*Journal of Computations & Modelling, Vol. 10, No. 2, 2020, 1-24*
*ISSN: 1792-7625 (print), 1792-8850 (online)*
*https://doi.org/10.47260/jcomod/1021*
*Scientific Press International Limited*

# Mathematical Study of Advanced Persistent Threat (APT) Hunting Techniques

**Argyrios (Argi) Alexopoulos[1] and Nicholas J. Daras[2]**

## Abstract

The paper documents, based mainly on **[3]-[6]** published papers where a consistent mathematical description of cyberspace and various types of Cyber-Attacks and protection measures are presented, a holistic mathematical approach to a rigorous description of Advanced Persistent Threat (APT) actors' modus operandi through various scenarios and Cyber Kill Chain stages **[2]**. After referring **[6]** to the various elements of Cyber-Attacks we propose some techniques (via 5 scenarios) of tracking the modus operandi of the most sophisticated and non-linear cyber actors, the Advanced Persistent Threat actors that are usually nation-state or nation-state backed and usually stay undetected for an extended time in later stages of Cyber Kill Chain in defenders' networks.

**Keywords:** Valuation of cyber assets, vulnerability of cyber assets, node supervision, sophistication of an attack germ of cyber-attack, cyber defense, proactive cyber protection, Advanced Persistent Threat (APT) actors, Indication of Compromise (IOC), Tactics, Techniques and Procedures (TTPs).

[1] Cyberspace Analyst staff in International Organization, Belgium.

[2] Department of Mathematics and Engineering Sciences, Hellenic Military Academy, 166 73, Vari Attikis, Greece.

Article Info: *Received:* October 12, 2020. *Revised*: October 27, 2020.
*Published online:* November 6, 2020.

# 1. Introduction

The aim of the present paper is, based on the previous published papers **[3], [4]. [5], [6]** to document a rigorous description of Advanced Persistent Threat (APT) actors' modus operandi through scenarios and various Cyber Kill Chain stages. To this end, Sections 2 to 6, based on all necessary elements (among others, definition of Cyberspace, Cyber Valuation/Vulnerability) from **[3]**, **[4], [5],** and **[6]** we describe the means to detect the modus operandi and some TTPs (Tactics, Techniques and Procedures) through 5 scenarios that the most sophisticated cyber actors (APTs) use to evolve cyber complex attacks **[1]**. Identifying these vectors through the Cyber Kill Chain the defenses are straight forward and no value would be added enumerating them.

# 2. APT Hunting Scenario 1

The APT actor, that in this section will be depicted as $\boldsymbol{Z_{APT}}$, clandestinely relays and possibly modifies the communication between two nodes who suppose that they are directly exchange info with each other.
In this scenario the **node** $\boldsymbol{Z_{APT}}$, that is the APT actor, cyber-interacts between nodes $\boldsymbol{U}$ and $\boldsymbol{V}$ . Actually in this "active" intersection attack, instead of this "normal" interaction we experience an active attack from node $\boldsymbol{Z_{APT}}$ to either or/and both of other nodes **using some resources of the other interacted node**. In such a case, a family of coherent interactions

$$\boldsymbol{\mathcal{F}} = \Big\{\boldsymbol{Z_{APT}} = \boldsymbol{Z_{APT_{(Y,X)}}}(\boldsymbol{t}) = \big((\mathbb{z}_{\mathbf{1}}, \mathbb{w}_{\mathbf{1}}), (\mathbb{z}_{\mathbf{2}}, \mathbb{w}_{\mathbf{2}}), (\mathbb{z}'_{\mathbf{1}}, \mathbb{w}'_{\mathbf{1}}), (\mathbb{z}'_{\mathbf{2}}, \mathbb{w}'_{\mathbf{2}})\big)(\boldsymbol{t}) \in \big(\mathbb{C}^{\mathbf{n}\times\boldsymbol{k}} \times \mathbb{C}^{\mathbf{m}\times\boldsymbol{k}}\big)^{\mathbf{4}}, \boldsymbol{t} \in \mathbb{I}\Big\},$$

lying in the partial danger sector $\mathcal{E} = \mathcal{E}_{\boldsymbol{Z_{APT}\to V}}$ to the node $\boldsymbol{V}$ from the node $\boldsymbol{Z_{APT}}$ during the entire time set $\mathbb{I}$, is a **germ [6] of (partial) active attack against the**

$(\boldsymbol{\mu_1}, \dots, \boldsymbol{\mu_\nu})-$ **device parts** $\boldsymbol{fr\left(dev_{\mu_1}^{(V)}\right)}$, $\boldsymbol{fr\left(dev_{\mu_2}^{(V)}\right)}$,..., $\boldsymbol{fr\left(dev_{\mu_\nu}^{(V)}\right)}$ **of** $\boldsymbol{V}$ **and the** $(\boldsymbol{\kappa_1}, \dots, \boldsymbol{\kappa_\lambda})-$ **resource parts** $\boldsymbol{fr\left(res_{\kappa_1}^{(V)}\right)}$, $\boldsymbol{fr\left(res_{\kappa_2}^{(V)}\right)}$,..., $\boldsymbol{fr\left(res_{\kappa_\lambda}^{(V)}\right)}$ **of** $\boldsymbol{V}$, during a given time set $\mathbb{I} \subset\subset [\mathbf{0}, \mathbf{1}]$, if, whenever $\boldsymbol{t} \in \mathbb{I}$, the pair $\big((\mathbb{z}_{\mathbf{1}}, \mathbb{w}_{\mathbf{1}}), (\mathbb{z}_{\mathbf{2}}, \mathbb{w}_{\mathbf{2}})\big) \in \big(\mathbb{C}^{\mathbf{n}\times\boldsymbol{k}} \times \mathbb{C}^{\mathbf{m}\times\boldsymbol{k}}\big)^{\mathbf{2}}$ of supervisory resource perceptions of $\boldsymbol{Z_{APT}}$ and $\boldsymbol{V}$ in the system of nodes $\boldsymbol{Z_{APT}}$ and $\boldsymbol{V}$ has the form
$\big((\mathbb{z}_{\mathbf{1}}, \mathbb{w}_{\mathbf{1}}), (\mathbb{z}_{\mathbf{2}}, \mathbb{w}_{\mathbf{2}})\big) =$

$$\left(\left(\begin{array}{ccc} a_{1,1}^{(Z_{APT}\rightsquigarrow V)} + i\ \widehat{a}_{1,1}^{(V\rightsquigarrow V)} & \cdots & a_{1,\mathfrak{n}}^{(Z_{APT}\rightsquigarrow V)} + i\ \widehat{a}_{1,\mathfrak{n}}^{(V\rightsquigarrow V)} \\ \cdots & \cdots & \cdots \\ a_{m_V,1}^{(Z_{APT}\rightsquigarrow V)} + i\ \widehat{a}_{m_V,1}^{(V\rightsquigarrow V)} & & a_{m_V,\mathfrak{n}}^{(Z_{APT}\rightsquigarrow V)} + i\ \widehat{a}_{m_V,\mathfrak{n}}^{(V\rightsquigarrow V)} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \\ a_{\mathcal{M}_V+1,1}^{(Z_{APT}\rightsquigarrow V)} + i\ \widehat{a}_{\mathcal{M}_V+1,1}^{(V\rightsquigarrow V)} & \cdots & a_{\mathcal{M}_V+1,\mathfrak{n}}^{(Z_{APT}\rightsquigarrow V)} + i\ \widehat{a}_{\mathcal{M}_V+1,\mathfrak{n}}^{(V\rightsquigarrow V)} \\ \cdots & \cdots & \cdots \\ a_{\mathcal{M}_V+\ell_V,1}^{(Z_{APT}\rightsquigarrow V)} + i\ \widehat{a}_{\mathcal{M}_V+\ell_V,1}^{(V\rightsquigarrow V)} & \cdots & a_{\mathcal{M}_V+\ell_V,\mathfrak{n}}^{(Z_{APT}\rightsquigarrow V)} + i\ \widehat{a}_{\mathcal{M}_V+\ell_V,\mathfrak{n}}^{(V\rightsquigarrow V)} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \end{array}\right), \right.$$

$$\left.\left(\begin{array}{ccc} b_{1,1}^{(Z_{APT}\rightsquigarrow V)} + i\ \widehat{b}_{1,1}^{(V\rightsquigarrow V)} & \cdots & b_{1,\mathfrak{m}}^{(Z_{APT}\rightsquigarrow V)} + i\ \widehat{b}_{1,\mathfrak{m}}^{(V\rightsquigarrow V)} \\ \cdots & \cdots & \cdots \\ b_{m_V,1}^{(Z_{APT}\rightsquigarrow V)} + i\ \widehat{b}_{m_V,1}^{(V\rightsquigarrow V)} & \cdots & b_{m_V,\mathfrak{m}}^{(Z_{APT}\rightsquigarrow V)} + i\ \widehat{b}_{m_V,\mathfrak{m}}^{(V\rightsquigarrow V)} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \\ b_{\mathcal{M}_V+1,1}^{(Z_{APT}\rightsquigarrow V)} + i\ \widehat{b}_{\mathcal{M}_V+1,1}^{(V\rightsquigarrow V)} & \cdots & b_{\mathcal{M}_V+1,\mathfrak{m}}^{(Z_{APT}\rightsquigarrow V)} + i\ \widehat{b}_{\mathcal{M}_V+1,\mathfrak{m}}^{(V\rightsquigarrow V)} \\ \cdots & \cdots & \cdots \\ b_{\mathcal{M}_V+\ell_V,1}^{(Z_{APT}\rightsquigarrow V)} + i\ \widehat{b}_{\mathcal{M}_V+\ell_V,1}^{(V\rightsquigarrow V)} & \cdots & b_{\mathcal{M}_V+\ell_V,\mathfrak{m}}^{(Z_{APT}\rightsquigarrow V)} + i\ \widehat{b}_{\mathcal{M}_V+\ell_V,\mathfrak{m}}^{(V\rightsquigarrow V)} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \end{array}\right)\right),$$

$$\left(\left(\begin{array}{ccc} a_{1,1}^{(V\rightsquigarrow Z_{APT})} + i\ \widehat{a}_{1,1}^{(Z_{APT}\rightsquigarrow Z_{APT})} & \cdots & a_{1,\mathfrak{n}}^{(V\rightsquigarrow Z_{APT})} + i\ \widehat{a}_{1,\mathfrak{n}}^{(Z_{APT}\rightsquigarrow Z_{APT})} \\ \cdots & \cdots & \cdots \\ a_{m_{Z_{APT}},1}^{(V\rightsquigarrow Z_{APT})} + i\ \widehat{a}_{m_{Z_{APT}},1}^{(Z_{APT}\rightsquigarrow Z_{APT})} & \cdots & a_{m_{Z_{APT}},\mathfrak{n}}^{(V\rightsquigarrow Z_{APT})} + i\ \widehat{a}_{m_{Z_{APT}},\mathfrak{n}}^{(Z_{APT}\rightsquigarrow Z_{APT})} \\ \mathbf{0} & & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \\ a_{\mathcal{M}_{Z_{APT}}+1,1}^{(V\rightsquigarrow Z_{APT})} + i\ \widehat{a}_{\mathcal{M}_{Z_{APT}}+1,1}^{(Z_{APT}\rightsquigarrow Z_{APT})} & \cdots & a_{\mathcal{M}_{Z_{APT}}+1,\mathfrak{n}}^{(V\rightsquigarrow Z_{APT})} + i\ \widehat{a}_{\mathcal{M}_{Z_{APT}}+1,\mathfrak{n}}^{(Z_{APT}\rightsquigarrow Z_{APT})} \\ \cdots & \cdots & \cdots \\ a_{\mathcal{M}_{Z_{APT}}+\ell_{Z_{APT}},1}^{(V\rightsquigarrow Z_{APT})} + i\ \widehat{a}_{\mathcal{M}_{Z_{APT}}+\ell_{Z_{APT}}Z,1}^{(Z_{APT}\rightsquigarrow Z_{APT})} & \cdots & a_{\mathcal{M}_{Z_{APT}}+\ell_{Z_{APT}},\mathfrak{n}}^{(V\rightsquigarrow Z_{APT})} + i\ \widehat{a}_{\mathcal{M}_{Z_{APT}}+\ell_{Z_{APT}},\mathfrak{n}}^{(Z_{APT}\rightsquigarrow Z_{APT})} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \end{array}\right),\right.$$

