COMSEC Group
Cyber & Information Security



SECURITY PERFORMANCE TEST REPORT

FOR

NYOTRON
SECURING THE WORLD

VERSION: 0.92
DATE: SUNDAY, 28 JULY 2016

Limitations on Disclosure and Use of This Report

This report contains information concerning Paranoid performance and potential vulnerabilities.

Comsec Consulting recommends that special precautions be taken to protect the confidentiality of both this document and the information contained herein.

Vulnerability assessments are an uncertain process, based on past experiences, currently available information, and known threats. It should be understood that all information security systems, which by their nature are designed by and therefore dependent on human beings, are vulnerable to some degree. Therefore, while Comsec considers the major security vulnerabilities of the systems that were analyzed to have been identified, there can be no assurance that any exercise of this nature will identify all possible vulnerabilities or propose exhaustive and operationally viable recommendations to mitigate these exposures.

In addition, the analysis set forth herein is based on the technologies and known threats as of the date of this report. As technologies and risks change over time, the vulnerabilities associated with the operation of Nyotron's systems described in this report, as well as the actions necessary to reduce the exposure to such vulnerabilities will also change. Comsec makes no undertaking to supplement or update this report on the basis of changed circumstances or facts of which we become aware after the date hereof, absent a specific written agreement to perform supplemental or updated analysis.

COPYRIGHT NOTICE

ACCEPTANCE AND RELEASE NOTICE

This is a managed document. Changes will only be issued upon approval of both parties. This document cannot be released for use until authorized by both Comsec Consulting and Nyotron.

AUTHORIZED: **Loir Marom, Account manager** DATE: 28/07/2016

Comsec Consulting

APPROVED & ACCEPTED: **Nir Shafrir, Senior Director** DATE: 31/07/2016

Nyotron

Table of Contents

[1] Executive Summary 5
1.1. Introduction 5
1.2. Test Result Summary 5
1.3. Overall conclusion 6
[2] Test Results 7
[3] Findings 9
3.1. Not All Common File Types Are Defined in the Default Policy 9
[4] Appendix - Scope of Work 10
[5] Appendix B Methodology Overview 11
5.1. Testing Process 11
5.2. Risk Level Evaluation 12

[1] Executive Summary

1.1. *Introduction*

This document describes the results of the security performance review performed during July 2016, on site at Nyotron's offices. The test took place on July 6, 2016. The retest took place July 17-19, 2016.

Nyotron Paranoid solution is focused on zero-day prevention. It is focused on preventing the damage caused at the final phase of an attack, when all other protection measures were exhausted.

Paranoid performs its tasks in three distinct stages:

- Detection of a malicious activity by using Paranoid paradigm – OS Behavioral Pattern Map (BPM).
- Prevention of potential damage created at the final stage of the attack (such as damage to files and registry, malicious communications and process manipulations)
- Responses by investigating the zero-day attack flow.

1.2. *Test Result Summary*

The test was focused mainly on ransomwares and malwares. However, the test also included user experience and system performance tests. No special setup was needed prior to the tests.

The tests were designed to prove Paranoid solution is a true zero-day solution. All threats tested were unknown to Paranoid, and treated as zero-day threats.

The test results were as follows:

Windows 7

- 100% of the tested ransomware were not able to cause damage to data (prevented encryption).
- 100% of the tested malwares were not able to cause any damage.
- Paranoid system could handle 1000 simultaneous threats.
- No performance or user experience issues were detected.

Windows 10

A Windows 10 Beta version was tested against a random sampling of ransomwares and malwares.

The following ransomware and malware were tested:

- deletesystem32.exe
- teslacrypt
- vipasana

Result: all ransomwares and malwares were monitored and prevented.

1.3. *Overall conclusion*

Comsec overall test and the retest procedure for ransomwares and malwares showed very high detection rates with continuous improvement in preventing zero-day damage of attack final stage, while performing zero-business interruption to the test user.

Main conclusions:

- Paranoid can handle a high volume of simultaneous zero-day attacks.
- Paranoid provides protection against Ransomware and malwares by preventing the damage caused in final phase of the attack.
- Paranoid treats any threat as a zero-day and provides protection based on relying on normative OS behavior security paradigm.
- Paranoid has the added value of allowing activity analysis of a zero-day threat.

In comparison with other zero-day protection products, Nyotron Paranoid is positioned as one of the leading zero-day prevention solutions available in the market.

