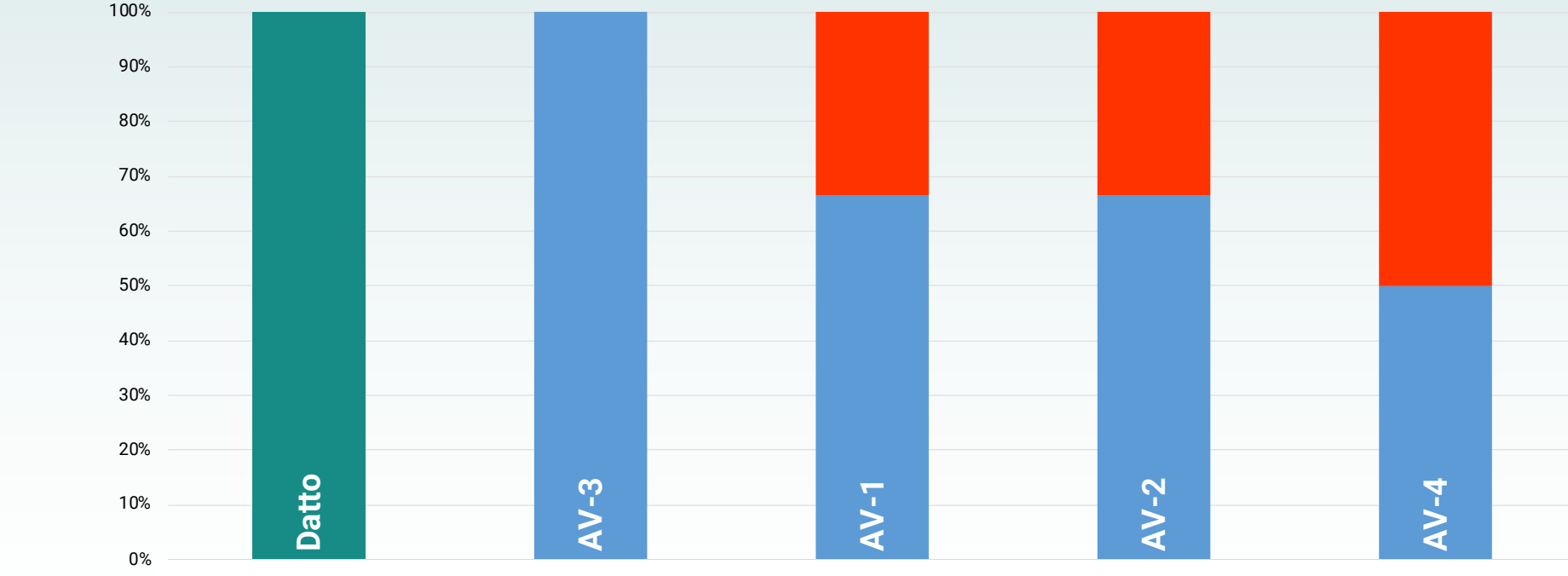
The table below shows the detailed results of the False positive test. This table is sorted alphabetically.

