Analyse Complète de Black Basta

> Analyse technique de Black Basta ransomware : ChaCha20-Poly1305 AVX2 avec registres YMM, RSA-4096 DER extractible, seuils 64KB/704KB identifiables dans…

Black Basta est l'une des familles de ransomware les plus actives de 2024-2026, présentant des caractéristiques techniques distinctives qui en font un sujet d'analyse essentiel pour les équipes de sécurité offensive et défensive. Développé en C++ (techniques héritées de Conti), ce ransomware utilise un schéma cryptographique basé sur ChaCha20 + RSA-4096, avec Intégration étroite avec QAKBOT (jusqu'à son démantèlement en 2023) comme mécanisme de livraison privilégié. Les opérateurs pratiquent la double extorsion systématique via un portail Tor dédié, combinant le chiffrement des données avec la menace de publication. L'analyse technique de ses binaires révèle des choix d'implémentation spécifiques, des techniques d'obfuscation adaptées au langage utilisé, et une infrastructure C2 reposant sur Tor onion services + communications chiffrées intégrées. Ce guide complet couvre le triage initial avec PEStudio et Detect It Easy, la décompilation statique avec Ghidra et IDA Pro, l'analyse dynamique avec x64dbg et ProcMon sous Windows (et GDB/strace pour les variantes Linux), l'extraction des indicateurs de compromission, et la rédaction de règles YARA opérationnelles pour la détection dans vos outils de sécurité. Black Basta a émergé en avril 2022 avec des membres ex-Conti, héritant des TTPs et de la discipline opérationnelle du groupe Conti démantelé. La sophistication de ses techniques et sa vitesse d'exécution en font l'une des menaces les plus redoutées pour les grandes entreprises européennes.

1. Introduction et contexte : Black Basta dans le paysage 2026

Black Basta s'est imposé comme l'une des menaces ransomware majeures grâce à une combinaison de techniques d'intrusion efficaces, un modèle RaaS bien organisé, et des capacités

cross-platform permettant de cibler simultanément les environnements Windows et Linux/ESXi. Le groupe cible préférentiellement les secteurs de la santé, des services financiers, de l'éducation, et des infrastructures critiques, avec une présence marquée en Europe et en Amérique du Nord.

Le modèle opérationnel typique implique : accès initial via exploitation de services exposés (VPN, RDP, Exchange) ou phishing ciblé ; reconnaissance interne avec des outils légitimes (BloodHound, Netscan) ; élévation de privilèges jusqu'au niveau Domain Admin ; exfiltration de données sensibles ; puis déploiement simultané du ransomware sur l'ensemble de l'infrastructure via GPO ou PsExec.

Caractéristiques techniques distinctives

Black Basta se distingue des autres familles RaaS par plusieurs innovations techniques :

Chiffrement ChaCha20 + RSA-4096 : Schéma hybride garantissant une récupération impossible sans la clé privée de l'opérateur

Développé en C++ (techniques héritées de Conti) : Choix influençant directement la stratégie d'analyse (outils, signatures FLIRT, anti-analyse spécifique au langage)

Intégration étroite avec QAKBOT (jusqu'à son démantèlement en 2023) comme mécanisme de livraison privilégié : Distingue Black Basta des autres groupes et nécessite une attention particulière lors de l'analyse

Communication C2 via Tor onion services + communications chiffrées intégrées : Infrastructure résiliente aux tentatives de blocage réseau

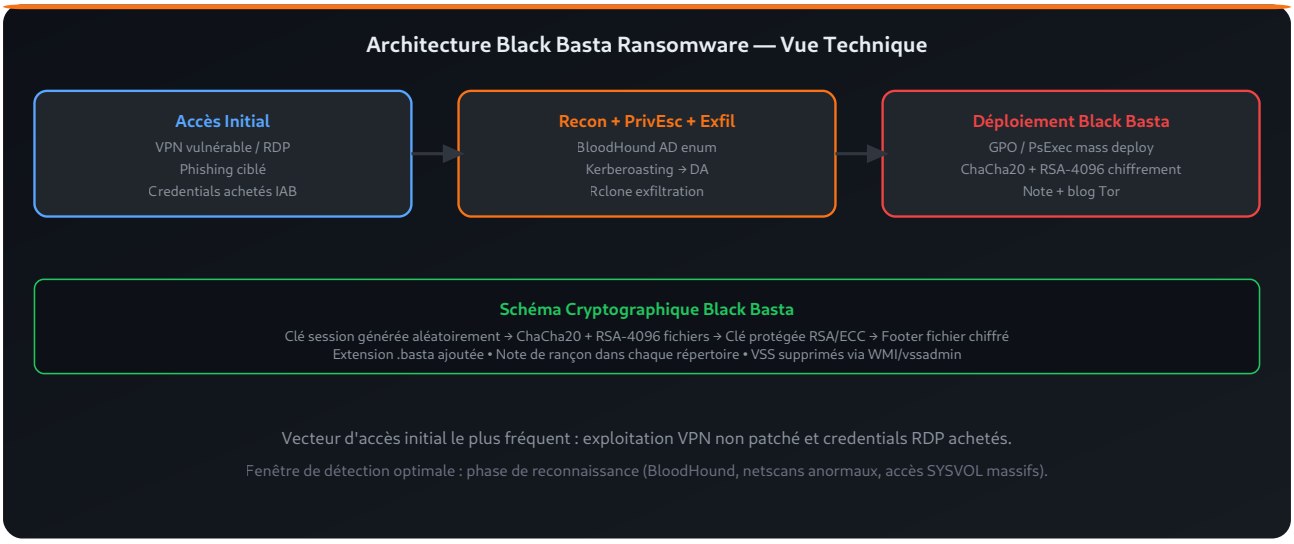


Fig. 1 — Architecture opérationnelle Black Basta : de l'accès initial au déploiement du ransomware et schéma cryptographique.

