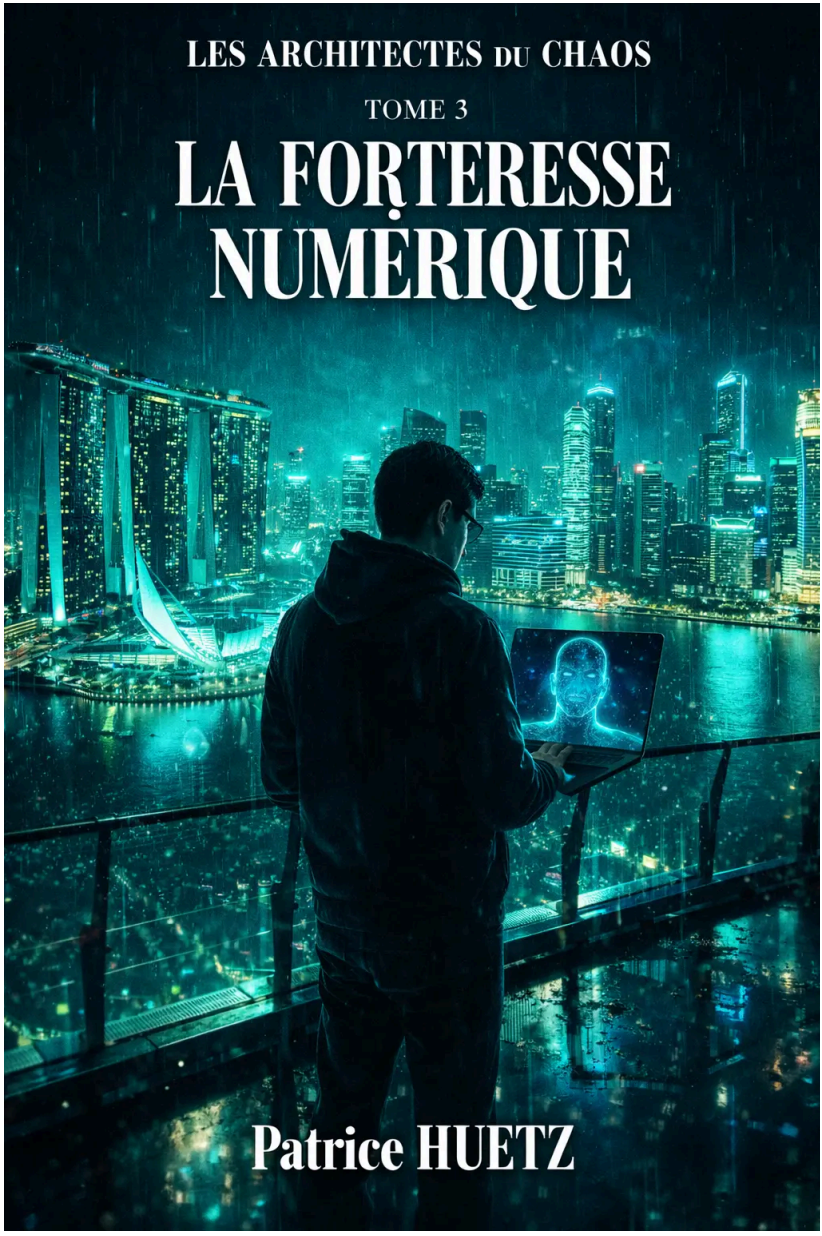
LES ARCHITECTES DU CHAOS
TOME 3
LA FORTERESSE NUMÉRIQUE
Patrice HUETZ

Les Architectes du Chaos — La Forteresse Numérique

Patrice Huetz

patrice-huetz.fr

patrice-huetz.fr · contact@patrice-huetz.fr

CHAPITRE 1

Singapour

Singapour, janvier 2017 — 34 °C à l'ombre

L'appartement était au vingt-deuxième étage d'une tour en verre du quartier de Tanjong Pagar, avec vue sur le détroit de Singapour et les porte-conteneurs alignés jusqu'à l'horizon comme une armée à l'ancre. La tour s'appelait Gateway Tower et son architecture de verre bleuté reflétait le ciel selon l'heure du jour — blanc le matin, or l'après-midi, noir la nuit. Karim avait choisi l'appartement 22F pour sa vue, pour son accès à la fibre de Singapore Telecom de 1 Gbps symétrique, et parce que la société de gestion immobilière était enregistrée aux Îles Caïmans et n'avait aucune obligation de coopération judiciaire avec les États de l'Union européenne ou les États-Unis.