[2] Test Results

Test	Category	Status	Notes
Simultaneous Start of 1000 Viruses	Performance		Paranoid prevented any harmful actions to be executed by the viruses. Log file transfer to the Management Server has increased by 33% (90 sec to 120sec).
Viruses started by Logic/Fork Bomb	Performance		N/A
Jigsaw	Ransomware	 [1]	Jigsaw targeted 226 different file types and edit the Windows registry to allow auto start of the ransomware after reboot. Encrypted files were created, but Paranoid prevented removal of the original files.
Petya (Ver. #1)	Ransomware		Petya overwrite the master boot recorder (MBR) and encrypt the master file table (MFT) thus, making the file system unreadable.
Petya (Ver. #2)	Ransomware		Petya overwrite the master boot recorder (MBR) and encrypt the master file table (MFT) thus, making the file system unreadable.
TeslaCrypt (Ver. #1) (Ver. #2) (Ver. #3)	Ransomware		TeslaCrypt targeted 185 files related to gamming and the updated versions also targeted media files and documents (word, pdf etc.).
Vipasana (Ver. #1) (Ver. #2) (Ver. #3)	Ransomware		Vipasana targeted 92 different file types. The encrypted files will than have the name by the following schema for example: email-vipasana4@aol.com.ver-CL 1.2.0.0.id-[ID]- [DATE-TIME].randomname-[RANDOM].[XYZ].CBF
Cerber	Ransomware		Cerber targeted 380 different file types and also targeted Windows shares and encrypt them even if they are not mapped to a specific computer.
Bart	Ransomware		Bart targeted 160 different file types and replace them with a Zip protected password. Also, there is no need for internet connection for the ransomware to work.

 MP3 file types were not protected by default, the organization will have to define it under a protection policy to have Paranoid protect these files.

BadBlock	Ransomware		BadBlock uses asymmetric cryptographic algorithm for the encryption of the files.
Cryptear	Ransomware		The main different with Cryptear is that the decryption key is saved on the local user computer and is encrypted by the ransomware.
Gricakova(a.k.a Satana)	Ransomware		Gricakova targeted 43 different file types and also targeted the master boot recorder (MBR) thus, preventing the computer from booting. The original MBR is moved by the ransomware to a random location on the file system.
Milarepa (a.k.a CrySiS)	Ransomware		Milarepa targeted 187 different file types on hard drives and removable drives as well as network shares. The ransomware uses RSA and AES encryption and also delete shadow copies of the files.
Locky	Ransomware		Locky targeted 138 different file types and uses an asymmetric encryption by connection to a command and control server for downloading the key.
Radamant	Ransomware		Radamant targeted 946 different file type and remove any shadow copies to prevent restoration of the files. The ransomware uses 256-AES encryption.
Cryptowall	Ransomware		Cryptowall uses 2048-RSA key for encryption of files and targeted 48 file types. When encrypting files, the malware also deletes volume shadow copies, and installs spyware that steals passwords and Bitcoin wallets.
Matsnu	Malware/ Ransomware		Matsnu run is based on receive instructions and configuration from a remote server. The malware disable access to task manager registry tools and prevent the option to restore the computer from restoration point. Also, Matsnu try to encrypt the file system and lock the use of the computer.
DeleteSystem32.exe	Malware		DeleteSystem32 is a malware that delete the folder system32 under windows directory.
Server.exe	Malware		Unknown behavior
Mqeyek.exe	Malware		Unknown behavior
HudsonMP3.exe	Malware		Unknown behavior
SendFileToMail.exe	Malware		The malwares try to send documents from the file system to an email account.

[3] Findings

3.1. *Not All Common File Types Are Defined in the Default Policy*

BPM retest version 601.52, Paranoid Agent retest version v0.12.012.2994

BPM previous test version 601.42, Paranoid Agent version v0.12.012.2994

Vulnerability Description:

Paranoid is an endpoint protection software that prevents any kind of harm to the system, such as: removal of system files, malicious encryption of the common file types that contain private/sensitive information, connection to the external servers to leak data from the workstations, addition of malicious registry keys and etc.

However, during the test it was found that not all common file types were protected from malicious encryption attempts. File types such as MP3, MP4 (audio file types were encrypted by the ransomware and should be added to protection policy manually to avoid being encrypted.

Retest Status: Fixed

Risk Level: Low

If an attacker succeeds to use ransomware to encrypt common file types that are not defined in the default policy of the Paranoid software, he/she can cause financial or prestige damage to companies (that use Paranoid to protect endpoint workstations) and reputational damage to Nyotron since Paranoid software only partially protected its clients.

However, as Paranoid allows additional file types to be added easily, the anti-encryption measures can be easily updated. As a result, the risk level of this vulnerability is further decreased to low.

Initial Recommendations:

- Add all commonly used file types to the Paranoid Default Policy. This includes such file types as:
  - Configuration files such as: INI, CFG, XML, YML etc.
  - Source Code files such as: PY, CPP, CS etc.
  - SSL/TLS and certificate related file such as: PEM, CER, DER, KEY, PFX, P12, JKS, BKS, Ketstore etc.

