Q3 2018

Advanced Threat Defense

Certification Testing Report

Nyotron Security
PARANOID

Tested against this standard

ICSA Labs Advanced Threat Defense Criteria v.1.0

October 3, 2018

Prepared by ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050
www.icsalabs.com

ICSA Labs Advanced Threat Defense – Report-at-a-Glance

Nyotron Security

NYOTRON
SECURING THE WORLD

PARANOID

www.nyotron.com

Executive Summary

During 33 days of testing during the third quarter of 2018, ICSA Labs tested the detection capabilities of Nyotron's PARANOID with a mix of over 1150 test runs. The mix was primarily composed of new and little-known malicious threats – i.e., recently harvested threats not detected by traditional security products.

Periodically, ICSA Labs launched innocuous applications and activities to additionally test the PARANOID product in terms of false positives. Throughout testing, ICSA Labs observed product logs to ensure not only that PARANOID indicated the existence of a malicious threat but also that logged threats were distinguishable from other logged traffic and events.

The PARANOID product passed, having met all criteria requirements. As seen in Figure 1 below, Nyotron's solution did remarkably well during this test cycle - detecting 100.0% of previously unknown threats while having just one false positive. Figures 2 and 3 below further highlight the solution's detection effectiveness and false positives (FPs).

Test Length	33 days	**Malicious Samples**	441	**Innocuous Apps**	721
Test Runs	1162	**% Detected**	**100.0%**	**% False Positives**	**0.1%**

Fig. 1 – High Detection Effectiveness & Few False Positives

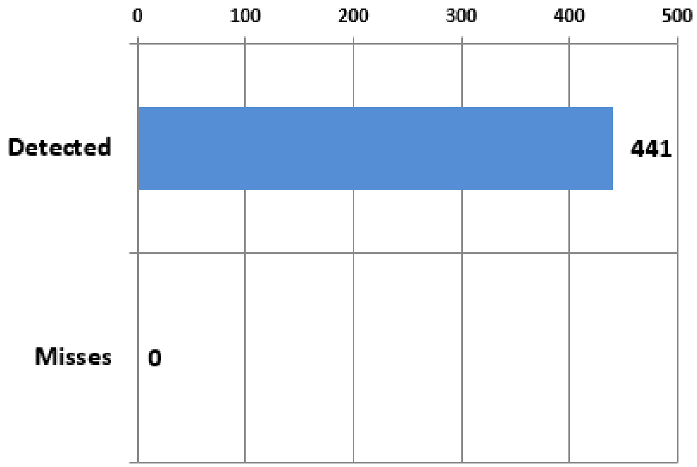


Fig. 2 – Detected 441 of 441 *New & Little-Known* Malicious Samples

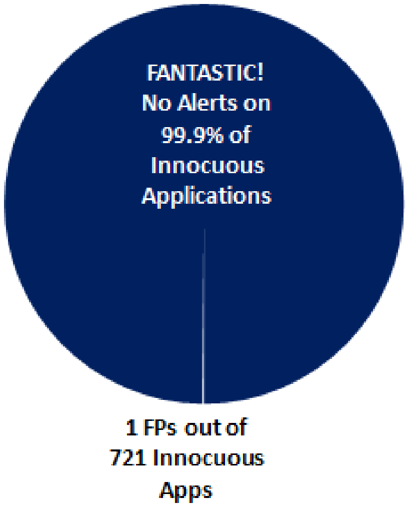


Fig. 3 – One Alert on Innocuous Applications

ICSA Labs
Advanced Threat Defense

Certified

Test Period:	Q3 2018
Certified Since:	10 / 2018

Introduction

This is Nyotron's first ICSA Labs Advanced Threat Defense Certification testing report for PARANOID.

Standard ICSA Labs Advanced Threat Defense (ATD) testing is aimed at vendor solutions designed to detect new threats that other traditional security products miss. Thus the focus is on how effectively vendor ATD solutions detect these unknown and little-known threats while minimizing false positives.