Il avait payé six mois de loyer en Bitcoin via trois couches de mixage. Sept mille dollars singapouriens par mois — quatre mille six cents euros environ au taux de janvier 2017. Un appartement de soixante-cinq mètres carrés avec vue sur le détroit, cuisine ouverte, salle de bain en marbre, et ce canapé en cuir blanc Cassina qui coûtait probablement plus cher que tous ses vêtements réunis.

Il avait vingt-cinq ans et vivait mieux qu'il n'avait jamais vécu.

Ce n'était pas de l'arrogance. C'était une fonction de ses coûts d'opération : un appartement anonyme dans un pays avec une connectivité excellente et peu de coopération judiciaire internationale valait le prix. Il aurait payé le même prix à Amsterdam ou à Tallinn ou à Tbilissi si les autres paramètres avaient été comparables. L'appartement de Tanjong Pagar était un outil. Le canapé blanc était un avantage collatéral.

Karim était assis sur ce canapé avec son ThinkPad X1 Carbon sur les genoux. Le modèle 2016 — sept cent grammes, processeur Intel Core i7-6600U, seize gigaoctets de RAM soudée pour éliminer le risque de cold boot attack physique, SSD NVMe chiffré avec LUKS en AES-256. Il avait acheté l'appareil chez un revendeur d'occasion à Munich, payé cash, remplacé le disque dur avant la première utilisation et installé Arch Linux depuis une clé USB bootable créée sur un système isolé.

Deux écrans supplémentaires montés sur bras articulés flanquaient sa position principale. À gauche, le moniteur LG 4K de quarante-deux pouces affichait le tableau de bord de surveillance réseau — un dashboard personnalisé en Python/Grafana qui consolidait les métriques de tous ses systèmes actifs : VPS en Islande, serveurs I2P en Roumanie, nœuds Tor en Suisse, connexions actives ORACLE en cours d'entraînement. À droite, le Samsung de vingt-sept pouces affichait son terminal principal — fond noir, texte vert pâle, police Hack Nerd Font taille 11.

Un troisième ordinateur dormait sur le bureau en teck artisanal qu'il avait commandé spécialement à un menuisier du quartier de Geylang. Cet ordinateur était air-gapped — pas de WiFi, Bluetooth désactivé au niveau matériel, aucune connexion réseau d'aucun type. Il servait uniquement pour le développement du code le plus sensible et l'analyse des données qu'il ne voulait jamais voir quitter un support physique isolé.

L'appartement du 22F était un bureau opérationnel. Le fait qu'il soit aussi beau était une coïncidence heureuse.

Il avait câblé l'appartement selon ses standards habituels — des standards qui avaient évolué sur cinq ans et qui représentaient maintenant une architecture cohérente, reproductible dans n'importe quel appartement en quarante-huit heures.

Le réseau local était structuré en quatre zones isolées par des VLANs configurés sur un routeur OpenWrt personnalisé — un TP-Link Archer C7 sur lequel il avait compilé sa propre version du firmware avec ses règles iptables intégrées. Zone 1 : l'ordinateur principal, accès internet via double VPN multi-hop. Zone 2 : les deux Raspberry Pi 4 servant de nœuds Tor dédiés. Zone 3 : le NAS Synology DS920+ pour les backups chiffrés. Zone 4 : réseau isolé pour les périphériques de surveillance.