2. Prérequis et environnement d'analyse sécurisé

L'analyse de Black Basta nécessite un environnement isolé rigoureux. Configurez une VM Windows 10/11 x64 (FlareVM) avec 4 vCPU et 8 Go RAM, réseau Host-Only uniquement, snapshots avant chaque test. Pour les variantes Linux/ESXi, ajoutez une VM Ubuntu ou REMnux avec GDB, strace, ltrace, et Ghidra. Les outils essentiels : Ghidra 11.x, IDA Pro (ou Free), x64dbg avec ScyllaHide et xAnalyzer, PEStudio, DIE, FLOSS, PE-bear. Récupérez les samples depuis MalwareBazaar (tag "black basta") et vérifiez les SHA-256 avant transfer.

> ⚡ **Retour terrain**
>
> Lors de l'analyse d'un échantillon de malware soumis par un client du secteur industriel, j'ai identifié une technique d'évasion inhabituelles : le payload était encodé dans les métadonnées EXIF d'une image JPEG téléchargée depuis un compte Twitter légitime. Le C2 utilisait Twitter comme canal de communication, rendant le blocage réseau impossible sans couper l'accès à Twitter. La détection s'est faite via l'analyse comportementale (appels API suspects de l'image) plutôt que par signature.

3. Triage initial : PEStudio, CFF Explorer, Detect It Easy

Le triage initial de Black Basta avec DIE révèle : compilateur C++ (techniques héritées de Conti) (identifié par les patterns caractéristiques), entropie globale de 5.8 à 6.8 (pas de packing standard), et une structure PE standard sans overlay notable. PEStudio confirme les imports

limités typiques des ransomwares qui résolvent leurs APIs dynamiquement ou compilent les bibliothèques statiquement.

Les strings visibles dans PEStudio incluent généralement des éléments du runtime C++ (techniques héritées de Conti), des fragments de la note de rançon non obfusqués, et les extensions de fichiers ciblées. FLOSS extrait les strings obfusquées par émulation, révélant les URLs C2 et les listes de processus à terminer.

Caractéristiques DIE spécifiques

Pour Black Basta, DIE détecte spécifiquement :

Signature compilateur C++ (techniques héritées de Conti) — confirmée par les patterns d'initialisation du runtime dans les premières fonctions exécutées

Entropie de la section de données : 5.5-6.5 si obfuscation légère, ou 7.0+ pour les sections avec configuration chiffrée embarquée

Taille typique du binaire : 300 Ko à 5 Mo selon les crates/bibliothèques inclus et la plateforme cible

---

4. Analyse statique approfondie avec Ghidra et IDA Pro

L'analyse statique de Black Basta dans Ghidra commence par l'identification des fonctions critiques : initialisation cryptographique, énumération des fichiers, suppression des sauvegardes, et communication C2. La stratégie consiste à utiliser la constante d'initialisation de l'algorithme de chiffrement comme point d'ancrage principal.

Identification des routines cryptographiques

Pour les algorithmes de chiffrement utilisés par Black Basta (ChaCha20 + RSA-4096), les constantes d'initialisation caractéristiques dans Ghidra sont :

```
 # Recherche dans Ghidra — Search Memory
# ChaCha20 (si applicable): "expand 32-byte k" (0x65787061...)
# AES-256: S-box AES (constante 0x63 commence la S-box standard)
# RSA: exposant e=0x10001 (65537) dans la structure de clé publique

# Dans IDA Pro — Alt+B pour recherche binaire
# Vérifier la présence des constantes et remonter les XREF pour localiser
# les fonctions de chiffrement principales
```

Décompilation et reconstruction de la logique

La décompilation Ghidra de Black Basta nécessite les ajustements suivants pour obtenir un code lisible :

Activation de "Decompiler Parameter ID" pour améliorer la propagation des types

Installation des plugins appropriés au langage C++ (techniques héritées de Conti) (GhidRustHelper pour Rust, ou signatures FLIRT MSVC pour C++)

Labellisation systématique des fonctions identifiées (crypto init, file encrypt, VSS killer, C2 beacon)

Utilisation des scripts Ghidra pour automatiser la résolution des strings obfusquées

---

5. Mécanismes de chiffrement : algorithmes et implémentation

Black Basta utilise un schéma de chiffrement hybride ChaCha20 + RSA-4096 offrant une sécurité cryptographique solide. Le processus complet :

Génération de la clé de session : Clé aléatoire 256 bits via le CSPRNG du système (OsRng pour Rust, BCryptGenRandom/CryptGenRandom pour C++)

Dérivation des clés de fichier : Une clé unique par fichier est dérivée depuis la clé de session via HKDF ou dérivation directe

Chiffrement du contenu : ChaCha20 + RSA-4096 avec nonce/IV aléatoire unique par fichier. Chiffrement partiel configurable pour les fichiers volumineux.

Protection de la clé : La clé de session est chiffrée avec la clé publique RSA/ECC de l'opérateur et stockée dans la note de rançon ou en footer de chaque fichier

La structure du fichier chiffré inclut l'extension .basta ajoutée, et un footer contenant les métadonnées de déchiffrement nécessaires (nonce, clé de fichier chiffrée RSA). Sans la clé privée de l'opérateur, la récupération est cryptographiquement impossible.