	Datto	AV-1	AV-2	AV-3	AV-4
Windows 10 PowerToys - Batch image resize	Allowed to run	Allowed to run	Allowed to run	Allowed to run	Allowed to run
Eraser - Erase file on disk	Allowed to run	Allowed to run	Allowed to run	Allowed to run	Allowed to run
IrfanView - Batch image resize	Allowed to run	Allowed to run	Allowed to run	Allowed to run	Allowed to run
IrfanView - Batch image resize with rename	Allowed to run	Allowed to run	Allowed to run	Allowed to run	Allowed to run
FastStone Photo Resizer - Batch image resize	Allowed to run	Allowed to run	Allowed to run	Allowed to run	Allowed to run
FastStone Photo Resizer - Batch image resize with rename	Allowed to run	Allowed to run	Allowed to run	Allowed to run	Allowed to run
XnResize - Batch image resize	Allowed to run	Allowed to run	Allowed to run	Allowed to run	Allowed to run
XnResize - Batch image resize with rename	Allowed to run	Allowed to run	Allowed to run	Allowed to run	Allowed to run
Total Commander - Batch file extension change	Allowed to run	Allowed to run	Allowed to run	Allowed to run	Allowed to run
Total Commander - Batch file rename	Allowed to run	Allowed to run	Allowed to run	Allowed to run	Allowed to run
Total Commander - Batch file hash calculation then write to disk	Allowed to run	Allowed to run	Allowed to run	Allowed to run	Allowed to run
FileOptimizer - Batch file optimalization	Allowed to run	Allowed to run	Allowed to run	Allowed to run	Blocked
CryptoForge - Batch file encryption	Allowed to run	Allowed to run	Allowed to run	Blocked	Allowed to run
Jetico BestCrypt - Batch file encryption	Allowed to run	Allowed to run	Allowed to run	Blocked	Allowed to run
Jetico BestCrypt - Batch file wiping	Allowed to run	Allowed to run	Allowed to run	Blocked	Allowed to run

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Ransomware Simulator test results

The table below shows the results of testing using Ransomware Simulator test results.



	Datto	AV-3	AV-1	AV-2	AV-4
Missed	0,00%	0,00%	33,33%	33,33%	50,00%
Blocked by AV	0,00%	100,00%	66,67%	66,67%	50,00%
Blocked by Datto	100,00%	0,00%	0,00%	0,00%	0,00%

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Detailed results of the Ransomware Simulator test

The table below shows the detailed results of the Ransomware Simulator test. This table is sorted alphabetically.

	Datto	AV-1	AV-2	AV-3	AV-4
ransomware_onyx_newfile.mrg (13376f9911d9d83921501bfd33ec83854014d11f9bc3441f717616a5bd8e574c)	Blocked by Datto	Blocked by AV	Blocked by AV	Blocked by AV	Missed
ransomware_onyx_rename.mrg (d8dcedd0390c5af156e15ade36506244f0ba78986671ea407230052560396296)	Blocked by Datto	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV
ransomware_powershell_newfile.zip (fd61bf34451024daaa290bae3893313a944d49bda00fa837fc2662bc3ee87317)	Blocked by Datto	Missed	Missed	Blocked by AV	Missed
ransomware_powershell_rename.zip (6b200fd7934b2e730e0ee450ca8de77058149869c5e077eb7bf3c353ab1245b7)	Blocked by Datto	Missed	Missed	Blocked by AV	Missed
ransomware_hiddentear_rename.exe (6cd56746be90d78472f67a86a4de2347270ff243f76d4e0af44a3de4dc362dce)	Blocked by Datto	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV
ransomware_hiddentear_newfile_2.mrg (828923e86fdf43811e35e9040d03aa6cf8913ed91c5ffbb9daad906edc4af733)	Blocked by Datto	Blocked by AV	Blocked by AV	Blocked by AV	Blocked by AV