[4] Appendix - Scope of Work

Nyotron has contracted the services of Comsec Information Security to perform a security performance review on their security software - Paranoid.

The high-level security performance assessment of Nyotron's Paranoid applications included activities that reviewed different levels of the application's security performance and efficiency such as:

- **Ransomware Test –** preventive efficiency of Paranoid with active ransomware. The attack attempted to encrypt all files with sensitive/private information or encrypt the entire hard drive.
- **Classic Malware Test** – preventive efficiency of Paranoid with active malware. The attack attempted to damage system files, send files from the workstation to the external server and add malicious entries to the registry.
- **Performance Test** – efficiency and the responsiveness of Paranoid under heavy system load.

[5] Appendix B Methodology Overview

5.1. *Testing Process*

This review is based on information gathered from manual penetration testing or semi-automatic testing of specific threat scenarios. The review considered theoretical and practical methodical issues, as well as techniques of attacks performed by a malicious entity (e.g. hacker, spyware, virus, etc.) operating on a local or remote unit. Finally, the review's recommendations are based on well-known security best practices common within the industry and used to mitigate potential threats.

The Security Assessment was performed using a grey box security assessment approach. Grey box security testing is an approach in which the system owner (Nyotron) shares some limited information about the internal functionality of the system such as design documents as well user credentials for the application and its supporting infrastructure. However, we did not receive access to the application code or access to the hosting instance.

Based on the Comsec methodology for performing security reviews, the assessment of each system was comprised of the following key phases:

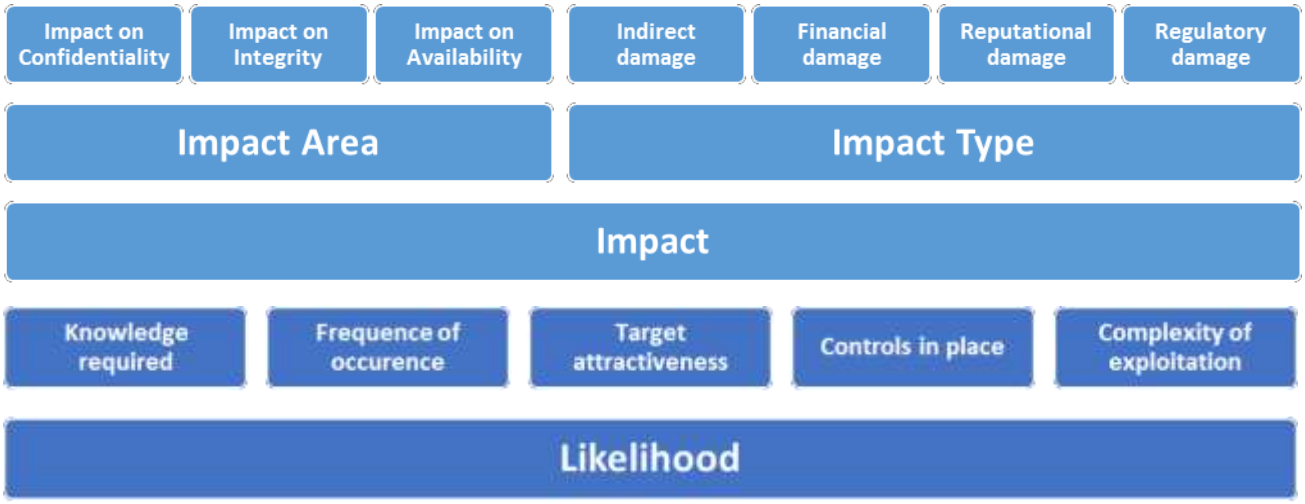
1. **Information Gathering** – During this phase the Comsec team obtained technical information regarding the systems being tested.
2. Initial **analysis** of the applications, their structure, interfaces, data flow, sensitive modules and concept.
3. Hands on **execution** of the security tests.
4. Thorough Risk **Analysis** and **Deliverables** formulation.

5.2. *Risk Level Evaluation*

The retesting procedure resulted in a total of **0** finding discovered across the retest.

Risk Level factors

The final Risk Level for each finding is computed based on two factors. “Impact” representing the amount of damage that exploitation of the vulnerability could cause and “Likelihood” representing the probability of the vulnerability being exploited. The graphic below shows the considerations that go into these two factors.



Final Risk Level

The risk for each finding is calculated as one of four levels: **Critical**, **High**, **Medium**, or **Low.** This is based on taking the Impact and Likelihood levels of the finding and computing the risk level based on the matrix below:

	Low Probability	Medium Probability	High Probability
Low Impact	Low	Low	Medium
Medium Impact	Low	Medium	High
High Impact	Medium	High	Critical

Comsec recommends using the risk level as the basis for defining the priorities and timetable for addressing the different breaches and transforming the recommendations into a concrete mitigation plan.