# Exhibit 57

**UNREDACTED VERSION OF DOCUMENT PROPOSED**

**TO BE FILED UNDER SEAL**

You no longer have access Support and Updates. Renew online, remind me later or never remind me again.



# Pegasus 3 Pony (WhatsApp Agent) Support Specification - DRAFT

Created by [redacted] last modified on Apr 27, 2020

**You are viewing an old version of this page. View the current version.**

Compare with Current · Restore this Version · View Page History

« Previous **Version 4** Next »

First draft



# 1. General

This document is a specification for the changes to be done in Pegasus in order to support the WhatsApp Agent (WAgent) on Android platforms..

Section 1 is informative, meaning that it provides an overview of the specification, but is **not** meant to be the definitive reference for implementation. Sections 2 and 3 are the formal parts of the specification: implementation and testing should be



HIGHLY CONFIDENTIAL - ATTORNEYS EYES ONLY NSO_WHATSAPP_00001241

based only on those sections. Section 4 describes future enhancements, Section 5 describes how the specification affects related systems, and Section 6 lists open issues.

## 1.1. Background

Erised-based covert installations are currently restricted to running in the context of the WhatsApp process. This limits the functionality of the agent to the permissions granted to the process. This document describes those limits, and specifies the changes required for Pegasus to support this.

## 1.2. Solution Overview

1. The installation flow is basically Erised. All differences are within the package and ABS.
2. Differences in user-visible agent capabilties are listed below, and can be handles under the existing Agent Capabilities framework.
3. Differences in behaviour that affect Pegasus, and how to deal with them, are listed below.

## 1.3. Limitations

## 1.4. Scope

The following components are affected by this spec:

- Pegasus 3
- UI
- Android Agent

**Redacted –Export Controlled**

- QA Automation

# 2. Requirements

**PRD - TBD**

## 2.1. Functional Requirements

1. Pony shall be installed at the end of the Covert Android Erised flow.
2. Aside from acitvity records, target information required for Pegasus operation and opsec shall be provided (IMEI, Current and Home MCC/MNC, MSISDN).
3. User shall have a visible indication for this type of agent
4. Capability restrictions shall be updated for this agent.

## 2.2. Requirement Mapping

This Section describes what components are affected by each requirement in the PRD.

**Legend**

Component is affected by requirement

Component is **not affected** by requirement

Unclear - clarification needed



HIGHLY CONFIDENTIAL - ATTORNEYS EYES ONLY NSO_WHATSAPP_00001242

⚠️ Action required from specific person

| Requirement | Description | Priority | Android Agent | iPhone Agent | Server | Comments |
|---|---|---|---|---|---|---|
| | | | | | | |

## 2.3. OpSec Requirements

None specific to Pony

# 3. Technical Solution

## 3.1. Android Side

### 3.1.1. Installer Sting

Installer shall report new agent type in sting [redacted]

### 3.1.2. Agent Log

Agent shall report new agent type in log # 1 : [redacted]

### 3.1.3. Data Limitations

1. IMSI - As Pony cannot access this data, it shall be synthesized as [redacted] are available).
2. IMEI - As Pony cannot access this data, a guaranteed unique and target-specific value shall be synthesized from other information and sent instead.

## 3.2. Server Side

1. Maintain information that this is a Pony agent
2. Enforce HMCC, CMCC logic as for other agents

## 3.3. UI Side

1. Special indication for Pony agent per Product requirement **TBD**
2. Do **not** show "fake" IMEI and IMSI data.

# 4. Future Enhancements

(discuss current tradeoffs and design decisions, describe alternatives that may be implemented in the fullness of time)

# 5. Considerations

## 5.1. QA

1. How is the feature tested end-to-end?



HIGHLY CONFIDENTIAL - ATTORNEYS EYES ONLY NSO_WHATSAPP_00001243

2. Is there a relevant difference between dev and staging/production environments?
3. QA automation

**Redacted –Export Controlled**

## 5.2. Maestro / exportData

Do we want to indicate ake IMSI/IMEI?