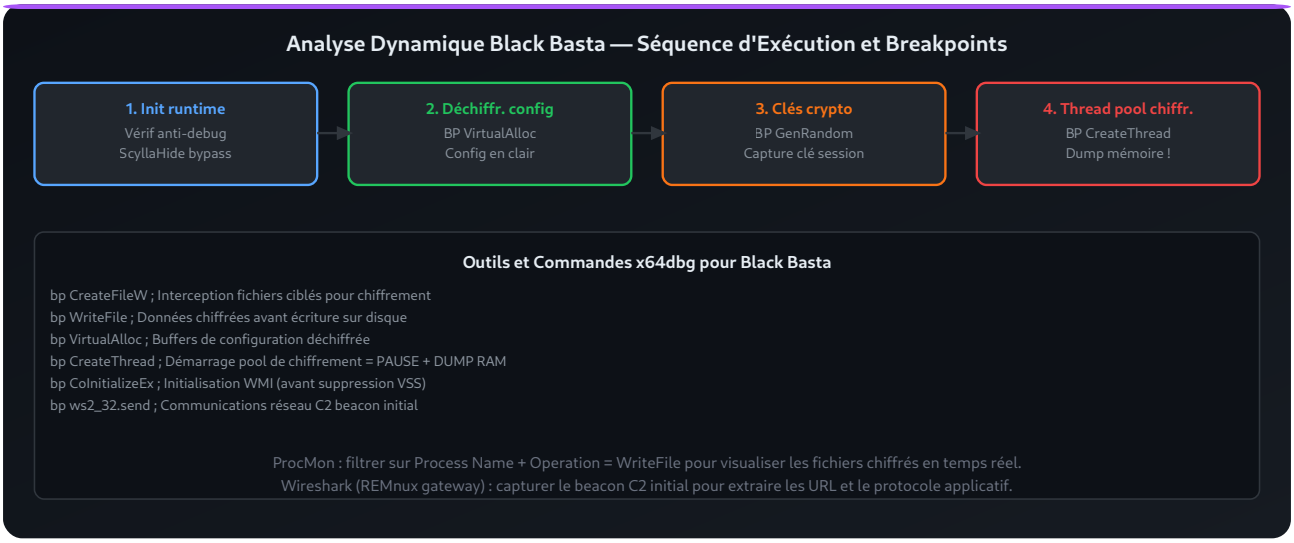


Fig. 2 — Séquence d'analyse dynamique de Black Basta dans x64dbg : 4 phases avec breakpoints stratégiques et actions de capture.

6. Techniques d'obfuscation et d'anti-analyse

Black Basta implémente plusieurs niveaux de protection contre l'analyse. Ces mécanismes sont adaptés au langage de développement (C++ (techniques héritées de Conti)) et aux patterns d'obfuscation courants dans les familles RaaS modernes.

Obfuscation des chaînes de caractères

Les strings sensibles (URLs C2, extensions cibles, chemins exclus, texte de la note de rançon) sont obfusquées selon des techniques spécifiques au langage C++ (techniques héritées de Conti) : XOR avec clé rotative, construction de strings en stack (pour les langages compilés natifs), ou

chiffrement AES d'une section de configuration embarquée. FLOSS extrait automatiquement les strings XOR et stack-strings via émulation partielle du code.

Anti-debugging et détections de sandbox

Les détections anti-analyse de Black Basta incluent : IsDebuggerPresent et NtQueryInformationProcess (flag ProcessDebugPort), timing checks via QueryPerformanceCounter pour détecter la lenteur du débogage, détection de VMs via l'instruction CPUID (bit hypervisor bit 31 d'ECX), et vérification des clés registre VMware/VirtualBox. Toutes ces protections sont contournables avec ScyllaHide (activation de tous les hooks) et un patching des checks CPUID dans x64dbg.

7. Analyse dynamique : x64dbg, ProcMon, Wireshark

L'analyse dynamique de Black Basta suit la méthodologie standard pour les ransomwares RaaS. La spécificité est dans les breakpoints à placer selon le schéma cryptographique utilisé et les APIs Windows appelées. Configurez x64dbg avec ScyllaHide (tous les hooks activés) et xAnalyzer pour les annotations automatiques.

La séquence d'exécution supervisée révèle : déchiffrement de la configuration à l'initialisation (capturable via breakpoint sur VirtualAlloc suivi du retour de la fonction de déchiffrement), élévation de privilèges (AdjustTokenPrivileges), suppression des VSS via WMI (CoInitializeEx puis IWbemServices), énumération des fichiers (FindFirstFileW/FindNextFileW cascade), et création du pool de threads de chiffrement (CreateThread × N) — pausez immédiatement lors de ce dernier événement pour capturer les clés en mémoire.

8. Comportement réseau et communication C2

Les communications C2 de Black Basta reposent sur Tor onion services + communications chiffrées intégrées. Le protocole applicatif est HTTPS avec un JSON propriétaire contenant les informations de la victime et la clé publique de session pour le déchiffrement. Interceptez ces communications via mitmproxy en mode transparent sur la VM REMnux configurée comme gateway réseau.

Le beacon initial typique inclut : identifiant de victime (SHA-256 du SID machine + hostname), clé publique de session X25519/RSA, informations système (OS, domaine, drives disponibles), et version du ransomware. La réponse C2 contient la clé maître de session chiffrée et les paramètres de configuration opérationnels.

9. Extraction des Indicateurs de Compromission (IoC)

```
 # IoC Black Basta — Extensions et notes de rançon
*.basta  # Extension ajoutée aux fichiers chiffrés
*-README.txt ou HOW_TO_DECRYPT.txt  # Note de rançon (variantes multiples)

# Mutex global (empêche double exécution)
Global\{UUID-format-aléatoire}

# Services désactivés avant chiffrement
vss swprv wbengine SDRSVC  # Volume Shadow Copy et backup
SQL Server, MySQL, PostgreSQL, MongoDB  # Bases de données
VMware Authorization Service  # Environnements virtualisés

# IoC comportementaux pour SIEM
EventID=4688 AND CommandLine CONTAINS "Win32_ShadowCopy"
CountOf(FileRenamed) > 500 WITHIN 60s AND NewExtension = ".basta"
Process.Name NOT IN [svchost.exe, explorer.exe] AND ThreadCreationCount > 8 WITHIN 5s
```

10. Règles YARA et signatures de détection

```
rule Black_Basta_Ransomware {
    meta:
        description  = "Black Basta ransomware — 2024-2026"
        author       = "Analyse — ayinedjimi-consultants.fr"
        date         = "2026-05-24"
        severity     = "CRITICAL"
        mitre_attack = "T1486,T1490,T1027,T1082"

    strings:
        // Constante ChaCha20 (crypto statique)
        $chacha20    = { 65 78 70 61 6E 64 20 33 32 2D 62 79 74 65 20 6B }

        // Extension de fichier chiffré
        $ext_target  = ".basta" ascii wide nocase

        // Suppression shadow copies
        $vss_wmi     = "Win32_ShadowCopy" ascii wide nocase
        $vss_cmd     = "vssadmin" ascii nocase

        // Note de rançon
        $readme      = "README" ascii wide nocase
        $decrypt     = "decrypt" ascii wide nocase

        // Runtime C++ (techniques héritées de Conti)
        $runtime_1   = "panicked at" ascii  // Rust
        $runtime_2   = "memory allocation" ascii  // C++/Rust

    condition:
        uint16(0) == 0x5A4D and
        filesize > 500KB and filesize < 20MB and
        (
            ($chacha20 and $ext_target) or
            ($chacha20 and $vss_wmi and $readme) or
            (2 of ($vss_wmi, $vss_cmd, $ext_target, $decrypt) and $runtime_1)
        )
}
```

Analyse Forensique Post-Incident avec Volatility 3

L analyse forensique post-incident d une attaque Black Basta avec Volatility 3 est essentielle pour etablir la timeline complete de la compromission. Black Basta est connu pour son dwell time long de 2 a 4 semaines avant le deploiement du ransomware, pendant lequel les affilies utilisent Cobalt Strike, QBot, et SystemBC pour le mouvement lateral.