Detailed results of the Experimental Ransomware Simulator test

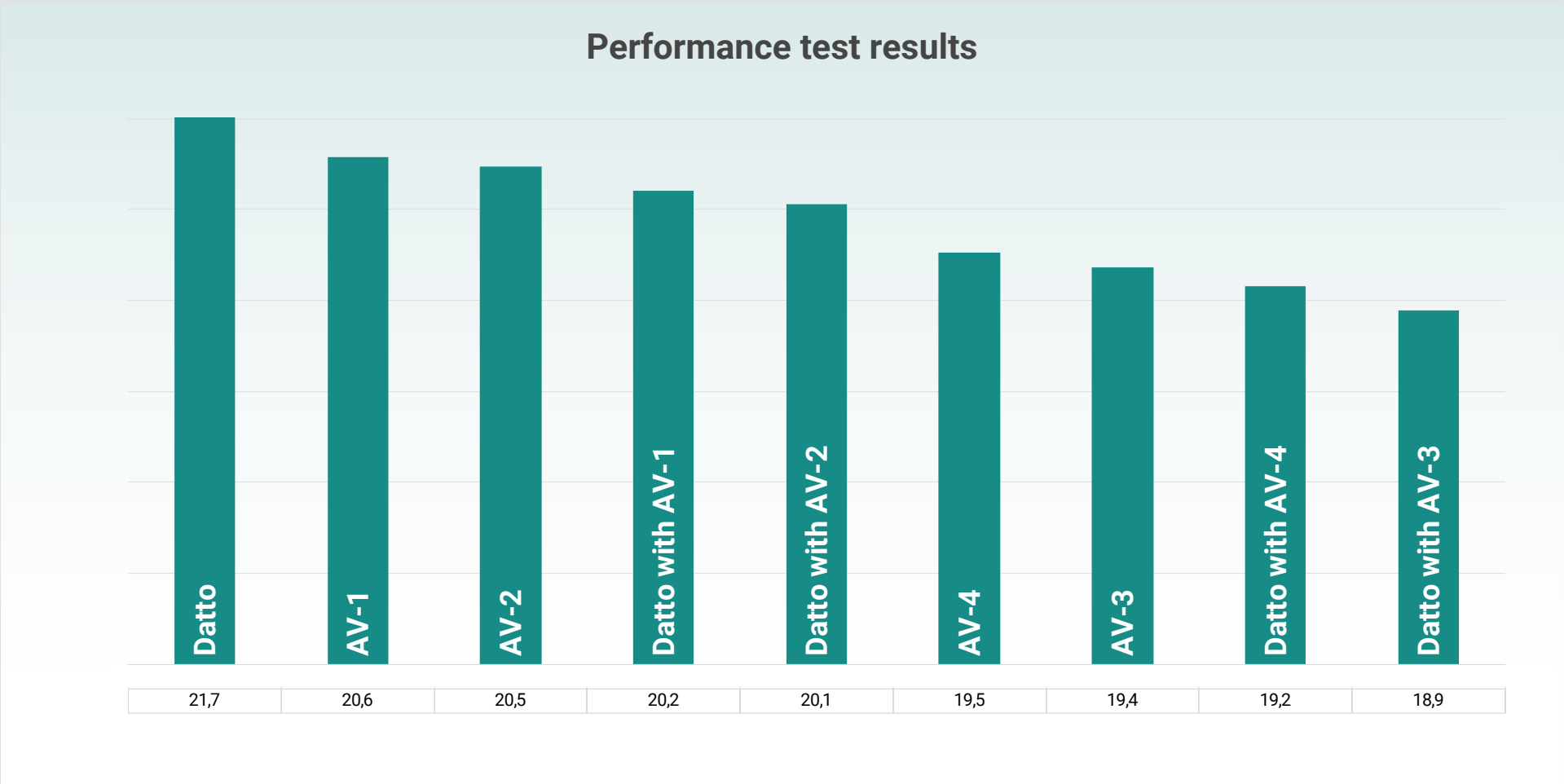
The table below shows the detailed results of the Experimental Ransomware Simulator test. This table is sorted alphabetically.

	Datto	AV-1	AV-2	AV-3	AV-4
ransomware_python_newfile.mrg (ec4ab943cea6c987774629535b18685a9c065a704713973a83d674e2216d0d61)	Missed	Blocked by AV	Blocked by AV	Missed	Missed
ransomware_python_rename.mrg (dcdfb49aabf5bbf622a13f2282e526aa1344d02bf76e5518df56a6fe400d1487)	Missed	Blocked by AV	Blocked by AV	Blocked by AV	Missed

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Performance test results

The table below shows the results of testing using Performance test results.



Scoring details can be found in "Appendix D".

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Detailed results of the performance test

The table below shows the detailed results of the performance test of the security products. This table is sorted alphabetically.