## 5.3. Tacticals

## 5.4. Deployment & Support

1. Installation changes, new/changed configurations
2. F5 configuration - new ports, headers, size limitations, etc.
3. VPNng capabilities, dependencies
4. Sync Server, Prettifier

**Redacted –Export Controlled**

## 5.5. NOC

What needs to be monitored by NOC? What triggers and alert and what should be the response?

## 5.6. BI

What data be collected and from where?

# 6. Related

Functionality - What's accessible in the WhatsApp context

# 7. Open Issues

No labels



HIGHLY CONFIDENTIAL - ATTORNEYS EYES ONLY NSO_WHATSAPP_00001244

# Exhibit 58

**UNREDACTED VERSION OF DOCUMENT PROPOSED**

**TO BE FILED UNDER SEAL**

You no longer have access Support and Updates. Renew online, remind me later or never remind me again.



# Heaven accounts availability - PS behavior

Created by [redacted] last modified on May 14, 2018

**You are viewing an old version of this page. View the current version.**

Compare with Current · Restore this Version · View Page History

« Previous **Version 9** Current »

**Check List -**

| Role | Name | Date | Status |
|---|---|---|---|
| Product Manger | [redacted] | 02/05/18 | Approved |
| Product Lead | | | |
| Frontend TL | | | |
| Backend TL | | | |
| Solution Architect | | | |

**Motivation (Problems today)-**

1. Installation can currently be initiated even when there are no WhatsApp account available (all WA accounts, FFP or attack, are either blocked by WA or expired in system)
2. Installation would fail if all WhatsApp attack accounts are in cool down (after the FFP attempt or during scheduled attack).

**Requirements -**

1. After pressing 'Install', check for at least 'MIN FP accounts' (should be considered if FFP is enabled) and 'MIN Attack accounts' available, i.e., not blocked or expired.
    a. If there is → continue to installation
    b. Else →
        i. UI pop up "Covert Android service is currently unavailable. Please contact your system administrator" (It was confirmed Hadas)
        ii. Add indicative log in the DB (agreed it will be in agent error log table, without ref table so it would NOT appear in the UI)
    c. Min FP accounts - X
    d. Min Attack account available - Y
    e. Support X=0 or Y=0 in the configuration (feature disable)

2. After FFP succeed/ FFP Failed/ FFP disabled (scheduler stage)



HIGHLY CONFIDENTIAL - ATTORNEYS EYES ONLY NSO_WHATSAPP_00001022

a. if all attack accounts are in cool down -> continue the installation until 'installation overall time expired' (check again in X min)
    i. Agreed it will be the same mechanisms of installation expiration today (1440 sec for overall installations)
b. if there were no accounts available during the attack stage time →installation should be failed
    i. There is no option to add indicative log, so we are assuming that Heaven installation that failed due to expiration limit will be because the attack accounts were unavailable.

No labels



HIGHLY CONFIDENTIAL - ATTORNEYS EYES ONLY NSO_WHATSAPP_00001023

# Exhibit 59

**UNREDACTED VERSION OF DOCUMENT PROPOSED**

**TO BE FILED UNDER SEAL**

You no longer have access Support and Updates. Renew online, remind me later or never remind me again.



# How to configure new ABS

Created by Unknown User [redacted] last modified on Apr 17, 2019

**You are viewing an old version of this page. View the current version.**

Compare with Current · Restore this Version · View Page History

« Previous **Version 2** Next »

[redacted]

[redacted]

5. [redacted]

Verify the file is configured as follows:

[redacted]



HIGHLY CONFIDENTIAL - ATTORNEYS EYES ONLY NSO_WHATSAPP_00001032

{
Redacted – PII
[redacted]
{
Redacted – PII
[redacted]
Redacted – PII
[redacted]
" Redacted – PII ----→WA server IP
[redacted]



HIGHLY CONFIDENTIAL - ATTORNEYS EYES ONLY NSO_WHATSAPP_00001033

6. Save and restart ABS - Make sure to set the IP in WIS  PROVIDERS file in PS config in case its new ABS with new IP

No labels



HIGHLY CONFIDENTIAL - ATTORNEYS EYES ONLY NSO_WHATSAPP_00001034

# Exhibit 60

**UNREDACTED VERSION OF DOCUMENT PROPOSED**

**TO BE FILED UNDER SEAL**

You no longer have access Support and Updates. Renew online, remind me later or never remind me again.