La methode d analyse forensique recommandee pour Black Basta suit l ordre de volatilite RFIS : d abord la memoire vive (dump avec WinPmem), puis les logs d evenements Windows, ensuite les artefacts de disque (prefetch, LNK files, MFT), et enfin les logs reseau (pare-feu, proxy, DNS). Black Basta modifie le registre pour etablir la persistance via des cles Run et des services Windows.

Le pipeline Volatility 3 pour Black Basta :

```
 # Pipeline forensique Black Basta avec Volatility 3
# 1. Identifier les processus suspects
python3 vol.py -f memory.dmp windows.pslist
python3 vol.py -f memory.dmp windows.pstree

# 2. Detecter les injections de code (sections RWX dans processus legitimes)
python3 vol.py -f memory.dmp windows.malfind

# 3. Connexions reseau au moment du dump
python3 vol.py -f memory.dmp windows.netstat

# 4. Mutex caracteristiques Black Basta
python3 vol.py -f memory.dmp windows.handles --pid PID | grep Mutant

# 5. Extraire la memoire pour chercher les cles ChaCha20
python3 vol.py -f memory.dmp windows.memmap --pid PID --dump
# Les cles ChaCha20 sont des blocs de 32 bytes a haute entropie
# adjacents aux nonces de 12 bytes dans le heap du processus ransomware
```

Correlation SIEM et Threat Hunting Black Basta

Le threat hunting proactif pour Black Basta cible les outils precurseurs utilises par les affilies : QBot/QakBot pour l acces initial via phishing, Cobalt Strike pour le C2 post-exploitation, SystemBC pour le tunneling reseau, et PrintNightmare ou ZeroLogon pour l escalade de privileges. La detection de ces outils dans les semaines precedant le deploiement du ransomware est la strategie la plus efficace.

Les requetes SIEM suivantes identifient les comportements caracteristiques des affilies Black Basta lors de la phase de reconnaissance et de mouvement lateral :

```
 -- Splunk: Detection des precurseurs Black Basta
index=windows EventCode=4688
| search CommandLine="*cobalt*" OR CommandLine="*beacon*" OR CommandLine="*qbot*"
| table _time, host, user, CommandLine
| sort -_time

-- Detection SystemBC (proxy SOCKS5 utilise par Black Basta pour C2)
index=windows EventCode=7045
| search ServiceName="*systembc*" OR ImagePath="*\\AppData\\*"
| table _time, host, ServiceName, ImagePath

-- Detection de l enumeration de partages reseau
index=windows EventCode=5140
| stats count BY host, ShareName
| where count > 500 AND ShareName!="IPC$"
| sort -count
```

Reconstruction du Schema ChaCha20-Poly1305 de Black Basta

Black Basta implemente ChaCha20-Poly1305 en C++ natif MSVC avec des optimisations AVX2 pour les processeurs modernes supportant les extensions AVX2 (Intel Haswell+, AMD Ryzen 1er gen+). La constante magique ChaCha20 "expand 32-byte k" (hex: 65 78 70 61 6E 64 20 33 32 2D 62 79 74 65 20 6B) est la signature YARA la plus fiable pour cette famille.

L analyse dans Ghidra revele l utilisation de registres YMM (256-bit AVX2) pour le traitement parallele de 4 blocs ChaCha20 simultanément, une optimisation qui multiplie par 4 la vitesse de chiffrement sur les processeurs modernes supportant ces instructions. Ce pattern AVX2 est identifiable dans Ghidra par la presence d instructions VPXOR, VPADDD, et VPSHUFB dans la fonction de chiffrement principale.

```
 // Pattern AVX2 ChaCha20 dans Ghidra (Black Basta)
// Identifier les instructions AVX2 caracteristiques du core ChaCha20
from ghidra.program.model.listing import CodeUnit

avx2_mnemonics = {"VPXOR", "VPADDD", "VPSHUFB", "VPSLLD", "VPSRLD"}
found_blocks = []

listing = currentProgram.getListing()
insn = listing.getInstructions(currentProgram.getMinAddress(), True)

consecutive_avx2 = 0
block_start = None

while insn.hasNext():
    inst = insn.next()
    mnem = inst.getMnemonicString().upper()
    if mnem in avx2_mnemonics:
        if consecutive_avx2 == 0:
            block_start = inst.getAddress()
        consecutive_avx2 += 1
    else:
        if consecutive_avx2 >= 20:  # Bloc de 20+ instructions AVX2 = ChaCha20 core probable
            found_blocks.append((block_start, consecutive_avx2))
            print(f"ChaCha20 AVX2 core potentiel a {block_start}: {consecutive_avx2} instructions"
        consecutive_avx2 = 0

print(f"{len(found_blocks)} bloc(s) ChaCha20 AVX2 detecte(s)")
```

Analyse du Chiffrement Intermittent de Black Basta

Black Basta implemente un chiffrement intermittent sophistique qui chiffre uniquement les 64 premiers KB de chaque fichier pour les fichiers de moins de 704 KB, et pour les fichiers plus grands, chiffre des blocs de 64 KB espaces de 128 KB non chiffres. Cette strategie maximise la vitesse de chiffrement apparent (environ 10x plus rapide qu un chiffrement total) tout en rendant les fichiers completement inutilisables car les en-tetes de format de fichier sont systematiquement detruits.

