Q4 2017

Advanced Threat Defense

Certification Testing Report

Fortinet, Inc.
Advanced Threat Protection Solution

Tested against these standards

ICSA Labs Advanced Threat Defense Criteria v.1.0

ICSA Labs Advanced Threat Defense - Email Criteria v.1.0

January 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

Fortinet, Inc.

Advanced Threat Protection Solution

www.fortinet.com

Executive Summary

ICSA Labs tested the Fortinet Advanced Threat Protection (ATP) for 28 days during Q4 2017 to determine how well it detected new and little-known malicious threats. Throughout 4 weeks of near-continuous testing during this quarterly test period, the Fortinet ATP solution faced close to 1800 total test runs. The result was Fortinet's ATP successfully met all requirements to maintain two ICSA Labs advanced threat defense (ATD) certifications:

- *Standard ICSA Labs Advanced Threat Defense,* and
- *ICSA Labs Advanced Threat Defense – Email*

Fortinet's solution did exceptionally well during the test cycle - detecting previously unknown threats and having minimal false positives. In fact during standard ATD testing, Fortinet ATP detected 99.6% of threats with a very low false positive rate while in ATD-Email testing Fortinet ATP detected 100% of threats with no false positives. Figure 1 shows the Fortinet ATP solution's effectiveness and false positive rates in ICSA Labs' standard ATD testing while Figure 2 shows the same characteristics in ICSA Labs' ATD-Email testing.

The Q4 2017 test set was comprised of 563 unique new and little-known malicious threats as well as 564 non-malicious samples. The former were recently harvested malicious threats not detected by traditional security products. The latter were used to test the Fortinet ATP solution in terms of false positives. Security product solutions participating in both standard ATD and ATD-Email testing, like the Fortinet ATD, are tested in the leading ways in which enterprises are being compromised with malware according to data in Verizon's Data Breach Investigations Report.

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

Fortinet ATP Solution

Certified Since December 2015

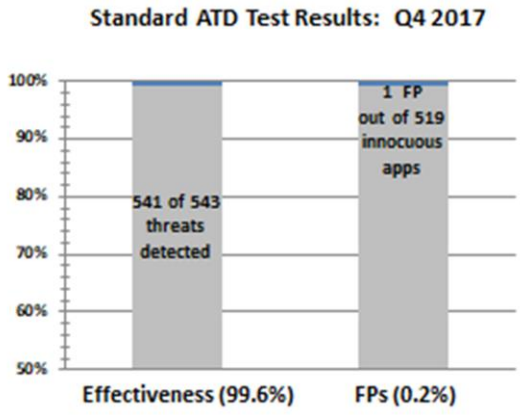

Fig. 1 – 1062 Standard ATD Test Runs

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE – EMAIL

Fortinet ATP Solution

Certified Since December 2016

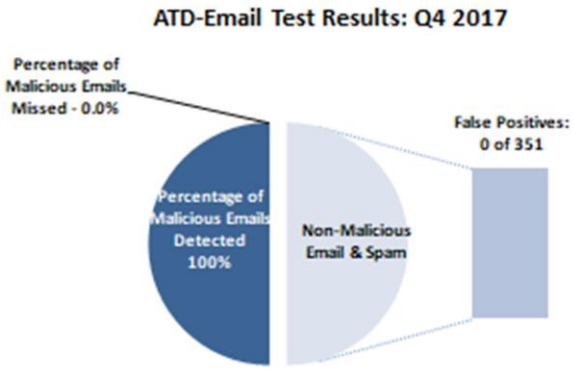

Fig. 2 – 701 ATD-Email Test Runs

Introduction

This is Fortinet's ninth consecutive ICSA Labs Advanced Threat Defense Certification testing report and fifth consecutive to include results from ICSA Labs Advanced Threat Defense E-Mail Certification.