# Opsec Rule Engine - PRD

Created by [redacted] last modified on Mar 29, 2020



**References**:

- The technical spec: Installation Limitation Specification - DRAFT
- This PRD document in presentation format: Attached

## Motivation

The Opsec operational guidelines assure that operations done via our system towards the outside world are performed at minimal risk of exposure.

These guidelines are defined by quantity limits, time limits (cool-down), and other abuse prevention rules - e.g. installation limitations, installation cool down periods, account activation limitations and command limitations.

The Opsec guidelines are currently enforced in several places across the system (platform, agents installation servers, Redacted – Export Controlled Redacted – Export Controlled mostly as hard coded rules.

As such, every addition or change to the guidelines logic requires coding, and is not clearly transparent to us (R&D and support).

## Solution goals

**Code independence** - Minimize the need for writing code to handle new Opsec requirements

**Coverage** - Aim to cover the full range Opsec cases, e.g. from general installation cases to the very specific vector and target identifier cases, from all systems involved.

**Centralized** – Have all Opsec requirements in one place.



HIGHLY CONFIDENTIAL - ATTORNEYS EYES ONLY NSO_WHATSAPP_00008986

**Multisystem service** - serve all systems/products that should enforce the Opsec requirements – C&C Platform, agents installation servers, Redacted – Export Controlled and new product

**Visibility** – all Opsec rules can be accessible and readable to R&D and support

**Performance** – Minimal impact on relevant flows, response time < 1 second.. For real-time scenarios (e.g. inline) < 100 ms

# The solution principals

**Engine** - A central rule based engine.

**Opsec rules** - A set of Opsec rules maintained by the Opsec team that can meet the full coverage of all use cases.

**Thresholds** - Thresholds to the rules defined by the Opsec team and support team.

**Request API** - The engine exposes an API that receives a request, checks it against the Opsec rules and reports back if the request is approved or denied.

**API use** - Our various systems/products embeds calls to the API in critical junctions of their workflows to determine if they can proceed with the workflow or not due to Opsec reasons.

The Opsec engine purpose is to provide a go/no go indication (allow or block) to Opsec critical steps in the system operation.

It should be incorporated as a check point in sensitive steps of operational workflows that involve interactions with target devices, 3rd party web services, or other entities in the 'outside" world.

As such it will be used in installation processes and command processes.

It should be integrated in the processes as an function that receives the desired operation (e.g. Covert installation) and its destination (e.g. target MSISDN), an return in response if the process is allowed to continue or not.

# Opsec rule examples

## Existing Opsec rules examples

MSISDN in black list

Max 1 attempt in progress per MSISDN

Max 3 installation attempts per MSISDN in last 24 hours

**Redacted – Export Controlled**

Max 7 links(actual and potential) per MSISDN in last 24 hours

Max 2 external links in last 24 hours

Max 2 Erised installation failed in in last 24 hours

**Redacted – Export Controlled**

Max 50 links in last 24 hours

**Redacted – Export Controlled**

OK to install if last successful installation to MSISDN > 3 days AND MSISDN did no communication > 1 day. (Max 1 successful installation per MSISDN in last 3 days AND Max agent last communication per MSISDN in last 24 hours)



HIGHLY CONFIDENTIAL - ATTORNEYS EYES ONLY NSO_WHATSAPP_00008987

Redacted – Export Controlled

Max 1 100Mb total file download per agent source MSISDN size in last 24 hours

Max 100 enabled certificates (in agents)

## Future Opsec rules examples

Max 3 installation attempts per IMEI in last 24 hours

Max 3 installation attempts per hashed MSISDN (deleted target) in last 24 hours

# Redacted – Export Controlled

Max 6 SMS messages per MSISDN in last 24 hours

Max 10 tap commands in last 24 hours

## Rule structure

- Rule id
- Priority/order (1-highest)
- Opsec rule definition
- User message
  (as today, messages should not state the reason, as not to reveal the fact that agent was installed by someone else. Optionally we could have a message conditional – a more informative message if the other installed target is in the operator's permissions group, and an obscure one if not in permission group)
- Can request again (No, Yes, Yes in X time_unit)
- Overrule level (1-highest)