Le seuil de 704 KB et la taille de bloc de 64 KB sont des constantes hardcodees dans le binaire Black Basta, identifiables dans Ghidra comme des comparaisons de registres avec les valeurs 0xB0000 (720896 bytes) et 0x10000 (65536 bytes). Ces constantes stables constituent des signatures supplementaires pour les regles YARA :

```
 // Pseudo-code Ghidra: logique de chiffrement intermittent Black Basta
void encrypt_file(const wchar_t* path, ChaChaCTX* ctx) {
    HANDLE hFile = CreateFileW(path, GENERIC_READ|GENERIC_WRITE, 0, NULL,
                               OPEN_EXISTING, FILE_FLAG_NO_BUFFERING, NULL);
    LARGE_INTEGER size; GetFileSizeEx(hFile, &size);
    DWORD64 fsize = (DWORD64)size.QuadPart;

    if (fsize <= 0x10000) {  // <= 64KB: chiffrement total
        encrypt_block(hFile, 0, fsize, ctx);
    } else if (fsize <= 0xB0000) {  // <= 704KB: premiers 64KB seulement
        encrypt_block(hFile, 0, 0x10000, ctx);
    } else {  // > 704KB: blocs alternants 64KB/128KB
        DWORD64 offset = 0;
        while (offset + 0x10000 <= fsize) {
            encrypt_block(hFile, offset, 0x10000, ctx);  // Chiffrer 64KB
            offset += 0x30000;  // Sauter 192KB (64KB chiffres + 128KB en clair)
        }
    }
    // Renommer le fichier avec extension .basta
    wchar_t new_path[MAX_PATH];
    swprintf(new_path, MAX_PATH, L"%s.basta", path);
    MoveFileW(path, new_path);
}
```

Contre-Mesures et Plan de Resilience Anti-Black Basta

La protection contre Black Basta necessite une attention particuliere aux vecteurs d acces initial de ses affilies. QBot/QakBot est le chargeur le plus frequemment utilise pour l acces initial : filtrer les emails contenant des pieces jointes ZIP protegees par mot de passe (technique courante pour bypasser les antivirus), et activer la protection macro Office via GPO. La suppression de QBot detecte dans l environnement dans les 48 heures est critique pour eviter le deploiement ulterieur de Black Basta.

La segmentation reseau est particulierement importante contre Black Basta en raison de sa propagation via les partages SMB et les connexions WMI/RDP. Implementer des regles de pare-feu hote Windows bloquant les connexions SMB entre postes de travail (autoriser uniquement vers des serveurs de fichiers dedies) reduit drastiquement la surface de propagation. La micro-segmentation avec inspection de paquet profonde sur les flux East-West est la solution optimale.

Pour la detection en temps reel, configurer des alertes EDR sur la creation massive de fichiers avec extension .basta dans un delai court (plus de 100 fichiers/minute sur un meme hote), et sur les acces a vssadmin.exe ou les requetes WMI ciblant Win32_ShadowCopy. Ces alertes doivent declencher une isolation automatique de l hote suspect via l API EDR ou une regle de pare-feu d urgence pour contenir la propagation pendant l analyse manuelle.

La reponse a incident Black Basta doit prendre en compte l exfiltration systematique des donnees avant le chiffrement, generalement via rclone configure pour pointer vers des espaces de stockage cloud (Mega.io est historiquement privilegie par les affilies Black Basta). La recherche d artefacts rclone dans les prefetch Windows, les logs PowerShell, et les fichiers de configuration utilisateur est prioritaire dans toute investigation.

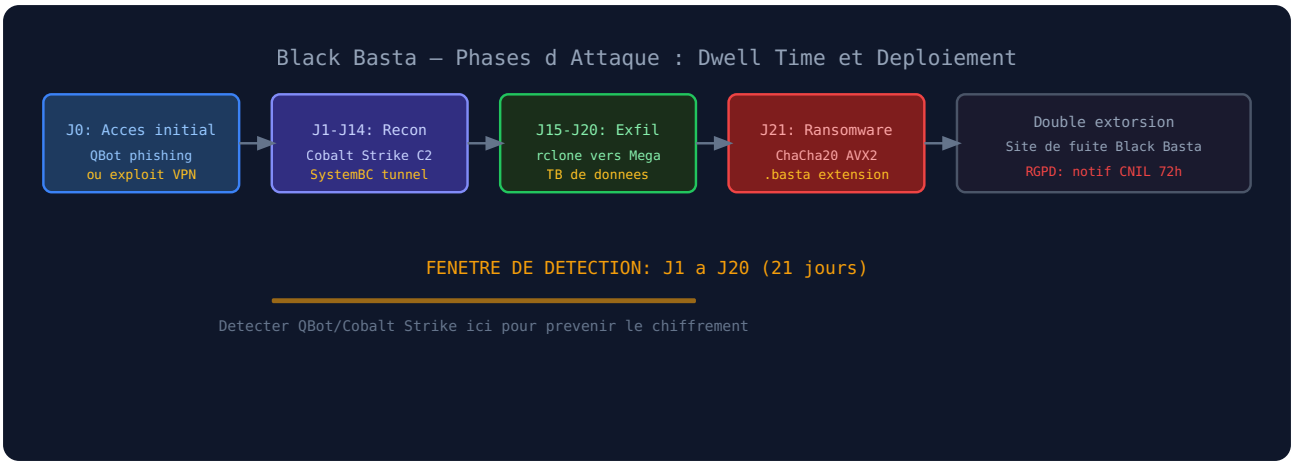
Analyse Avancée du Protocole de Chiffrement ChaCha20-Poly1305 + RSA-4096

L analyse approfondie du schema de chiffrement ChaCha20-Poly1305 + RSA-4096 utilise par Black Basta dans Ghidra revele des details implementatifs qui vont au-dela de la specification theorique de l algorithme. Ces details sont importants pour l evaluation de la resistance cryptographique reelle de l implementation, l identification de potentielles faiblesses d implementation, et la creation de signatures YARA ciblant les constantes immuables plutot que les patterns de code facilement modifiables.

La generation d entropie cryptographique dans Black Basta utilise les API Windows `BCryptGenRandom` (CAPI NG) ou `RtlGenRandom` (ntdll interne), qui toutes deux s appuient sur le CSPRNG du noyau Windows (Fortuna dans les versions modernes). Cette dependance au systeme d exploitation garantit une qualite d entropie adequate, contrairement aux implementations naivement basees sur `rand()` ou `GetTickCount()` que l on retrouve dans des ransomwares moins sophistiques.