All ICSA Labs advanced threat defense (ATD) testing focuses on determining how effectively ATD solutions detect the unknown and little-known threats that more traditional security products miss while minimizing false positives. The remainder of the report presents a more detailed look at how the Fortinet ATP performed during the Q4 2017 test cycle in both ICSA Labs:

- Standard Advanced Threat Defense Certification Testing, and
- Advanced Threat Defense – Email Certification Testing.

ICSA Labs additionally presents data concerning the combined effectiveness of Fortinet's solution against a collection of malicious threats applicable to and separately seen by both the email security components and the other ATD components of the Fortinet ATP Solution. Finally, to better understand how to interpret the results, this report documents the threat vectors, sample sources, and kinds of samples that ICSA Labs employed for this cycle of ATD testing against the Fortinet ATP Solution.

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 during the test cycle. Below in Figure 3 is information about the test cycle from which this findings report is based.

Start Date	Oct. 17, 2017	**Days Tested**	28
End Date	Nov. 13, 2017	**Test Runs**	1,763

Fig. 3 – This Test Cycle

ATD Solution Tested

During this testing cycle, ICSA Labs tested the Advanced Threat Protection (ATP) Solution from Fortinet Inc. The ATP is a multi-component solution. Three ATP components were tested in standard ATD testing while two ATP components were provided for ATD-Email testing. One of the components, the FortiSandbox, was common to both standard ATD and ATD-Email testing. All Fortinet ATP components in the lab along with the corresponding versions tested during this test cycle are listed and described below.

- Components used in ICSA Labs' standard ATD testing
  - FortiGate 500D: v5.6.2, build1486 (GA)

    The FortiGate component's role in the solution is to stop as many network-borne threats as possible with its threat prevention technologies before submitting remaining objects to FortiSandbox for further analysis. It also serves as a key element to quickly mitigate previously unknown threats that are identified by FortiSandbox.

- FortiClient: v5.6 (latest version)

  FortiClient runs on endpoint devices including PCs, Macs, smartphones and tablets. Its role is to ensure that all objects that reach the endpoint, on or off the network, are inspected with its threat prevention technologies to block as many identifiable threats as possible – with the option to send the remainder to FortiSandbox for additional analysis – while either holding them before install, or quarantining them as necessary afterwards, based on results. Note that during testing, FortiClient was run on a PC.

- Component used in ICSA Labs' ATD Email testing
  - FortiMail VM04 – v5.4, build 703,171006

    FortiMail is an effective, high performance secure email gateway that applies the threat intelligence of FortiGuard Labs to block spam, malware and advanced threats. It also includes integrated DLP, encryption and archiving for a complete email security solution available as a physical or virtual appliance, SaaS, or managed security service. The FortiMail VM04 used in testing is a virtual appliance aimed at mid-to-large enterprises with up to 3000 users.

- Component in common for both standard ATD and ATD-Email testing
  - FortiSandbox-3000D: v2.4.1, build0270 (Interim)

    The FortiSandbox uses instrumented VMs (as well as various pre- and post-filters) to run and analyze unknown objects, assign risk ratings and provide threat intelligence to speed response to previously unknown threats. It can obtain those objects directly off the wire, or from file share locations, manual submissions from security staff and other integrated Fortinet devices such as FortiGate, FortiMail, FortiWeb and FortiClient.

For more information about the Fortinet Advanced Threat Protection Solution, its component parts and related information please go to:

https://www.fortinet.com/solutions/enterprise-midsize-business/advanced-threat-protection.html

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 5 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 4 below illustrates the most common malware-related threat vectors that lead to enterprise breaches during 2016 alone (2017 DBIR).