	Windows 10 Base	Datto	Datto with AV-1	Datto with AV-2	Datto with AV-3	Datto with AV-4	AV-1	AV-2	AV-3	AV-4
Bootup time (s)	29,6	33,4	34,8	36,5	53,6	42,5	31,0	34,7	49,8	38,7
Security software size on disk (Mb)	n/a	233,4	652,9	2719,2	2184,0	364,0	419,5	2485,8	1950,6	130,6
Browser Operations (s)										
Website Open	1,7	2,3	2,0	3,6	3,1	2,5	2,5	3,7	3,6	3,0
File Download	10,1	10,2	10,8	12,4	18,2	11,2	10,6	12,2	18,1	11,0
File Operations (s)										
File Copy	1,5	1,9	2,0	2,1	1,9	2,6	2,2	2,2	1,8	2,8
File Compression	36,3	36,9	37,2	38,0	38,2	37,4	37,5	37,4	38,5	37,8
Archive Extraction	5,0	5,4	7,5	5,7	17,2	5,5	8,2	5,6	17,8	6,1
Office File Opening (s)										
Excel	6,2	6,4	6,5	6,4	8,2	7,5	6,4	6,4	8,1	7,3
Word	2,4	2,4	2,5	2,5	3,3	2,9	2,5	2,5	3,3	2,9
Security software update										
Time (s)	n/a	n/a	23,0	31,7	67,3	n/a	23,0	31,7	67,3	n/a
CPU usage (%)	n/a	n/a	37,7	36,9	26,8	n/a	37,7	36,9	26,8	n/a
Memory usage (Mb)	n/a	n/a	11,7	171,6	454,6	n/a	11,7	171,6	454,6	n/a
Physical disk usage (%)	n/a	n/a	13,0	62,5	8,2	n/a	13,0	62,5	8,2	n/a
Network interface usage (B/s)	n/a	n/a	178351,5	74494,3	7998,5	n/a	178351,5	74494,3	7998,5	n/a
Security software scanning - C:\										
Time (s)	n/a	n/a	818,7	206,0	618,0	586,0	818,7	206,0	618,0	586,0
CPU usage (%)	n/a	n/a	67,1	27,8	29,1	45,5	67,1	27,8	29,1	45,5
Memory usage (Mb)	n/a	n/a	430,1	68,2	739,8	105,4	430,1	68,2	739,8	105,4
Physical disk usage (%)	n/a	n/a	26,6	17,6	8,6	23,4	26,6	17,6	8,6	23,4
Network interface usage (B/s)	n/a	n/a	621,0	1363,2	1103,2	27781,7	621,0	1363,2	1103,2	27781,7

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Difficulties and issues

During testing, several technical difficulties and issues have been encountered. Some of the issues have been sorted out prior to the closure of this report, others are still under active investigation. Due to time constraints, this section summarizes the problems and highlights the aspects that require some further investigation.

Compatibility issues between AV-4 and Datto RW monitor

The issue was raised during the Datto RW Simulator test. Upon running the test batch, we noticed that we received more missed samples from the Datto + AV-4 Image than we did from the solo Datto image. A quick cross-check was done to make sure that the machine reported back to the Console. During this quick check, the Datto client seemed to work normally. The monitor was active, and all updates were applied through the central console.

After 24 hours, a re-test was carried out. As the samples were already known by AV-4, all the samples were now blocked by AV-4. We tried suspending/disabling AV-4 in the image to allow Datto to recover or to find compatibility issues – as Datto in its solo image was able to successfully detect the now-missed samples. After doing so, we were unable to repair the Datto client, indicating that AV-4 took a rather unconventional method and basically made it impossible for the Datto RW monitor to operate.

As a result, it was concluded that there was a possible compatibility issue as we did not experience any kind of compatibility issues in other images.

Recommendations
In our opinion, further investigation is needed, and potential AV originated incompatibilities need to be taken into account when designing tests for the RW monitor app.

Blue Screen of Death (BSOD) issues

We found some cases where a BSOD occurred.

Having a thorough analysis regarding these test cases, we found the following root causes:

Scenario 1. Termination of critical system processes

BSOD regularly occurred when Datto tried to kill a RW process that called or hooked into a system-critical process, thus Datto was trying to kill a critical process. Our suspicion on this case is quite strong, despite the fact that BSOD events were not 100% reproducible.