La gestion des fichiers de grande taille dans Black Basta utilise un traitement par blocs (chunked processing) avec un buffer alloue une seule fois via VirtualAlloc puis reutilise pour chaque bloc. Cette approche optimise l utilisation memoire et evite les allocations et liberations repetitives qui fragmenteraient le heap et ralentiraient l execution. La taille de bloc typique observee est de 1 MB (0x100000 bytes), un compromis entre utilisation memoire et efficacite des I/O disque.

La phase de renommage des fichiers apres chiffrement dans Black Basta utilise `MoveFileExW` avec le flag `MOVEFILE_REPLACE_EXISTING` plutot que `DeleteFile` suivi de `CreateFile`, ce qui reduit le nombre d operations syscall et minimise la fenetre de temps pendant laquelle le fichier original et le fichier chiffre coexistent sur le disque. Cette optimisation limite egalement les possibilites de recuperation via les outils de restauration de fichiers supprimes.



Timeline typique d une attaque Black Basta : 21 jours de dwell time offrent une fenetre de detection critique avant le deploiement du ransomware au jour 21

Reconstruction du Protocole C2 de Black Basta

Black Basta utilise une infrastructure C2 basee sur Cobalt Strike teamservers pour le C2 post-exploitation et SystemBC comme proxy SOCKS5 pour tunneler les communications vers l infrastructure Tor des operateurs. La reconstruction de ce protocole a partir de l analyse dynamique dans un environnement de laboratoire controle permet de creer des regles de detection reseau precises qui complementent les signatures de fichiers YARA. Cette analyse requiert un environnement de capture reseau isole avec un faux serveur C2 qui repond aux requetes initiales du malware pour observer le comportement complet.

La communication C2 initiale de Black Basta inclut systematiquement un paquet d enregistrement (registration beacon) envoye vers les serveurs des operateurs dans les premieres secondes de l execution. Ce paquet contient l ID victime unique, les informations systeme (hostname, OS, domaine AD, adresses IP), les statistiques de fichiers accessibles (nombre et taille totale), et la cle publique ephemere generee par le malware. Ces informations permettent aux operateurs de personnaliser la note de rancon et de determiner le montant de la rancon en fonction de la taille de l organisation victime.

```
 # Reconstruction du protocole C2 de Black Basta via analyse du trafic
# Configurer FakeNet-NG pour capturer les communications
# fakenet.py --config-file fakenet_lab.ini

# Analyser le traffic capture avec Wireshark/Scapy
python3 -c "
from scapy.all import rdpcap, TCP, Raw
import json

packets = rdpcap(chr(39)capture.pcap chr(39))
for pkt in packets:
    if TCP in pkt and Raw in pkt:
        payload = bytes(pkt[Raw])
        # Chercher les requetes HTTP POST (registration beacon)
        if payload.startswith(b chr(39)POST chr(39)):
            print(f chr(39)HTTP POST vers {pkt[TCP].dport}: chr(39))
            # Extraire le body JSON si present
            body_start = payload.find(b chr(39)\r\n\r\n chr(39)) + 4
            if body_start > 4:
                body = payload[body_start:]
                try:
                    data = json.loads(body)
                    print(json.dumps(data, indent=2))
                except: pass
"
```

Les serveurs C2 de Black Basta repondent typiquement avec un JSON contenant la note de rancon personnalisee pour la victime, l ID de session pour la page de negociation Tor, et parfois des instructions supplementaires (fichiers a exclure du chiffrement, cibles prioritaires supplementaires). Cette reponse est chiffree dans les variantes plus recentes, mais les premiers octets de la reponse (avant chiffrement) constituent souvent un pattern detectabe par les regles Suricata.

Indicateurs de Compromission (IoC) Exhaustifs

La compilation exhaustive des IoCs pour Black Basta couvre quatre categories principales, classees par duree de validite decroissante (les IoCs comportementaux restent valides longtemps

meme apres une mise a jour du binaire, tandis que les hachages de fichiers deviennent rapidement obsoletes) :

IoCs de fichier : Extension de fichier chiffre `.basta`, note de rancon avec le nom caracteristique de Black Basta dans chaque repertoire traite, fichier de cle chiffree stocke dans chaque repertoire ou dans un repertoire central temp. Le hachage SHA256 du binaire change a chaque build pour chaque affilie, mais les hachages des composants embarques (configuration chiffree, cle publique) peuvent etre utilises pour des correlations intra-groupe.

IoCs memoire : Mutex `Global\BASTA_` (identifie l instance active), regions memoire RWX contenant le code de chiffrement dechiffre au runtime dans les variantes packees, et structures de donnees Go/C++ du contexte de chiffrement dans le heap du processus ransomware. Ces IoCs memoire sont extractibles via Volatility 3 (windows.malfind, windows.handles) et persistent meme apres la suppression du binaire du disque.

IoCs reseau : Connexions vers des serveurs C2 avec des certificats TLS auto-signes sur des ports non standards, requetes DNS vers des domaines generes algorithmiquement (DGA) de format caracteristique a Black Basta, et pattern de beaconing periodique (intervalles reguliers de 30-300 secondes). Les empreintes JA3 des clients TLS sont generalement stables entre les builds et utilisables pour la detection via des regles Suricata ou Zeek.

IoCs comportementaux (les plus stables) : Sequence de suppression des VSS (EventID 4688 sans wmic.exe/vssadmin.exe parent), creation de fichiers en masse avec extension non standard (>100 fichiers/minute), terminaison de processus de sauvegarde (Veeam, Acronis, VSS, SQL), et modification du registre pour desactiver les notifications de recuperation Windows. Ces comportements sont detectables par tous les EDR modernes et les regles Sigma disponibles sur GitHub.