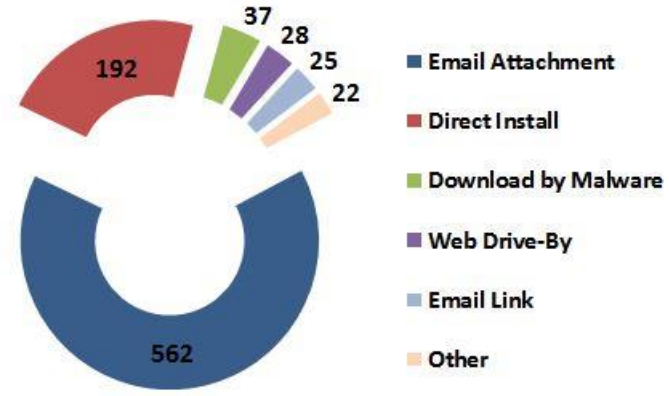

Fig. 4 – Top Threat Vectors Leading to Breaches in 2016 (per 2017 DBIR data)

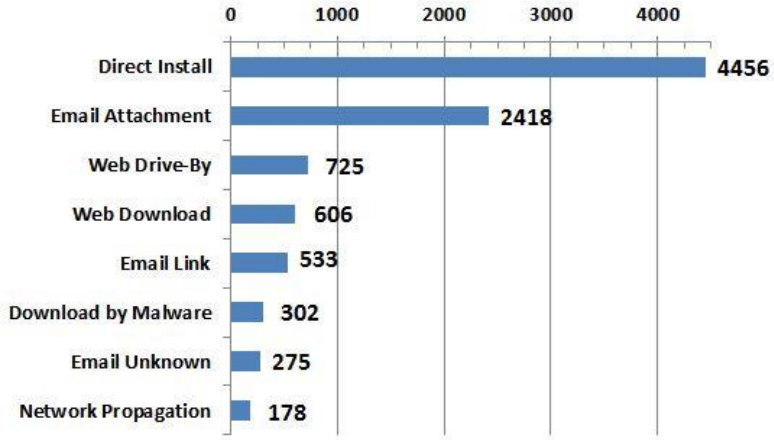

Fig. 5 – Malware-Related Threat Vectors Involved in Incidents (DBIR All-Time)

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 4 above).

Detection Effectiveness – Standard ATD

In this section, ICSA Labs presents the Fortinet ATP's detection effectiveness against all non-email threat vectors mentioned in the "Threat Vectors" section, including web download, web drive-by, and download by malware".

To meet the standard ICSA Labs ATD testing criteria requirements and attain (or retain) certification, advanced threat defense solutions must be at least 75% effective at detecting new and little-known malicious threats. As shown in Figure 6, the Fortinet ATP Solution detected 99.6% of the threats it encountered during standard ATD testing, considerably better than the percentage required for certification.

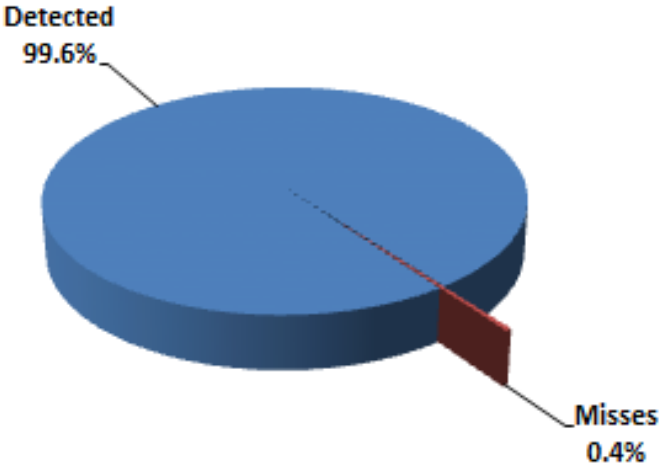

Fig. 6 – Detection Effectiveness of Fortinet ATP (All Non-Email Threats)

The next two plots take a deeper dive into the detection provided by Fortinet ATP in ICSA Labs' standard ATD testing.

The plot in Figure 7 sheds light on whether or not the ATP did better or worse – the newer the malicious sample. The Fortinet ATP Solution detected 98.6% of threats that were less than an hour old. The Fortinet ATP Solution was perfect detecting 100% of malicious samples two hours old and later. In fact, only two malicious samples went undetected in samples less than 24 hours old.