The remainder of the report presents a more detailed look at how Nyotron's PARANOID advanced threat defense solution performed during this cycle of standard ICSA Labs ATD Certification testing. To better understand how to interpret the results, this report documents not just the testing results themselves but the threat vectors, sample sources, and kinds of samples that ICSA Labs employed for this cycle of ATD testing against Nyotron's PARANOID product.

Test Cycle Information

This report reflects the results of one test cycle at ICSA Labs. Standard ATD and ATD-Email test cycles are performed by ICSA Labs each calendar quarter and typically range from three to five weeks in duration. To be eligible for certification, security vendor solutions must be tested for at least 3 weeks. Because testing is performed quarterly, ICSA Labs tests ATD solutions four times during a calendar year.

During each test cycle ICSA Labs subjects advanced threat defense solutions to hundreds of test runs. The test set is comprised of a mix of new threats, little-known threats and innocuous applications and activities – delivered and launched one after another continuously for the length of testing. Below in Figure 4 is information about the test cycle from which this findings report is based.

Start Date	Jul. 17, 2018	**Days of Continuous Testing**	33
End Date	Aug. 20, 2018	**Test Runs**	1162

Fig. 4 – This Test Cycle

ATD Solution Tested

During this testing cycle, ICSA Labs tested Nyotron's PARANOID advanced threat defense solution.

- Nyotron PARANOID – 2.18.9100.0

  According to Nyotron, PARANOID is a game-changing endpoint protection solution that works seamlessly with your existing endpoint security solutions to create an almost impenetrable defense against even the most sophisticated attacks. Acting as the last line of defense – after threats bypass all perimeter and endpoint security layers – PARANOID protects your data from deletion, exfiltration, encryption, sabotage and more.

  Delivering the first-ever OS-Centric Positive Security, PARANOID distinguishes between legitimate activities carried out by a program or user and threatening activities carried out by attacks.

  For more information about the Nyotron PARANOID please visit:

  https://www.nyotron.com/paranoid/

Detection Effectiveness

To meet the criteria requirements and attain (or retain) certification through ICSA Labs testing, advanced threat defense solutions must be at least 75% effective at detecting new malicious threats. As shown in Figure 5 the Nyotron PARANOID platform detected 100.0% of the threats it encountered during testing, considerably better than the percentage required for certification.

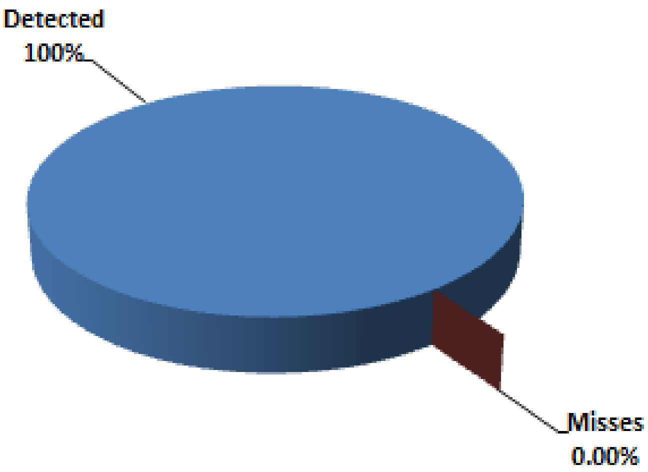


Fig. 5 – Detection Effectiveness of Nyotron's PARANOID

A second plot depicting the detection effectiveness of PARANOID appears in Figure 6. For Nyotron's solution the chart sheds light on whether or not the PARANOID did better or worse – the newer the malicious sample. As is evident both below and in the previous figure, regardless of how new or how old the threat, the Nyotron PARANOID platform detected all new and little-known malicious threats. Nyotron PARANOID platform provided this excellent detection effectiveness and had one false positives during this test cycle, which is impressive.