Sa vérification matinale ressemblait à une routine médicale — pas parce qu'il était paranoïaque, mais parce qu'un professionnel vérifiait ses outils avant de travailler.

```
kr4m@ghost:~$ nmap -sV --version-intensity 5 -p 22,8
0,443,9050 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org )

Host: 192.168.1.1   [OpenWrt router]
  22/open  ssh    OpenSSH_7.9

Host: 192.168.1.105 [RPi-node1/guard]
  9050/open socks5 Tor 0.4.5.10

Host: 192.168.1.106 [RPi-node2/exit]
  9050/open socks5 Tor 0.4.5.10

Host: 192.168.1.200 [NAS-Synology-DS920]
  5001/open https  nginx

Nmap done: 256 IP addresses (4 hosts up) scanned in 1
4.32 seconds

kr4m@ghost:~$ # Infrastructure stable. 0 anomalies.
```

Tout en ordre. Il referma le terminal, ouvrit le channel GHOST sur I2P, vit cinq messages non lus depuis la nuit — Thomas avait partagé un article technique sur les nouvelles techniques d'OPSEC pour les développeurs, Yasmin avait posé une question sur la configuration d'un outil de pentest, Dragan avait signalé une nouvelle CVE critique dans un composant qu'ils utilisaient parfois.

La routine. La bonne routine.

Trois mois à Singapour. Après Bruxelles, six semaines pour laisser refroidir MINERVA et attendre que Léa Vandenberg témoigne devant la commission LIBE du Parlement européen. Puis Amsterdam, un mois, parce que Thomas y avait des contacts techniques utiles. Puis Bangkok, trois semaines, parce que c'était moins cher et que la chaleur de Bangkok lui rappelait quelque chose qu'il n'arrivait pas encore à nommer.

Puis Singapour. Choisi pour la connectivité, pour le cadre légal pragmatique, pour la distance géographique avec l'Europe, et pour une raison qu'il n'avait pas explicitement formulée mais qui existait néanmoins : il voulait être quelque part où personne ne le connaissait, pas même sous un pseudonyme.

Son téléphone buzza à 16h22. Un message de Samir sur Wire — l'application de messagerie chiffrée qu'ils utilisaient pour les communications non-urgentes, Signal pour l'urgence, les canaux I2P pour tout ce qui devait rester dans l'infrastructure GHOST.

"J'ai une proposition. Appelle-moi en sécurisé."

Karim appela via le tunnel Tor, protocole Signal, clés éphémères activées. Samir décrocha à la deuxième sonnerie.

Samir Aït, trente et un ans, alias GHOST dans le collectif — le surnom venait de ses premières années de hacking quand il disparaissait des forums pendant des mois puis réapparaissait avec des techniques qui semblaient surgir de nulle part. Il avait les mêmes origines que Karim — parents algériens, enfance en France, autodidacte en informatique, passage par des cercles de hackers en

ligne avant de rencontrer Karim dans un forum fermé en 2013. Il était plus calme que Karim, plus patient, meilleur pour la logistique et les systèmes hardware. C'est lui qui construisait les infrastructures physiques de GHOST quand elles existaient — les serveurs dans des appartements, les systèmes de communication sécurisés, les relais Tor dédiés.

Il appelait depuis Prague, où il s'était installé provisoirement après Budapest. Sa voix portait cette légère tension que Karim reconnaissait — pas du stress, mais de l'excitation contenue, l'excitation d'un homme qui a quelque chose d'intéressant et qui modère son enthousiasme pour paraître plus crédible.

« Un gouvernement, dit Samir. Europe de l'Est. Je ne donne pas le nom sur ce canal. »

« Qu'est-ce qu'ils veulent ? »

« Un audit de sécurité complet. Pen-testing de leur infrastructure critique — réseaux gouvernementaux, systèmes de vote électronique pilotes, trois centrales d'énergie connectées au réseau national. Durée : douze semaines. Périmètre : tout ce qui est numérique. »

Karim garda le silence un moment. Par la fenêtre panoramique du 22F, un cargo de la Evergreen Marine négociait lentement sa sortie du port, guidé par deux remorqueurs qui semblaient ridiculement petits à côté du monstre orange. Le détroit de Singapour, quarante kilomètres de large entre la péninsule malaise et l'île de Sumatra, était l'un des passages maritimes les plus fréquentés au monde. Deux cent cinquante navires par jour. Une autoroute maritime.