$$\begin{pmatrix} \boldsymbol{b}_{1,1}^{(V\rightsquigarrow Z_{APT})}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{1,1}^{(Z_{APT}\rightsquigarrow Z_{APT})} & \cdots & \boldsymbol{b}_{1,\mathfrak{m}}^{(V\rightsquigarrow Z_{APT})}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{1,\mathfrak{m}}^{(Z_{APT}\rightsquigarrow Z_{APT})} \\ \cdots & & \cdots \\ \boldsymbol{b}_{m_Z,1}^{(V\rightsquigarrow Z_{APT})}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{m_{Z_{APT}},1}^{(Z_{APT}\rightsquigarrow Z_{APT})} & \cdots & \boldsymbol{b}_{m_{Z_{APT}},\mathfrak{m}}^{(V\rightsquigarrow Z_{APT})}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{m_{Z_{APT}},\mathfrak{m}}^{(Z_{APT}\rightsquigarrow Z_{APT})} \\ \mathbf{0} & & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \\ \boldsymbol{b}_{\mathcal{M}_{Z_{APT}}+1,1}^{(V\rightsquigarrow Z_{APT})}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{\mathcal{M}_{Z_{APT}}+1,1}^{(Z_{APT}\rightsquigarrow Z_{APT})} & \cdots & \boldsymbol{b}_{\mathcal{M}_{Z_{APT}}+1,\mathfrak{m}}^{(V\rightsquigarrow Z_{APT})}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{\mathcal{M}_{Z_{APT}}+1,\mathfrak{m}}^{(Z_{APT}\rightsquigarrow Z_{APT})} \\ \cdots & & \cdots \\ \boldsymbol{b}_{\mathcal{M}_{Z_{APT}}+\ell_{Z_{APT}},1}^{(V\rightsquigarrow Z_{APT})}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{\mathcal{M}_{Z_{APT}}+\ell_{Z_{APT}}Z,1}^{(Z_{APT}\rightsquigarrow Z_{APT})} & \cdots & \boldsymbol{b}_{\mathcal{M}_{Z_{APT}}+\ell_{Z_{APT}},\mathfrak{m}}^{(V\rightsquigarrow Z_{APT})}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{\mathcal{M}_{Z_{APT}}+\ell_{Z_{APT}},\mathfrak{m}}^{(Z_{APT}\rightsquigarrow Z_{APT})} \\ \mathbf{0} & & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \end{pmatrix}$$

and is depicted, at a next moment $\boldsymbol{t'}=\boldsymbol{t}+\Delta\boldsymbol{t}$, at a pair $\left((\mathbb{z}_{\mathbf{1}}',\mathbb{w}_{\mathbf{1}}'),(\mathbb{z}_{\mathbf{2}}',\mathbb{w}_{\mathbf{2}}')\right)\in\left(\mathbb{C}^{\mathfrak{n}\times\boldsymbol{\kappa}}\times\mathbb{C}^{\mathfrak{m}\times\boldsymbol{\kappa}}\right)^{\mathbf{2}}$ of supervisory resource perceptions of $\boldsymbol{Z_{APT}}=\boldsymbol{Z}$ and $\boldsymbol{V}$ having the form

$\left((\mathbb{z}_{\mathbf{1}}',\mathbb{w}_{\mathbf{1}}'),(\mathbb{z}_{\mathbf{2}}',\mathbb{w}_{\mathbf{2}}')\right)=$

$$\left(\left(\begin{pmatrix} \boldsymbol{a'}_{1,1}^{(Z\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{1,1} & \cdots & \boldsymbol{a'}_{1,\mathfrak{n}}^{(Z\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{1,\mathfrak{n}} \\ \cdots & & \cdots \\ \boldsymbol{a'}_{m_V,1}^{(Z\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{m_V,1} & & \boldsymbol{a'}_{m_V,\mathfrak{n}}^{(Z\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{m_V,\mathfrak{n}} \\ \mathbf{0} & & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \\ \boldsymbol{a'}_{\mathcal{M}_V+1,1}^{(Z\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,1} & \cdots & \boldsymbol{a'}_{\mathcal{M}_V+1,\mathfrak{n}}^{(Z\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{n}} \\ \cdots & & \cdots \\ \boldsymbol{a'}_{\mathcal{M}_V+\ell_V,1}^{(Z\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} & \cdots & \boldsymbol{a'}_{\mathcal{M}_V+\ell_V,\mathfrak{n}}^{(Z\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{n}} \\ \mathbf{0} & & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \end{pmatrix}\right),$$

$$\begin{pmatrix} \boldsymbol{b'}_{1,1}^{(Z\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{1,1} & \cdots & \boldsymbol{b'}_{1,\mathfrak{m}}^{(Z\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{1,\mathfrak{m}} \\ \cdots & & \cdots \\ \boldsymbol{b'}_{m_V,1}^{(Z\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{m_V,1} & \cdots & \boldsymbol{b'}_{m_V,\mathfrak{m}}^{(Z\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{m_V,\mathfrak{m}} \\ \mathbf{0} & & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \\ \boldsymbol{b'}_{\mathcal{M}_V+1,1}^{(Z\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,1} & \cdots & \boldsymbol{b'}_{\mathcal{M}_V+1,\mathfrak{m}}^{(Z\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{m}} \\ \cdots & & \cdots \\ \boldsymbol{b'}_{\mathcal{M}_V+\ell_V,1}^{(Z\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} & \cdots & \boldsymbol{b'}_{\mathcal{M}_V+\ell_V,\mathfrak{m}}^{(Z\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{m}} \\ \mathbf{0} & & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \end{pmatrix},$$

$$\left(\begin{array}{c}\left(\begin{array}{ccc} a'^{(V\rightsquigarrow Z)}_{1,1}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{1,1} & \cdots & a'^{(V\rightsquigarrow Z)}_{1,\mathfrak{n}}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{1,\mathfrak{n}} \\ \cdots & \cdots & \cdots \\ a'^{(V\rightsquigarrow Z)}_{m_Z,1}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{m_Z,1} & \cdots & a'^{(V\rightsquigarrow Z)}_{m_Z,\mathfrak{n}}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{m_Z,\mathfrak{n}} \\ \mathbf{0} & & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & & \mathbf{0} \\ a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+1,1}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{Z+1,1} & \cdots & a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+1,\mathfrak{n}}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+1,\mathfrak{n}} \\ \cdots & & \cdots \\ a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,1}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,1} & & a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,\mathfrak{n}}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,\mathfrak{n}} \\ a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,1}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,1}=a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_W+1,1}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_W+1,1} & \cdots & a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,\mathfrak{n}}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,\mathfrak{n}}=a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_W+1,\mathfrak{n}}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_W+1,\mathfrak{n}} \\ \cdots & & \cdots \\ a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+N,1}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+N,1}=a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_W+\ell_W,1}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_W+\ell_W,1} & \cdots & a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+N,\mathfrak{n}}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+N,\mathfrak{n}}=a'^{(V\rightsquigarrow Z)}_{\mathcal{M}_W+\ell_W,\mathfrak{n}}+i\,\widehat{a}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_W+\ell_W,\mathfrak{n}} \\ \mathbf{0} & & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & & \mathbf{0} \end{array}\right), \\ \left(\begin{array}{ccc} b'^{(V\rightsquigarrow Z)}_{1,1}+i\,\widehat{b}'^{(Z\rightsquigarrow Z)}_{1,1} & \cdots & b'^{(V\rightsquigarrow Z)}_{1,\mathfrak{m}}+i\,\widehat{b}'^{(Z\rightsquigarrow Z)}_{1,\mathfrak{m}} \\ \cdots & \cdots & \cdots \\ b'^{(V\rightsquigarrow Z)}_{m_V,1}+i\,\widehat{b}'^{(Z\rightsquigarrow Z)}_{m_V,1} & \cdots & b'^{(V\rightsquigarrow Z)}_{m_V,\mathfrak{m}}+i\,\widehat{b}'^{(Z\rightsquigarrow Z)}_{m_V,\mathfrak{m}} \\ \mathbf{0} & & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & & \mathbf{0} \\ b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_V+1,1}+i\,\widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_V+1,1} & \cdots & b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_V+1,\mathfrak{m}}+i\,\widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_V+1,\mathfrak{m}} \\ \cdots & & \cdots \\ b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_V+\ell_V,1}+i\,\widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_V+\ell_V,1} & & b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_V+\ell_V,\mathfrak{m}}+i\,\widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_V+\ell_V,\mathfrak{m}} \\ b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,1}+i\,\widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,1}=b'^{(V\rightsquigarrow U)}_{\mathcal{M}_U+1,1}+i\,\widehat{b}'^{(Z\rightsquigarrow U)}_{\mathcal{M}_U+1,1} & \cdots & b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,\mathfrak{m}}+i\,\widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,\mathfrak{m}}=b'^{(V\rightsquigarrow U)}_{\mathcal{M}_U+1,\mathfrak{m}}+i\,\widehat{b}'^{(Z\rightsquigarrow U)}_{\mathcal{M}_U+1,\mathfrak{m}} \\ \cdots & & \cdots \\ b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+N,1}+i\,\widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+N,1}=b'^{(V\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,1}+i\,\widehat{b}'^{(Z\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,1} & \cdots & b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+N,\mathfrak{m}}+i\,\widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+N,\mathfrak{m}}=b'^{(V\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{m}}+i\,\widehat{b}'^{(Z\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{m}} \\ \mathbf{0} & & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & & \mathbf{0} \end{array}\right)\end{array}\right).$$

Following the same process, the identical attack may be conducted against $\boldsymbol{U}$ node without the knowledge of node $\boldsymbol{V}$. According to [6] the sophistication of this attack is low to medium.

Stated in [6], and given that involved nodes have smooth valuations and smooth vulnerabilities, the following status applies during this scenario:

| $\boldsymbol{\varphi^{(U\rightsquigarrow V)}(t), \widehat{\varphi}^{(V\rightsquigarrow V)}(t)}$ | $\boldsymbol{\psi^{(U\rightsquigarrow V)}(t), \widehat{\psi}^{(V\rightsquigarrow V)}(t)}$ |
|---|---|
| $\boldsymbol{\varphi^{(U\rightsquigarrow V)}(t) < 0}$ | $\boldsymbol{\psi^{(U\rightsquigarrow V)}(t) > 0}$ |
| $\boldsymbol{\widehat{\varphi}^{(V\rightsquigarrow V)}(t) < 0}$ | $\boldsymbol{\widehat{\psi}^{(V\rightsquigarrow V)}(t) > 0}$ |
| $\boldsymbol{\varphi^{(V\rightsquigarrow U)}(t) < 0}$ | $\boldsymbol{\psi^{(V\rightsquigarrow U)}(t) > 0}$ |
| $\boldsymbol{\widehat{\varphi}^{(U\rightsquigarrow U)}(t) < 0}$ | $\boldsymbol{\widehat{\psi}^{(U\rightsquigarrow U)}(t) > 0}$ |
| $\boldsymbol{\varphi^{(Z_{APT}\rightsquigarrow V)}(t) < 0}$ | $\boldsymbol{\psi^{(Z_{APT}\rightsquigarrow V)}(t) > 0}$ |
| $\boldsymbol{\varphi^{(V\rightsquigarrow Z_{APT})}(t) > 0}$ | $\boldsymbol{\psi^{(V\rightsquigarrow Z_{APT})}(t) < 0}$ |
| $\boldsymbol{\widehat{\varphi}^{(Z_{APT}\rightsquigarrow Z_{APT})}(t) > 0}$ | $\boldsymbol{\widehat{\psi}^{(Z_{APT}\rightsquigarrow Z_{APT})}(t) < 0}$ |
| $\boldsymbol{\varphi^{(Z_{APT}\rightsquigarrow U)}(t) < 0}$ | $\boldsymbol{\psi^{(Z_{APT}\rightsquigarrow U)}(t) > 0}$ |
| $\boldsymbol{\varphi^{(U\rightsquigarrow Z_{APT})}(t) > 0}$ | $\boldsymbol{\psi^{(U\rightsquigarrow Z_{APT})}(t) < 0}$ |