Opsec rule definition:

- Who – Identifier type or family of identifier types – MSISDN, IMEI, MAC, IMSI, hashed MSISDN, token, source id or any other identifier
- What – action or family of actions – Redacted – Export Controlled durable android, inline, external link, Redacted – Export Controlled certificate placement, fingerprint, SMS message, Redacted – Export Controlled. Can also be split into Action, action type, action subtype – e.g. Install>[redacted]covert or Activate_account>Dropbox
- When - Period
- Condition –
  - related the results of prior similar actions or to prior different actions (e.g. a new request for 1-click installation that is conditioned to prior covert installation)
  - conditions can be based on
    - sent installation attempt/messages/links/activation/fingerprint/commands
    - successful installations/activation/commands
    - failed installations/activation/commands and their failure reason
    - expired installations/activation/commands
    - other (e.g. blacklist)
- How many - Limit

For more complex rule the When+Condition+How many could be multiplied with AND operator between them. For the example: Max 1 successful installation per MSISDN in last 3 days AND Max agent last communication per MSISDN in last 24 hours



HIGHLY CONFIDENTIAL - ATTORNEYS EYES ONLY NSO_WHATSAPP_00008988

For family of identifier types, single identifier type would be mapped into families. “Any” – identifier is not applicable to rule

For family of actions, single actions would be mapped into families. “Any” – action is not applicable to rule, while “Any installation” should list all installation types

# Opsec rule definition examples

**Vector limit**

- [redacted]

[redacted]

**Vector per target limit**

- [redacted]

[redacted]

**Vector per target limit for specific failure**

- [redacted]

[redacted]

**Attempt in progress**

- [redacted]

[redacted]

**File request command**

- [redacted]

[redacted]



HIGHLY CONFIDENTIAL - ATTORNEYS EYES ONLY NSO_WHATSAPP_00008989

# Request API

Processes of the different systems should use the API at predefined stages of the workflow to determine if the workflow can proceed.

**Engine call parameters:**

- Identifiers (type and value)– MSISDN, IMEI, IMSI, MAC…
- Action – [Redacted – Export Controlled] durable android, [Redacted – Export Controlled] certificate placement, …
- Additional data (e.g. requested file size)

**Engine call response:**

- OK/block
- Block period: always, duration/till, none
- Message to user
- Rule id

# Request handling

Scan the defined rules by their order/priority, for each rule

**Step 1: Whitelist check**

If request identifier in whitelist

and

rule overrule level >= identifier overrule level in whitelist

then proceed to next rule (rule whitelisted)

else proceed to step 2

**Step 2: Rule match**

If request identifier type match the rule identifier type or belongs to rule identifier family

and

if request action match the rule action or belongs to rule action family

then proceed to Step 3

else proceed to next rule

**Step 3: Rule check**

Count records that fit rule condition in period

If count < rule limit proceed to next rule

If count >= rule limit return Block, rule block period, rule message to user



HIGHLY CONFIDENTIAL - ATTORNEYS EYES ONLY NSO_WHATSAPP_00008990

If all rules scanned, return OK

# Potential API

## Potential for target

Use case examples:

In the UI we would like to know which vectors are available for specific MSISDN

In the UI we would like to know if the reinstall button can be enabled

In the UI block file request of files bigger that 20Mb

In the UI block certificate if certificate quota reached

**Engine call parameters:**

- Identifiers (type & value) – MSISDN, IMEI, IMSI,…
- Action family
- Additional data (e.g. requested file size)

**Engine call response:**

- List of currently available actions
- Time of next action “release” (e.g. when device can be installed again)

## Potential for vector

Use case examples:

In the Ui, show how many installations remaining for s specific vector

In the Ui, show when installing via a specific vector will be available again

**Engine call parameters:**

- Action or action family

**Engine call response:**

- Action limit
- Number of available actions
- Action period
- Time of next action “release” (when it no longer relevant to the vector)

# Rules management

Morpheus support



HIGHLY CONFIDENTIAL - ATTORNEYS EYES ONLY NSO_WHATSAPP_00008991

Phase 1: set all rules parameters - thresholds and periods – with defaults. Some values are read-only and some can be configured per customer manually or by templates.