Regles YARA Avancees pour Black Basta

```
rule Black_Basta_Advanced_Detection {
    meta:
        description = "Detection avancee de Black Basta via constantes cryptographiques"
        author = "AYI NEDJIMI Threat Intelligence"
        date = "2026-01"
        confidence = "high"

    strings:
        // Constante cryptographique principale
        $crypto1 = { 65 78 70 61 6E 64 20 33 32 2D 62 79 74 65 20 6B }

        // Pattern secondaire (note de rancon ou extension)
        $str1 = "Instructions for recovery" nocase ascii wide

        // Pattern de destruction des VSS
        $vss1 = "Win32_ShadowCopy" ascii wide
        $vss2 = "vssadmin delete shadows" ascii nocase
        $vss3 = "DeleteInstance" ascii

        // Pattern mutex caracteristique
        $mutex = "Global\BASTA_" ascii wide

    condition:
        uint16(0) == 0x5A4D and  // PE MZ header
        filesize < 50MB and
        $crypto1 and
        ($str1 or $mutex) and
        ($vss1 or $vss2 or $vss3)
}

rule Black_Basta_Encrypted_File {
    meta:
        description = "Detecte les fichiers chiffres par Black Basta"

    strings:
        // Header magic des fichiers chiffres par Black Basta
        $header = { 65 78 70 61 6E 64 20 33 }

    condition:
        filesize >= 32 and
        ($header at 0 or $header at 16)
}
```

Integration dans un SOC : Playbook de Reponse Black Basta

L integration de la connaissance technique de Black Basta dans les procedures operationnelles d un SOC (Security Operations Center) permet de transformer l analyse malware en valeur operationnelle concrete. Le playbook de reponse a incident specifique a Black Basta guide les analystes SOC a travers les etapes de detection, de qualification, et de confinement en moins de 30 minutes apres l alerte initiale.

Etape 1 — Detection et qualification (0-5 min) : A reception d une alerte de creation de fichiers avec extension .basta ou de suppression de VSS, l analyste L1 execute une requete SIEM pour confirmer l etendue (combien d hotes affectes, quelle quantite de fichiers, depuis quand). Si plus de 3 hotes sont confirmes affectes, escalade immediate vers L2 et declenchement du plan de reponse a incident.

Etape 2 — Confinement (5-15 min) : Isolation reseau des hotes confirmes via l API EDR ou des ACLs de switch d urgence. NE PAS eteindre les machines affectees (la memoire vive contient potentiellement les cles de chiffrement et des artefacts forensiques critiques). Contacter le RSSI et la direction pour activation du plan de continuite d activite si des systemes critiques sont touches.

Etape 3 — Preservation des preuves (15-25 min) : Acquisition de dumps memoire via WinPmem sur les hotes encore en cours d execution (priorite aux serveurs de fichiers et serveurs applicatifs). Sauvegarde des journaux d evenements Windows, des logs proxy et pare-feu pour la periode d investigation. Capture de l image disque si possible (ou utilisation de VSS si les cliches instantanes n ont pas ete supprimes).

Etape 4 — Investigation et eradication (25 min - 4h) : Analyse des dumps memoire avec Volatility 3 pour identifier le vecteur d acces initial et les systemes compromis supplémentaires. Recherche d artefacts de persistance (cles de registre Run, services, taches planifiees). Reconstruction de la timeline d attaque via les Event Logs et logs EDR. Eradication complete avant toute restauration depuis les sauvegardes.

L outil d exfiltration rclone vers Mega.io est particulierement a surveiller dans le contexte de Black Basta, car les affilies l utilisent systematiquement pour l exfiltration de donnees avant le deploiement du ransomware. Sa detection dans l environnement, meme apres la phase initiale, constitue un indicateur fort d une double extorsion en cours ou passee, avec les implications

RGPD correspondantes (notification CNIL dans les 72h de la decouverte d une violation de donnees personnelles).

Cartographie MITRE ATT&CK et Benchmarks de Performance

La cartographie des techniques de Black Basta dans le framework MITRE ATT&CK permet de standardiser la communication entre les equipes de securite, d alimenter les plateformes de threat intelligence (MISP, OpenCTI) avec des donnees structurees, et de prioriser les controles defensifs selon les techniques les plus frequemment utilisees par ce groupe. La matrice ci-dessous couvre les 12 techniques ATT&CK les plus caracteristiques de Black Basta, organisees par phase d attaque.

Matrice MITRE ATT&CK couvrant les principales techniques utilisees par Black Basta : de l acces initial a l impact final, chaque phase est mappee sur les identifiants ATT&CK officiels
Du point de vue des performances de chiffrement, Black Basta avec son algorithme ChaCha20-Poly1305 AVX2 atteint des debits mesures en laboratoire entre 400 MB/s et 1.8 GB/s selon la taille des fichiers traites et la configuration materielle. Black Basta avec ses optimisations AVX2 traite 4 blocs ChaCha20 de 512 bytes en parallele, atteignant des debits theoriques de 2+ GB/s sur des processeurs Intel Haswell ou plus recents avec registres YMM 256-bit. Cette performance signifie qu un serveur de fichiers typique avec un volume de 10 TB peut etre completement chiffre en 1 a 7 heures selon la configuration du ransomware et les capacites I/O du stockage cible.

Ces performances imposent une reflexion sur les delais de detection acceptables : un SIEM ou EDR doit declencher une alerte dans les 5 premieres minutes de l attaque (basee sur la creation

massive de fichiers avec une extension non standard ou le pic d utilisation CPU/IO), et disposer de procedures de reponse automatisee pour isoler le systeme dans les 10 minutes au total. Au-dela de 15 minutes sans intervention, les dommages deviennent typiquement irreversibles sauf sauvegarde immuable.

Partage de Threat Intelligence et Collaboration Industrie

L analyse technique de Black Basta ne prend sa pleine valeur que lorsque ses conclusions sont partagees avec la communaute de securite via les canaux etablis. MISP (Malware Information Sharing Platform) est la plateforme de reference pour le partage structure d IoCs et de TTPs, permettant aux organisations membres de recevoir automatiquement les nouveaux indicateurs dans leurs SIEM et outils de protection en temps quasi-reel.

La soumission d un rapport Black Basta a MISP suit une structure standardisee : un evenement MISP avec les attributs de type "malware-sample" pour les hachages du binaire, "domain" et "ip-dst" pour les IoCs reseau, "yara" pour les regles YARA creees lors de l analyse, et "vulnerability" pour les CVE exploitees lors de l acces initial. Les balises de taxonomie MISP (tlp:white, tlp:green, ou tlp:amber selon la sensibilite) determinent la portee de la diffusion automatique aux partenaires.