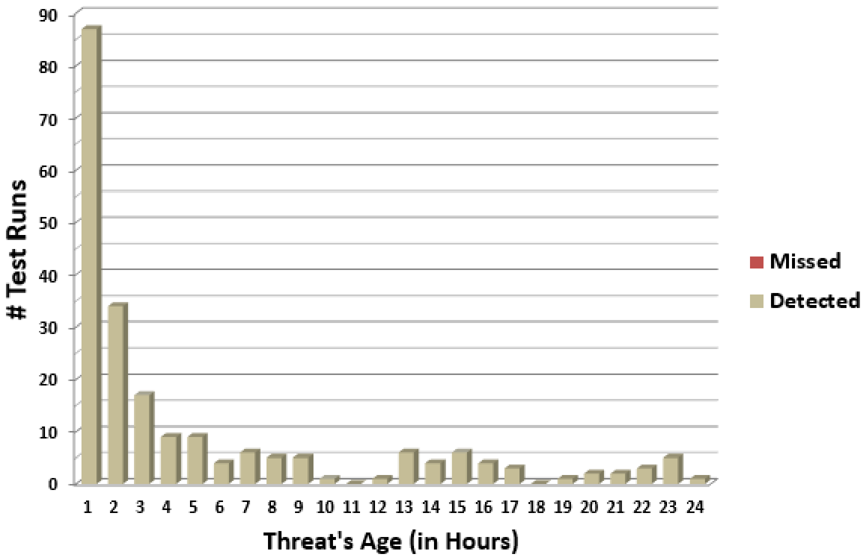


Fig. 6 – Detection Effectiveness by Age of Threat (Threats < 24 Hours Old)

A final effectiveness-related plot to consider for Nyotron Labs' advanced threat defense solution PARANOID during this test cycle is Figure 7 below. Plotted below is each of the 33 days during the test cycle along with how effective the PARANOID solution was on each of those days. For an impressive 33 of 33 days during the test cycle, the Nyotron PARANOID solution was 100% effective against the new and little-known threats used in testing.

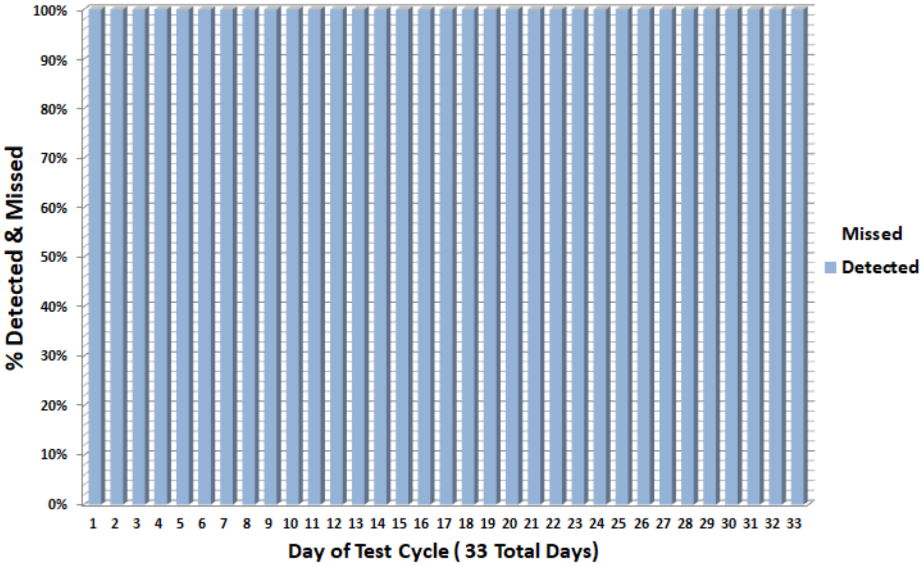


Fig. 7 – Detected & Missed Threats by Day of Test Cycle

Threat Vectors

In testing, ICSA Labs delivers new and little-known malicious threats to security vendor solutions using many of the top threat vectors that have led to enterprise cybersecurity incidents and breaches as reported in the latest Verizon Data Breach Investigation Report (DBIR).

DBIR data indicates that malware has been a key factor in thousands of security events where an information asset had its integrity, confidentiality, and/or availability compromised. Figure 9 on the following page depicts the threat vectors involved in these malware-related security incidents throughout the over ten year history of Verizon's DBIR. Figure 8 below illustrates the most common malware-related threat vectors that lead to enterprise breaches during 2016 alone (2017 DBIR).