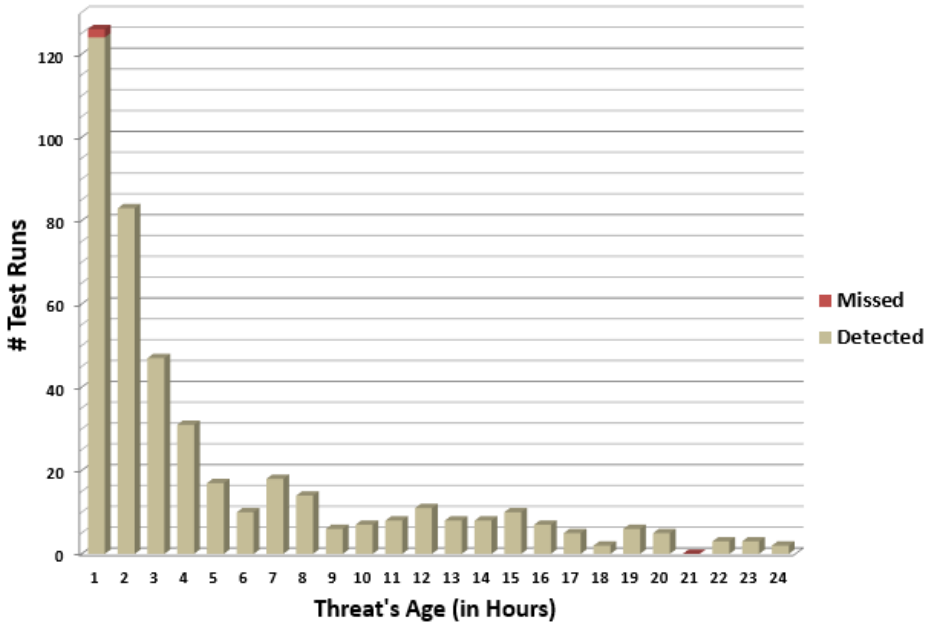

Fig. 7 – Detection Effectiveness by Age of Threat (Threats < 24 Hours Old)

A final effectiveness-related plot to consider for the Fortinet ATP Solution during standard ATD testing this test cycle is Figure 8 below. Plotted below is each of the 28 days during the test cycle along with how effective the ATP was on each of those days. The Fortinet ATP Solution was 100% effective on all but two days. On those two days, the Fortinet ATP solution was at least 94% effective.