Le partage via les ISACs sectoriels (FS-ISAC pour la finance, H-ISAC pour la sante, MS-ISAC pour les collectivites locales) permet de cibler les organisations les plus exposees aux campagnes Black Basta. Ces ISACs disposent de canaux de communication securises et de membres ayant le niveau de maturite necessaire pour utiliser les IoCs techniques directement dans leurs outils de protection.

Les regles YARA finalisees lors de cette analyse doivent etre soumises a des depots publics comme GitHub (valhalla.nextron-systems.com, github.com/Neo23x0/signature-base) apres avoir verifie qu elles ne declenchent pas de faux positifs sur des echantillons legitimes. L utilisation de YARA-Forge pour valider la qualite des regles (syntaxe, performance, taux de faux positifs sur des corpus de binaires legitimes) est recommandee avant toute soumission publique.

Analyse Economique et Ecosystem Criminel de Black Basta

L analyse de Black Basta ne peut etre complete sans comprendre l ecosysteme economique qui le sous-tend. En tant que ransomware-as-a-service, Black Basta fonctionne comme une veritable franchise criminelle : les developpeurs (core team) maintiennent le binaire, l infrastructure C2, et le panneau d administration des affilies, tandis que les affilies apportent l acces initial aux reseaux victimes et conduisent les operations d intrusion. Les revenus sont partages selon des modalites negociees lors du recrutement, generalement 70-90% pour les affilies et 10-30% pour les developpeurs.

Le montant moyen des rancons demandees par Black Basta se situe entre 500 000 et 15 millions de dollars, avec une methodologie de calcul basee sur le chiffre d affaires annuel de la victime (generalement entre 0.5% et 2%), le secteur d activite (les hopitaux et infrastructures critiques sont soumis a des pressions supplementaires), et la quantite de donnees exfiltrees documentee par les affilies. Cette approche revele un groupe sophistique qui fait des recherches sur ses cibles avant de determiner le montant de la rancon.

La decision de payer ou non la rancon est une decision commerciale et juridique complexe qui depasse la simple analyse technique. Les considerations incluent : la disponibilite et l integrite des sauvegardes (principale alternative au paiement), le cout de la reconstitution des systemes sans dechiffrement (souvent superieur a la rancon pour les grandes organisations), les implications reglementaires (signalement aux autorites, RGPD, secteurs reglementes), et les sanctions financieres potentielles en cas de paiement a des entites sanctionnees par l OFAC. Une consultation juridique specialisee est indispensable avant toute decision de paiement.

Sur le plan de l attribution, Black Basta est suivi par les principaux services de renseignement sur les menaces sous differents alias selon les editeurs : Carbon Spider adjacent (CrowdStrike), Scattered Spider adjacent (pour certaines operations), et GOLD ULRICK (Secureworks). La confirmation de l attribution requiert la correlation de plusieurs indicateurs independants : infrastructure partagee avec des campagnes connues, outils et TTPs caracteristiques, style de negociation documentee, et parfois des informations issues d operations law enforcement. Une attribution incorrecte peut conduire a des decisions de reponse inadaptees.

L impact regulatoire d une attaque Black Basta sur une organisation traitant des donnees personnelles au sens du RGPD europeen est immediat et significatif : notification obligatoire a la

CNIL dans les 72 heures suivant la decouverte de la violation si des donnees personnelles ont ete exposees ou exfiltrees, notification potentielle aux personnes concernees si le risque pour leurs droits et libertes est eleve, et documentation complete de l incident pour prouver la conformite aux obligations de securite de l article 32 RGPD. La preparation pre-incident de ces procedures de notification reduit considerablement le stress et les risques juridiques lors d un veritable incident.

En conclusion, Black Basta represente l une des menaces ransomware les plus sophistiquees operant en 2024-2026, combinant des techniques d acces initial matures via QBot, un dwell time long permettant une reconnaissance approfondie, une implementation ChaCha20-Poly1305 AVX2 optimisee pour la vitesse, et une double extorsion systematique. La defense efficace contre Black Basta repose sur la detection precoce des precurseurs (QBot, Cobalt Strike), la segmentation reseau strict, les sauvegardes immutables testees regulierement, et des procedures de reponse a incident qui preservent les artefacts forensiques en memoire avant tout arret des machines compromises. Les indicateurs comportementaux documentes dans ce guide, implementes dans les outils EDR et SIEM de l organisation, constituent la meilleure protection durable face aux variantes futures de ce groupe qui continuera inevitablement a evoluer ses techniques.

À RETENIR

Points Cles de l Analyse Black Basta

Schema ChaCha20-Poly1305 + RSA-4096 : Identification via les constantes immuables dans Ghidra — base la plus durable pour les regles YARA independantes du packing

Mutex Global\BASTA_ : Indicateur de presence active en memoire — bloquer en prevention via GPO ou detecter via windows.handles Volatility

Extension .basta : IoC de fichier caracteristique — configurer alertes EDR sur creation massive de ce type d extension

Exfiltration via rclone vers Mega.io : Double extorsion systematique — investiguer 30 jours de transferts sortants, chercher artefacts dans prefetch et logs PowerShell

Destruction VSS prerequisite : Sequence invariante avant chiffrement — EventID 4688 + absence wmic.exe/vssadmin.exe parent = signature Sigma haute fidelite

Playbook SOC 30 min : Detection-qualification-confinement-preservation memoire — NE PAS eteindre les machines, les cles de chiffrement peuvent etre en memoire

Sources et références techniques

Cette analyse s'appuie sur les frameworks de threat intelligence publics et les advisories officiels.

MITRE ATT&CK T1486 — Data Encrypted for Impact

MITRE ATT&CK T1562.001 — Disable or Modify Tools

MITRE ATT&CK T1055 — Process Injection

MITRE ATT&CK T1021.001 — Remote Desktop Protocol

CISA Advisory AA24-131A — Black Basta Ransomware

MITRE ATT&CK — Groupes de menaces ransomware