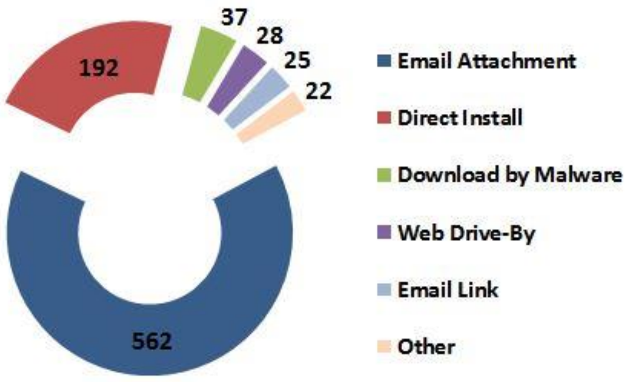


Fig. 8 – Top Threat Vectors Leading to Breaches in 2016 (per 2017 DBIR data)

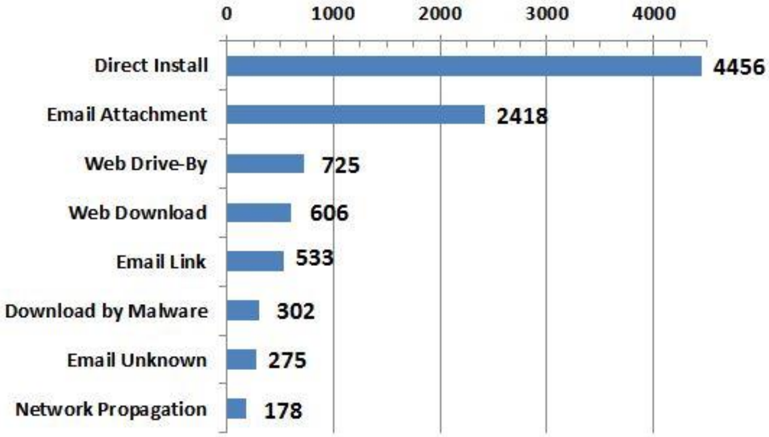


Fig. 9 – Malware-Related Threat Vectors Involved in Incidents (DBIR All-Time)

Standard ICSA Labs ATD testing includes the threat vector that is by far the most prevalent over time, “Direct Install”. In addition, standard ATD testing includes the threat vectors labeled “Web Download”, “Web Drive-By”, and “Download by Malware”. In the separate but related, ICSA Labs ATD-Email testing, ICSA Labs delivers new and little-known malware in URLs and attachments, corresponding to DBIR threat vectors “Email Link” and “Email Attachment”, the latter being the single most common threat vector leading to enterprise breaches according to the 2017 DBIR (refer to Figure 8 above).

Source of Samples

A number of sample sources feed ICSA Labs’ standard ATD and ATD-Email testing.

One source is the spam ICSA Labs collects. The labs’ spam honeypots receive approximately 250,000-300,000 spam email messages/day. For ICSA Labs ATD testing, the team harvests attachments in that spam, making use of the ones that are malicious.

Samples may also come from malicious URLs. Some of these come from the spam mentioned above. From feeds like this ICSA Labs filters and checks the URLs to see if there is a malicious file on the other end of that URL -- either as a direct file link or a series of steps (e.g. a drive-by attack with a multi-stage download process) leading to it. If so, ICSA Labs collects the sample for potential use in testing.

ICSA Labs additionally uses other tools and techniques to create unique malicious files as an attacker or penetration tester might do. In some cases these are trojanized versions of clean executables. In other cases they may be original executables that are malicious.

Still another source of samples is the samples themselves. Any dropped files resulting from running another malicious sample are also evaluated and potentially used in testing.

Finally – and importantly to test for false positives – ICSA Labs also launches legitimate executables. Running innocuous applications helps ensure that vendor solutions aren’t just identifying everything as malicious.

Regarding the Samples from this Test Cycle

Samples harvested for use in ATD testing are often unmodified and used as is. That is the case if ICSA Labs determines that the sample is new enough and/or not being detected by traditional security products. In many cases malicious samples require modification before they can avoid detection by traditional security products.