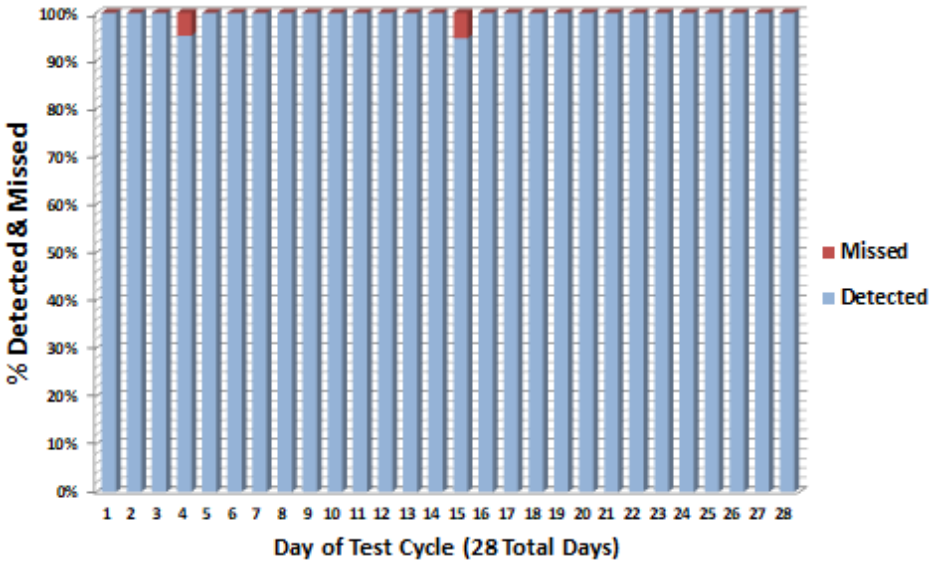

Fig. 8 – Detected & Missed Threats by Day of Test Cycle

Detection Effectiveness – ATD Email

In this section, ICSA Labs presents the Fortinet ATP's detection effectiveness against malicious email threats using the vectors mentioned in the "Threat Vectors" section. In this test cycle the primarily vector for delivering threats was via malicious attachments. The secondary threat vector was emails with malicious URLs.

As with the standard ATD testing, to meet the ICSA Labs ATD-Email testing criteria requirements and attain (or retain) certification, email security solutions must be at least 75% effective at detecting new and little-known malicious threats delivered via typical email threat vectors. As shown in Figure 9, the Fortinet ATP Solution did very well, detecting 100% of the malicious email threats it encountered with no false positives in 701 total ATD-Email test runs.

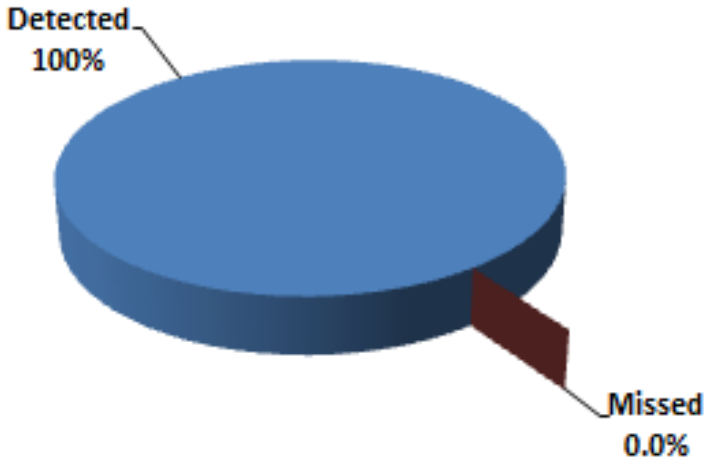

Fig. 9 – Detection Effectiveness of Fortinet ATP Versus Malicious Email Threats

Effectiveness Against Threats Delivered Multiple Ways

In the preceding two sections ICSA Labs presented the effectiveness results, first for standard ATD testing then for ATD-Email testing. Those sections described the solution's efficacy against 543 malicious test runs in standard ATD testing and 350 malicious test runs in ATD-Email testing.

Used in those tests were 563 unique malicious test samples. Figure 10 below shows that some of the 563 were applicable only to standard ATD testing (213) while some of the test runs were relevant only to ATD-Email testing (20).

The remaining 330 malicious samples in the center of Figure 10 were applicable to both and were therefore delivered twice - once via web download and separately as malicious email attachments (or at the other end of a malicious URL). By virtue of the fact that the FortiMail component detected all of the threats, the Fortinet ATP Solution was 100% effective against the 330 samples delivered these two ways. This combined effectiveness demonstrates the power of ATD components covering multiple threat vectors working together.

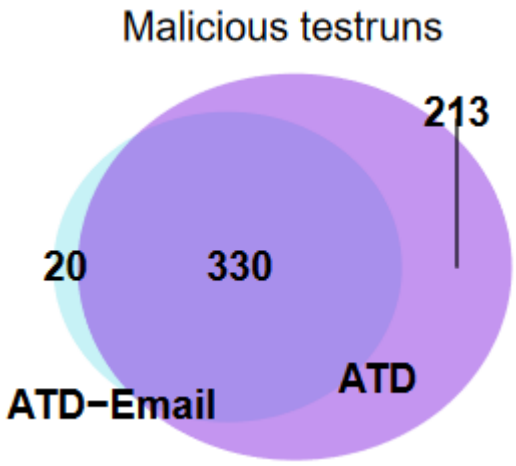

Fig. 10 – 563 Malicious Test Runs

One of the benefits of a solution like Fortinet's that combines both network and email defense is that any email threats are typically held for sandbox analysis and can be stopped unlike network threats that are initially detected but require a more immediate response to further contain any threats and protect the organization's network.