Il regardait souvent ce détroit quand il réfléchissait.

« Legal ? »

« Contrat signé. Scope défini avec précision. Immunité judiciaire pour la durée de la mission — une clause explicite, validée par les avocats des deux parties. Pas du flou — du contractuel. »

« Combien ? »

« Cinq cent mille euros. Deux cent cinquante mille à la signature. Deux cent cinquante mille au rapport final. »

Un silence de sept secondes. Karim compta.

« C'est trois fois ce qu'on a jamais facturé à quelqu'un.

— Oui.

— Pourquoi nous ? »

La question importait plus que le chiffre. Il ne posait pas cette question par modestie — GHOST était bon, objectivement, et Karim le savait. Il la posait parce que comprendre les motivations d'un client était aussi important que comprendre les systèmes qu'on allait tester. Un client qui vous surévalue est dangereux. Un client qui vous recrute pour une raison précise a des attentes précises.

« L'article de Léa, dit Samir. Ils ont lu "le collectif qui surveille les surveillants". Ils ont pensé : si ce groupe peut infiltrer MINERVA sans être détecté pendant dix-huit mois, il peut trouver nos failles. CrowdStrike coûte le même prix et a une liste de clients de deux cents pages. Nous n'avons pas de liste de clients. Ce qui les rassure. »

Karim nota mentalement de trouver un moyen de remercier Léa Vandenberg. Elle n'avait pas su, en publiant son article, qu'elle leur créait une réputation commerciale. Ou peut-être qu'elle l'avait su.

« Risque politique si ça fuite.

— Le risque politique d'un audit de sécurité contractuel est gérable. Des gouvernements font ça depuis des années. La différence, c'est l'identité du prestataire. Ce qui est couvert par la clause de confidentialité.

— Tu as donné une réponse préliminaire ?

— J'ai dit que je consultais mon collectif. »

Il convoqua le vote sur le channel GHOST à 17h30, heure de Singapour.

La règle était établie depuis la création du collectif, en 2013, dans un appartement de Saint-Denis quand GHOST n'était que trois personnes avec un accès internet partagé et beaucoup d'ambition. Pas

de mission sans unanimité. Pas de majorité, pas de vote à cinq contre deux, pas de décision par le coordinateur principal en cas d'absence. L'unanimité ou le refus.

C'était une règle qui avait semblé naïve à certains membres au fil des années — trop rigide, trop lente. Viktor Sorokin l'avait contestée ouvertement lors d'une réunion en 2015, arguant qu'une majorité qualifiée était suffisante pour des décisions urgentes. Karim avait tenu bon. Huit semaines plus tard, Viktor était l'infiltrateur qui avait failli les détruire.

La règle de l'unanimité n'empêchait pas toutes les trahisons. Mais elle ralentissait les décisions précipitées. Et dans GHOST, la précipitation était l'ennemi principal.

Les réponses arrivèrent sur deux heures et demie. Thomas depuis Munich — il lisait les nouvelles techniques de fuzzing à 9h du matin et avait répondu en vingt minutes. Yasmin depuis Amsterdam — elle était réveillée depuis 6h et avait manifestement attendu la convocation. Dragan depuis Zagreb — il avait répondu depuis son téléphone, en route vers quelque chose. Pixel depuis Tel Aviv — il était 11h du soir là-bas et son "oui" était accompagné d'une question sur le scope des systèmes SCADA. Samir depuis Prague — il avait posté "oui" en même temps qu'il transmettait sa propre réponse au client.

[THOMASGHOST] Oui. Avec les conditions habituelles sur le scope et la documentation.

[YASMIN_X] Oui. Mais je veux lire le contrat complet avant qu'on signe quoi que ce soit. Et la clause immunité doit être explicite et non ambiguë.

[PIXEL] Oui. Le scope couvre les systèmes SCADA ? Ce n'est pas le même type de test que les apps web. Dragan devrait superviser cette partie.

[DRAGAN] Oui. SCADA, je m'en occupe. J'ai les certifications Siemens.