Of the 441 malicious samples, Figure 10 shows that there were more original samples used and fewer samples that required some kind of modification before use in testing. Of the 253 original samples, 5 were dropped, or left behind by other malware. Figure 13 reveals the source of the 248 malicious samples used in testing that were neither modified nor dropped.

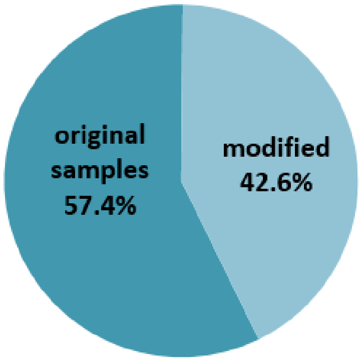


Fig. 10 –Malicious Samples – Original vs. Modified

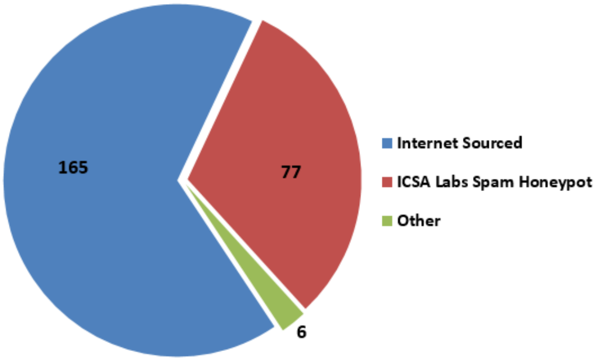


Fig. 11 – Unmodified/Non-Dropped Sample Sources

Prior ATD Reports

With this report, Nyotron's PARANOID advanced threat defense solution passed all the test cases to attain ICSA Labs Advanced Threat Defense Certification. Therefore there are no prior reports.

This certification testing report can be found on the ICSA Labs web site at:

https://www.icsalabs.com/product/paranoid

Significance of the Test & Results

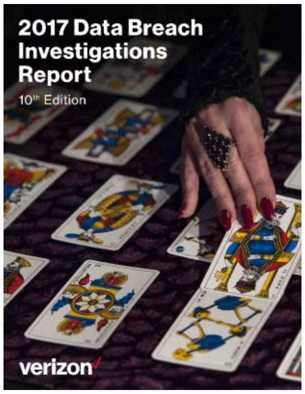
Readers of certification testing reports often wonder what the testing and results really mean. They ask, “In what way is this report significant?” The four statements below sum up what this ICSA Labs Advanced Threat Defense Certification Testing report should indicate to the reader:

1. ICSA Labs tested the Nyotron Labs’ PARANOID advanced threat defense solution using the primary threat vectors leading to enterprise breaches according to Verizon’s Data Breach Investigations Report (DBIR).

2. ICSA Labs tests with malicious threats including new and little-known Ransomware that other security products typically miss.

3. Nyotron’s PARANOID demonstrated superb threat detection effectiveness against all of the over 440 *new and little-known* threats.

4. The Nyotron PARANOID product had just one false positive during this test cycle, which is excellent.



Authority

This report is issued by the authority of the General Manager, ICSA Labs. Tests are done under normal operating conditions.

Sebastien Mazas, General Manager, ICSA Labs

ICSA Labs

The goal of ICSA Labs is to significantly increase user and enterprise trust in information security products and solutions. For more than 25 years, ICSA Labs, an independent division of Verizon, has been providing credible, independent, 3rd party security product testing and certification for many of the world's top security product developers and service providers. Enterprises worldwide rely on ICSA Labs to set and apply objective testing and certification criteria for measuring product compliance and performance.

ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050

Nyotron Security

Nyotron provides the industry's first OS-Centric Positive Security to strengthen laptop, desktop and server protection. By mapping legitimate operating system behavior, Nyotron's PARANOID understands all normative ways that may lead to damage, such as file deletion, data exfiltration, encryption, and more. Focusing on finite "good" actions allows PARANOID to be completely agnostic to threats and attack vectors. PARANOID works seamlessly with antivirus and next-generation antivirus solutions to provide the last line of defense from modern state-level attacks. Nyotron is headquartered in Santa Clara, CA with an R&D office in Israel.

Nyotron Security
2880 Lakeside Drive, Suite 237
Santa Clara, CA 95054