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.

Ransomware in Archives

The amount of archive-based Ransomware received into ICSA Labs' spam honeypot during Q4 2017 was down about 85% compared to the levels seen during the previous quarter. Figure 11 indicates that an average of 6,125 spam messages with attached Ransomware archives were daily received during the Q4 2017 testing period by ICSA Labs' spam honeypots. While levels of archive-based Ransomware were far less than Q3 2017, or the off-the-chart levels observed a year earlier during Q4 2016, it continues to represent a significant malicious threat.

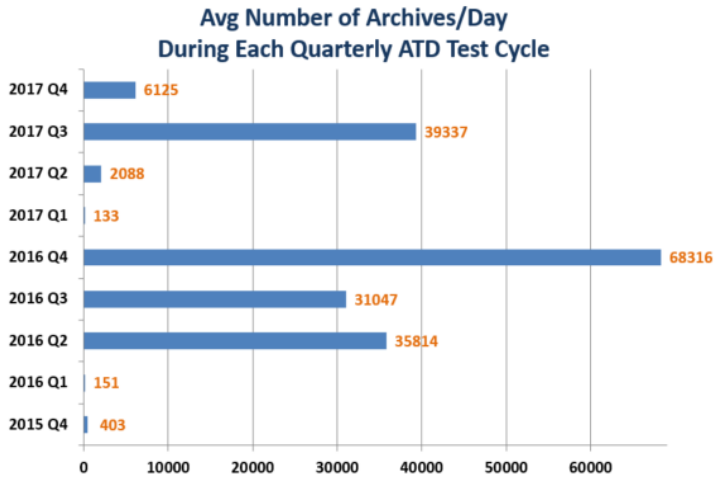

Fig. 11 – Ransomware Per Day Averages During Recent ATD Test Cycles

Most likely as part of the same Ransomware-spam campaign, the vast majority of these malicious spam email with attached Ransomware archives – over 170,000 – arrived on test cycle days 2 and 3. The emails contained different 7-Zip files with a variety of VBS scripts that all downloaded the same Locky Ransomware binary.

Pulling back the lens ICSA Labs examined - not just the 28 days of the Q4 2017 test cycle but - all the 7-Zip archives containing malicious scripts received in the ICSA Labs spam honeypot during Q4 2017. As seen in Figure 12 below, Q4 2017 once again proved, as was the case in the latter half of Q3 2017, to be a quarter that filled the labs' spam honeypot with malicious 7-Zip archives.

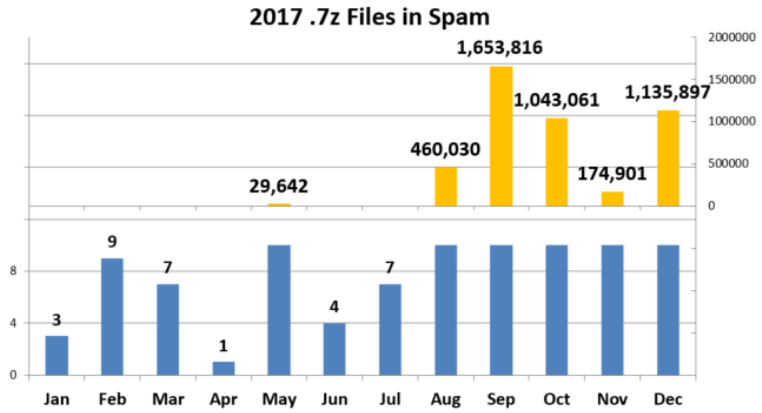

Fig. 12 – Monthly spam honeypot counts of 7-Zip (.7z) attachments

Regarding the Samples from This Test Cycle

Samples harvested for use in standard ATD and ATD-Email 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 563 unique malicious samples in standard ATD and ATD-Email testing, Figure 13 shows that there were many more original samples used and far fewer samples that required some kind of modification before use in testing. Of the original samples, 95 were dropped, or left behind by other malware. Figure 14 reveals the source of the 436 malicious samples used in testing that were neither modified nor dropped.

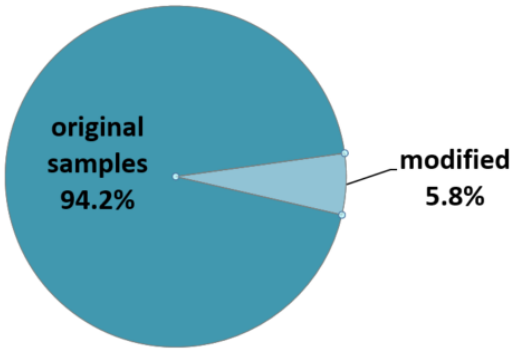

Fig. 13 – Malicious Samples – Original vs. Modified

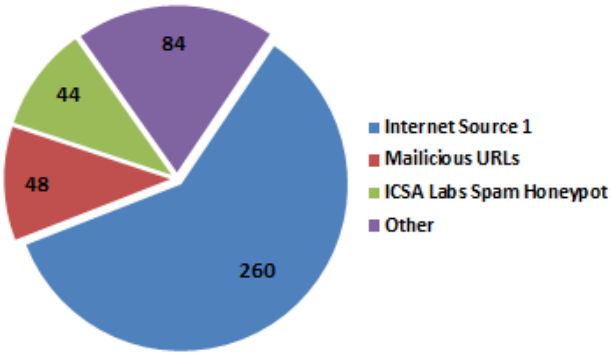

Fig. 14 – Unmodified/Non-Dropped Sample Sources

Prior ATD Reports

Following the 28 days of continuous advanced threat defense testing during the 4th quarter 2017 test cycle, the Fortinet, Inc. ATP Solution maintained both ICSA Labs' standard Advanced Threat Defense (ATD) Certification and ICSA Labs Advanced Threat Defense – Email Certification.

This and all earlier ATP Solution certification testing reports can be found on the ICSA Labs web site at:

https://www.icsalabs.com/product/advanced-threat-protection-framework

Successful completion of this test cycle marks Fortinet's 5th consecutive quarter satisfying the ICSA Labs ATD-Email certification testing criteria and its 9th consecutive quarter having met the ICSA Labs ATD certification testing criteria.

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 five statements below sum up what this ICSA Labs Advanced Threat Defense Certification Testing report should indicate to the reader:

1. ICSA Labs tested the Fortinet ATP 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. The Fortinet ATP Solution demonstrated superb threat detection effectiveness against over 560 unique *new and little-known* threats.
4. The Fortinet ATP Solution had one false positive over nearly 1800 test runs.
5. With its ATP Solution, Fortinet provides highly effective, comprehensive defense including excellent recognition of previously unknown email-borne threats with few false positives.

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

Fortinet, Inc.

Fortinet's mission is to deliver the most innovative, highest performing network security platform to secure and simplify your IT infrastructure. We are a leading global provider of network security appliances for carriers, data centers, enterprises and distributed offices. Because of our custom ASICs, hardware systems, network software, management capabilities and security research, we have a large, rapidly growing customer base, including the majority of the Fortune Global 100. Our market position and solution effectiveness has been widely validated by industry analysts, independent testing labs, business organizations, and the media worldwide. Our broad product line of complementary solutions goes beyond Network Security to help secure the extended enterprise.

www.fortinet.com

Fortinet, Inc.
899 Kifer Road
Sunnyvale, CA 94086