This might be due to the fact that a typical ransomware operation is a multi-stage process and Datto's protective measures can kick in before or after a successful process injection step. This theory is backed up by the fact that on the GUI console, we regularly saw misdetections in process names of hooking samples.

Scenario 2. Potential AV-3 and Datto incompatibility

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Another set of BSOD events took place in the Datto + AV-3 image. Having checked the logs, we found that the BSOD took place when both the AV (AV-3) and Datto tried to terminate the same process roughly at the same time.

Recommendations

In our opinion, some further investigation is necessary. All logs, samples and other relevant information has been provided to Datto.

Alert management

Our team consists of professionals with a significant amount of hands-on Security Operations Centre (SOC) environment experience. In such use cases, should a threat notification arrive, analysts aim to identify and assess the risk as soon as possible and any software needed to be used in a smooth and efficient fashion must ensure quick and intuitive access to relevant information regarding newly-detected threats.

During testing, we had a chance to use both the web dashboard and the on-device agent and found that the single most counterintuitive feature is that for a given workstation, an alert needs to be manually resolved by an administrator before another alert can be registered. In our opinion, this behaviour, while understandable in its objective not to overwhelm analysts with an excessive number of alerts, can do more harm than good in practical scenarios. Specifically, this behaviour makes it really hard (even impossible) to create a timeline of events as is the standard procedure after an incident in an SOC.

Furthermore, in a multi-stage attack scenario, valuable information might be lost after the initial detection. Considering the fact that there is no visual feedback on the client, a sophisticated social engineering attack might even continue, despite a successful detection of the first stage.

Recommendations

We recommend a re-work of the alert management framework.

1. Provide visual feedback on the client machines, should a detection occur and inform the user about the risk.
2. Provide means to collect alerts even after the first notifications.

Web dashboard UX issues

As an overall experience, the console GUI could use some improvements to be used in a focused and streamlined fashion.

Our analysts were focusing on triaging detections and tracking down each sample that has been started on our victim VMs, which is a rather typical use case. As it turned out, a couple of simple changes could make the GUI way more straightforward in SOC-type environments.

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Recommendations

We recommend addressing the following problems.

1. In the new GUI, we could not find how to list resolved alerts. As a workaround, we utilised the old GUI, which is quite a bit more straightforward.
2. It is hard to identify the path of the initial link in the infection chain. Related information can be found in the diagnostic summary section, however, should the sample inject itself into another process as part of the infection, the detection notes the host process, instead of the actual executable (for instance, the analyst will have to manually try to analyse the workstation to find out which process injected into WmiPrvSE, which is a system process).
3. In order to make triaging easier, we recommend displaying the unique alert ID and other details of the actual incident on a more prominent place. Currently, essential information is missing from the GUI and we had to resort to timestamp correlation analysis, a highly cumbersome and unreliable process.

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Appendix

A: Methodology used in the “In-the-Wild Ransomware” test

1. Windows 10 Enterprise 64-bit operating system is installed on a hardened virtual machine, all updates are applied, and third-party applications installed and updated.
2. An image of the operating system is created.
3. A clone of the imaged systems is made for each of the security applications used in the test.
4. An individual security application is installed using default settings on each of the systems created in (3) and then, where applicable, updated. If the vendor provided a non-default setting, we check that this setting is realistic. If yes, the changes are documented, applied, and added to the appendix section of the report.
5. A clone of the system as at the end of (4) is created.
6. Downloading a single binary executable from its native URL using Chrome to the Downloads folder and then executing the binary in the clean, unprotected system. If the sample works, the sample is saved in a replay proxy to provide the same binary throughout the test.
7. The sample is selected for the test and tested in the systems where a security product is installed.
    - **The test case is marked as “Blocked by Datto”** where the malicious binary could have been executed and it was blocked by the Datto product.
    - **The test case is marked as “Blocked by AV”** where the security application blocked the malicious binary whilst it was being downloaded to the desktop or before it could have been executed.
    - **The test case is marked as “Detected**” if the sample was allowed to run and was not blocked by the security application or the Datto product, but an alert was raised in DRMM.
    - **The test case is marked as “Missed”** if either security application fails to block or detect the malicious sample.
8. Tests were conducted with all systems having internet access.