Phase 2: UI to define rules (+ export and import), whitelist overrule levels

# Logging

Log

- All requests sent to engine (request and potential APIs)
- Return status (OK / blocked by rule id xxx / potential).
- Intelligence data should be hashed

Log use

- Alerts
- Maintenance investigation
- BI analysis
  (which rules are used, locate rules that can be removed, response time, fine tune rules parameters)

# Special considerations:

- Engine does not need to know which vectors are available to the customer (PS responsibility to do the matching)
- In 1-click SMS installations, an insulation attempt could contain several messages and several links, we count actual links that were sent to the device and potential links. Potential links are scheduled to be sent later, if sent they'll change from potential to actual, but can be aborted by user or system, and then they are no longer counted as potential. .
- Daily usage should show available installations per vector, and time of next available installation with a vector that is now not available.
- White list in Morpheus will have overrule level. We can implement this mechanism later and start with default of 1 – meaning white list overrules all rules (including blacklist)

# Development plans

Engine development stages – TBD

Systems and processes migration to requests API– TBD

Platform migration to potential API – TBD

Automation testing – TBD

Morpheus support for parameter settings, rules definition - TBD

No labels



HIGHLY CONFIDENTIAL - ATTORNEYS EYES ONLY NSO_WHATSAPP_00008992

# Exhibit 61

**UNREDACTED VERSION OF DOCUMENT PROPOSED**

**TO BE FILED UNDER SEAL**

You no longer have access Support and Updates. Renew online, remind me later or never remind me again.



# New OpSec Alerts - Prioritization

Created by Unknown User [redacted] last modified on Dec 04, 2019

**You are viewing an old version of this page. View the current version.**

Compare with Current · Restore this Version · View Page History

« Previous **Version 29** Next »

Details about each alert can be found at OpSec Alerts Documentation.

The current priority, from high to low, is elaborated in the following table:

| Task | Status | Data Location | Notes |
|---|---|---|---|
| check bootique agent not communicating | | PS DB | Decide on threshold based on splunk info |
| Implement Vitaly's prettifier / DNS / iptables log analysis script | | | Use AV vendors / Google / [redacted] / CL (ASN based search) for suspicious ranges |
| check multiple token invalidations on a target | | | ▪ Check where the data is saved<br>▪ Decide on threshold along with [redacted] personal |
| check multiple token invalidations on a cloud | | | • Check where the data is saved<br>• Decide on threshold along with [redacted] personal |
| Check access to IS without correct referrer | | F5 logs | Waiting for support to deploy the referrer to the F5 logs<br>▪ Check with Mano if it can be implemented |
| Check port scan on PS | | | • Waiting for development |
| Check port scan on IS | | | • Waiting for development |
| Remove "Check Source Suicide" with code 3502 from monitor | READY FOR EINI | | |
| Enhance the "Check IM Info" (looks for dangerous phrases is IM) so that it won't alert on messages older than 1 year. | READY FOR EINI | | |
| Remove the "Geo Validation Forbidden MCC" from monitor | READY FOR EINI | | |



HIGHLY CONFIDENTIAL - ATTORNEYS EYES ONLY NSO_WHATSAPP_00001079

| | | | |
|---|---|---|---|
| Deploy the new "Check Subscriber Info MCC Undetermined during Installation" alert | READY FOR EINI | | The relevant PS version which adds this alert is 4.9 and will be deployed on 5/12.<br>The code to monitor is [redacted] |
| Deploy the new "check certificate pinning failure" alert | READY FOR EINI | | 1. More details on the implementation in OpSec Alerts Documentation<br>2. [redacted] - If the current MITM alert is indeed referring this one, please modify the name to: "Agent Certificate Pinning Failure". Otherwise, implement the new one.<br>a. Verify the name change with Maor & the NOC |
| Plan the "Sinkhole Monitoring" alert | | | Scripts currently in development |
| Plan "Certificate Monitoring" alert using CT | | | Scripts currently in development |
| Implement the "check Erised failure" ratio with the Nagios system | | | checked every 6 hours and will alert us if in the last 12 hours there have been no successful Erised attempts and at least 10 failures<br>Discuss how to implement because it is cross-customers |
| Deploy the "check access with pre-trident URL format" alert, based on IS logs | READY FOR EINI | | I've verified with @Unknown User [redacted] and such requests will reach the IS, as the F5 doesn't perform validation on the URL. |
| Inline sensor | | | |
| Check string timings anomalies | | | Currently on server-side development |
| | | | |

No labels



HIGHLY CONFIDENTIAL - ATTORNEYS EYES ONLY NSO_WHATSAPP_00001080

# Exhibit 62

**UNREDACTED VERSION OF DOCUMENT PROPOSED**

**TO BE FILED UNDER SEAL**

You no longer have access Support and Updates. Renew online, remind me later or never remind me again.



# Abuse Prevention

Created by [redacted] last modified on Jun 19, 2018

**Check List -**

| Role | Name | Date | Status |
|---|---|---|---|
| Product Lead | [redacted] | 09.04.18 | Approved |
| Backend TL | | | |
| Frontend TL | | | |

## Background & Motivation

- OpSec limitations defining time intervals between installation attempts per phone number should be different per installation vector, the installation stage and the scratch in front of the target
- Joint limitations defined for installation vectors requires configuring the time interval per the "worst case scenario" ending in many requests from clients to detour the limitations and add numbers to the white list
- Lack of persistency is urging clients to re-install the same targets many times in short time frames

## Requirements

The allowed time interval between installation attempts per phone number should be as following:

| Installation type | Time between successful installations | Time from last communication ⭐ | Time between failed installations | Time between unsupported device failures | Time between failed installations on GeoIP |
|---|---|---|---|---|---|
| **SMS** | 3 days | 24H (installations on the same phone number are not allowed if 24H didn't pass) | 3 days | 7 days | 7 days **it was not developed in 2.70** |
| **Redacted – Export Controlled** | | | **Redacted – Export Controlled** | | |
| **Heaven** | 3 days | | Before a call was performed: 0 days<br>After a call was performed: 3 days | Per the new state "Device not supported for Covert Android": 7 day | |
| **WAP** | 3 days | | 3 days | 7 days | |

⭐ in addition to 'time between successful installations'



HIGHLY CONFIDENTIAL - ATTORNEYS EYES ONLY NSO_WHATSAPP_00008916

in green - currently exist, in black - should be part of 2.70.

Note: Generated links (Hotspot, Multishot, tactical) are not limited within this process

Changes needed in 2.70:

UI:

- Separate between vectors (according to the table) cross all scenarios according to table
- Regarding Heaven failed installations - requires Server to define the state (before and after call)

Server:

- Separate state for heaven installation prior and after a call was performed
- Opsec limitations – need to finalize reqs with Kfir [redacted]

No labels

## 6 Comments

**Redacted – Export Controlled**

Unknown User Redacted – PII

Regarding:

- Separate between vectors (according to the table) cross all scenarios according to table

Do we want to separate even for the values that are the same across all vectors, such as **Time from last communication?**

Unknown User [redacted]

No need to separate "Time from last communication" and Geo IP. but do separate the 1-click and Heaven even if both are 3 days in "Successful".

like in the table - if separated - separate. if not- can be united for all

**Redacted – Export Controlled**

Unknown User Redacted – PII

1. Our assumption is that [redacted] is always lower than [redacted]
2. If there's a previous failure but no status code in [redacted] (for example, the failed installation was via sms), UI will take the [redacted]



HIGHLY CONFIDENTIAL - ATTORNEYS EYES ONLY NSO_WHATSAPP_00008917

HIGHLY CONFIDENTIAL - ATTORNEYS EYES ONLY NSO_WHATSAPP_00008918