## 3. APT Hunting Scenario 2

In second scenario, APT activity is actually a passive attack and the hunting comprises of the monitoring of Cyber activity. A group of coherent interactions

$$\boldsymbol{\mathcal{F} = \{\mathcal{Z} = \mathcal{Z}_{(Y,X)}(t) = \big((\mathbb{z}_1, \mathbb{w}_1), (\mathbb{z}_2, \mathbb{w}_2), (\mathbb{z}'_1, \mathbb{w}'_1), (\mathbb{z}'_2, \mathbb{w}'_2)\big)(t) \in \big(\mathbb{C}^{n\times k} \times \mathbb{C}^{m\times k}\big)^4, t \in \mathbb{I}\}},$$

lying in a partial danger sector $\boldsymbol{\mathcal{E} = \mathcal{E}_{U\rightarrow V}}$ to the node $\boldsymbol{V}$ from the node $\boldsymbol{Z_{APT} = Z}$ during the entire time set $\mathbb{I}$, is a **germ of (partial) passive attack from an intermediate node $\boldsymbol{Z}$ against the $\boldsymbol{(\kappa_1, \dots, \kappa_\lambda)-}$ resource parts $\boldsymbol{fr\left(res^{(V)}_{\kappa_1}\right)}$, $\boldsymbol{fr\left(res^{(V)}_{\kappa_2}\right)}$,…, $\boldsymbol{fr\left(res^{(V)}_{\kappa_\lambda}\right)}$** of $\boldsymbol{V}$, during a given time subset $\mathbb{I} \subset\subset [\mathbf{0}, \mathbf{1}]$, if, whenever $\boldsymbol{t} \in \mathbb{I}$, the pair $\boldsymbol{\big((\mathbb{z}_1, \mathbb{w}_1), (\mathbb{z}_2, \mathbb{w}_2)\big) \in \big(\mathbb{C}^{n\times k} \times \mathbb{C}^{m\times k}\big)^2}$ of supervisory resource perceptions of $\boldsymbol{U}$ and $\boldsymbol{V}$ in the system of nodes $\boldsymbol{U}$ and $\boldsymbol{V}$ has the form

$$\boldsymbol{\big((\mathbb{z}_1, \mathbb{w}_1), (\mathbb{z}_2, \mathbb{w}_2)\big) =}$$

$$\left(\left(\left(\begin{matrix} \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \\ \boldsymbol{a}^{(Z \rightsquigarrow V)}_{\mathcal{M}_V+1,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(V \rightsquigarrow V)}_{\mathcal{M}_V+1,1} & \cdots & \boldsymbol{a}^{(Z \rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(V \rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{n}} \\ \cdots & \cdots & \cdots \\ \boldsymbol{a}^{(Z \rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(V \rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} & \cdots & \boldsymbol{a}^{(Z \rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(V \rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{n}} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \end{matrix}\right),\right.\right.$$

$$\left.\left.\left(\begin{matrix} \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \\ \boldsymbol{b}^{(Z \rightsquigarrow V)}_{\mathcal{M}_V+1,1} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(V \rightsquigarrow V)}_{\mathcal{M}_V+1,1} & \cdots & \boldsymbol{b}^{(Z \rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(V \rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{m}} \\ \cdots & \cdots & \cdots \\ \boldsymbol{b}^{(Z \rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(V \rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} & \cdots & \boldsymbol{b}^{(Z \rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(V \rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{m}} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \end{matrix}\right)\right),$$

$$\left(\left(\left(\begin{matrix} \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \\ \boldsymbol{a}^{(V \rightsquigarrow Z)}_{\mathcal{M}_Z+1,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(Z \rightsquigarrow Z)}_{\mathcal{M}_Z+1,1} & \cdots & \boldsymbol{a}^{(V \rightsquigarrow Z)}_{\mathcal{M}_Z+1,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(Z \rightsquigarrow Z)}_{\mathcal{M}_Z+1,\mathfrak{n}} \\ \cdots & \cdots & \cdots \\ \boldsymbol{a}^{(V \rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(Z \rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,1} & \cdots & \boldsymbol{a}^{(V \rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(Z \rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,\mathfrak{n}} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \end{matrix}\right),\right.\right.$$

$$\left.\left.\left(\begin{matrix} \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \\ \boldsymbol{b}^{(V \rightsquigarrow Z)}_{\mathcal{M}_Z+1,1} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(Z \rightsquigarrow Z)}_{\mathcal{M}_Z+1,1} & \cdots & \boldsymbol{b}^{(V \rightsquigarrow Z)}_{\mathcal{M}_Z+1,\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(Z \rightsquigarrow Z)}_{\mathcal{M}_Z+1,\mathfrak{m}} \\ \cdots & \cdots & \cdots \\ \boldsymbol{b}^{(V \rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,1} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(Z \rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,1} & \cdots & \boldsymbol{b}^{(V \rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(Z \rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,\mathfrak{m}} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \end{matrix}\right)\right)\right)$$

and is depicted, at a next moment $\boldsymbol{t}' = \boldsymbol{t} + \Delta\boldsymbol{t}$, at a pair $\left((\mathbb{z}'_{\mathbf{1}}, \mathbb{w}'_{\mathbf{1}}), (\mathbb{z}'_{\mathbf{2}}, \mathbb{w}'_{\mathbf{2}})\right) \in \left(\mathbb{C}^{\mathfrak{n}\times\mathfrak{k}} \times \mathbb{C}^{\mathfrak{m}\times\mathfrak{k}}\right)^{\mathbf{2}}$ of supervisory resource perceptions of $\boldsymbol{Z}$ and $\boldsymbol{V}$ having the form

$$\left((\mathbb{z}'_{\mathbf{1}}, \mathbb{w}'_{\mathbf{1}}), (\mathbb{z}'_{\mathbf{2}}, \mathbb{w}'_{\mathbf{2}})\right) =$$

$$\left(\left(\begin{pmatrix} \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \boldsymbol{a}'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+1,1} + \boldsymbol{i}\ \widehat{\boldsymbol{\beta}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,1} & & \boldsymbol{a}'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{n}} \\ \cdots & & \cdots \\ \boldsymbol{a}'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} & & \boldsymbol{a}'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{n}} \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \end{pmatrix}, \right.$$

$$\left.\begin{pmatrix} \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \boldsymbol{b}'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+1,1} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,1} & & \boldsymbol{b}'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{m}} \\ \cdots & & \cdots \\ \boldsymbol{b}'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} & & \boldsymbol{b}'^{(Z\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{m}} \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \end{pmatrix}\right),$$

$$\left(\begin{pmatrix} \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \boldsymbol{a}'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+1,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+1,1} & & \boldsymbol{a}'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+1,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+1,\mathfrak{n}} \\ \cdots & & \cdots \\ \boldsymbol{a}'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,1} & & \boldsymbol{a}'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,\mathfrak{n}} \\ \boldsymbol{a}'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,1} & & \boldsymbol{a}'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,\mathfrak{n}} \\ \cdots & & \cdots \\ \boldsymbol{a}'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+\nu,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+\nu,1} & & \boldsymbol{a}'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+\nu,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+\nu,\mathfrak{n}} \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \end{pmatrix}\right),$$

$$\begin{pmatrix} \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+1,1} + i\ \widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+1,1} & & b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+1,\mathfrak{n}} + i\ \widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+1,\mathfrak{n}} \\ \cdots & & \cdots \\ b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,1} + i\ \widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,1} & & b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,\mathfrak{n}} + i\ \widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z,\mathfrak{n}} \\ b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,1} + i\ \widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,1} & & b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,\mathfrak{n}} + i\ \widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+1,\mathfrak{n}} \\ \cdots & & \cdots \\ b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+\nu,1} + i\ \widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+\nu,1} & & b'^{(V\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+\nu,\mathfrak{n}} + i\ \widehat{b}'^{(Z\rightsquigarrow Z)}_{\mathcal{M}_Z+\ell_Z+\nu,\mathfrak{n}} \\ \mathbf{0} & & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \end{pmatrix}.$$

It is possible an identical attack to be conducted against $\boldsymbol{U}$ node without the knowledge of $\boldsymbol{V}$. Most of the times, according to [6] the sophistication of this attack is medium to high due to "passive" orientation of this.
Specifically, during this APT attack the following states applies:

| $\boldsymbol{\varphi^{(U\rightsquigarrow V)}(t), \widehat{\varphi}^{(V\rightsquigarrow V)}(t)}$ | $\boldsymbol{\psi^{(U\rightsquigarrow V)}(t)\psi^{\varphi}, \widehat{\psi}^{(V\rightsquigarrow V)}(t)\ \psi^{c}}$ |
|---|---|
| $\boldsymbol{\varphi^{(U\rightsquigarrow V)}(t) = 0}$ | $\boldsymbol{\psi^{(U\rightsquigarrow V)}(t) = 0}$ |
| $\boldsymbol{\widehat{\varphi}^{(V\rightsquigarrow V)}(t) = 0}$ | $\boldsymbol{\widehat{\psi}^{(V\rightsquigarrow V)}(t) = 0}$ |
| $\boldsymbol{\varphi^{(V\rightsquigarrow U)}(t) = 0}$ | $\boldsymbol{\psi^{(V\rightsquigarrow U)}(t) = 0}$ |
| $\boldsymbol{\widehat{\varphi}^{(U\rightsquigarrow U)}(t) = \mathbf{0}}$ | $\boldsymbol{\widehat{\psi}^{(U\rightsquigarrow U)}(t) = 0}$ |
| $\boldsymbol{\varphi^{(Z\rightsquigarrow V)}(t) < 0}$ | $\boldsymbol{\psi^{(Z\rightsquigarrow V)}(t) > 0}$ |
| $\boldsymbol{\varphi^{(V\rightsquigarrow Z)}(t) = 0}$ | $\boldsymbol{\psi^{(V\rightsquigarrow Z)}(t) = 0}$ |
| $\boldsymbol{\widehat{\varphi}^{(Z\rightsquigarrow Z)}(t) > 0}$ | $\boldsymbol{\widehat{\psi}^{(Z\rightsquigarrow Z)}(t) < 0}$ |
| $\boldsymbol{\varphi^{(Z\rightsquigarrow U)}(t) < 0}$ | $\boldsymbol{\psi^{(Z\rightsquigarrow U)}(t) > 0}$ |
| $\boldsymbol{\varphi^{(U\rightsquigarrow Z)}(t) = 0}$ | $\boldsymbol{\psi^{(U\rightsquigarrow Z)}(t) = 0}$ |

## 4. APT Hunting Scenario 3

According to this evolved scenario a highly sophisticated attack, where intruder gains **access** to a device/system and compromise it, takes place. Similarly here the node $\boldsymbol{U}$ is the APT actor that conducts the attack. During this attack the following

general form of cyber-effect applies **[5]**:

$$\boldsymbol{g = g_t}\colon \boldsymbol{\mathcal{Q}_5^{(V)}(U)(t) \to \mathcal{P}_{11}^{(U)}(V)(t')}$$

where $\boldsymbol{\mathcal{Q}_5^{(V)}(U)(t)}$ and $\boldsymbol{\mathcal{P}_{11}^{(U)}(V)(t')}$ are the combinatorial triplets

$$\boldsymbol{\mathcal{Q}_5^{(V)}(U)(t)} = \left(\boldsymbol{\mathfrak{D}^{(fraction)}(U), \mathcal{S}_V\mathfrak{D}^{(fraction)}(U), \mathcal{U}_V\mathfrak{D}^{(fraction)}(U)}\right) \text{ and}$$

$$\boldsymbol{\mathcal{P}_{11}^{(U)}(V)(t')} = \left(\boldsymbol{\mathfrak{D}_{available}^{(fraction)}(V), \mathcal{S}_U\mathfrak{D}_{available}^{(fraction)}(V), \mathcal{U}_U\mathfrak{D}_{available}^{(fraction)}(V)}\right),$$

respectively **([5]).**

In such a case, a family of coherent interactions

$$\boldsymbol{\mathcal{F}} = \left\{\boldsymbol{\mathcal{Z} = \mathcal{Z}_{(Y,X)}(t)} = \left((\mathbb{z}_1, \mathbb{w}_1), (\mathbb{z}_2, \mathbb{w}_2), (\mathbb{z}'_1, \mathbb{w}'_1), (\mathbb{z}'_2, \mathbb{w}'_2)\right)(t) \in \left(\mathbb{C}^{n\times k} \times \mathbb{C}^{m\times k}\right)^4, t \in \mathbb{I}\right\},$$

lying in (a partial danger sector $\mathcal{E} = \mathcal{E}_{U\to V}$ to) the node $\boldsymbol{V}$ from the node $\boldsymbol{U}$ during the entire time set $\mathbb{I}$, is a **germ of (partial) access attack against the** $(\boldsymbol{\mu_1, \dots, \mu_v})-$ **device parts** $\boldsymbol{fr\left(dev_{\mu_1}^{(V)}\right)}$, $\boldsymbol{fr\left(dev_{\mu_2}^{(V)}\right)}$,..., $\boldsymbol{fr\left(dev_{\mu_v}^{(V)}\right)}$ **of** $\boldsymbol{V}$ during a given time subset $\mathbb{I} \subset\subset [\mathbf{0}, \mathbf{1}]$, if, whenever $\boldsymbol{t} \in \mathbb{I}$, the pair $\left((\mathbb{z}_1, \mathbb{w}_1), (\mathbb{z}_2, \mathbb{w}_2)\right) \in \left(\mathbb{C}^{n\times k} \times \mathbb{C}^{m\times k}\right)^2$ of supervisory resource perceptions of $\boldsymbol{U}$ and $\boldsymbol{V}$ in the system of nodes $\boldsymbol{U}$ and $\boldsymbol{V}$ has the form

$$\left((\mathbb{z}_1, \mathbb{w}_1), (\mathbb{z}_2, \mathbb{w}_2)\right) =$$

$$\left(\left(\begin{pmatrix} a_{1,1}^{(W\nrightarrow V)} + i\ \widehat{a}_{1,1}^{(V\nrightarrow V)} & \dots & a_{1,n}^{(W\nrightarrow V)} + i\ \widehat{a}_{1,n}^{(V\nrightarrow V)} \\ \dots & \dots & \dots \\ a_{m_V,1}^{(W\nrightarrow V)} + i\ \widehat{a}_{m_V,1}^{(V\nrightarrow V)} & \dots & a_{m_V,n}^{(W\nrightarrow V)} + i\ \widehat{a}_{m_V,n}^{(V\nrightarrow V)} \\ \mathbf{0} & \dots & \mathbf{0} \\ \dots & & \dots \\ \mathbf{0} & & \mathbf{0} \end{pmatrix},\right.\right.$$

$$\left.\left.\begin{pmatrix} b_{1,1}^{(U\nrightarrow V)} + i\ \widehat{b}_{1,1}^{(V\nrightarrow V)} & \dots & b_{1,m}^{(U\nrightarrow V)} + i\ \widehat{b}_{1,m}^{(V\nrightarrow V)} \\ \dots & \dots & \dots \\ b_{m_V,1}^{(U\nrightarrow V)} + i\ \widehat{b}_{m_V,1}^{(V\nrightarrow V)} & \dots & b_{m_V,m}^{(U\nrightarrow V)} + i\ \widehat{b}_{m_V,m}^{(V\nrightarrow V)} \\ \mathbf{0} & \dots & \mathbf{0} \\ \dots & \dots & \dots \\ \mathbf{0} & \dots & \mathbf{0} \end{pmatrix}\right)\right),$$

$$\left(\begin{pmatrix} \boldsymbol{a}_{1,1}^{(V\rightsquigarrow U)} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}_{1,1}^{(U\rightsquigarrow U)} & \cdots & \boldsymbol{a}_{1,\mathfrak{n}}^{(V\rightsquigarrow U)} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}_{1,\mathfrak{n}}^{(U\rightsquigarrow U)} \\ \cdots & \cdots & \cdots \\ \boldsymbol{a}_{m_U,1}^{(V\rightsquigarrow U)} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}_{m_U,1}^{(U\rightsquigarrow U)} & \cdots & \boldsymbol{a}_{m_U,\mathfrak{n}}^{(V\rightsquigarrow U)} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}_{m_U,\mathfrak{n}}^{(W\rightsquigarrow W)} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \end{pmatrix},\right.$$

$$\left.\begin{pmatrix} \boldsymbol{b}_{1,1}^{(V\rightsquigarrow U)} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}_{1,1}^{(U\rightsquigarrow U)} & \cdots & \boldsymbol{b}_{1,\mathfrak{m}}^{(V\rightsquigarrow U)} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}_{1,\mathfrak{m}}^{(U\rightsquigarrow U)} \\ \cdots & \cdots & \cdots \\ \boldsymbol{b}_{m_U,1}^{(V\rightsquigarrow U)} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}_{m_U,1}^{(U\rightsquigarrow U)} & \cdots & \boldsymbol{b}_{m_U,\mathfrak{m}}^{(V\rightsquigarrow U)} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}_{m_U,\mathfrak{m}}^{(U\rightsquigarrow U)} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \end{pmatrix}\right)\right)\right)$$

and is transformed, at a next moment $\boldsymbol{t}' = \boldsymbol{t} + \Delta\boldsymbol{t}$, at a pair $\left((\mathbb{z}_{\mathbf{1}}', \mathbb{w}_{\mathbf{1}}'), (\mathbb{z}_{\mathbf{2}}', \mathbb{w}_{\mathbf{2}}')\right) \in \left(\mathbb{C}^{\mathfrak{n}\times\mathfrak{k}} \times \mathbb{C}^{\mathfrak{m}\times\mathfrak{k}}\right)^{\mathbf{2}}$ of supervisory resource perceptions of $\boldsymbol{U}$ and $\boldsymbol{V}$ having the form

$\left((\mathbb{z}_{\mathbf{1}}', \mathbb{w}_{\mathbf{1}}'), (\mathbb{z}_{\mathbf{2}}', \mathbb{w}_{\mathbf{2}}')\right) =$

$$\left(\left(\left(\begin{pmatrix} \boldsymbol{a}'^{(U\rightsquigarrow V)}_{\mathbf{1},\mathbf{1}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{\mathbf{1},\mathbf{1}} & \cdots & \boldsymbol{a}'^{(U\rightsquigarrow V)}_{\mathbf{1},\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{\mathbf{1},\mathfrak{n}} \\ \cdots & \cdots & \cdots \\ \boldsymbol{a}'^{(U\rightsquigarrow V)}_{\boldsymbol{m}_V,\mathbf{1}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{\boldsymbol{m}_V,\mathbf{1}} & & \boldsymbol{a}'^{(U\rightsquigarrow V)}_{\boldsymbol{m}_V,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{\boldsymbol{m}_V,\mathfrak{n}} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \end{pmatrix},\right.\right.\right.$$

$$\left.\left.\left.\begin{pmatrix} \boldsymbol{b}'^{(U\rightsquigarrow V)}_{\mathbf{1},\mathbf{1}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{\mathbf{1},\mathbf{1}} & \cdots & \boldsymbol{b}'^{(U\rightsquigarrow V)}_{\mathbf{1},\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{\mathbf{1},\mathfrak{m}} \\ \cdots & \cdots & \cdots \\ \boldsymbol{b}'^{(U\rightsquigarrow V)}_{\boldsymbol{m}_U,\mathbf{1}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{\boldsymbol{m}_U,\mathbf{1}} & \cdots & \boldsymbol{b}'^{(U\rightsquigarrow V)}_{\boldsymbol{m}_U,\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{\boldsymbol{m}_U,\mathfrak{m}} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \end{pmatrix}\right)\right)\right),$$

$$\left(\begin{array}{ccc} a'^{(V\rightsquigarrow U)}_{1,1} + i\ \widehat{a}'^{(U\rightsquigarrow U)}_{1,1} = a'^{(U\rightsquigarrow V)}_{1,1} + i\ \widehat{a}'^{(V\rightsquigarrow V)}_{1,1} & \cdots & a'^{(V\rightsquigarrow U)}_{1,\mathfrak{n}} + i\ \widehat{a}'^{(U\rightsquigarrow U)}_{1,\mathfrak{n}} = a'^{(U\rightsquigarrow V)}_{1,\mathfrak{n}} + i\ \widehat{a}'^{(V\rightsquigarrow V)}_{1,\mathfrak{n}} \\ \cdots & \cdots & \cdots \\ a'^{(V\rightsquigarrow U)}_{m_U,1} + i\ \widehat{a}'^{(U\rightsquigarrow U)}_{m_U,1} = a'^{(U\rightsquigarrow V)}_{m_V,1} + i\ \widehat{a}'^{(V\rightsquigarrow V)}_{m_V,1} & \cdots & a'^{(V\rightsquigarrow U)}_{m_U,\mathfrak{n}} + i\ \widehat{a}'^{(U\rightsquigarrow U)}_{m_U,\mathfrak{n}} = a'^{(U\rightsquigarrow V)}_{m_V,\mathfrak{n}} + i\ \widehat{a}'^{(V\rightsquigarrow V)}_{m_V,\mathfrak{n}} \\ a'^{(U\rightsquigarrow V)}_{m_V+1,1} + i\ \widehat{a}'^{(V\rightsquigarrow V)}_{m_V+1,1} & \cdots & a'^{(U\rightsquigarrow V)}_{m_V+1,\mathfrak{n}} + i\ \widehat{a}'^{(V\rightsquigarrow V)}_{m_V+1,\mathfrak{n}} \\ \cdots & \cdots & \cdots \\ a'^{(U\rightsquigarrow V)}_{m_V+\lambda,1} + i\ \widehat{a}'^{(V\rightsquigarrow V)}_{m_V+\lambda,1} & \cdots & a'^{(U\rightsquigarrow V)}_{m_V+\lambda,\mathfrak{n}} + i\ \widehat{a}'^{(V\rightsquigarrow V)}_{m_V+\lambda,\mathfrak{n}} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \end{array}\right),$$

$$\left(\begin{array}{ccc} b'^{(V\rightsquigarrow U)}_{1,1} + i\ \widehat{b}'^{(U\rightsquigarrow U)}_{1,1} = b'^{(U\rightsquigarrow V)}_{1,1} + i\ \widehat{b}'^{(V\rightsquigarrow V)}_{1,1} & \cdots & b'^{(V\rightsquigarrow U)}_{1,\mathfrak{n}} + i\ \widehat{b}'^{(U\rightsquigarrow U)}_{1,\mathfrak{n}} = b'^{(U\rightsquigarrow V)}_{1,\mathfrak{n}} + i\ \widehat{b}'^{(V\rightsquigarrow V)}_{1,\mathfrak{n}} \\ \cdots & \cdots & \cdots \\ b'^{(V\rightsquigarrow U)}_{m_U,1} + i\ \widehat{b}'^{(U\rightsquigarrow U)}_{m_U,1} = b'^{(U\rightsquigarrow V)}_{m_V,1} + i\ \widehat{b}'^{(V\rightsquigarrow V)}_{m_V,1} & \cdots & b'^{(V\rightsquigarrow U)}_{m_U,\mathfrak{n}} + i\ \widehat{b}'^{(U\rightsquigarrow U)}_{m_U,\mathfrak{n}} = b'^{(U\rightsquigarrow V)}_{m_V,\mathfrak{n}} + i\ \widehat{b}'^{(V\rightsquigarrow V)}_{m_V,\mathfrak{n}} \\ b'^{(U\rightsquigarrow V)}_{m_V+1,1} + i\ \widehat{b}'^{(V\rightsquigarrow V)}_{m_V+1,1} & \cdots & b'^{(U\rightsquigarrow V)}_{m_V+1,\mathfrak{n}} + i\ \widehat{b}'^{(V\rightsquigarrow V)}_{m_V+1,\mathfrak{n}} \\ \cdots & \cdots & \cdots \\ b'^{(U\rightsquigarrow V)}_{m_V+\lambda,1} + i\ \widehat{b}'^{(V\rightsquigarrow V)}_{m_V+\lambda,1} & \cdots & b'^{(U\rightsquigarrow V)}_{m_V+\lambda,\mathfrak{n}} + i\ \widehat{b}'^{(V\rightsquigarrow V)}_{m_V+\lambda,\mathfrak{n}} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{0} \end{array}\right).$$

According to [6] the sophistication of this vector is medium to high. During this scenario the following state applies:

| $\boldsymbol{\varphi^{(U\rightsquigarrow V)}(t), \widehat{\varphi}^{(V\rightsquigarrow V)}(t)}$ | $\boldsymbol{\psi^{(U\rightsquigarrow V)}(t), \widehat{\psi}^{(V\rightsquigarrow V)}(t)}$ |
|---|---|
| $\boldsymbol{\varphi^{(U\rightsquigarrow V)}(t) < 0}$ | $\boldsymbol{\psi^{(U\rightsquigarrow V)}(t) > 0}$ |
| $\boldsymbol{\widehat{\varphi}^{(V\rightsquigarrow V)}(t) = 0}$ | $\boldsymbol{\widehat{\psi}^{(V\rightsquigarrow V)}(t) = 0}$ |
| $\boldsymbol{\varphi^{(V\rightsquigarrow U)}(t) = 0}$ | $\boldsymbol{\psi^{(V\rightsquigarrow U)}(t) = 0}$ |
| $\boldsymbol{\widehat{\varphi}^{(U\rightsquigarrow U)}(t) > 0}$ | $\boldsymbol{\widehat{\psi}^{(U\rightsquigarrow U)}(t) < 0}$ |

It is clear that during this scenario the attack $\boldsymbol{\mathcal{F}}$ from $\boldsymbol{U}$ that plays the role of APT actor against the $(\boldsymbol{\mu_1, \dots, \mu_\nu}) -$ device parts $\boldsymbol{fr\left(dev^{(V)}_{\mu_1}\right)}$, $\boldsymbol{fr\left(dev^{(V)}_{\mu_2}\right)}$,…, $\boldsymbol{fr\left(dev^{(V)}_{\mu_\nu}\right)}$ of $\boldsymbol{V}$, the following elementary properties hold.

**i.** The (Euclidean) norm $\left\| \boldsymbol{a'^{(U\rightsquigarrow V)}} \right\|$ of the resulting overall valuation in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next

moment $\boldsymbol{t'}$ is less than the (Euclidean) norm $\left\|\boldsymbol{a}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})}\right\|$ of the initial overall valuation in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the preceding moment $\boldsymbol{t}$:

$$\left\|\boldsymbol{a}'^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})}\right\| < \left\|\boldsymbol{a}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})}\right\|.$$

**ii.** The (Euclidean) norm $\left\|\boldsymbol{b}'^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})}\right\|$ of the resulting overall vulnerability in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next moment $\boldsymbol{t'}$ is greater than the (Euclidean) norm $\left\|\boldsymbol{b}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})}\right\| := \left(\sum_{j=1}^{\mathfrak{m}}\sum_{\lambda=1}^{\ell_V}\left|\boldsymbol{b}_{\mathcal{M}_U+\lambda,j}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})}\right|^2\right)^{1/2}$ of the initial overall vulnerability in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the preceding moment $\boldsymbol{t}$:

$$\left\|\boldsymbol{b}'^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})}\right\| > \left\|\boldsymbol{b}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})}\right\|.$$

**iii.** The (Euclidean) norm $\left\|\widehat{\boldsymbol{a}}'^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{U})}\right\|$ of the resulting overall valuation in the variant node $\boldsymbol{U}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next moment $\boldsymbol{t'}$ is greater than the (Euclidean) norms

$$\left\|\widehat{\boldsymbol{a}}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{U})}\right\| \text{ and } \left\|\boldsymbol{a}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})}\right\|$$

of the initial overall valuations in the nodes $\boldsymbol{U}$ and $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the preceding moment $\boldsymbol{t}$:

$$\left\|\widehat{\boldsymbol{\beta}}'^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{U})}\right\| > \boldsymbol{max}\left\{\left\|\widehat{\boldsymbol{\beta}}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{U})}\right\|, \left\|\boldsymbol{\beta}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})}\right\|\right\}.$$

**iv.** The (Euclidean) norm $\left\|\widehat{\boldsymbol{b}}'^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{U})}\right\|$ of the resulting overall vulnerability in the variant node $\boldsymbol{U}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next moment $\boldsymbol{t'}$ is less than the (Euclidean) norms

$$\left\|\widehat{\boldsymbol{b}}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{U})}\right\| \text{ and } \left\|\boldsymbol{b}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})}\right\|$$

of the initial overall vulnerabilities in the nodes $\boldsymbol{U}$ and $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the preceding moment $\boldsymbol{t}$:

$$\left\|\widehat{\boldsymbol{b}}'^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{U})}\right\| < \boldsymbol{min}\left\{\left\|\widehat{\boldsymbol{b}}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{U})}\right\|, \left\|\boldsymbol{b}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})}\right\|\right\}. \blacksquare$$

In the special case where there is a fully successful access attack the following hold:

$$\left\| \boldsymbol{a}'^{(\boldsymbol{U}\twoheadrightarrow\boldsymbol{V})} \right\| \approx \mathbf{0},\ \left\| \boldsymbol{a}'^{(\boldsymbol{U}\twoheadrightarrow\boldsymbol{U})} \right\| = \sqrt{\boldsymbol{m_U}},\ \left\| \boldsymbol{b}'^{(\boldsymbol{U}\twoheadrightarrow\boldsymbol{V})} \right\| = \sqrt{\boldsymbol{m_U}}. \blacksquare$$

An access attack, besides a reflexive homomorphism, can take place **physically** when an attacker $\boldsymbol{U}$, physically gains access of victim node devices $\boldsymbol{V}$.

## 5. APT Hunting Scenario 4

In this scenario the actual attack vector which involves an unauthorized detection mapping and services to steal data. This attack may potentially take place both actively and passively. Specifically, in passive scenario 4, an intruder monitors system for vulnerabilities without interaction, through techniques like session capture. In active scenario, the intruder engages with the target system through techniques like port scans. Again, here the node that plays the role of the APT actor is the $\boldsymbol{U}$.
Thus, during this attack the following general form of cyber-effect applies:

$$\boldsymbol{g} = \boldsymbol{g_t}: \boldsymbol{\mathcal{Q}_9^{(V)}}(\boldsymbol{U})(\boldsymbol{t}) \to \boldsymbol{\mathcal{P}_7^{(U)}}(\boldsymbol{V})(\boldsymbol{t}')$$

where $\boldsymbol{\mathcal{Q}_9^{(V)}}(\boldsymbol{U})(\boldsymbol{t}')$ and $\boldsymbol{\mathcal{P}_7^{(U)}}(\boldsymbol{V})(\boldsymbol{t}')$ are the combinatorial triplets

$$\boldsymbol{\mathcal{Q}_9^{(V)}}(\boldsymbol{U}) = \boldsymbol{\mathcal{Q}_9^{(V)}}(\boldsymbol{U})(\boldsymbol{t}') =$$

$$(\boldsymbol{\mathfrak{R}_{available}}(\boldsymbol{V}), \boldsymbol{\mathcal{S}_U}\boldsymbol{\mathfrak{R}_{available}}(\boldsymbol{V}), \boldsymbol{\mathcal{U}_U}\boldsymbol{\mathfrak{R}_{available}}(\boldsymbol{V}))$$ and

$$\boldsymbol{\mathcal{P}_7^{(U)}}(\boldsymbol{V})(\boldsymbol{t}') = (\boldsymbol{\mathfrak{C}_{available}}(\boldsymbol{V}), \boldsymbol{\mathcal{S}_U}\boldsymbol{\mathfrak{C}_{available}}(\boldsymbol{V}), \boldsymbol{\mathcal{U}_U}\boldsymbol{\mathfrak{C}_{available}}(\boldsymbol{V}))$$

respectively **([5]).**

The scope of this attack is for node $\boldsymbol{U}$ to uncover all constituents' vulnerabilities of node $\boldsymbol{V}$.

A family of coherent interactions

$$\boldsymbol{\mathcal{F}} = \left\{ \boldsymbol{\mathcal{Z}} = \boldsymbol{\mathcal{Z}_{(Y,X)}}(\boldsymbol{t}) = \left((\mathbb{z}_1, \mathbb{w}_1), (\mathbb{z}_2, \mathbb{w}_2), (\mathbb{z}'_1, \mathbb{w}'_1), (\mathbb{z}'_2, \mathbb{w}'_2)\right)(\boldsymbol{t}) \in \right.$$

$$\left. \left(\mathbb{C}^{\mathbf{n}\times\boldsymbol{k}} \times \mathbb{C}^{\mathbf{m}\times\boldsymbol{k}}\right)^{\mathbf{4}}, \boldsymbol{t} \in \mathbb{I} \right\},$$

lying in (the partial danger sector $\mathcal{E} = \mathcal{E}_{\boldsymbol{U}\to\boldsymbol{V}}$ to) the node $\boldsymbol{V}$ from the node $\boldsymbol{U}$ during the entire time set $\mathbb{I}$, is **a germ of scenario 4 attack against the** $(\boldsymbol{\mu_1}, \dots, \boldsymbol{\mu_\nu})-$ **device parts** $\boldsymbol{fr}\left(\boldsymbol{dev}_{\boldsymbol{\mu_1}}^{(\boldsymbol{V})}\right)$, $\boldsymbol{fr}\left(\boldsymbol{dev}_{\boldsymbol{\mu_2}}^{(\boldsymbol{V})}\right)$,..., $\boldsymbol{fr}\left(\boldsymbol{dev}_{\boldsymbol{\mu_\nu}}^{(\boldsymbol{V})}\right)$ **and the** $(\boldsymbol{\kappa_1}, \dots, \boldsymbol{\kappa_\lambda})-$ **resource parts** $\boldsymbol{fr}\left(\boldsymbol{res}_{\boldsymbol{\kappa_1}}^{(\boldsymbol{V})}\right)$, $\boldsymbol{fr}\left(\boldsymbol{res}_{\boldsymbol{\kappa_2}}^{(\boldsymbol{V})}\right)$,..., $\boldsymbol{fr}\left(\boldsymbol{res}_{\boldsymbol{\kappa_\lambda}}^{(\boldsymbol{V})}\right)$ **of** $\boldsymbol{V}$ during a given time set $\mathbb{I} \subset\subset [\mathbf{0}, \mathbf{1}]$, if, whenever $\boldsymbol{t} \in \mathbb{I}$, the pair

$\left((\mathbb{z}_{\mathbf{1}}, \mathbb{w}_{\mathbf{1}}), (\mathbb{z}_{\mathbf{2}}, \mathbb{w}_{\mathbf{2}})\right) \in \left(\mathbb{C}^{\mathfrak{n}\times\mathfrak{k}} \times \mathbb{C}^{\mathfrak{m}\times\mathfrak{k}}\right)^{\mathbf{2}}$ of supervisory constituents perceptions of $\boldsymbol{U}$ and $\boldsymbol{V}$ in the system of nodes $\boldsymbol{U}$ and $\boldsymbol{V}$ has the form

$\left((\mathbb{z}_{\mathbf{1}}, \mathbb{w}_{\mathbf{1}}), (\mathbb{z}_{\mathbf{2}}, \mathbb{w}_{\mathbf{2}})\right) =$

$$\left(\left(\begin{pmatrix} \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \boldsymbol{a}^{(U\rightsquigarrow V)}_{\mathcal{M}_V+1,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,1} & \cdots\cdots & \boldsymbol{a}^{(U\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{n}} \\ \cdots & & \cdots \\ \boldsymbol{a}^{(U\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} & \cdots\cdots & \boldsymbol{a}^{(U\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{n}} \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \end{pmatrix}, \right.$$

$$\left.\begin{pmatrix} \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \boldsymbol{b}^{(U\rightsquigarrow V)}_{\mathcal{M}_V+1,1} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,1} & \cdots\cdots & \boldsymbol{b}^{(U\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{m}} \\ \cdots & & \cdots \\ \boldsymbol{b}^{(U\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} & \cdots\cdots & \boldsymbol{b}^{(U\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{m}} \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \end{pmatrix}\right),$$

$$\left(\begin{pmatrix} \boldsymbol{a}^{(V\rightsquigarrow U)}_{1,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(U\rightsquigarrow U)}_{1,1} & \cdots\cdots & \boldsymbol{a}^{(V\rightsquigarrow U)}_{1,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(U\rightsquigarrow U)}_{1,\mathfrak{n}} \\ \cdots & & \cdots \\ \boldsymbol{a}^{(V\rightsquigarrow U)}_{m_U,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(U\rightsquigarrow U)}_{m_U,1} & \cdots\cdots & \boldsymbol{a}^{(V\rightsquigarrow U)}_{m_U,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(U\rightsquigarrow U)}_{m_U,\mathfrak{n}} \\ \cdots & & \cdots \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \boldsymbol{a}^{(V\rightsquigarrow U)}_{\mathcal{M}_U+1,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(U\rightsquigarrow U)}_{\mathcal{M}_U+1,1} & \cdots\cdots & \boldsymbol{a}^{(V\rightsquigarrow U)}_{\mathcal{M}_U+1,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(U\rightsquigarrow U)}_{\mathcal{M}_U+1,\mathfrak{n}} \\ \cdots & & \cdots \\ \boldsymbol{a}^{(V\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(U\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,1} & \cdots\cdots & \boldsymbol{a}^{(V\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(U\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{n}} \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \end{pmatrix}\right),$$

$$\left(\begin{array}{ccc} \boldsymbol{b}_{1,1}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{1,1}^{(U\rightsquigarrow U)} & & \boldsymbol{b}_{1,\mathfrak{n}}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{1,\mathfrak{n}}^{(U\rightsquigarrow U)} \\ \cdots & \cdots\cdots\cdots & \cdots \\ \boldsymbol{b}_{m_U,1}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{m_U,1}^{(U\rightsquigarrow U)} & & \boldsymbol{b}_{m_U,\mathfrak{n}}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{m_U,\mathfrak{n}}^{(U\rightsquigarrow U)} \\ \cdots & & \cdots \\ \boldsymbol{0} & & \boldsymbol{0} \\ \cdots & \cdots\cdots\cdots & \cdots \\ \boldsymbol{b}_{\mathcal{M}_U+1,1}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{\mathcal{M}_U+1,1}^{(U\rightsquigarrow U)} & & \boldsymbol{b}_{\mathcal{M}_U+1,\mathfrak{n}}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{\mathcal{M}_U+1,\mathfrak{n}}^{(U\rightsquigarrow U)} \\ \cdots & & \cdots \\ \boldsymbol{b}_{\mathcal{M}_U+\ell_U,1}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{\mathcal{M}_U+\ell_U,1}^{(U\rightsquigarrow U)} & & \boldsymbol{b}_{\mathcal{M}_U+\ell_U,\mathfrak{n}}^{(V\rightsquigarrow U)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}}_{\mathcal{M}_U+\ell_U,\mathfrak{n}}^{(U\rightsquigarrow U)} \\ \boldsymbol{0} & \cdots\cdots\cdots & \boldsymbol{0} \\ \cdots & & \cdots \\ \boldsymbol{0} & & \boldsymbol{0} \end{array}\right)\Bigg)\Bigg)\Bigg)$$

and is depicted, at a next moment $\boldsymbol{t'}=\boldsymbol{t}+\Delta\boldsymbol{t}$, at a pair $\left((\mathbb{z}_{\boldsymbol{1}}',\mathbb{w}_{\boldsymbol{1}}'),(\mathbb{z}_{\boldsymbol{2}}',\mathbb{w}_{\boldsymbol{2}}')\right)\in\left(\mathbb{C}^{\mathfrak{n}\times\mathfrak{k}}\times\mathbb{C}^{\mathfrak{m}\times\mathfrak{k}}\right)^{\boldsymbol{2}}$ of supervisory resource perceptions of $\boldsymbol{U}$ and $\boldsymbol{V}$ having the form

$\left((\mathbb{z}_{\boldsymbol{1}}',\mathbb{w}_{\boldsymbol{1}}'),(\mathbb{z}_{\boldsymbol{2}}',\mathbb{w}_{\boldsymbol{2}}')\right)=$

$$\Bigg(\Bigg(\Bigg(\left(\begin{array}{ccc} \boldsymbol{0} & & \boldsymbol{0} \\ \cdots & \cdots\cdots\cdots & \cdots \\ \boldsymbol{0} & & \boldsymbol{0} \\ \boldsymbol{a'}_{\mathcal{M}_V+1,1}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}'}_{\mathcal{M}_V+1,1}^{(V\rightsquigarrow V)} & \cdots\cdots\cdots & \boldsymbol{a'}_{\mathcal{M}_V+1,\mathfrak{n}}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}'}_{\mathcal{M}_V+1,\mathfrak{n}}^{(V\rightsquigarrow V)} \\ \cdots & & \cdots \\ \boldsymbol{a'}_{\mathcal{M}_V+\ell_V,1}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}'}_{\mathcal{M}_V+\ell_V,1}^{(V\rightsquigarrow V)} & & \boldsymbol{a'}_{\mathcal{M}_V+\ell_V,\mathfrak{n}}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{a}'}_{\mathcal{M}_V+\ell_V,\mathfrak{n}}^{(V\rightsquigarrow V)} \\ \boldsymbol{0} & \cdots\cdots\cdots & \boldsymbol{0} \\ \cdots & & \cdots \\ \boldsymbol{0} & & \boldsymbol{0} \end{array}\right),$$

$$\left(\begin{array}{ccc} \boldsymbol{0} & & \boldsymbol{0} \\ \cdots & \cdots\cdots\cdots & \cdots \\ \boldsymbol{0} & & \boldsymbol{0} \\ \boldsymbol{b'}_{\mathcal{M}_V+1,1}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}'}_{\mathcal{M}_V+1,1}^{(V\rightsquigarrow V)} & \cdots\cdots\cdots & \boldsymbol{b'}_{\mathcal{M}_V+1,\mathfrak{m}}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}'}_{\mathcal{M}_V+1,\mathfrak{m}}^{(V\rightsquigarrow V)} \\ \cdots & & \cdots \\ \boldsymbol{b'}_{\mathcal{M}_V+\ell_V,1}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}'}_{\mathcal{M}_V+\ell_V,1}^{(V\rightsquigarrow V)} & & \boldsymbol{b'}_{\mathcal{M}_V+\ell_V,\mathfrak{m}}^{(U\rightsquigarrow V)}+\boldsymbol{i}\ \widehat{\boldsymbol{b}'}_{\mathcal{M}_V+\ell_V,\mathfrak{m}}^{(V\rightsquigarrow V)} \\ \boldsymbol{0} & \cdots\cdots\cdots & \boldsymbol{0} \\ \cdots & & \cdots \\ \boldsymbol{0} & & \boldsymbol{0} \end{array}\right)\Bigg),$$

$$\left(\begin{array}{c} \left(\begin{array}{ccc} a'^{(V\nrightarrow U)}_{1,1} + i\ \widehat{a}'^{(U\nrightarrow U)}_{1,1} & \cdots\cdots & a'^{(V\nrightarrow U)}_{1,\mathfrak{n}} + i\ \widehat{a}'^{(U\nrightarrow U)}_{1,\mathfrak{n}} \\ \cdots & & \cdots \\ a'^{(V\nrightarrow U)}_{m_U,1} + i\ \widehat{a}'^{(U\nrightarrow U)}_{m_U,1} & & a'^{(V\nrightarrow U)}_{m_U,\mathfrak{n}} + i\ \widehat{a}'^{(U\nrightarrow U)}_{m_U,\mathfrak{n}} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \\ \cdots & \cdots\cdots & \cdots \\ a'^{(V\nrightarrow U)}_{\mathcal{M}_U+1,1} + i\ \widehat{a}'^{(U\nrightarrow U)}_{\mathcal{M}_U+1,1} & & a'^{(V\nrightarrow U)}_{\mathcal{M}_U+1,\mathfrak{n}} + i\ \widehat{a}'^{(U\nrightarrow U)}_{\mathcal{M}_U+1,\mathfrak{n}} \\ \cdots & & \cdots \\ a'^{(V\nrightarrow U)}_{\mathcal{M}_U+\ell_U,1} + i\ \widehat{a}'^{(U\nrightarrow U)}_{\mathcal{M}_U+\ell_U,1} & & a'^{(V\nrightarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{n}} + i\ \widehat{a}'^{(U\nrightarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{n}} \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \end{array}\right), \\ \left(\begin{array}{ccc} b'^{(V\nrightarrow U)}_{1,1} + i\ \widehat{b}'^{(U\nrightarrow U)}_{1,1} & \cdots\cdots & b'^{(V\nrightarrow U)}_{1,\mathfrak{n}} + i\ \widehat{b}'^{(U\nrightarrow U)}_{1,\mathfrak{n}} \\ \cdots & & \cdots \\ b'^{(V\nrightarrow U)}_{m_U,1} + i\ \widehat{b}'^{(U\nrightarrow U)}_{m_U,1} & & b'^{(V\nrightarrow U)}_{m_U,\mathfrak{n}} + i\ \widehat{b}'^{(U\nrightarrow U)}_{m_U,\mathfrak{n}} \\ b'^{(V\nrightarrow U)}_{m_U+1,1} + i\ \widehat{b}'^{(U\nrightarrow U)}_{m_U+1,1} & & b'^{(V\nrightarrow U)}_{m_U+1,\mathfrak{n}} + i\ \widehat{b}'^{(U\nrightarrow U)}_{m_U+1,\mathfrak{n}} \\ \cdots & & \cdots \\ b'^{(V\nrightarrow U)}_{m_U+\ell_V,1} + i\ \widehat{b}'^{(U\nrightarrow U)}_{m_U+\ell_V,1} & & b'^{(V\nrightarrow U)}_{m_U+\ell_V,n} + i\ \widehat{b}'^{(U\nrightarrow U)}_{m_U+\ell_V,n} \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \\ b'^{(V\nrightarrow U)}_{\mathcal{M}_U+1,1} + i\ \widehat{b}'^{(U\nrightarrow U)}_{\mathcal{M}_U+1,1} & & b'^{(V\nrightarrow U)}_{\mathcal{M}_U+1,\mathfrak{n}} + i\ \widehat{b}'^{(U\nrightarrow U)}_{\mathcal{M}_U+1,\mathfrak{n}} \\ \cdots & & \cdots \\ b'^{(V\nrightarrow U)}_{\mathcal{M}_U+\ell_U,1} + i\ \widehat{b}'^{(U\nrightarrow U)}_{\mathcal{M}_U+\ell_U,1} & & b'^{(V\nrightarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{n}} + i\ \widehat{b}'^{(U\nrightarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{n}} \\ b'^{(V\nrightarrow U)}_{\mathcal{M}_U+\ell_U+1,1} + i\ \widehat{b}'^{(U\nrightarrow U)}_{\mathcal{M}_U+\ell_U+1,1} & & b'^{(V\nrightarrow U)}_{\mathcal{M}_U+\ell_U+1,n} + i\ \widehat{b}'^{(U\nrightarrow U)}_{\mathcal{M}_U+\ell_U+1,n} \\ \cdots & \cdots\cdots & \cdots \\ b'^{(V\nrightarrow U)}_{\mathcal{M}_U+\ell_U+\ell_V1} + i\ \widehat{b}'^{(U\nrightarrow U)}_{\mathcal{M}_U+\ell_U+\ell_V,1} & & b'^{(V\nrightarrow U)}_{\mathcal{M}_U+\ell_U+\ell_V,n} + i\ \widehat{b}'^{(U\nrightarrow U)}_{\mathcal{M}_U+\ell_U+\ell_V,n} \\ \mathbf{0} & & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \end{array}\right) \end{array}\right).$$

The sophistication, according to [6], of this attack is very low and highly "transparent" to attacked node. Most often after this attack a more sophisticated vector is planned. Specifically, during scenario 4 attack the following states applied:

| $\boldsymbol{\varphi^{(U\nrightarrow V)}(t), \widehat{\varphi}^{(V\nrightarrow V)}(t)}$ | $\boldsymbol{\psi^{(U\nrightarrow V)}(t), \widehat{\psi}^{(V\nrightarrow V)}(t)}$ |
|---|---|
| $\boldsymbol{\varphi^{(U\nrightarrow V)}(t) < 0}$ | $\boldsymbol{\psi^{(U\nrightarrow V)}(t) > 0}$ |
| $\boldsymbol{\widehat{\varphi}^{(V\nrightarrow V)}(t) = 0}$ | $\boldsymbol{\widehat{\psi}^{(V\nrightarrow V)}(t) = 0}$ |
| $\boldsymbol{\varphi^{(V\nrightarrow U)}(t) = 0}$ | $\boldsymbol{\psi^{(V\nrightarrow U)}(t) = 0}$ |
| $\boldsymbol{\widehat{\varphi}^{(U\nrightarrow U)}(t) > 0}$ | $\boldsymbol{\widehat{\psi}^{(U\nrightarrow U)}(t) < 0}$ |

It is obvious that during this attack $\boldsymbol{\mathcal{F}}$ from $\boldsymbol{U}$ against the $(\boldsymbol{\mu_1}, \dots, \boldsymbol{\mu_v})-$ resource parts $\boldsymbol{fr\left(res_{\mu_1}^{(V)}\right)}$, $\boldsymbol{fr\left(res_{\mu_2}^{(V)}\right)}$,…, $\boldsymbol{fr\left(res_{\mu_v}^{(V)}\right)}$ of $\boldsymbol{V}$, the following elementary properties hold:

**i.** The (Euclidean) norm $\left\| \boldsymbol{a'^{(U\nrightarrow V)}} \right\|$ of the resulting overall valuation in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next moment $\boldsymbol{t'}$ is much less than the (Euclidean) norm $\left\|\boldsymbol{a^{(U\nrightarrow V)}}\right\|$ of the initial overall valuation in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the preceding moment $\boldsymbol{t}$:

$$\left\| \boldsymbol{a'^{(U\nrightarrow V)}} \right\| \ll \left\|\boldsymbol{a^{(U\nrightarrow V)}}\right\|.$$

**ii.** The (Euclidean) norm $\left\| \boldsymbol{b'^{(U\nrightarrow V)}} \right\|$ of the resulting overall vulnerability in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next moment $\boldsymbol{t'}$ is much greater than the (Euclidean) norm $\left\|\boldsymbol{b^{(U\nrightarrow V)}}\right\| := \left(\sum_{j=1}^{\mathfrak{m}} \sum_{\lambda=1}^{\ell_V} \left|\boldsymbol{b_{\mathcal{M}_U+\lambda,j}^{(U\nrightarrow V)}}\right|^2\right)^{1/2}$ of the initial overall vulnerability in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the preceding moment $\boldsymbol{t}$:

$$\left\| \boldsymbol{b'^{(U\nrightarrow V)}} \right\| \gg \left\|\boldsymbol{b^{(U\nrightarrow V)}}\right\|.$$

**iii.** The (Euclidean) norm $\left\|\boldsymbol{\widehat{a}'^{(U\nrightarrow U)}}\right\|$ of the resulting overall valuation in the variant node $\boldsymbol{U}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next moment $\boldsymbol{t'}$ is much greater than the (Euclidean) norms

$$\left\|\boldsymbol{\widehat{a}^{(U\nrightarrow U)}}\right\| \text{ and } \left\|\boldsymbol{a^{(U\nrightarrow V)}}\right\|$$

of the initial overall valuations in the nodes $\boldsymbol{U}$ and $\boldsymbol{V}$ as evaluated from

the viewpoint of the user(s) of $\boldsymbol{U}$ at the preceding moment $\boldsymbol{t}$:

$$\left\|\widehat{\boldsymbol{a}}^{\prime(U \rightsquigarrow U)}\right\| \gg \boldsymbol{max}\{\left\|\widehat{\boldsymbol{a}}^{(U \rightsquigarrow U)}\right\|, \left\|\boldsymbol{a}^{(U \rightsquigarrow V)}\right\|\}.$$

**iv.** The (Euclidean) norm $\left\|\widehat{\boldsymbol{b}}^{\prime(U \rightsquigarrow U)}\right\|$ of the resulting overall vulnerability in the variant node $\boldsymbol{U}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next moment $\boldsymbol{t}'$ is less than the (Euclidean) norms

$$\left\|\widehat{\boldsymbol{b}}^{(U \rightsquigarrow U)}\right\| \text{ and } \left\|\boldsymbol{b}^{(U \rightsquigarrow V)}\right\|$$

of the initial overall vulnerabilities in the nodes $\boldsymbol{U}$ and $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the preceding moment $\boldsymbol{t}$:

$$\left\|\widehat{\boldsymbol{b}}^{\prime(U \rightsquigarrow U)}\right\| < \boldsymbol{min}\{\left\|\widehat{\boldsymbol{b}}^{(U \rightsquigarrow U)}\right\|, \left\|\boldsymbol{b}^{(U \rightsquigarrow V)}\right\|\}. \blacksquare$$

The criticality of this attack is high since most of times it is the omen of a more severe or more sophisticated attack.

## 6. APT Hunting Scenario 5

In this scenario we orient 2 attack vectors that intent to sophisticatedly deny services and generally resources to authorized users. The attacker $\boldsymbol{U}$ that again plays the role of the APT actor makes a computing or memory resource too busy or too full to handle legitimate requests, thus denying legitimate user access to an asset. The difference between these 2 types of attacks is actually the source. In the first type the attack is initiated by only one node. On the other hand, the second vector has the engagement of a multitude of nodes (intentionally or not, e.g. via Botnets).

Thus, during this kind of attack the following general form of cyber-effect applies:

$$\boldsymbol{g} = \boldsymbol{g}_{\boldsymbol{t}}: \boldsymbol{\mathcal{Q}}_{\mathbf{9}}^{(V)}(\boldsymbol{U})(\boldsymbol{t}) \rightarrow \boldsymbol{\mathcal{P}}_{\mathbf{9}}^{(U)}(\boldsymbol{V})(\boldsymbol{t}')$$

where $\boldsymbol{\mathcal{Q}}_{\mathbf{9}}^{(V)}(\boldsymbol{U})(\boldsymbol{t}')$ **and** $\boldsymbol{\mathcal{P}}_{\mathbf{9}}^{(U)}(\boldsymbol{V})(\boldsymbol{t}')$ are the combinatorial triplets

$$\boldsymbol{\mathcal{Q}}_{\mathbf{9}}^{(V)}(\boldsymbol{U}) = \boldsymbol{\mathcal{Q}}_{\mathbf{9}}^{(V)}(\boldsymbol{U})(\boldsymbol{t}') =$$

$$(\boldsymbol{\mathfrak{R}}_{\boldsymbol{available}}(\boldsymbol{V}), \boldsymbol{\mathcal{S}}_{\boldsymbol{U}}\boldsymbol{\mathfrak{R}}_{\boldsymbol{available}}(\boldsymbol{V}), \boldsymbol{\mathcal{U}}_{\boldsymbol{U}}\boldsymbol{\mathfrak{R}}_{\boldsymbol{available}}(\boldsymbol{V})) \text{ and}$$

$$\boldsymbol{\mathcal{P}}_{\mathbf{9}}^{(U)}(\boldsymbol{V})(\boldsymbol{t}') = (\boldsymbol{\mathfrak{R}}_{\boldsymbol{available}}(\boldsymbol{V}), \boldsymbol{\mathcal{S}}_{\boldsymbol{U}}\boldsymbol{\mathfrak{R}}_{\boldsymbol{available}}(\boldsymbol{V}), \boldsymbol{\mathcal{U}}_{\boldsymbol{U}}\boldsymbol{\mathfrak{R}}_{\boldsymbol{available}}(\boldsymbol{V}))$$

respectively ([5]).

It is obvious that the purpose of this attack is for node $\boldsymbol{U}$ to keep all resources/services of node $\boldsymbol{V}$ occupied in order to make them unavailable to all

users when needed.
A family of coherent interactions

$$\boldsymbol{\mathcal{F}} = \big\{\boldsymbol{\mathcal{Z}} = \boldsymbol{\mathcal{Z}}_{(\boldsymbol{Y},\boldsymbol{X})}(\boldsymbol{t}) = \big((\mathbb{z}_{\mathbf{1}}, \mathbb{w}_{\mathbf{1}}), (\mathbb{z}_{\mathbf{2}}, \mathbb{w}_{\mathbf{2}}), (\mathbb{z}'_{\mathbf{1}}, \mathbb{w}'_{\mathbf{1}}), (\mathbb{z}'_{\mathbf{2}}, \mathbb{w}'_{\mathbf{2}})\big)(\boldsymbol{t}) \in \big(\mathbb{C}^{\mathfrak{n}\times\boldsymbol{\mathcal{k}}} \times \mathbb{C}^{\mathfrak{m}\times\boldsymbol{\mathcal{k}}}\big)^{\mathbf{4}}, \boldsymbol{t} \in \mathbb{I}\big\},$$

lying in the partial danger sector $\mathcal{E} = \mathcal{E}_{\boldsymbol{U}\to\boldsymbol{V}}$ to the node $\boldsymbol{V}$ from the node $\boldsymbol{U}$ during the entire time set $\mathbb{I}$, is a **germ of scenario 5 attack against the** $(\boldsymbol{\mu_1}, \dots, \boldsymbol{\mu_\nu})$ − $\boldsymbol{fr}\big(\boldsymbol{dev}^{(\boldsymbol{V})}_{\boldsymbol{\mu_2}}\big)$ **,...,** $\boldsymbol{fr}\big(\boldsymbol{dev}^{(\boldsymbol{V})}_{\boldsymbol{\mu_\nu}}\big)$ **resource parts** $\boldsymbol{fr}\big(\boldsymbol{res}^{(\boldsymbol{V})}_{\boldsymbol{\kappa_1}}\big)$ **,** $\boldsymbol{fr}\big(\boldsymbol{res}^{(\boldsymbol{V})}_{\boldsymbol{\kappa_2}}\big)$**,...,** $\boldsymbol{fr}\big(\boldsymbol{res}^{(\boldsymbol{V})}_{\boldsymbol{\kappa_\lambda}}\big)$ **of** $\boldsymbol{V}$ during a given time set $\mathbb{I} \subset\subset [\mathbf{0}, \mathbf{1}]$, if, whenever $\boldsymbol{t} \in \mathbb{I}$, the pair $\big((\mathbb{z}_{\mathbf{1}}, \mathbb{w}_{\mathbf{1}}), (\mathbb{z}_{\mathbf{2}}, \mathbb{w}_{\mathbf{2}})\big) \in \big(\mathbb{C}^{\mathfrak{n}\times\boldsymbol{\mathcal{k}}} \times \mathbb{C}^{\mathfrak{m}\times\boldsymbol{\mathcal{k}}}\big)^{\mathbf{2}}$ of supervisory constituents perceptions of $\boldsymbol{U}$ and $\boldsymbol{V}$ in the system of nodes $\boldsymbol{U}$ and $\boldsymbol{V}$ has the form

$$\big((\mathbb{z}_{\mathbf{1}}, \mathbb{w}_{\mathbf{1}}), (\mathbb{z}_{\mathbf{2}}, \mathbb{w}_{\mathbf{2}})\big) =$$

$$\left(\left(\left(\begin{matrix} \mathbf{0} \\ \dots \\ \mathbf{0} \\ \boldsymbol{a}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}_V}+\mathbf{1},\mathbf{1}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}_V}+\mathbf{1},\mathbf{1}} \\ \dots \\ \boldsymbol{a}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}_V}+\boldsymbol{\ell_V},\mathbf{1}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}_V}+\boldsymbol{\ell_V},\mathbf{1}} \\ \mathbf{0} \\ \dots \\ \mathbf{0} \end{matrix} \quad \begin{matrix} \dots\dots\dots \\ \\ \dots\dots\dots \\ \\ \dots\dots\dots \end{matrix} \quad \begin{matrix} \mathbf{0} \\ \dots \\ \mathbf{0} \\ \boldsymbol{a}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}_V}+\mathbf{1},\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}_V}+\mathbf{1},\mathfrak{n}} \\ \dots \\ \boldsymbol{a}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}_V}+\boldsymbol{\ell_V},\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}_V}+\boldsymbol{\ell_V},\mathfrak{n}} \\ \mathbf{0} \\ \dots \\ \mathbf{0} \end{matrix}\right),\right.$$

$$\left.\left.\left(\begin{matrix} \mathbf{0} \\ \dots \\ \mathbf{0} \\ \boldsymbol{b}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}_V}+\mathbf{1},\mathbf{1}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}_V}+\mathbf{1},\mathbf{1}} \\ \dots \\ \boldsymbol{b}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}_V}+\boldsymbol{\ell_V},\mathbf{1}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}_V}+\boldsymbol{\ell_V},\mathbf{1}} \\ \mathbf{0} \\ \dots \\ \mathbf{0} \end{matrix} \quad \begin{matrix} \dots\dots\dots \\ \\ \dots\dots\dots \\ \\ \dots\dots\dots \end{matrix} \quad \begin{matrix} \mathbf{0} \\ \dots \\ \mathbf{0} \\ \boldsymbol{b}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}_V}+\mathbf{1},\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}_V}+\mathbf{1},\mathfrak{m}} \\ \dots \\ \boldsymbol{b}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}_V}+\boldsymbol{\ell_V},\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(\boldsymbol{V}\rightsquigarrow\boldsymbol{V})}_{\boldsymbol{\mathcal{M}_V}+\boldsymbol{\ell_V},\mathfrak{m}} \\ \mathbf{0} \\ \dots \\ \mathbf{0} \end{matrix}\right)\right),$$

$$\left(\left(\begin{matrix} \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \\ \boldsymbol{a}^{(V\rightsquigarrow U)}_{\mathcal{M}_U+1,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(U\rightsquigarrow U)}_{\mathcal{M}_U+1,1} & \cdots\cdots & \boldsymbol{a}^{(V\rightsquigarrow U)}_{\mathcal{M}_U+1,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(U\rightsquigarrow U)}_{\mathcal{M}_U+1,\mathfrak{n}} \\ \cdots & & \cdots \\ \boldsymbol{a}^{(V\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(U\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,1} & & \boldsymbol{a}^{(V\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}^{(U\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{n}} \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \end{matrix}\right),\right.$$

$$\left.\left(\begin{matrix} \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \\ \boldsymbol{b}^{(V\rightsquigarrow U)}_{\mathcal{M}_U+1,1} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(U\rightsquigarrow U)}_{\mathcal{M}_U+1,1} & \cdots\cdots & \boldsymbol{b}^{(V\rightsquigarrow U)}_{\mathcal{M}_U+1,\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(U\rightsquigarrow U)}_{\mathcal{M}_U+1,\mathfrak{m}} \\ \cdots & & \cdots \\ \boldsymbol{b}^{(V\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,1} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(U\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,1} & & \boldsymbol{b}^{(V\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}^{(U\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{m}} \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \end{matrix}\right)\right)\right)$$

and is depicted, at a next moment $\boldsymbol{t}' = \boldsymbol{t} + \Delta\boldsymbol{t}$, at a pair $\left((\mathbb{z}'_{\mathbf{1}}, \mathbb{w}'_{\mathbf{1}}), (\mathbb{z}'_{\mathbf{2}}, \mathbb{w}'_{\mathbf{2}})\right) \in \left(\mathbb{C}^{\mathfrak{n}\times\boldsymbol{k}} \times \mathbb{C}^{\mathfrak{m}\times\boldsymbol{k}}\right)^{\mathbf{2}}$ of supervisory resource perceptions of $\boldsymbol{U}$ and $\boldsymbol{V}$ having the form

$$\left((\mathbb{z}'_{\mathbf{1}}, \mathbb{w}'_{\mathbf{1}}), (\mathbb{z}'_{\mathbf{2}}, \mathbb{w}'_{\mathbf{2}})\right) =$$

$$\left(\left(\left(\begin{matrix} \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \\ \boldsymbol{a}'^{(U\rightsquigarrow V)}_{\mathcal{M}_V+1,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,1} = \mathbf{0} & \cdots\cdots & \boldsymbol{a}'^{(U\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{n}} = \mathbf{0} \\ \cdots & & \cdots \\ \boldsymbol{a}'^{(U\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} = \mathbf{0} & & \boldsymbol{a}'^{(U\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{n}} = \mathbf{0} \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \end{matrix}\right)\right),\right.$$

$$\begin{pmatrix} \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \\ \boldsymbol{b'}^{(U\rightsquigarrow V)}_{\mathcal{M}_V+1,1} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,1} = \mathbf{1} & \cdots\cdots & \boldsymbol{b'}^{(U\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+1,\mathfrak{m}} = \mathbf{1} \\ \cdots & & \cdots \\ \boldsymbol{b'}^{(U\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,1} = \mathbf{1} & & \boldsymbol{b'}^{(U\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(V\rightsquigarrow V)}_{\mathcal{M}_V+\ell_V,\mathfrak{m}} = \mathbf{1} \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \end{pmatrix}\Bigg)\Bigg),$$

$$\Bigg(\Bigg(\begin{pmatrix} \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \\ \boldsymbol{a'}^{(V\rightsquigarrow U)}_{\mathcal{M}_U+1,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(U\rightsquigarrow U)}_{\mathcal{M}_U+1,1} & \cdots\cdots & \boldsymbol{a'}^{(V\rightsquigarrow U)}_{\mathcal{M}_U+1,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(U\rightsquigarrow U)}_{\mathcal{M}_U+1,\mathfrak{n}} \\ \cdots & & \cdots \\ \boldsymbol{a'}^{(V\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,1} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(U\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,1} & & \boldsymbol{a'}^{(V\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{n}} + \boldsymbol{i}\ \widehat{\boldsymbol{a}}'^{(U\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{n}} \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \end{pmatrix}\Bigg),$$

$$\begin{pmatrix} \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \\ \boldsymbol{b'}^{(V\rightsquigarrow U)}_{\mathcal{M}_U+1,1} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(U\rightsquigarrow U)}_{\mathcal{M}_U+1,1} & \cdots\cdots & \boldsymbol{b'}^{(V\rightsquigarrow U)}_{\mathcal{M}_U+1,\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(U\rightsquigarrow U)}_{\mathcal{M}_U+1,\mathfrak{m}} \\ \cdots & & \cdots \\ \boldsymbol{b'}^{(V\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,1} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(U\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,1} & & \boldsymbol{b'}^{(V\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{m}} + \boldsymbol{i}\ \widehat{\boldsymbol{b}}'^{(U\rightsquigarrow U)}_{\mathcal{M}_U+\ell_U,\mathfrak{m}} \\ \mathbf{0} & \cdots\cdots & \mathbf{0} \\ \cdots & & \cdots \\ \mathbf{0} & & \mathbf{0} \end{pmatrix}\Bigg)\Bigg)\Bigg).$$

During this scenario injects that reside in previous matrices are usually temporary and only strictly during the application of the attack. According to [6] the sophistication of this attack is low and highly "transparent" to attacked node since the lack of resources is more than obvious. Frequently, after or during this attack a more sophisticated attack is expected. Specifically, during these attacks the following states applied:

| $\boldsymbol{\varphi^{(U\rightsquigarrow V)}(t), \widehat{\varphi}^{(V\rightsquigarrow V)}(t)}$ | $\boldsymbol{\psi^{(U\rightsquigarrow V)}(t), \widehat{\psi}^{(V\rightsquigarrow V)}(t)}$ |
|---|---|
| $\boldsymbol{\varphi^{(U\rightsquigarrow V)}(t) < 0}$ | $\boldsymbol{\psi^{(U\rightsquigarrow V)}(t) > 0}$ |
| $\boldsymbol{\widehat{\varphi}^{(V\rightsquigarrow V)}(t) < 0}$ | $\boldsymbol{\widehat{\psi}^{(V\rightsquigarrow V)}(t) > 0}$ |
| $\boldsymbol{\varphi^{(V\rightsquigarrow U)}(t) > 0}$ | $\boldsymbol{\psi^{(V\rightsquigarrow U)}(t) < 0}$ |
| $\boldsymbol{\widehat{\varphi}^{(U\rightsquigarrow U)}(t) > 0}$ | $\boldsymbol{\widehat{\psi}^{(U\rightsquigarrow U)}(t) < 0}$ |

It is obvious that during this scenario's attack $\boldsymbol{\mathcal{F}}$ from $\boldsymbol{U}$ against the $(\boldsymbol{\mu_1}, \dots, \boldsymbol{\mu_v})-$ resource parts $\boldsymbol{fr\left(res_{\mu_1}^{(V)}\right)}$, $\boldsymbol{fr\left(res_{\mu_2}^{(V)}\right)}$,…, $\boldsymbol{fr\left(res_{\mu_v}^{(V)}\right)}$ of $\boldsymbol{V}$, the following elementary properties hold:

**i.** The (Euclidean) norm $\left\| \boldsymbol{a'^{(U\rightsquigarrow V)}} \right\|$ of the resulting overall valuation in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next moment $\boldsymbol{t'}$ is temporary $\boldsymbol{0}$:

$$\left\| \boldsymbol{a'^{(U\rightsquigarrow V)}} \right\| = \boldsymbol{0}.$$

**ii.** The (Euclidean) norm $\left\| \boldsymbol{b'^{(U\rightsquigarrow V)}} \right\|$ of the resulting overall vulnerability in the node $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next moment $\boldsymbol{t'}$ is temporary $\boldsymbol{1}$:

$$\left\| \boldsymbol{b'^{(U\rightsquigarrow V)}} \right\| = \boldsymbol{1}.$$

**iii.** The (Euclidean) norm $\left\| \boldsymbol{\widehat{a}'^{(U\rightsquigarrow U)}} \right\|$ of the resulting overall valuation in the variant node $\boldsymbol{U}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next moment $\boldsymbol{t'}$ is much greater than the (Euclidean) norms

$$\left\| \boldsymbol{\widehat{a}^{(U\rightsquigarrow U)}} \right\| \text{ and } \left\| \boldsymbol{a^{(U\rightsquigarrow V)}} \right\|$$

of the initial overall valuations in the nodes $\boldsymbol{U}$ and $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the preceding moment $\boldsymbol{t}$:

$$\left\| \boldsymbol{\widehat{\beta}'^{(U\rightsquigarrow U)}} \right\| \geq \boldsymbol{max}\left\{ \left\| \boldsymbol{\widehat{\beta}^{(U\rightsquigarrow U)}} \right\|, \left\| \boldsymbol{\beta^{(U\rightsquigarrow V)}} \right\| \right\}.$$

**iv.** The (Euclidean) norm $\left\|\widehat{\boldsymbol{b}}'^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{U})}\right\|$ of the resulting overall vulnerability in the variant node $\boldsymbol{U}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the next moment $\boldsymbol{t}'$ is less than the (Euclidean) norms

$$\left\|\widehat{\boldsymbol{b}}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{U})}\right\| \text{ and } \left\|\boldsymbol{b}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V}^{\prime\prime})}\right\|$$

of the initial overall vulnerabilities in the nodes $\boldsymbol{U}$ and $\boldsymbol{V}$ as evaluated from the viewpoint of the user(s) of $\boldsymbol{U}$ at the preceding moment $\boldsymbol{t}$:

$$\left\|\widehat{\boldsymbol{b}}'^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{U})}\right\| < \boldsymbol{min}\left\{\left\|\widehat{\boldsymbol{b}}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{U})}\right\|, \left\|\boldsymbol{b}^{(\boldsymbol{U}\rightsquigarrow\boldsymbol{V})}\right\|\right\}. \blacksquare$$

The importance of this attack is high since most of the time, especially during distributed one, the nodes that participate are already compromised via Access attack that has already discussed.

## References

[1] Nikos Virvilis, Dimitris Gritzalis, Theodoros Apostolopoulos Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?

[2] https://attack.mitre.org/resources/enterprise-introduction/ ATT&CK for Enterprise Introduction

[3] Daras, N.J.: *On the mathematical definition of cyberspace*, Theoretical Mathematics & Applications, vol.8, no.1, 2018, 9-45, , Scienpress Ltd, 2018

[4] Daras, N.J and Alexopoulos, A.: *Mathematical description of cyber-attacks and proactive defenses*, Journal of Applied Mathematics & Bioinformatics, vol.7, no.1, 2017, pp. 71-142

[5] Daras, N.J and Alexopoulos, A.: *Modeling Cyber-Security*, Journal of Applied Mathematics & Bioinformatics, vol.7, no.1, 2017, pp. 71-142

[6] Alexopoulos, A. and Daras, N.: Mathematical Study of Various Types of Cyber-Attacks and Protection, Journal of Computations & Modelling, vol.8, no.2, 2018