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

B: Methodology used in the “False Positive Test”

1. Windows 10 Enterprise 64-bit operating system is installed on a hardened virtual machine, all updates are applied, and third-party applications installed and updated.
2. An image of the operating system is created.
3. A clone of the imaged systems is made for each of the security applications used in the test.
4. An individual security application is installed using default settings on each of the systems created in (3) and then, where applicable, updated. If the vendor provided a non-default setting, we check whether this setting is realistic. If yes, the changes are documented, applied, and added to the appendix section of the report.
5. A clone of the system as at the end of (4) is created.
6. False-positive test application is downloaded and installed to the machine if needed.
7. The test is performed according to the description of the test case.
8. The sample is selected for the test and tested in the systems where a security product is installed.
    - **The test case is marked as "Allowed to run"** if the sample was not blocked or detected as a malicious one**.**
    - **The test case is marked as "False block"** if the security application blocked or detected the sample application as malicious.
9. Tests were conducted with all systems having internet access.

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

C: Methodology used in the “Ransomware Simulator Test”

1. Windows 10 Enterprise 64-bit operating system is installed on a hardened virtual machine, all updates are applied, and third-party applications installed and updated.
2. An image of the operating system is created.
3. A clone of the imaged systems is made for each of the security applications used in the test.
4. An individual security application is installed using default settings on each of the systems created in (3) and then, where applicable, updated. If the vendor provided a non-default setting, we checked whether this setting is realistic. If yes, the changes are documented, applied, and added to the appendix section of the report.
5. A clone of the system as at the end of (4) is created.
6. Downloading a single binary executable from an in-house generated URL using Chrome to the Downloads folder and then executing the binary in one of our clean, unprotected test environments. If the sample works, the sample is saved in a replay proxy to provide the same binary throughout the test.
7. The sample is selected for the test and tested in the systems where a security product is installed.
    - **The test case is marked as “Blocked by Datto”** where the malicious binary could have been executed and it was blocked by the Datto product.
    - **The test case is marked as “Blocked by AV”** where the security application blocked the malicious binary whilst it was being downloaded to the desktop or before it could have been executed.
    - **The test case is marked as “Detected”** if the sample was allowed to run and was not blocked by the security application or the Datto product, but an alert was raised in DRMM.
    - **The test case is marked as “Missed”** if either security application fails to block or detect the malicious sample.
8. Tests were conducted with all systems having internet access.

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

D: Methodology used in the “Performance Test”

1. Windows 10 Enterprise 64-bit operating system is installed on a physical machine, all updates are applied, and third-party applications installed and updated.
2. A backup image of the operating system is created.
3. The security application is installed, with the same configuration used in the other tests.
4. The following performance metrics are measured:
    - Operating system boot time
    - Size of the files installed and created by the security application. The size is measured at least one week after the installation, after virus definition updates, scans, and time passed with normal computer usage.
    - Copy time of files
    - Archive operation time
    - Opening time for (clean) files in Office applications
    - Downloading files via browser
    - Website loading time in browser. The browser should fully load a popular, complex website, from a local network URL or replay proxy to eliminate network latency.
    - AV product update time
    - System disk scan time

Every performance result is a calculated average of at least three measurements.

Performance score calculation

- The security product reaching the best result in the category was rewarded with 8 points, the second received 7 points and so on. Once every performance category was measured, the points were added together and the final calculation was made by dividing the summarized points by the number of tests the product’s result could have measured.

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Physical machine specification

- OS: Windows 10 x64
- CPU: Intel Core i5
- Memory: 8GB
- Storage: 100GB SSD

Hardened virtual machine specification

- OS: Windows 10 x64
- CPU: 2 core processor
- Memory: 4GB
- Storage: 100GB SSD

Copyright © 2021 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder